Enpass User Manual - iOS

version 6.7

Enpass Technologies Inc.

August 19, 2021

Contents

User Manual

Enpass Version– 6.7

Welcome to the Enpass user manual for iOS. This user guide describes how you can use Enpass to easily and securely manage your passwords, credit cards, bank accounts, and other confidential items. You will also find tips that help you make use of the wider capabilities of Enpass.

Introduction to Enpass

Enpass is a simple and secure app to take care of your passwords and other credentials. It lets you securely save every kind of information using existing templates. Whether it's passwords, logins, bank accounts, credit cards, National ID, Passport and more. All this data will be encrypted by a master password.

You can also generate a unique and robust password with a single tap, and you don't need to remember them as Enpass can fill them automatically in apps and browsers. All your data is saved offline on your device, and you can rest easy knowing we offer military grade encryption. You can even sync across your multiple devices using your cloud accounts. Enpass is cross-platform and is available for all major platforms from your desktop to your smartphone.

Prerequisites

From version 6.2.0 onwards, Enpass requires iOS 9.3 or later.

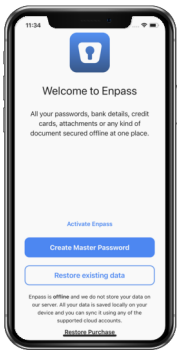
Getting Started

You can start using Enpass either as a new user or as an existing user.

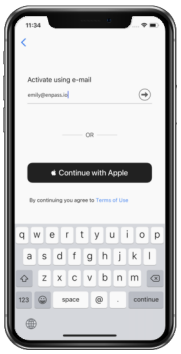
Activate Enpass

If you have purchased Enpass on a platform, we recommend you register your purchase. The purpose of registration is to link your purchase with a valid email address so that you don't have to buy it separately on all platforms. This section will show you how to activate/restore your Enpass license across multiple platforms via following steps:

1. Click on **Active Enpass**.

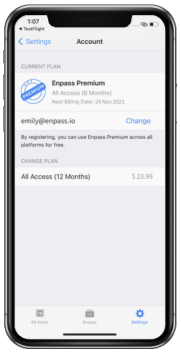


2. Enter your registered email address.



3. Verify it via OTP

3. Once verified, the app will restore the license linked with the registered email address.

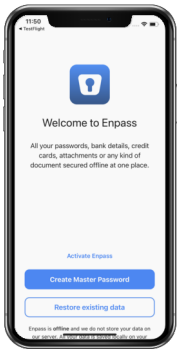


As a New User

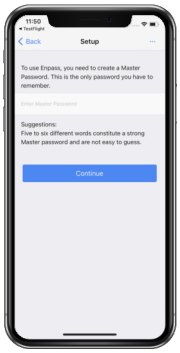
If you're a new user, you first need to set up a master password before adding any items. Enpass encrypts all your data with the master password. Read more about master password.

To create a master password, follow these steps:

1. On the Welcome screen of Enpass, tap **I am a New User**.



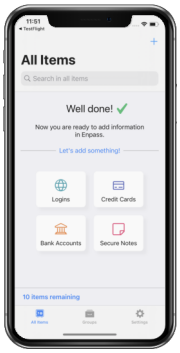
2. Create your master password.



3.Tap **Continue** (See figure above).

> ***Note***
>
> This is the only password you need to remember. Because you need it to open/unlock Enpass, keep the master password safe and secure.

You are now a trial user of Enpass and can add up to ten items. See Adding items.

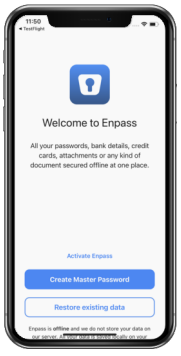


By registering, you can remove this limit.

As an Existing User

If you are an existing user of Enpass, you would be having your data somewhere, either on any cloud where you have synced before or a local backup of data. You can directly restore that data from a Backup File or from a cloud.

- Open Enpass. On the Welcome screen you can see the option, **Restore existing data**. Tap to continue.



Restore data using your cloud service provider. You will require the master password for this.

Import Passwords from Other Sources

It might be possible that you already have some passwords saved in other password managers, browsers, CSV files, etc. You can install Enpass on your desktop to import data from other sources and use cloud sync to seamlessly synchronize data in Enpass between the desktop and mobile.

Master password

Enpass encrypts all your data using the master password. You also unlock the app with it. Make the master password strong. If you lose it, we cannot help you recover it. Write and store it in a safe, secure place. For tips on creating a strong password, see this blog post.

> ***Caution!***
>
> The master password is irrecoverable. If you forget the master password, it can not be retrieved by any means.

Keyfiles

Advanced users can add another layer of security by using a keyfile with the password. Enpass appends the characters in the keyfile to the password and uses them together to encrypt your data.

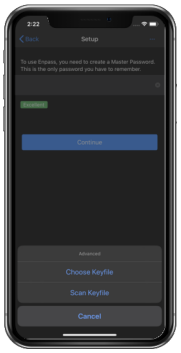
To add a keyfile to your iOS device you need to:

1. Generate the keyfile.
2. Add it to your iOS device.

Generating the keyfile

You need to generate keyfiles from Enpass on your desktop. See generating keyfiles.

Adding the keyfile



To add a keyfile, follow these steps:

1. From Enpass on your iOS device, tap **Settings > Security > Change master password**.
2. In the **Change password** screen, tap the **More options** button at the top right.
3. To add the keyfile:
   - Tap **Scan keyfile** and scan the QR code from your desktop (See generating QR code).
   - Tap **Choose keyfile** if you have transferred the keyfile by other means.
4. Enter the master password again.
5. Tap **Done**.

Important

Keep the keyfile safe and secure as you will not be able to log in to Enpass without it. It is also irrecoverable- so backup all your keyfiles. If you have created multiple vaults and added keyfiles to them, you will need them to open these vaults.

Removing keyfiles

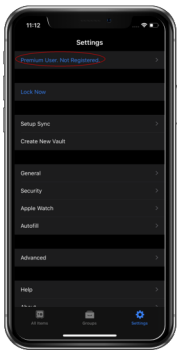
To remove keyfiles, use Enpass on your desktop (See removing keyfiles).

Registration

Registration in Enpass is the process of linking your Enpass purchase with your email ID. This helps to restore your purchase on other platforms for free.

To register you purchase, follow these steps:

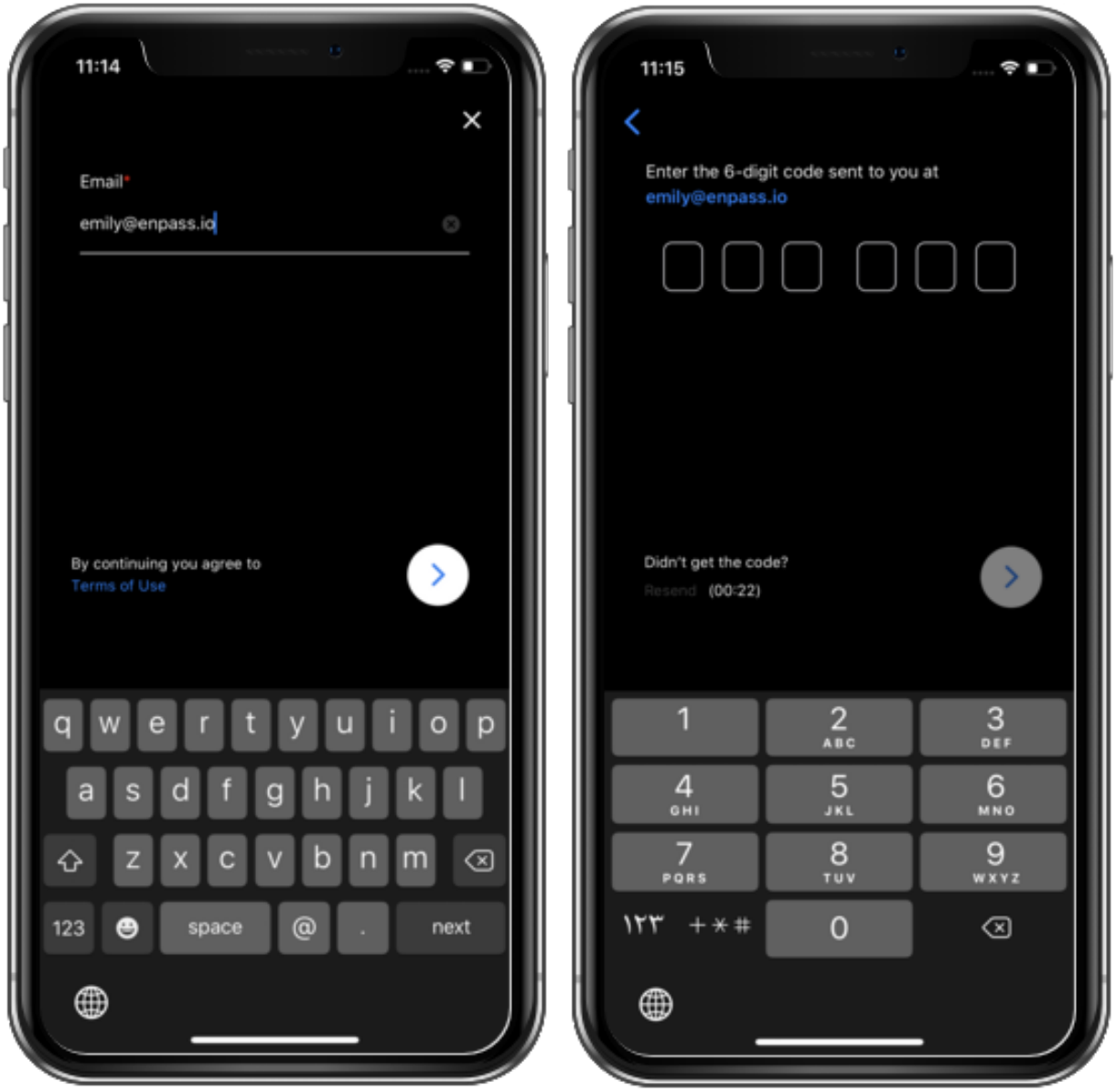
- On the **Settings** screen, tap your registration status at the top of the screen. This will start the registration process.



