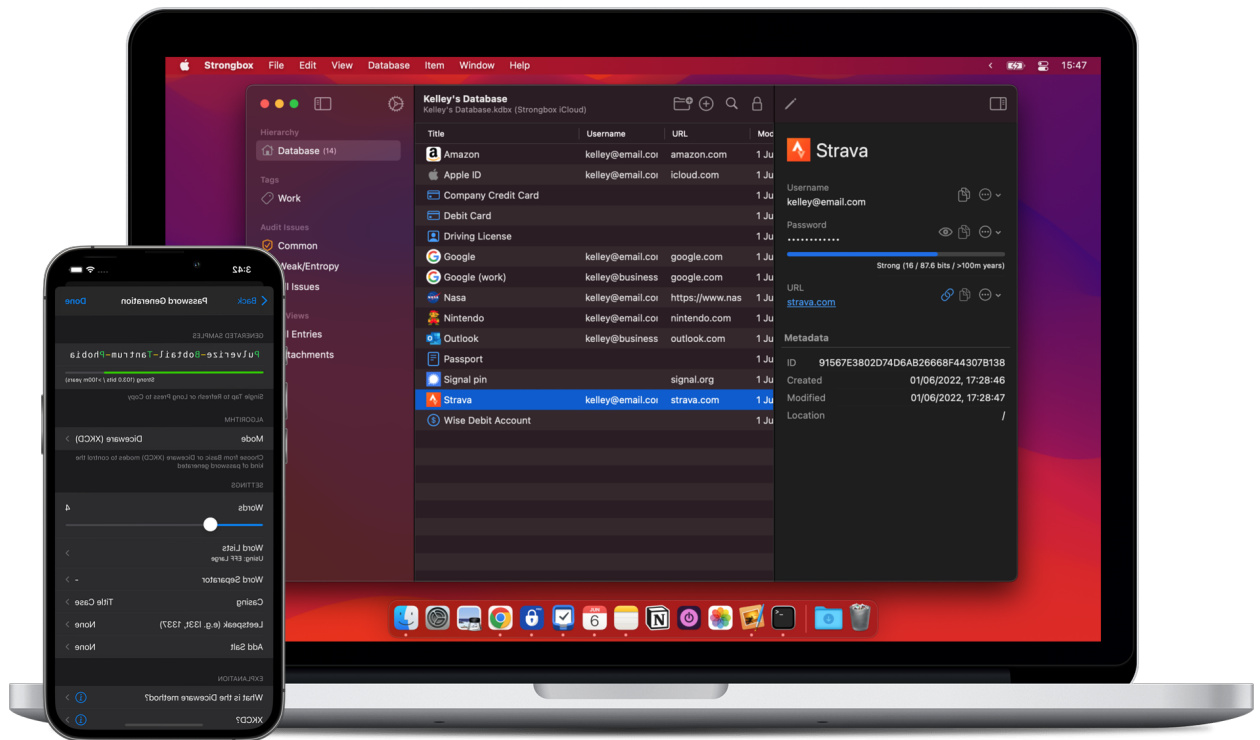




Getting Started With Strongbox

Learn how to set up Strongbox to start storing your passwords, credit cards and other secrets.



Version 1.1

© 2022 Phoebe Code Limited.

Contents

[What Is Strongbox?](#)

[Why You Should Use A Password Manager](#)

[What Makes Strongbox Different From Other Password Managers?](#)

[Storage](#)

[Security](#)

[Portability](#)

[Creating A New Database](#)

[To Create A New Database](#)

[On Mac](#)

[On iPhone And iPad](#)

[Choosing A Master Password](#)

[Moving To Strongbox From Another App](#)

[1Password](#)

[Exporting your 1Password Database](#)

[Importing your 1Password Database on Mac](#)

[Importing Your 1Password Database On iPhone And iPad](#)

[Other Password Managers And Browsers](#)

[Exporting To CSV](#)

[Importing Your Database On Mac](#)

[Importing Your Database On iPhone](#)

[KeePass](#)

[On Mac](#)

[On iPhone And iPad](#)

[Syncing Your Database Between Your Devices](#)

[Creating Your First Entry](#)

[To Create A New Entry](#)

[On iPhone And iPad](#)

[On Mac](#)

[AutoFill Passwords In Safari](#)

[On iPhone And iPad](#)

[On Mac](#)

[Next Steps](#)



What Is Strongbox?

