

Documentation

A software solution by MATTA (<https://www.trustmatta.com>)

safepass.me version 4.0.5

Contents

About safepass.me	3
Before you start	4
Overview	4
Requirements	4
Disk Space	4
Memory	4
Supported Windows Versions	4
Versioning and release-engineering details	5
Installation	6
Download the software	6
Verify its digital signature	6
Accept the EULA	8
Install safepass.me	9
Deploy the License File	10
Reboot	10
Licensing	10
Online & Offline Licensing Options	10
Configuration	11
Configuration Options	11
Administrative override (enterprise)	11
Exclude Users (enterprise)	11
Enable Demo Mode (enterprise)	12
Configure a custom dictionary (professional & enterprise)	12
Support Issues	13
List of Files	13
Privacy	15
Changelog	16

safepass.me

The smartest password filter

About safepass.me

safepass.me is currently the only fully-offline, efficient and cost-effective secure password enforcement tool for organisations of any size.

Deployed on all Active Directory Domain Controllers, it is the ideal solution to both prevent users from making poor password choices, and satisfy the latest password guidelines from international standard bodies like the NIST and NCSC - who have determined that existing 'complexity/rule' based password policies are inadequate.

safepass.me detects any attempt from a user to set a password that has been compromised and leaked online in breached databases - for instance LinkedIn, Adobe, or Dropbox.

Unlike other password filters, its strength lies in its speed, simplicity and straight forward set up; safepass.me can be deployed rapidly, so there is no need to spend hours configuring it.

There are currently three versions of safepass.me:

- **Home;** a no-frills version, completely free for non corporate users.
- **Professional;** A basic but fully functional version for small teams that don't have custom requirements.
- **Enterprise;** Fully tailored experience for larger corporations with custom requirements.

safepass.me

The smartest password filter

Before you start

Overview

At safepass.me, we know your time is precious so we have worked hard to ensure that the installation process is as streamlined as possible; you will be able to set safepass.me up in under three minutes.

The installation process is as simple as running through the provided Windows MSI installer on your DCs.

You will find screenshots of the process below for your convenience. We have also created a demo video of the installation process, as well as how to test the software once it is installed:

- <https://safepass.me/demo-video>

Requirements

Want to protect your entire corporate domain quickly and efficiently? There's good news in store. safepass.me takes up a fraction of the space of most enterprise software you may have running - so when you install safepass.me on your Domain Controller you should already have sufficient capacity.

Disk Space

safepass.me takes up minimal disk space (less than 500MB on disk!), plus the size of any custom wordlist file you might want to add.

Memory

safepass.me has a very small memory footprint of less than 400MB of RAM, which sets it apart from the competition.

Supported Windows Versions

*Versions of windows supported, **only 64-bit editions.***

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Copyright Matta Consulting Ltd. For more information visit <https://safepass.me/> and <https://www.trustmatta.com/>

safepass.me

The smartest password filter

- Windows 2008 R2
- Windows 2008
- Windows 2003 R2
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista
- Windows XP

safepass.me has been tested and works on Server Core builds.

Versioning and release-engineering details

safepass.me version numbers are composed of three digits and an optional qualifier
MAJOR.MINOR.PATCH-FLAVOR

- MAJOR represents the HIBP release being tracked (we guarantee that we block all passwords present in the matching HIBP release). We aim at having one within weeks of every new release of the HIBP dataset.
- MINOR represents incremental feature improvements that we deem worthy of being evaluated for deployment by customers.
- PATCH represents minor improvements that either address bespoke requirements or bug fixes for bugs that are not severe enough to warrant deploying to all customers. Customers we are interacting with at the time (typically through support requests) may be informed and asked to upgrade from one patch version to the next.

FLAVOR represents a build-ID

Generally speaking, we will only communicate about MAJOR and MINOR releases.