Note

The text of your registration status may differ as per the status of your license.

- There are two ways to register your purchase with Enpass. One is with the email ID and other is using the Apple account.
- For email, tap **Use Email**, enter the email ID and proceed. This will send a six-digit one time code to your email id.



- Enter the code. Now you are a registered Enpass Pro/Premium user. You can use the same email ID to restore the purchase on other platforms as well.

> ***Note***
>
> We do not collect any of your data other than your email. Your secured data always remains on your device and isn't stored on our server.

Adding and Managing items

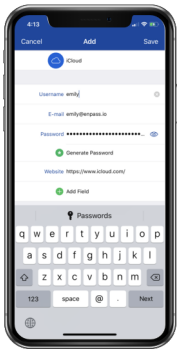
Your information is stored in the form of records, we refer them as **Items**. You can perform the following operations on these items:

Adding Item

Every single record you save in Enpass is described as an item. Here are the simple steps to add an item in Enpass:

- On the **All Items** tab, tap the **+** button.

- Select the template from the provided list of categories. If you have multiple vaults, you can select the vault in which you want to add the item.
- Fill in the details and save the item.
- Also you can customize the fields, generate passwords, add tags, **TOTP**, attachments and so much more.

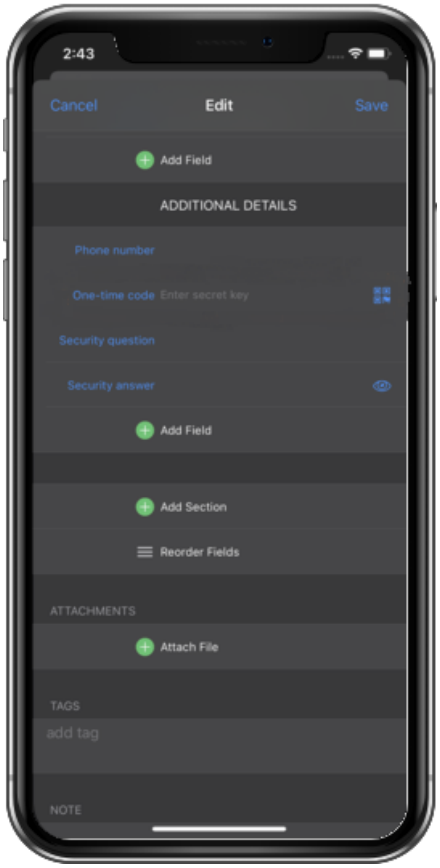


> ***Tip***
>
> To generate strong and unique passwords, we recommend that you use the built-in Password Generator. Every password field has its button next to it.

Adding One-Time Code

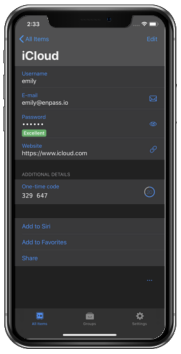
Enpass can also be used as an authenticator app to store one-time codes for websites that support Two-Factor Authentication. You can refer Audit to know the items for which you can add one-time codes. To add One-time code in Enpass, follow the steps below:

- Select the item where you wish to add One-time code.
- Tap on the `Edit` button. If the item is of a **login** type there is a default field of *One-time code* type, just scroll down to that and tap on QR code that appears at the right corner of the field.



- For the items other than login, you first need to add a customized field of type *One-time password*.
- Drag the scanner over the QR code on the website from where you wish to add One-time code, or you can copy and paste the secret key into the text field manually.

- Tap on the *Save* button.
- Enpass runs a countdown of 30 seconds so that you know when the code expires. When the time runs-out, new code will automatically be generated and the countdown restarts.



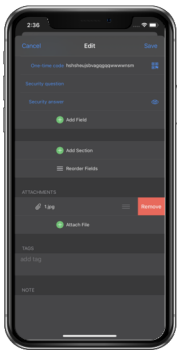
Adding Attachments

You can attach files such as photos, pdfs and files of any other format to any item in Enpass.

> **Note**
>
> There's restriction on uploading files more than 5 MB.

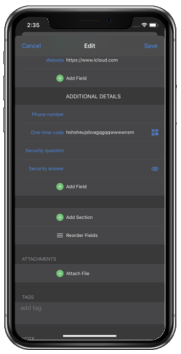
Attach Photo

You can attach photos saved in the device or a new one using the camera as an attachment to Enpass. Just `Edit` item → Tap on `Attach File` → Select Source → Capture photo or select from device → Crop the photo → Tap *Done* → Add a Filename → Save the photo.



Attach file

Same way, you can attach a file saved in your device as an attachment. Simply `Edit` item → Tap on `Attach File` → Select `iCloud Drive` → Choose a file from iCloud → Tap on *Save* to finally save the item.



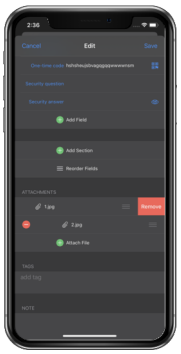
> **Note**
>
> All the items having attachments are directly accessible from the Groups → Attachments.

View Attachment

To view an attachment, go to the `Detail` page of the item → Tap on attachment.

Delete Attachment

To delete an attachment, `Edit` the item and scroll down to the *Attachments* section. Tap on ■ visible on the attachment field → `Remove` to delete it. A warning message will appear, tap on *Continue*. To pertain the changes, you need to **save** the item as well.



Tags

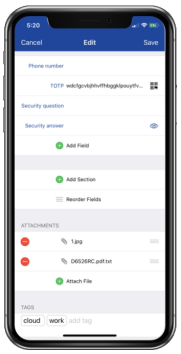
Tags allow you to manage your data in a more organized and convenient way.

Tagging items

The following steps will guide you to add tags to your items.

From Edit page

`Edit` the item and scroll down where you can see the Tags field. Add the tag name in the tags field and enter Comma (,). This way you can also add multiple tags to the same item. Once done adding the tags, you can save the item to pertain the changes.



- You can also add tags in a hierarchy using the following pattern- Tag:Subtag:Subsubtag.

Note

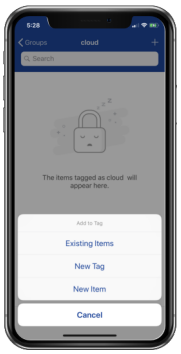
You can quickly access all the tags saved in Enpass from the `Groups` in Tab Bar. Just tap on Tags from the Groups, and you'll be presented with the list of all the existing tags in Enpass.

From Tab Bar

You can also create tags from tag-listing in Tab Bar and then manage items.

Add a new item under a tag

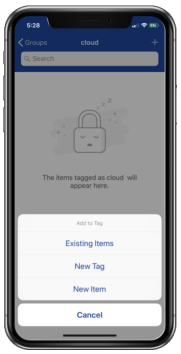
Tap the *Tag* with which you want to add a new item. Tap on + → Select *New Item* → choose the vault (In case of multiple vaults only) → Choose category → If you're having multiple vaults, you can Add item details → Tap *Save*



Add existing Items under a tag

You can also add the existing items to the tag by following these simple steps:

Tap the *Tag* in which you want to add a new item. Tap + → Select *Existing Items* → Mark the items you want to tag → Tap *Done*.