Strongbox is a password manager that is beautifully designed and extremely secure.

Use Strongbox to securely store all of your passwords and other secrets—credit cards, identification documents, notes, and more—so that you never forget them.

Strongbox makes it easy to use unique and complex passwords that are difficult for hackers to crack.

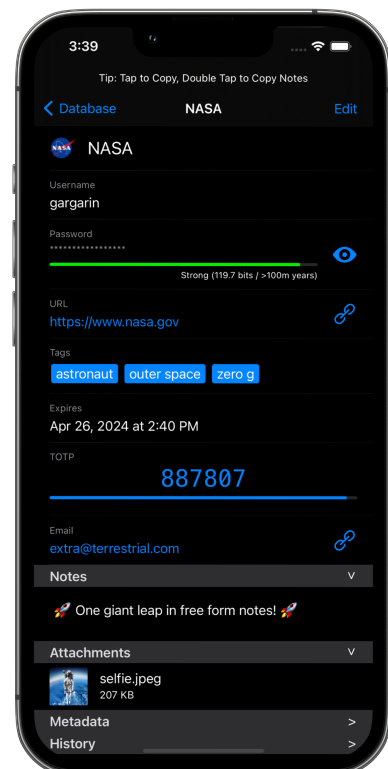
Why You Should Use A Password Manager

The most secure passwords are unique, complex and long. Unfortunately this also makes them very difficult to remember.

This leads many people to use a small collection of simple and short passwords that they share across multiple apps and websites. This makes them an easy target for cybercriminals.

Simple and short passwords are easy for hackers to crack in seconds or minutes using automated tools. Complex and long passwords would take multiple years to crack using those same tools, making the risk no longer worth the reward.

Furthermore, if you're using the same password across multiple sites, then all of those sites could be vulnerable if a single one of them is compromised.



Meaning if a hacker obtained your credentials for one site, for example Netflix, they would try those same credentials on other sites, such as Google or Facebook.

What Makes Strongbox Different From Other Password Managers?

Strongbox gives you **more control** over how your passwords and other secrets are stored, secured and opened.

Storage

Unlike most other password managers, with Strongbox you can choose to store your password database file anywhere.

Most Strongbox users choose to store their databases in their cloud storage provider of choice, such as Dropbox, OneDrive, iCloud, etc. Others set up their own server or even keep their database local-only. It's up to you!

Security

Strongbox supports a wide range of state-of-the-art cryptographic technologies with which to secure your data from hackers.

By default Strongbox uses various symmetric ciphers like the DOD standard AES256 algorithm, but you can also choose the Bruce Schneier designed TwoFish or a modern stream cipher like ChaCha20. Strongbox supports a host of new technologies and options, such as the award winning GPU-resistant Argon2 KDF, as well as hardware keys such as YubiKey, and more.

Portability

Strongbox is built on industry leading and open source standards. This means you can open your password database with a wide variety of different password managers that are based on these same standards, on every imaginable platform. And if you decide to leave Strongbox you can do so easily and immediately. **There's zero lock-in.**



Creating A New Database

The first thing to do is create a new database to store your entries in. Entries are passwords, credit cards, identification documents, or anything else that you want to keep secret and secure.

You can keep all of your entries in a single database, or create several databases for different projects or areas of your life, e.g. Work or Personal, or perhaps a shared Family database.

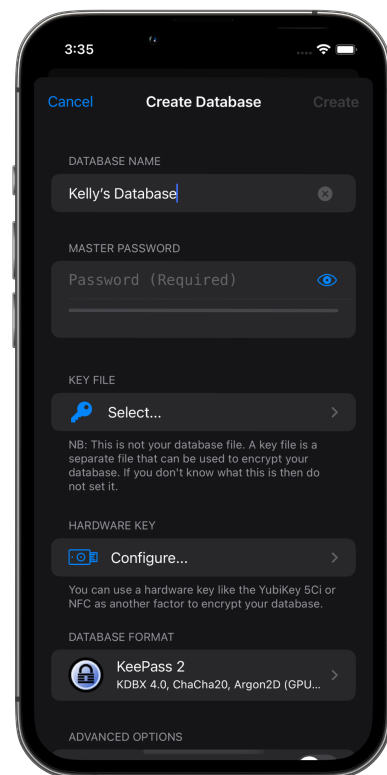
To Create A New Database

On Mac

1. In the menu bar at the very top of your screen, click **File**
2. Click **New**
3. Choose **Next** on the Select Database Format screen (the default is ideal for most people)
4. Create a strong and memorable master password ([see below](#)) and click **OK**