In terms of communication:

We call “General Availability” builds that have gone through all of our QA processes (involving unit/regression testing, ad-hoc testing, field-tests at selected customers and progressive ramp-up starting with new customers). These are the builds we will make available to all customers. GA builds may or may not be the latest.

We call “Release Candidate” builds that have gone through most of our QA processes (involving unit/regression testing, ad-hoc testing, and currently are being field-tested). These are the builds we consider and will most likely make Generally Available.

We call “Engineering builds” builds that have a different FLAVOR that are meant to address specific bugs or introduce new features. They are available exclusively to our Enterprise customers and while they do receive some level of testing they are not as “road-tested” as

Copyright Matta Consulting Ltd. For more information visit <https://safepass.me/> and <https://www.trustmatta.com/>

safepass.me

The smartest password filter

our GA builds. We do support them and can produce them at short notice, typically in response to a support request. We do not recommend that you aim at upgrading to the very latest engineering unless you have a specific reason to.

Installation

Download the software

The current version of safepass.me can be downloaded from our CDN using the following link:

- <https://safepass.me/download>



download prompt

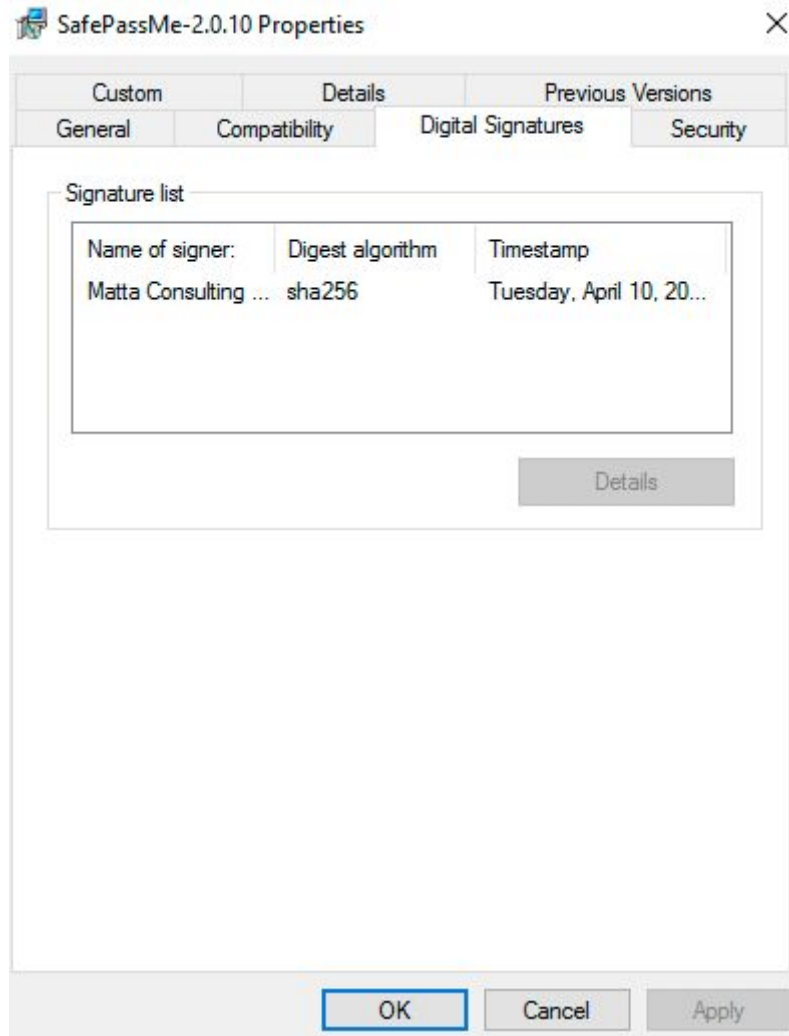
Verify its digital signature

safepass.me is distributed as a signed Windows Installer (MSI). The binary is signed by **Matta Consulting Ltd**, a leading UK-registered, boutique security consultancy outfit established in 2001 that is in effect the legal structure behind safepass.me.