Nested Tags

You can add the sub-tags in an existing tag in Enpass. To add a sub-tag, go to `Groups` → Tags → Select the *Tag* in which you want to add a sub-tag. Tap on + button → Tap on *New Tag* → Add tag name and save. This way you can create tags in the hierarchy, you want.

Editing Tags

Go to **Tags** from the `Groups` in Tab Bar. Swipe left on the Tag name and tap *Edit* → edit tag name → Save and done. On the same screen, you can also delete the tag by tapping the *Delete Tag* button.

Untag an Item

To untag an item, go to **Tags** from the `Groups` in Tab Bar → Select the tag → Swipe left on the item and tap `Untag`.

Deleting and Archiving

You can move items to *Trash* which are no longer in use and from there you can permanently delete them. Also, Enpass lets you *Archive* items which you don't want to trash.

Trash

- To move an item to Trash, tap on the item → Hit ■ button → *Move to Trash*.
- To restore an item from Trash, tap on *Trashed* under *Others* in the `Groups` on Tab Bar → Tap on the item → Tap *Restore*.
- If you want to delete the item permanently, delete it from the *Trashed* under *Others* in `Groups`.

> ***Note***
>
> Deleting an item from Trash will permanently delete it from your device and other synced devices.

Archive

You can also archive the items which you don't need now but are not sure when they might be required in future.

- To archive an item, tap on the item → tap on ■ → Archive.

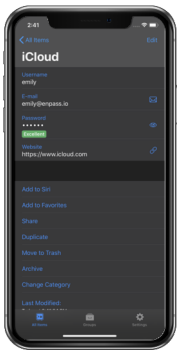
> ***Note***
>
> The Archived item will remain in Enpass but will not appear in the search results.

- To unarchive an item, tap on *Archived* under *Others* in `Groups` → Tap on the item → Tap *Restore*.

Duplicating item

Duplicating an item is especially beneficial when you have customized the fields of any item and want to create similar items. Here are the steps to help you with duplicating items:

- Tap on the item which you want to replicate → Tap on ■ button → Duplicate.



- A new item will be ready for editing. After making the changes, tap **Save**.

> ***Note***
>
> The attachments will not be copied to the duplicated item.

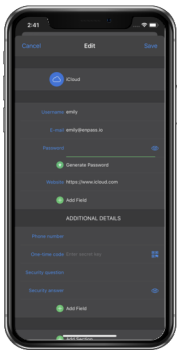
Customizing Fields

You can customize an item by adding new fields or editing the pre-existing fields.

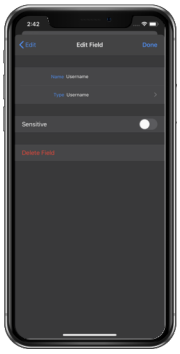
Editing field type

You can edit field's label and field's type of any item as per your requirements.

- While you are at the Edit screen, tap that field's label.



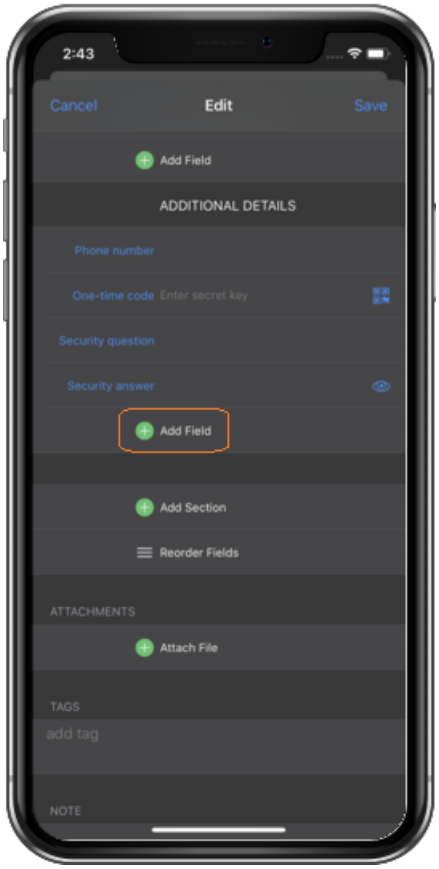
- You can change the field-type along with its name, and also, you can choose the field type to be sensitive. Tap **Done** after making the changes.



Adding fields

Sometimes you might need to add new fields to any item. Following steps will guide you for that.

- While you are at the Edit screen, select *Add Field*.



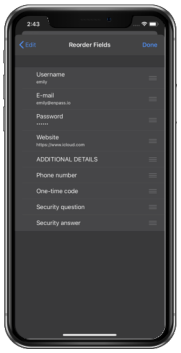
- Enter the new field's name and choose the appropriate type. You can also mark the field type to be as *Sensitive*.
- Tap **Save** to pertain the changes.

> ***Important***
>
> We recommend that you keep the **Sensitive** mode ON for passwords or security answers. This way your passwords, PINs and other similar texts will stay safe from shoulder surfers when you use the app in public places.

Re-ordering Fields

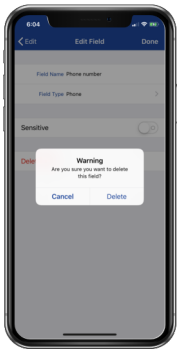
You can also re-arrange the order of the fields in an item.

- Tap on `Reorder Fields` on Edit screen.
- Hold and drag the fields using ≡ icon to Re-arrange them and tap *Done* to save.



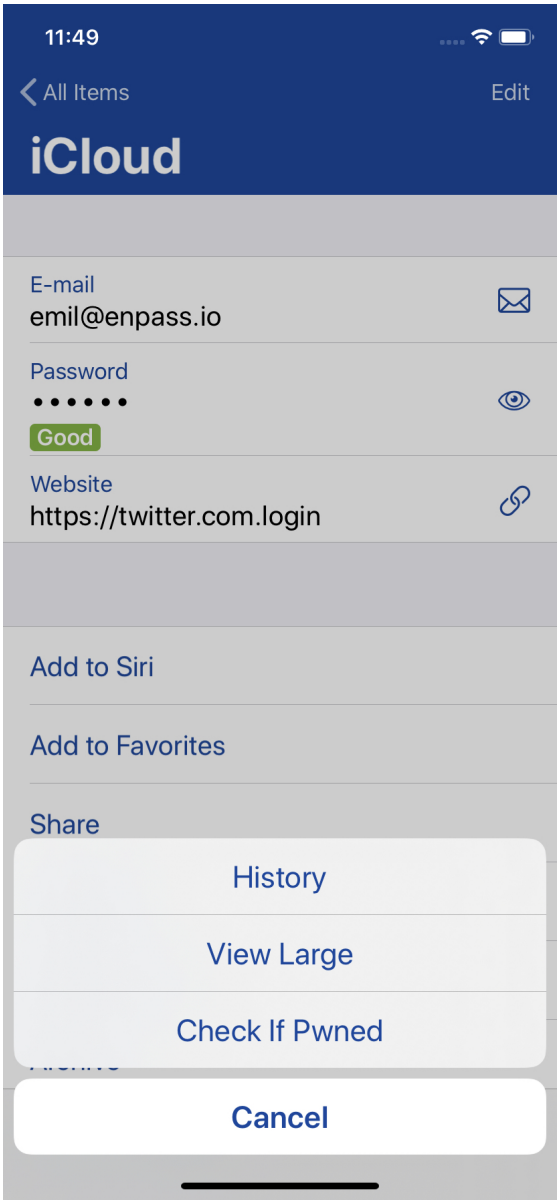
Deleting fields

- While you are at the Edit screen, tap the label of that field you want to delete. Let's say you tapped *Phone*. Field's details will be loaded on the next screen. Tap on the delete icon. A warning message will be displayed for confirmation of deletion. Tap **Delete** to remove the field. To pertain the changes finally, you need to tap **Done**.



Field History

Once you've updated any field, its changes get recorded as *Field History* in Enpass. To see the field history, tap on the field from the details screen → tap on `More` → *History*.



Customizing Password Fields

Unlike other field types, password field has additional options which allow you to set an expiry date to that particular password and exclude the password from the **`Audit`**.

Exclude from Audit

- To exclude the password from Password Audit, tap on the *Password Field* from the Edit screen → Enable *Exclude from Audit* → Save the field → Save the item.

Set Password Expiry

- To set an expiry date to the password, tap on the *Password Field* from the Edit screen → Enter the number of days → Save the field → Save the item.

Note

To set the expiry date to a password, make sure `Exclude from Audit` is disabled.