On iPhone And iPad

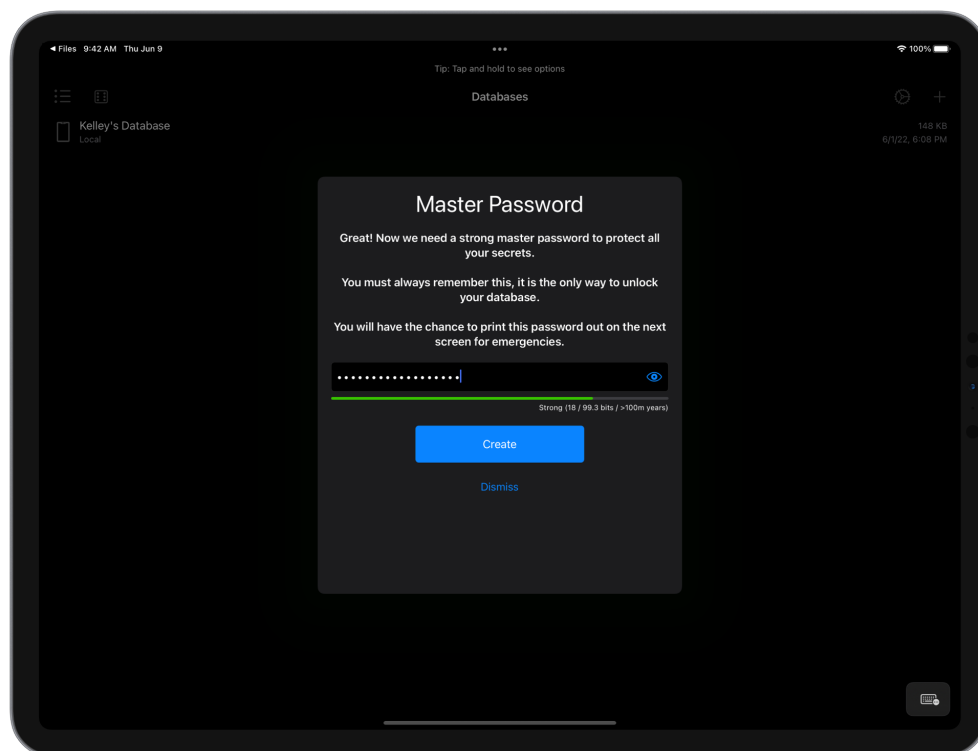
1. Tap the **+** button in the top right of the screen and select **New Database**.
2. Enter a name for your database, such as 'Kelley's Database' or 'Personal'. Then tap **Next**.
3. Create a strong and memorable master password ([see below](#)) and tap **Create**.



Choosing A Master Password


All of your passwords and other entries will be stored behind your master password. It needs to be something that you will remember but also something that's very secure, so that it cannot be guessed by another person.

Your master password will be the only password that you ever need to remember once you start using Strongbox.



There are many ways to create a master password that is both memorable and secure. Generally speaking, the total length of the password is more important than the variety of characters that are used. Therefore, a password made up of several recognisable words can be stronger than a shorter password that includes numbers and symbols. For more information, check out the following article from The Intercept:

[Passphrases That You Can Memorize — But That Even The Nsa Can't Guess.](#)

 Remember, if you forget your master password you will not be able to unlock your database!



Moving To Strongbox From Another App

It's easy to import your passwords to Strongbox from another password manager, such as KeePass or 1Password.

1Password

It's super easy to migrate your data over from 1Password to Strongbox.

Exporting your 1Password Database

1. Open 1Password on your computer
2. Unlock your vault
3. Click **File > Export > All Items**.
4. Save the '.1pif' file somewhere on your computer

Importing your 1Password Database on Mac

1. Open Strongbox on your Mac
2. Click on File > Import > Import 1Password (1Pif)
3. Locate and select the 1Pif file that you exported in Step 1 above

See our full guide for more detailed instructions: [Import your data from 1Password \(macOS\)](#).

Importing Your 1Password Database On iPhone And iPad

1. Save the 1Pif file to the Files app on your iPhone or iPad
2. Open Strongbox and tap the **plus icon (+)** in the top right of the screen
3. Tap **More**
4. Tap **Import 1Password**
5. Navigate to and tap on your 1Pif file

Other Password Managers And Browsers

If you're coming from another password manager, such as LastPass or Dashlane, you will need to export your existing database to a CSV file. The same goes if you're using your internet browser to store your passwords.