In order to verify the integrity and authenticity of your safepass.me build, you should validate the authenticode signature of the MSI installer. You can do so easily by right clicking on the MSI file you have just downloaded and selecting *Properties -> Digital Signatures*

safepass.me

The smartest password filter



Should the signature verification fail, please report the error to us and **DO NOT INSTALL THE SOFTWARE !**

Common cause for signature verification failures include:

- Inaccurate time on the host
- Missing or Untrusted Certificate Authority
- Corrupted, mangled or otherwise tampered with download
- Missing windows patches that may impact the availability of cryptographic primitives used for the authenticode validation

safepass.me

The smartest password filter

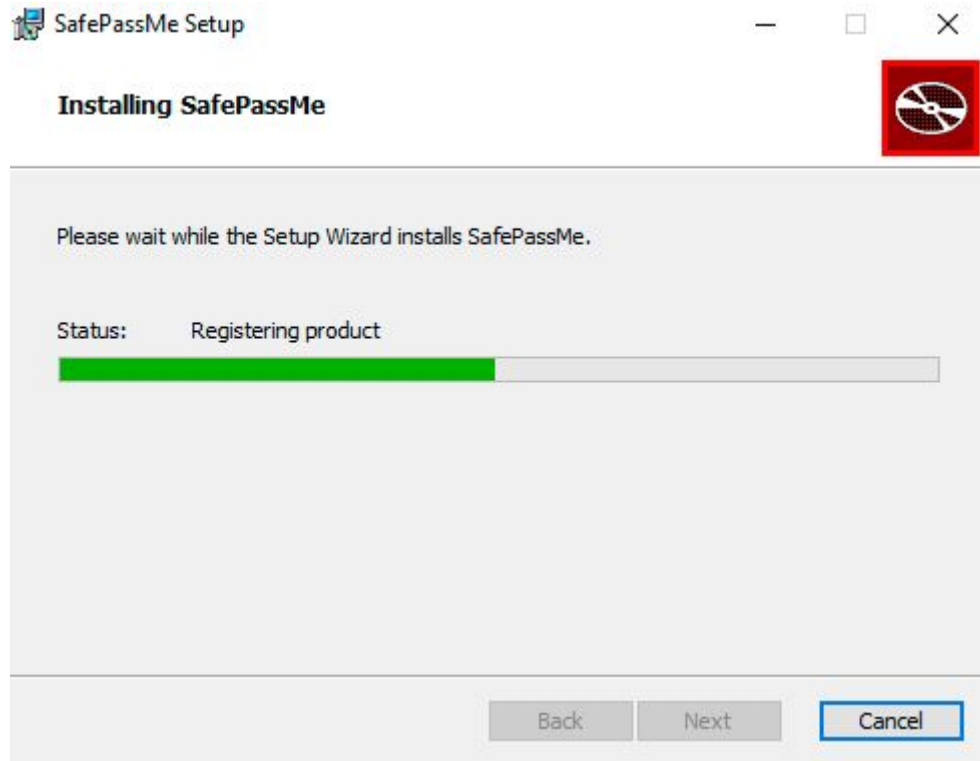
Accept the EULA



safepass.me

The smartest password filter

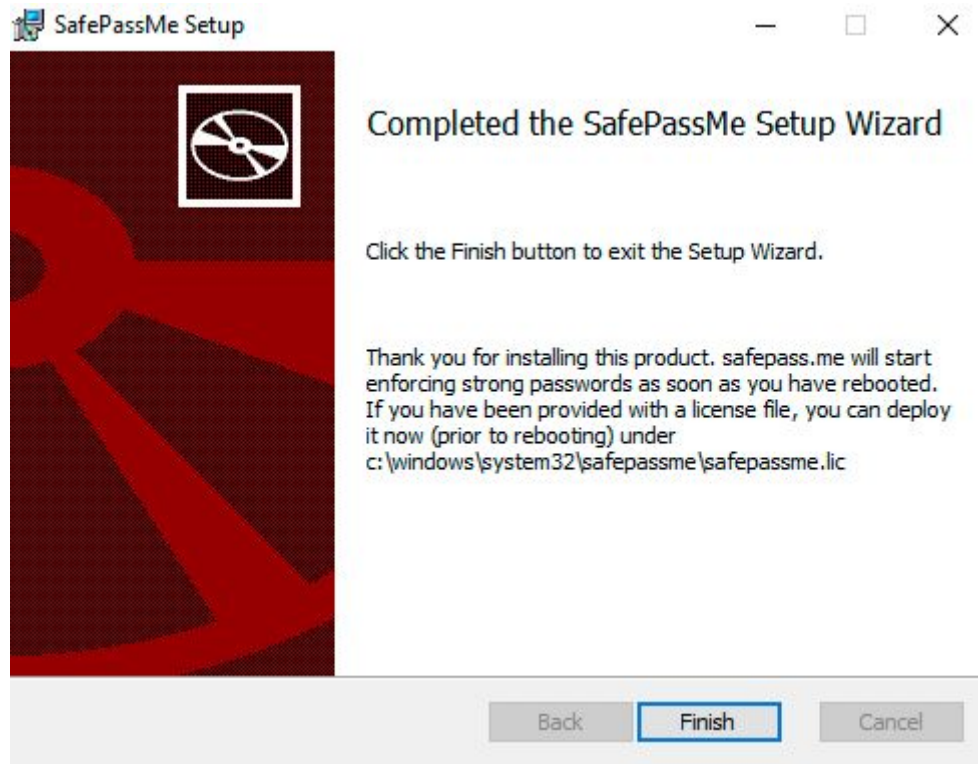
Install safepass.me



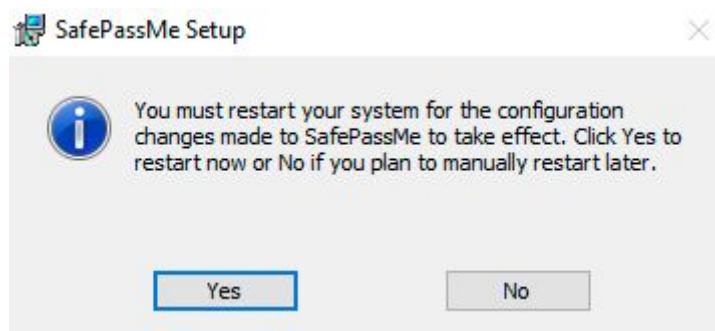
safepass.me

The smartest password filter

Deploy the License File



Reboot



Licensing

Online & Offline Licensing Options

Provided your Domain Controller has internet access the online licensing scheme will work automatically. If you have an air-gapped network, then you can take advantage of our Enterprise offline licensing option. We will provide you with a license file enabling you to use

safepass.me

The smartest password filter

your entitlement offline. As with everything else, we have designed the process with simplicity in mind.

Copy the file we have provided into the following folder:

%System32%\safepassme\safepassme.lic (usually this is
C:\Windows\System32\safepassme\safepassme.lic)

It will be picked up by the software upon reboot or in the next few hours. Where possible, it is best to deploy it immediately after installing the software (and just before rebooting).

Configuration

Configuration Options

safepass.me does not require any configuration and is secure out of the box: we have made it extremely straightforward to deploy and it starts protecting all users as soon as it is set-up. However, there are some custom options depending on the edition of the product you are using :

Administrative override (enterprise)

safepass.me can determine whether a password change was initiated by a user or was initiated by a privileged user (a password reset). It defaults to treating both the same (enforcing the password policy) but can be configured to distinguish both cases and always let administrative password resets go through (regardless of the qualities of the password chosen).