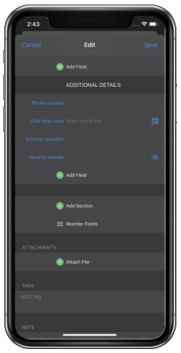
Sensitive

Sensitive fields are concealed by bullets, so it is recommended to set all the password fields as *Sensitive*.

Adding Section

Follow the steps below to add sections in the item:

- Go to the edit screen of the item → Tap on `Add Section`
- Enter Section Name.
- Tap *Done* to save the section.
- Finally *Save* the item to pertain the changes.



Customizing icons

When you add an item, Enpass assigns it a standard (default) icon based on the url contained in the item. Enpass lets you customize the default icons in two ways:

- By using the website icons (favicons)
- By using your own images as custom icons

Using website icons

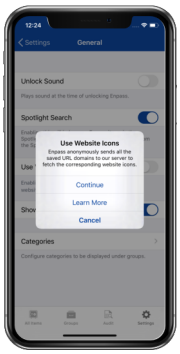
Generally, website icons are small, iconic images (favicons) associated with a particular website which appear in the address bar of the browser.

Enpass can download the website icons of the saved items and replace them with default icons. They make your items more recognizable, saving time while glancing through the long list for a particular item.

> ***Important***
>
> Enpass does not sync website icons across devices; you need to enable them individually on each device.

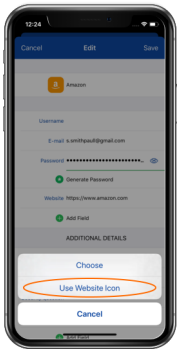
To enable website icons, follow these steps:

Tap **Settings** → **General** → Enable **Use Website Icons** option → **Continue**.



Enabling website icons for a particular site:

1. Open the item and tap **Edit**.
2. Tap the icon of the item → **Use Website Icon**. The icon reverts to the favicon of the website.



3. Tap **Save**.

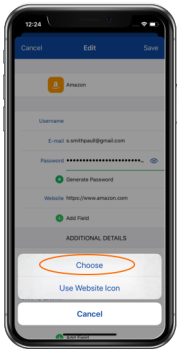
Note

Custom icons are not replaced when you enable website icons.

Using your own images as custom icons

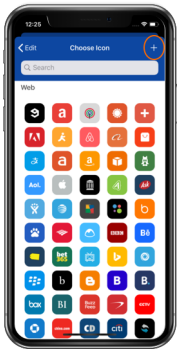
You can also select and use your own icons for each item. These are the steps:

1. Open the item from the main window.
2. Tap **Edit**.
3. Tap the icon of the item.
4. Select **Choose**. Enpass displays a collection of icons from which you can select your icon for the item.



To use images from your device as an icon, follow these steps:

1. Tap **+** at the top right corner of the screen.

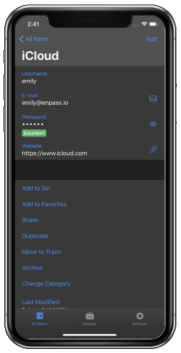


2. Locate the image in your phone; resize it if necessary.
3. Tap **Save**.

Changing Category

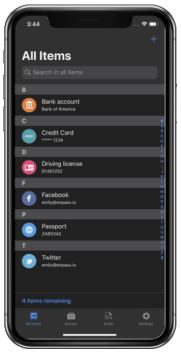
Here are the steps that will help you to change the category of item in Enpass.

- Open the item → Tap on **Change Category** → Select the the category you want to set for the item.

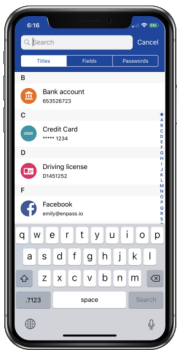


Search

Enpass assist you in searching an item directly from the search bar for quick access. Every list in Enpass (namely All Items, Favorites, Categories, Trashed and Archived items) is provided with a search bar on top.



Just tap on the *Search Bar*, choose your search preference from the segmented control bar and type to search. Enpass will search the currently selected vault and will refine the results as you type. You can also refine the results using the options displayed on the segmented control button bar.



Moving Items to Other Vaults

If you've multiple vaults in Enpass, you can easily move/copy the item from one vault to other vault. See how.

- Go to the detail screen of the item → Tap on more options (3-dots) → Tap on **Add to Vault** → Select the vault where you want to move/copy the item → Tap on **Move/Copy** to add the item to the selected vault.

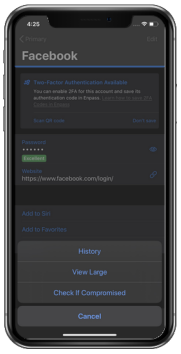
Checking Compromised Passwords

Enpass checks your passwords against a list of breached passwords managed by haveibeenpwned to see if any of your passwords have appeared in data breaches. It's a trustworthy procedure, ensuring that your passwords are secure in Enpass and are never sent to the internet.

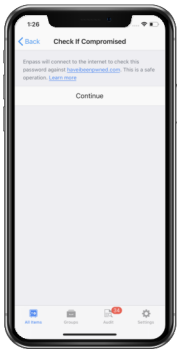
There are two ways to check for compromised passwords in Enpass -

Checking Individual Password

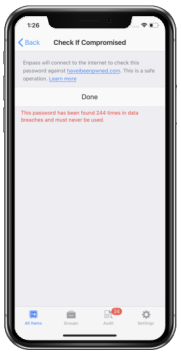
From the detail screen of an item, tap on the password field → More → `Check if Compromised`.



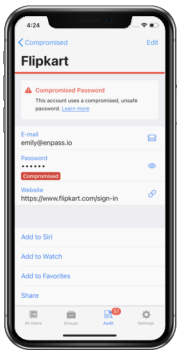
On the next screen, you'll see a message to validate the operation. Tap `Continue`.



Enpass checks for the compromised passwords and displays results. Tap on **Done**



You will now see the results.



Checking All Passwords

You can check multiple passwords at once from the Audit section.

How does it work?

It works on the k-Anonymity model where the first five characters of your SHA1 hashed password (the 40-character hash created from your password) is sent to haveibeenpwned.com. In response, it sends the list of all the leaked passwords starting with those same five characters. Enpass then locally compares the passwords' hash to the list, and if it finds any matching password, you get a warning that the password has been leaked on the internet and must never be used.

What to do if you have Compromised Passwords?

It is highly risky to use a compromised password because it is out there on the internet and visible to attackers. An attacker may not know that you have used that password, but you should still change it.

Change Password Immediately

We recommend to change the password immediately and create a unique and robust password for such accounts. You can use the built-in password generator to create strong passwords.

Enable Two-Factor Authentication

2FA is a stronger form of security that double-checks your identity upon login. Enpass can identify the websites where you can turn on 2FA. It can also act as the authenticator and generate one-time codes for supported accounts saved in the app.

Regularly keep a check on Passwords' Health

You can keep a track on overall health of your passwords and logins from the Audit section.

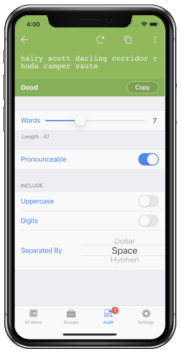
Using Password Generator

Enpass has a built-in password generator to help you in creating unique and robust passwords for all your accounts on the go.

Generating Passwords

The password generator provides you with multiple options to choose from and generate passwords basis the inputs you provide.

You can generate password from `Edit` page of any item by tapping the *Generate* button right next to password field.

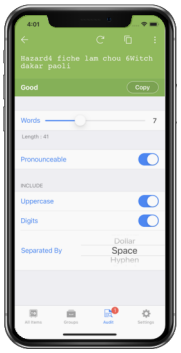


You can alter the password's complexity using the various advanced controls provided on the generator.

You can create *pronounceable* as well as *random* passwords using the password generator tool.

Pronounceable Passwords

Pronounceable passwords are created with Diceware methodology using 14400 English dictionary words.

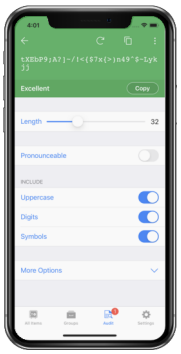


Words means the total number of words you wish to have in your password.