The process for exporting your passwords is slightly different for each password manager and browser. The process to then import the CSV file into Strongbox is the same in all cases.

Exporting To CSV

See the individual guides below:

- [Exporting from your browser \(Chrome, Firefox and Safari\)](#)
- [Exporting from LastPass](#)
- [Exporting from Dashlane](#)
- [Exporting from Bitwarden](#)


Once you have the CSV file saved on your device, follow the steps below to import that file into Strongbox.

Importing Your Database On Mac

1. Export your LastPass database as a CSV file
2. Open Strongbox
3. In the menu bar at the very top of your screen, click **File**
4. Select **Import**
5. Click **Import CSV...**
6. Navigate to and select your CSV file
7. Click **Open**

Importing Your Database On iPhone

1. Open Strongbox
2. Tap the **plus icon (+)** in the top right of the screen
3. Tap **More**
4. Tap **Import CSV**
5. Navigate to and tap on your CSV file

 **Make sure to delete the exported CSV file when you're finished.**
This file is unencrypted, meaning if someone else was to get access to it there would be nothing stopping them stealing all of your data!

KeePass

KeePass is natively supported by Strongbox. This means that you can use your existing KeePass databases, and Strongbox will read and edit them for you, no need to change formats.

On Mac

5. Open the Strongbox app
6. In the menu bar at the very top of your screen, click **File**
7. Click **Open...**
8. Navigate to and select your KeePass database file
9. Click **Open**

On iPhone And iPad

1. Add your KeePass database to your iPhone or iPad – either locally in the Files app or in a cloud storage provider of your choice
2. Open the Strongbox app
3. Tap the **plus icon (+)** in the top right of the screen
4. Tap **Add Existing**
5. Select the storage location where your database is located (e.g. Dropbox)
6. Navigate to and tap on your database file
7. Tap **Add**

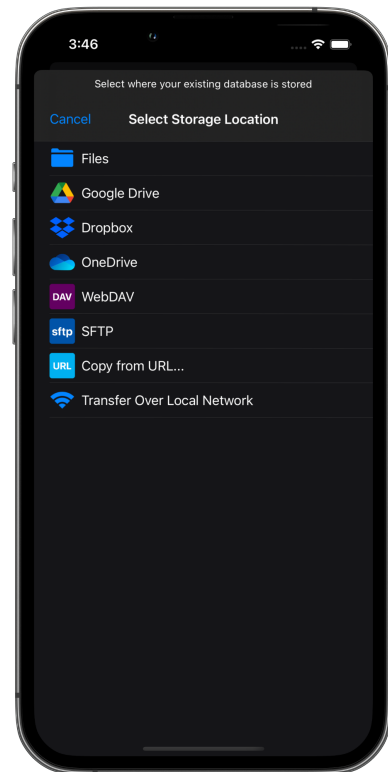


Syncing Your Database Between Your Devices

Syncing means keeping your passwords and other entries up to date across your devices, such as your iPhone, iPad and Mac. Strongbox is different to most other password managers in that it allows you to control where you store your data.

For most people, we recommend you use a cloud provider to store and sync your data, as this means that you won't lose your passwords and other entries if your device is lost or damaged.

You can select from Dropbox, OneDrive, Google Drive, and iCloud when you create a new database. You can use any cloud storage app that integrates with the iOS Files app.





Creating Your First Entry

Entries can consist of any information that you want to keep secret and secure. That could be a password, credit card or even a document or image, such as a scan of your passport.

To Create A New Entry

Let's assume you want to store the login information for a website.

On iPhone And iPad

1. Tap **More (...)** in the top right of the screen
2. Tap **New Entry**
3. Enter a title for your entry, for example 'Strava'
4. Enter the username you use for that website (this is often your email address)
5. Enter your password for that website
6. Enter the URL for that website
7. Tap **Done**