With this option you can instruct safepass.me to always let administrative password resets through by doing the following:

- Create a file at C:\Windows\System32\safepassme\allow-admin.override

Exclude Users (enterprise)

Sometimes excluding a user or user group is needed to appease an application setting or system setting, or there are service accounts that you would rather not tamper with.

With this option you can instruct safepass.me to ignore certain users by doing the following:

- Create a text file at C:\Windows\System32\safepassme\exempted-users.txt
- Put the full username (*sAMAccountName attribute*) of the user you want to exclude from the password policy enforcement on its own line

safepass.me

The smartest password filter

Enable Demo Mode (enterprise)

Demo mode is for companies that wish to ensure a smooth transition by testing the impact the software has on their password change processes. Demo mode provides a context-based view of the solution without enforcement, and in turn this helps to facilitate change management, and to ensure the best user experience.

To enable demo mode:

- Create a file at C:\Windows\System32\safepassme\dry.run

Configure a custom dictionary (professional & enterprise)

You can also extend the built-in dictionary of safepass.me by using a custom wordlist.

The matching in the custom wordlist is done in a case-insensitive fashion, based on the Damerau-Levenshtein distance in between each line of the file and the candidate password the user is trying to set. If the distance is lower than 4, the password will be blocked.

What this means in practice is that you do not need to set different cases for each possibility and you can even forbid a specific character from being present in any password by adding it on its own line.

Let's take an example and assume you have "company" in the wordlist, the following passwords will be blocked:

COMPANY (case-insensitive)
ComPaNy (case-insensitive)
compani (distance of 1)
C0mpany (distance of 1)
c0mp4ny (distance of 2)
company! (distance of 1)
company99! (distance of 3)
9com9pany9 (distance of 3)

safepass.me

The smartest password filter

Support Issues

safepass.me is generally hassle-free software: it will simply sit there in the background, ensuring your users don't pick compromised passwords! However, if you have any trouble installing or using it and/or have feedback or questions of any kind, we would love to hear from you.

Please email us at hello@safepass.me or call us on any of the numbers listed below :

+1-855-561-4185 (US/CAN Toll Free)
+44-203-966-5365 (UK)
+61-286-075-104 (AUS)
+883-5100-0990-3984 (iNUM)

Extended live support options are available with the Enterprise Plan.

List of Files

Once installed, safepass.me deploys the following files in the %SystemRoot%\System32\ folder:

safepassme.dll

in the %SystemRoot%\System32\SafePassMe\ folder:

db.dat
SafePassMe.exe
wordlist.txt

safePASS.me

The smartest password filter

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

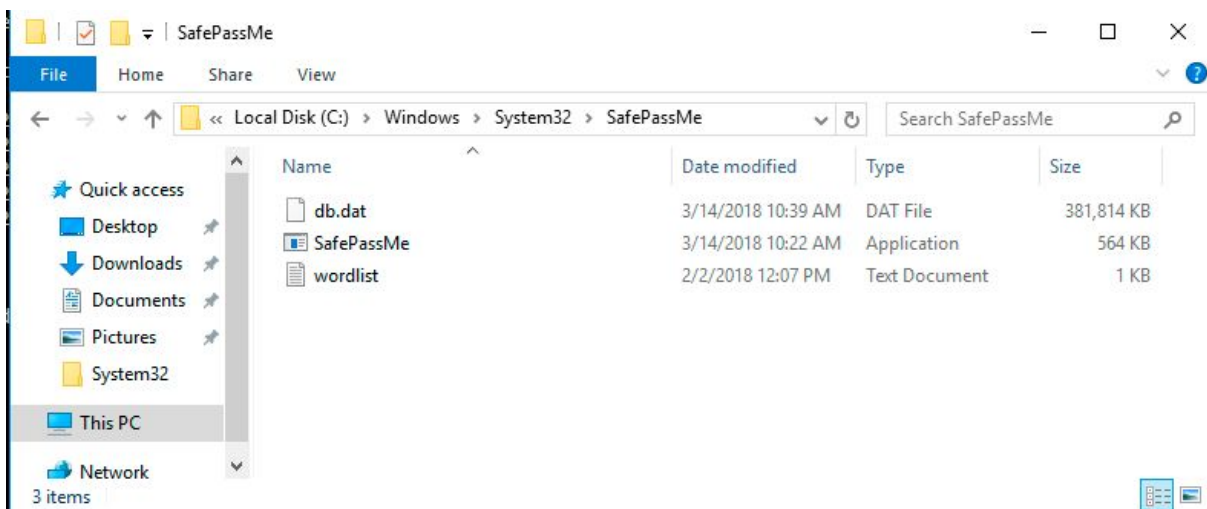
C:\Users\Administrator>cd \Windows\System32\SafePassMe