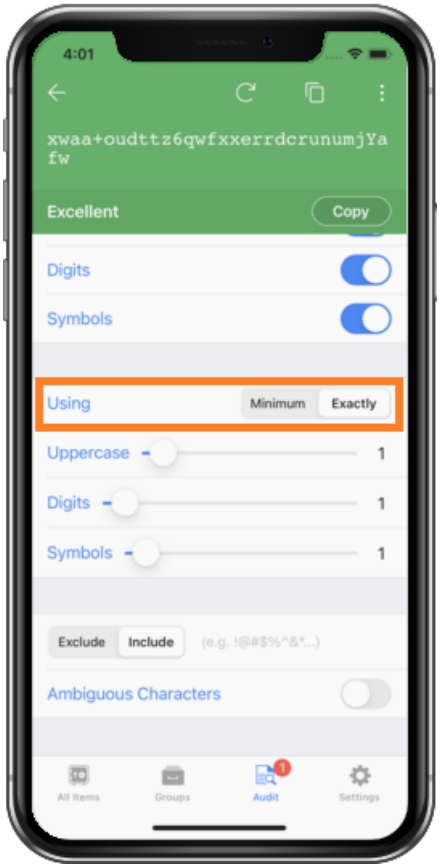
You can choose to **Include** any uppercase letters, digits, along with the special characters with which you wish to separate the words.

Random Passwords

Password Generator also allows you to generate **Random** passwords. Choosing a random password is useful when you want to create passwords for websites that have restrictions on the number of characters your password should have.



Similar to pronounceable passwords, you can modify the password length, uppercase letters, digits, and symbols. Random password generator is unique as it allows you to also specify either *minimum* or *exact* number of letters, digits, and symbols you wish to add.



Some websites force you to use only a particular set of characters in the password. Enpass password generator gives you the flexibility to *exclude* and *include* any special character in the **Symbols** textbox.

If the option of `Ambiguous Characters` is off, Enpass will not include following letters in your password: 1 (*one*), l (*small L*) and I (*eye*); O (*oh*) and 0 (*zero*).

Password History

Enpass keeps a record of the passwords that you used, along with their respective timestamps. This feature is especially useful when you have to change a website's password using the Enpass password generator.

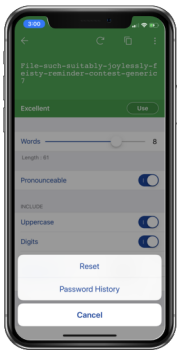
Password history of an item

To check the password history of any item, open the item and tap on the password field, you'll see a swipe menu with 3-dots. Tapping on that will present a context menu with *History* and Check if Compromised option. Select `History` to see the previously used passwords.

History of all the passwords

You can check the history of all the passwords created using Enpass password generator by following these steps:

- Open the password generator → tap on the options menu (3-dots) → History. A list of all the passwords generated using password generator will appear.



Password Strength

Entropy is a measure of password strength. Enpass uses Zxcvbn for calculation of entropy of random passwords. More details about zxcvbn are here.

If a password is pronounceable, Enpass calculate both Zxcvbn and Diceware entropy and least of them will be used to show strength. Strength meter is calibrated for following corresponding entropy to display values.

Entropy	Strength
<35	Very poor
35-50	Weak
50-70	Average
70-100	Good
>100	Excellent

Syncing Data

Enpass lets you sync your data with other devices through any of the supported clouds, or locally using Wi-Fi or Folder on your device/network. Syncing across Enpss is completely secure as all your data is transmitted in encrypted format, and cryptography is always performed locally on the device itself.

Cloud Sync

By the term cloud-sync, we mean that your data can be synced with the cloud of your choice (check supported clouds) and not with our server as we don't store any of your private data.

Sync creates an **automatic back-up** over the cloud. Hence, you can be reassured of data-restore, in case of device-damage or theft.

Supported clouds

Currently, Enpass supports syncing of data across devices through your own account on following clouds.

- Dropbox
- Google Drive
- OneDrive (Personal/Business)
- iCloud
- Box

- WebDAV
- Nextcloud

Setup Cloud Sync

Here are the steps to set up cloud sync in your vault.

> **Note**
>
> Please note that only one vault can be synced with one cloud account at a time. You can not sync multiple vaults with one cloud account. However, you can use multiple accounts of the same cloud, e.g., Dropbox to sync multiple vaults.

Cloudless Sync

With cloudless sync, you can sync your data over a local Wi-Fi or network across devices without the need of any cloud service.

Wi-Fi Sync

Wi-Fi Sync in Enpass lets you sync data between devices connected to same network. To use Wi-Fi Sync, you need to start Wi-Fi Sync server from a desktop device on the network and host the vaults from that desktop to which other device on the network can connect and sync. So it's a two step process–

1. Setting up Wi-Fi Sync Server
2. Configuring Sync on other devices

> **Note**
>
> Wi-Fi Sync in Enpass is a bit complicated, and its functionality depends on your network setup, software, and OS configuration. In case you face any challenges in setting it up flawlessly, head straight to the troubleshooting page.

Sync Timings

- Every time you unlock your Enpass keychain, an auto-sync is initiated. (If Sync is turned on).
- Auto-sync also happens after every 15 secs, while the app is in the foreground.
- When you save any change in item details or master password, Enpass waits for 5 secs and initiates an auto-sync.

Time Stamps

Enpass keeps you informed about the latest successful data sync by updating Last Synchronized time stamps.

> **Note**
>
> Time taken in completion of a sync process depends on the data size, i.e, the no. of items and attachments in Enpass.

- Any changes in settings are not synced to cloud (except for the master password).

Autofilling Passwords

Enpass auto-fills your login details on websites while you surf the net. That means, no more copy/paste of sensitive information. By the end of this section, you'd know how to use Enpass to browse through internet in a seamless and secure manner.

The following real-life examples should be relatable to your online experiences:

- While browsing, you landed on an interesting Twitter profile and now you have to sign-in to follow it.
- You filled a cart while shopping online and you need to sign-in to checkout.
- You need to change your password while on the go.

This list could go on and on! In all the above cases, you'd just have to click on the **sign in** button and Enpass would pick your login credentials from Enpass database and auto-fill them for you. For this purpose, you can use either of Safari extension or Password AutoFill. Know more about these two here:

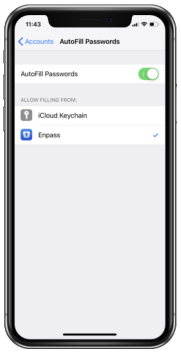
Password Autofill

In the iOS 12, Apple introduced a new Password AutoFill API that allows the password managers to autofill logins in the Safari and the third-party browsers.

We have successfully incorporated this feature in the Enpass version 5.6.0 and later versions. You will see how smooth and easy have become entering logins details to your desired apps.

How to Set Up?

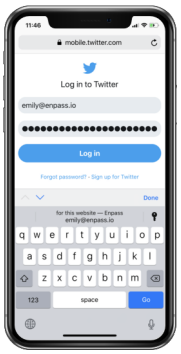
Once you've installed the Enpass, you need to head straight to Settings> Passwords & Accounts > AutoFill Passwords and turn on the AutoFill Passwords. Also, make sure you select the Enpass from the provided options to allow autofilling in the third-party apps.



Autofill in Safari and Third-party Apps

Enpass already supported autofilling logins in Safari browser in the previous versions, but with the new implementation in iOS 12, the process has become more streamlined, and you can now autofill in the other apps as well. In the Safari browser and the apps that support AutoFill API in iOS 12, you can follow these steps to autofill your logins.

- On the login page, tap on the username/password field, and QuickType keyboard will automatically ask to fill your info. → Tap on the key symbol, choose Enpass, authenticate using Touch/Face ID, or Master Password to log in → Choose the item you want to use for autofill and done (Here you can also create a new item for that particular URL by selecting *Create new item*) → Tap on the login if needed, and you're in.

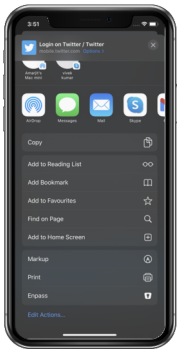


Safari Browser Extension

Enpass integrates directly into Safari as an extension and does autofilling for you. First, you will have to enable its browser extension.

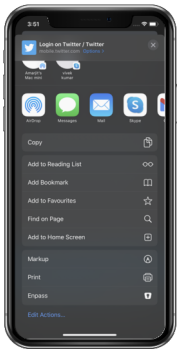
Enable Safari Extension

- Tap the **Share** button in your Safari Browser → Swipe left the bottom row and tap **more** → Enable **Enpass** → Tap **Done**.



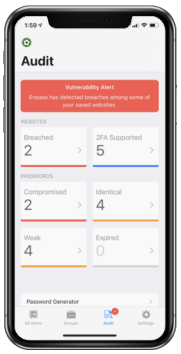
Autofill with Safari Browser

- Once you have reached the login page in the browser, tap **Share** → Select **Enpass** from the list. Now, you'll have to unlock Enpass database → Select the credentials you want from a list of all matching credentials that Enpass shows



Checking Password Health

You can check the health of saved passwords using Audit. Audit tells you about data breaches, compromised passwords, and potential security problems with the items you have saved in Enpass. It keeps you on top of security as you don't need to keep a check on each item.