On Mac

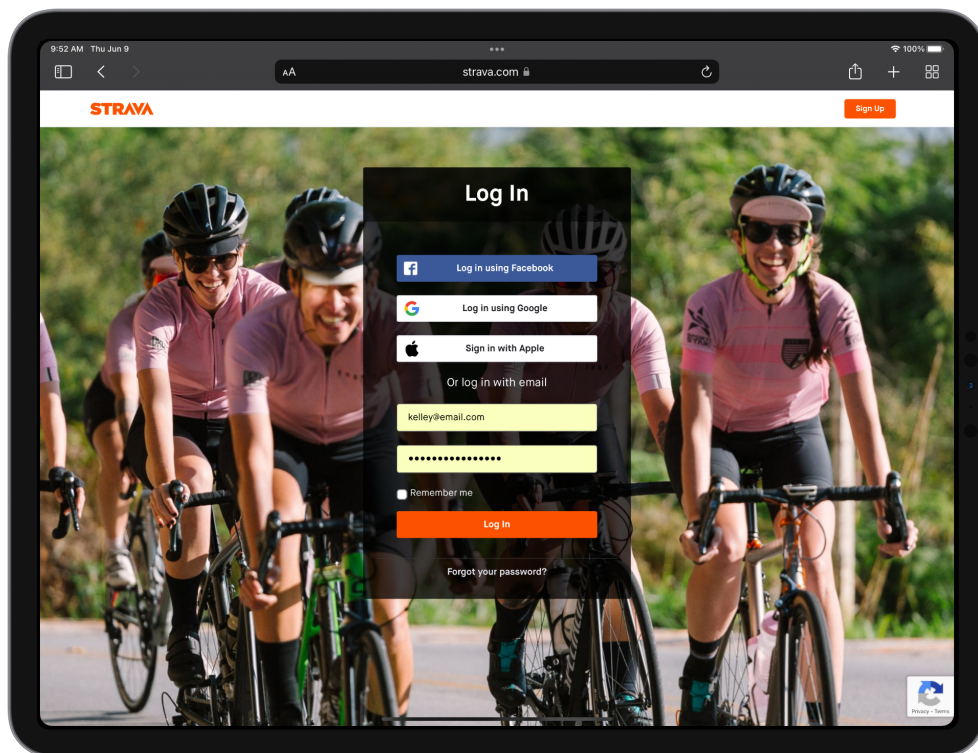
1. Click the **plus icon (+)** in the top right of the screen, next to the search bar
2. Enter a title for your entry, for example 'Strava'
3. Enter the username you use for that website (this is often your email address)
4. Enter your password for that website
5. Enter the URL for that website
6. Click **Commit & Close**

Now you've saved the password, you're ready to log into that website using AutoFill for Safari.



AutoFill Passwords In Safari

Once you've saved your login information as an entry in the Strongbox app, you can automatically log into that website when browsing the web with Safari.



On iPhone And iPad

Step 1: Setup AutoFill

1. Open the **Settings** app on your iOS device, scroll down and tap **Passwords**
2. Use Touch ID, Face ID or your passcode to authenticate
3. Tap **AutoFill Passwords**
4. Make sure AutoFill passwords is turned on

5. Make sure that under the **Allow Filling From** section, Strongbox is ticked

Step 2: Automatically Login To A Website In Safari

1. Open the **Safari** app
2. Navigate to a website for which you've stored a password in Strongbox
3. Go to login to that site
4. Tap on the username or password field on the website
5. Select the username you want to use from your device's keyboard
6. Use Touch ID, Face ID or your phone's passcode to authenticate
7. Login!

On Mac

Step 1: Setup AutoFill

1. Open the **System Preferences** app on your Mac
2. Click on **Extensions**
3. Click on **Password AutoFill**
4. Tick the checkbox next to the Strongbox app

Step 2: Automatically Login To A Website In Safari

1. Open the **Safari** app
2. Navigate to a website which you have a saved password in Strongbox for
3. Go to login to that site
4. In the username or password field on the website, click the small key icon
5. Select **Strongbox...**
6. Enter your master password and click **Unlock**
7. From the list of entries in your database, select the website you're logging into
8. Login

Learn More

- [How do I enable and use AutoFill on iOS?](#)
- [AutoFill on MacOS \(Big Sur+\)](#)
- [Does MacOS Password AutoFill work on Chrome/Edge/Firefox?](#)



Next Steps

If you would like to learn more about Strongbox and how you can make the most of its powerful features, check out these resources:

- Visit the [Helpdesk](#) for more information on how to make the most of Strongbox
- Join the discussion in [our subreddit](#)
- [Follow us on Twitter](#) or [subscribe to our newsletter](#) to get the latest updates

We hope you enjoy using Strongbox! If you do, please consider [leaving us a review](#). It helps us out immensely.