C:\Windows\System32\SafePassMe>dir
Volume in drive C has no label.
Volume Serial Number is F8F3-88C8

Directory of C:\Windows\System32\SafePassMe

04/05/2018  02:13 AM    <DIR>          .
04/05/2018  02:13 AM    <DIR>          ..
03/14/2018  10:39 AM             390,977,304  db.dat
03/14/2018  10:22 AM             577,224    SafePassMe.exe
02/02/2018  01:07 PM              680    wordlist.txt
           3 File(s)      391,555,208 bytes
           2 Dir(s)    52,614,582,272 bytes free

C:\Windows\System32\SafePassMe>
```



safepass.me

The smartest password filter

Privacy

We take your information and privacy very seriously. We've been running an IT security company for almost two decades and have seen terribly insecure setups so we're extra aware of how important this is; that's why we collect the absolute minimum information required to deliver the best service possible.

This is what we collect to enable and enforce licensing:

- Number of active users of the domain (user accounts that are active, not disabled).
- AD domain name
- AD domain GUID
- NETBIOS Name of the computer the software is running on
- The IP address the software is used from (as seen from the Internet)

We believe it's of paramount importance to also make it crystal clear that we have built the tool to check your passwords completely offline. None of your users' passwords are ever sent outside of your network by safepass.me nor do we do collect any password statistics.

Just like every other site we use cookies to provide a customised experience to our website by using analytics to give us insight on what information is most valuable to our visitors so we can ensure we can make improvements over time. We only use this information internally and we never share any of this information with any third party nor do we monetise on your data.

A comprehensive privacy policy on the cookies we set and how they are used can be found on our website at <https://safepass.me/>

Changelog

4.0.X

major

- Upgrade to HIBPv4 (551M passwords)
- Encrypt sensitive data exchanged through IPCs (using libsodium and a per-machine key), in a bid to mitigate against EDR solutions potentially “spilling out” sensitive data
- Add pre-installation checks to the installer based on feedback we obtained from support requests

minor

- Add a few words to the default wordlist deployed with new installations
- Improve the integrity validation of our software (Pin our certificate rather than trust all CAs)
- Add extra compiler hardening (-fstack-clash-protection)
- Bugfix: 4.0.1: fix a corner-case that may prevent the integrity level of the subprocess from being lowered from SYSTEM to MEDIUM
- Bugfix: 4.0.5: fix a corner-case that may prevent the telemetry from working

3.0.X

major

- Upgrade to HIBPv3 (517M passwords)
- Allow “in-place” upgrades from one version to the next
- Add extra compiler hardening (-fstack-protector-strong)

minor

- Bugfix: 3.0.1: Fix the paragraph numbering in the EULA

2.0.X

major

- Upgrade to HIBPv2 (501M passwords)
- 2.0.10: change the way we open the database to encourage Windows to cache it
- Introduce a minimum, mandatory 8 character length for passwords
- Substring and reverse-substring matching from the blacklist
- Dry-run mode
- User exemption
- 2.0.11: allow-admin.override
- Offline licensing
- Bugfix: 2.0.10: change how we obtain the licensing information (to avoid EDR interferences)

minor

- Bugfix: 2.0.10: exclude HealthMailbox accounts by default