Audit highlights the security concerns and sorts them into separate categories so you can identify the affected passwords.

If any of your items require action, you'll see an alert at the top of the item listed in Audit.

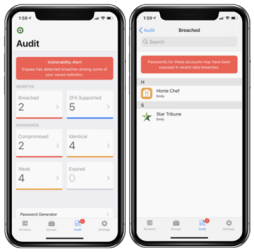
Websites

Under Website section, you can see all the accounts saved in Enpass whose websites have suffered data breaches in the past along with the list of login items supporting Two-Factor authentication.

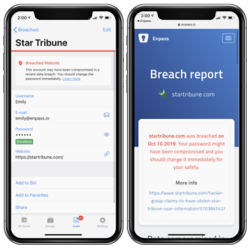
Breached

Here, you will see the list of the logins for those websites where a security breach has been reported, and you haven't changed your password since the breach.

To check for breached accounts in Enpass, go to `Audit` > Tap on *Breached*.



For all such items, you will see a warning at the top of the item's details page until you change the password.



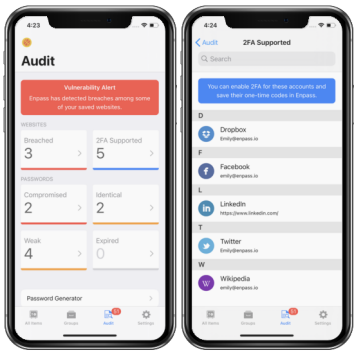
Caution!

We recommend that you immediately change the passwords for accounts that are listed under Breached.

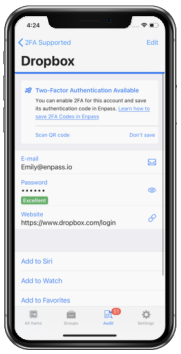
2FA Supported

Here, you can see the list of accounts for websites that support two-factor authentication but don't have a one-time password saved in Enpass. You can go through the list and choose not to save the one-time codes for those logins in Enpass where you're using any other method like call, email, or text for second-factor authentication.

To check for 2FA compatible logins in Enpass, go to `Audit` > Tap on *2FA Supported*.



You can see details for the item that supports 2FA authentication.



You can save One-time codes for the items in Enpass which have been listed under 2FA Supported to enhance account security.

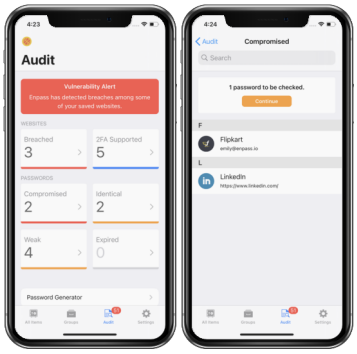
Passwords

Here you can view the list of items with compromised, weak, identical, and expired passwords.

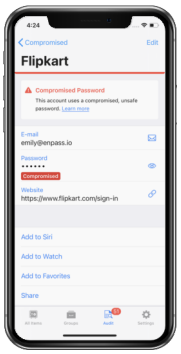
Compromised Passwords

Here, you will see the list of passwords that have appeared in data breaches. You might be unknowingly using such passwords that are available to attackers over the internet. We suggest changing the passwords of such accounts that are listed as Compromised.

To check all the compromised passwords in Enpass, go to the `Audit` > Tap on *Compromised*.



On tapping a particular item, you can see the details for that item.

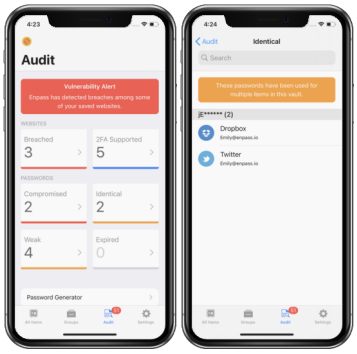


For items with Compromised passwords, you will always see an alert at the top of item's detail page prompting you to change the password.

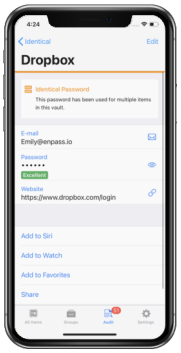
Identical Passwords

Using the same password in multiple online accounts is a bad practice and puts your accounts at risk. If any one of these accounts is compromised, all you other accounts are at risk.

To check all the identical passwords, go to `Audit` > tap on *Identical*.



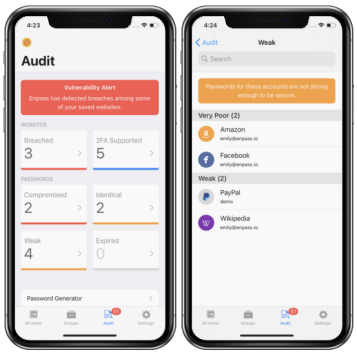
Tapping on a particular item will take you to its details.



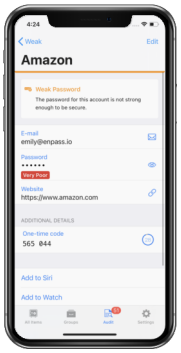
Weak Passwords

Weak passwords are those which can be easily guessed, or discovered by people who are not supposed to know them. They consist of most common passwords such as personal infomation like birthday dates, family members' anniversary, etc.

To check all the weak passwords, go to `Audit` > tap on *Weak*.



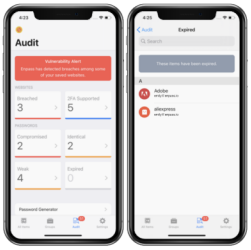
You can check the details of an individual item by tapping it.



Expired Items

Here, you will see list of items that either have expired passwords, or credit cards that have expired.

To check for expired items in Enpass, go to `Audit` > *Expired*.



Note

The passwords which have been exluded from Password Audit will not appear in the Audit results.

Expiring Soon

Here, you will see the items that have a password expiry date set, and the passwod for those items will expire in less than 6 days.

Password Generator

You can invoke the built-in password generator to generate unique and strong passwords for any of your accounts that are listed under Audit.

Organizing Data

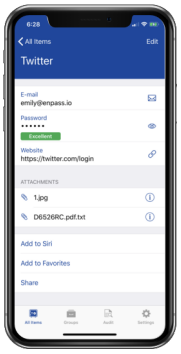
In Enpass, you can efficiently organize your credential using the following ways:

Marking Favorites

To get quick access to the frequently used items just mark them as favorite by following simple way:

From detail screen

- Tap `Add to Favorites` on the detail screen of the item.



Using Tags

Tags allow you to organize your data in your own way. The steps described here will guide you how to add tags in an item. You can navigate between tags from `Groups` in Tab Bar.

Using Categories

Enpass is having a wide number of categories and predefined templates to help you store your information quickly in a more organized way. Putting the items in their proper categories is the simplest way for organization.

Change Category

Steps described here will guide you to change the category of an existing item.

Add custom categories and templates

The desktop version of Enpass allows you to create your own customized categories and templates.

Using Multiple Vaults

Multiple vaults can help you segregate your data esp. for collaboration with Family and Team members through shared cloud accounts. To know more about multiple vaults read here.

Sharing Items

Here you'll learn about how to share an item with others and how the recipient can add the shared item into his Enpass.

Sharing

From Enpass you can share any item with others in the following two ways:

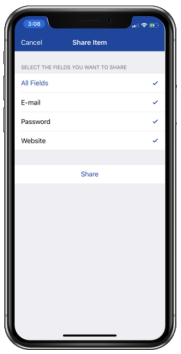
1. Normal sharing
2. Encrypted with Pre-shared Key

In both ways, a single item at a time can be shared outside Enpass through a medium of your choice; be it, e-mail, Whatsapp, Messages etc.

Normal sharing

This is the regular way of sharing where the fields of shared item are visible in plain text. Along with that the data of selected fields get appended in message in the form of BASE64 encoded URL, which is also encrypted with a fixed pre-defined key. Sharing an item in plain text format is not considered secure as it can easily be read by anyone who gets the hand on it.

- Open the item which you want to share → Tap on share. An alert with a warning message will appear, tap on *I Understand* → Choose the fields which you want to share → Tap on *Share Button* → Choose the medium to share your item, and finally you can share the item.



Warning

Plain text poses a security threat, in case of sensitive data. Sharing private data in plain text should be avoided unless it's urgency.

Encrypted with Pre-shared Key

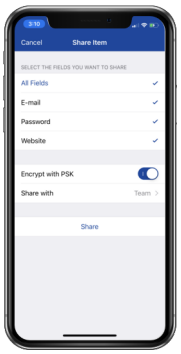
This way you can encrypt any item with a passphrase (call it, Pre-Shared Key) before sharing it with others. The recipient can access the shared item only by providing the correct PSK. It's a secure way of sharing items with other Enpass users. You first need to create a pre-shared key (PSK) for the intended recipient from the advanced settings of Enpass, and then you'll see an option to encrypt the item with PSK while sharing.

Note

It is recommended to share the PSK with the recipient through a medium different than the one used for sharing the encrypted item.

To share an encrypted item:

- Open the item which you want to share.
- Tap on *Share*. An alert with a warning message will appear.
- Choose the fields which you want to share. Enable the option *Encrypt with PSK*.
- Now you can select the name of recipient for which you created the PSK in advanced settings.
- Tap on *Share*, and Choose the medium through which you want to share your item.



Attention!

- Always use a secure channel/medium for sharing. i.e., No one must listen in on or temper with the medium.
- Double check that you are sending it to the correct person.
- Delete the shared text after being sent and ask the recipient to delete the same as well after importing the item in their Enpass database.

Adding a shared item

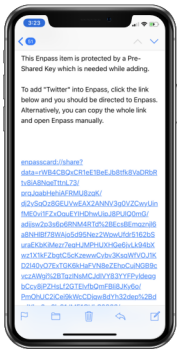
A shared item can be added to Enpass by directly opening the shared link or by copying that to the clipboard.

Adding by opening link

If the shared item (in scrambled form) is detected as a link, directly clicking that link will open the installed Enpass application and ask you to add the shared item.

Warning

Sometimes the shared URL is not detected, and Enpass fails to import the shared item with an error message. In that case, you should try to add that item by another way, i.e. copying the whole link on the clipboard and open the Enpass manually.



If the shared item is encrypted with a PSK, you'll be asked to enter the PSK right before adding the item to Enpass.

Note

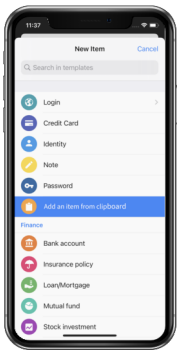
Attachments in the shared item will only be added to Enpass if the item is encrypted with a PSK. Otherwise, only the fields will be added.

Adding through clipboard

- Copy the whole shared link on clipboard.
- When you come to the main screen (with the data on clipboard) of Enpass, click **+** button and select **Add item from clipboard**. You will be asked to add the item to the database.

Note

You can also enable the option from Enpass Settings to let Enpass automatically read the clipboard. If enabled, Enpass will automatically read the clipboard while entering the foreground to check for any shared Enpass item.



If the shared item is encrypted with a PSK, you'll be asked to enter the PSK right before adding the item to Enpass.

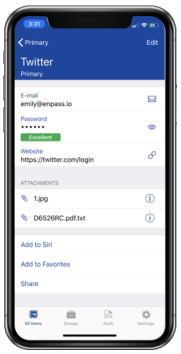
Note

Attachments in the shared item will only be added to Enpass if the item is encrypted with a PSK. Otherwise, only the fields will be added.

Share Attachment

You can share each attachment via email or by using other apps on your device by following these simple steps.

- Go to the detail screen of the item where you've stored the attachment.



- Click on the attachment you want to share. You will be provided with the preview of the attachment.
- Click on the share button and you'll be provided with the list of sharing apps. Select the one you want to share the attachment with, and done.

Important

You must share the attachments using the reliable sources to avoid the data breach.

Using Multiple Vaults

All your Enpass items reside in a database that we call as a *Vault*. Multiple Vaults mean you can have more than one database in Enpass. It helps you to easily collaborate with family or team members through a shared cloud account. There are two types of vaults in Enpass; Primary and Secondary vaults.

Primary Vault

The very first vault you create/add in Enpass is referred to as the Primary vault, and rest of the other vaults are considered as the secondary vaults in Enpass. You can not rename the Primary vault. The password of the Primary vault acts as the master password of Enpass.

When you create multiple vaults, the passwords of other vaults are stored securely in Primary vault and are removed when you delete the vault. That's why when you unlock Enpass, all the vaults get unlocked automatically.

Multiple Vaults

From version 6 onwards, Enpass allowed saving data in multiple vaults.

When to use

Although the use of the multiple vaults varies as per the user's requirements. But it is recommended to use multiple vaults only when you have to sync data of each vault to different cloud account; the purpose could be having a shared vault with a small team or family members. If the purpose is not sharing, you should not use multiple vaults to segregate your own data, rather you should organize it by using some other ways as mentioned here.

Cloud Setup

See the steps described here in the vault settings to sync your vault with a cloud account.

Note

Please note that no two vaults can be synced to a same cloud account on the same device and each vault in Enpass must be synced to a distinguished cloud. However, you can use same cloud service provider (i.e. Dropbox, Google Drive etc) but the accounts must be different per vault.

Passwords of Vaults

As mentioned above, the primary vault by-default holds the passwords of all secondary vaults to unlock them automatically. In case you want to save passwords of secondary vaults in Enpass for reference in future, you can do with an option displayed while setting up the secondary vault.

- As long as the secondary vault is there in Enpass, you can always check its password from the vault setting page. Tap on ■ button → *Show Password*. You'll be asked to authorize yourself by entering the master password of Enpass. After authorization, you can see the password of the vault.

Backup and Restore

Enpass lets you take manual backups of your Enpass data and restore them.

Taking backup

Backups can be taken for a specific vault or of whole Enpass data; to other device over WiFi or on local storage of device.

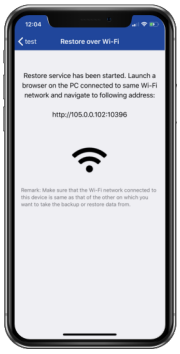
Restoring backup

Backups can be restored Over Wi-Fi or from the local storage. See the steps below:

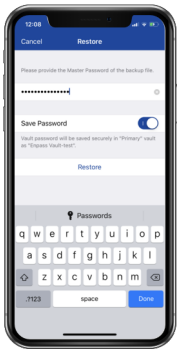
Over Wi-Fi

Make sure that your Mobile device and PC are connected to the **same Wi-Fi** and your Mobile's screen remains in **foreground** throughout the following process:

- Using a browser on other system, navigate to the IP address visible in the *Restore over Wi-Fi* screen in your Mobile device.



- Tap **Choose File** on your system and navigate to the backup file's location. Tap on Upload. Now you'll be asked to enter the password of the file in your device once the upload is finished.

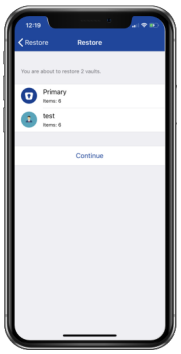


Note

While restoring data in secondary vault, you have to choose the vault you need to restore. In case if your backup contain multiple vaults and you restore all of them, you need to Erase everything and start over by restoring data from backup file.

From local storage

Tap on `Files` and select the file from the device. You'll be presented with the list of vaults to be restored in Enpass. Tap on *Continue* and you'll be asked to enter the master password of the file. After entering the password, tap on Restore and your data will be restored in Enpass.



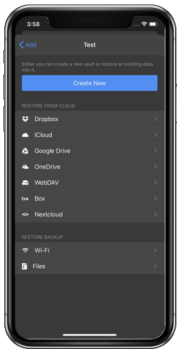
Note

If you're restoring data in the secondary vault, you can only restore from a single vault file. You can restore the multiple vault file while creating the Primary vault only.

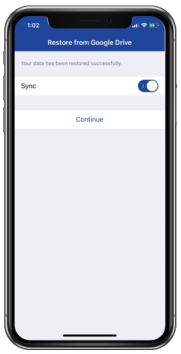
Restore from Cloud

Following steps review the process of restoring from cloud:

Select your cloud from the list. You will be re-directed to the authentication screen of that cloud. Enter your credentials and grant permissions to Enpass to continue with the sync process.



Your data will be synced successfully. Time stamps will also get updated.



Note

Only one vault can be synced with one cloud account at a time. You can not sync multiple vaults with one cloud account. However, you can use multiple accounts of the same cloud, e.g., Dropbox to sync multiple vaults.

Settings Overview

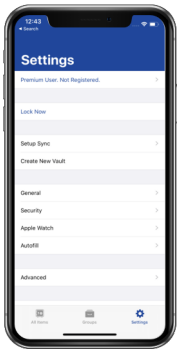
Following are the settings that you can alter in Enpass.

Registration status

The first item on the Settings screen is your registration status. See Registration for details.

Lock Now

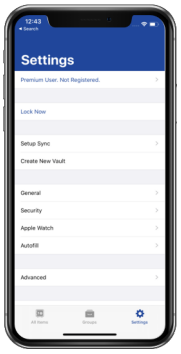
Click **Lock now** to lock the device immediately.



Working with vaults

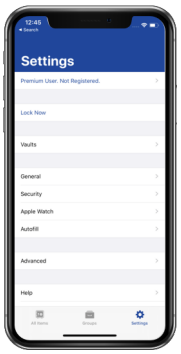
Here you will find all the vault specific settings of Enpass.

For Single Vault users



If you haven't added any secondary vault, then you can manage the settings for the primary vault from the link Setting up sync for single vault users.

Managing Multiple Vaults

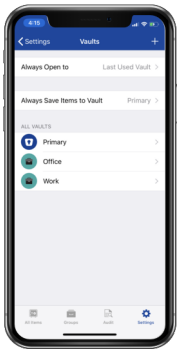


If you created any secondary vault, you will have multiple vaults. The following sections describe the settings for multiple vault users.

Always Open to

This setting will only appear if you have multiple vaults in Enpass. Enpass will preserve the vault you select here and will always open this vault every time you execute a new instance of Enpass.

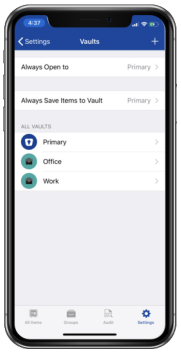
- Go to Settings > Vaults > Always Open to and choose the vault of your choice.



Always Save Items to Vault

This setting will only appear if you've multiple vaults in Enpass. The vault you select here will be used by default to save every new item you create in Enpass. The option to choose vault will also be provided to you while creating the item.

In the Enpass settings go to Vaults > Always Save Items to Vault > select vault and done.



Create Vault

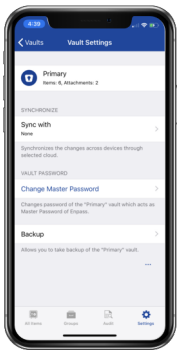
To create a new vault, go to Settings > Vaults > Tap on + button > Add the vault name > Tap on **Create New** > Enter vault password and tap *Continue* > Verify the vault password on next page > Optionally, you may choose to save this vault password as an item in the Primary vault, otherwise tap *Continue*. Done.

Vault settings

To manage the settings of any particular vault, go to Settings > Vaults > Choose the vault. You'll be directed to the *Vaults Settings* page where you can customize the vault specific settings described below.

Change Vault Password

- Tap on the Change password > You'll be directed to the Authorization screen where you need to enter the master password to authorize yourself > Enter a new password and confirm the password > Tap *Done*.



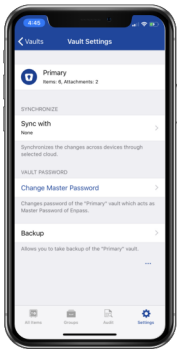
- The password of the Primary vault acts as the master password of the Enpass, so changing this password means changing the master password of Enpass.
- **Remove Keyfile:** While changing the password of the vault on the *Change Password* screen, tap on the **3-Dots** and select **Remove Keyfile** from the options menu.

> ***Note***
>
> If you have enabled sync, the new password for Enpass data will get updated to the cloud during the next sync operation. The other devices syncing with that cloud will show error during the next sync attempt.

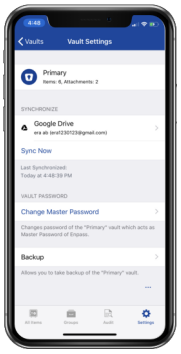
Set up Cloud Sync

Following steps will guide you through the cloud sync process:

- Select your cloud from the list. You will be directed to the authentication screen of that cloud. Enter your credentials in its login screen. Grant permissions to the cloud to continue with the sync process.



- Your data will be synced successfully. Time stamps will also get updated. In case, you have restored your data in a new device, you'd notice the following screen at the completion of the sync process.



Set up Wi-Fi Sync

Wi-Fi Sync in Enpass lets you sync data between devices connected to same network. To use Wi-Fi Sync, you need to start Wi-Fi Sync server from a desktop device on the network and host the vaults from that desktop to which other device on the network can connect and sync. The complete details of setting up Wi-Fi sync and configuring sync on other devices are described here.

Backup

This feature lets you take backup of your vault data on your desktop over Wi-Fi or locally on your device.

Over Wi-Fi

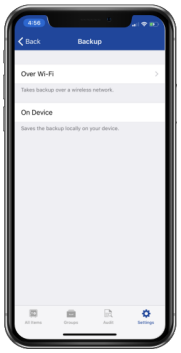
Make sure that your device and PC are connected to the **same Wi-Fi** and your Enpass's screen remains in **foreground** throughout the following process:

- Tap on over Wi-Fi and you'll see an IP address of your local network. Use this address in your

- Using a browser on your PC, navigate to this address and you'll be redirected to *Backup Service* page from where you can download the backup. Your Enpass backup will be saved in an encrypted format in your PC.

On Device

Tap on *On Device* and choose the location to save your backup in your device. Tap on *Done* and your data will be saved in the specified location.



Vault Info

You can get the necessary information about the vault from here.

Show Password

Tap on the options menu (3-dots) button and tap on *Show Password*. You'll be asked to authorize yourself by entering the master password of Enpass. After authorization completes, you can see the password of the vault.

Remove Vault

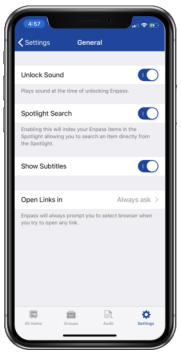
Tap on the options menu (3-dots) button and tap on *Remove Vault*. You'll be asked to authorize yourself by entering the master password of Enpass. After authorization completes, you'll see a warning message to ensure removing the vault. You'll also be provided with an option to save the vault password as an item in Enpass for future reference. Unselect the option if you don't want to save the password. Tap on *Remove* button, and done.

General

General settings deal with the behavioral setup of Enpass which you can control using the settings described below.

Unlock Sound

By default, Enpass plays sound (and vibrates) as feedback at the time of unlocking the app (or when you enter an incorrect password).



Spotlight Search

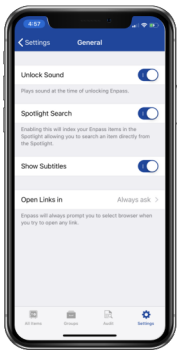
Enabling this will index your Enpass items in the Spotlight allowing you to search an item directly from the Spotlight.

Use website icons

Please see Customizing Icons.

Show Subtitles

Enabling this will show the subtitle of the items in the `All Items` list.

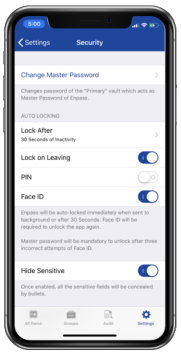


Open Links in

This option displays if you have multiple browsers installed.Enpass prompts you to select the browser when you open any link.

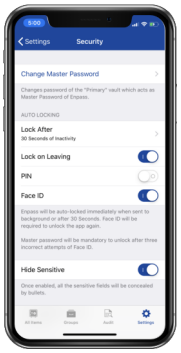
Security

This section deals with the security settings of Enpass.



Change Master Password

- To change your master password, tap on *Change Master Password* > Enter Master Password > Enter New Password > Confirm New Password > Done.



Auto Locking

Autolocking protects your data from unauthorized access by locking the Enpass keychain, even when your device's privacy has been compromised.

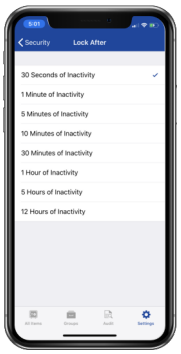
By default, you are supposed to enter the master password for unlocking the app. This could be a tedious process, especially when you have to authenticate every autofill activity while autofilling using your master password.

Quick unlock features namely, PIN Code and Touch ID, save you from entering your master password every time you want to open the app. Users **must** enable device passcode to use Quick unlock facilities.

The following settings can control the whole behavior of autolocking and quick-unlock:

Lock After

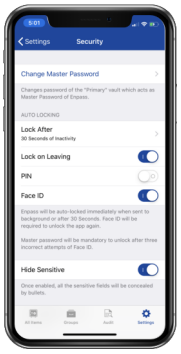
The default setting is **30 Seconds of Inactivity**, which means that Enpass auto locks itself if left unattended for 30 Seconds.



You can change it according to your preferences.

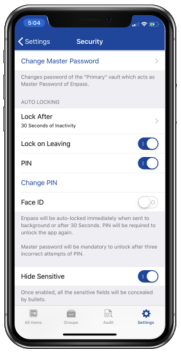
Lock on Leaving

This feature allows the app to lock itself immediately when sent to background, irrespective of the inactivity-time setting. By default, this feature is enabled.



PIN

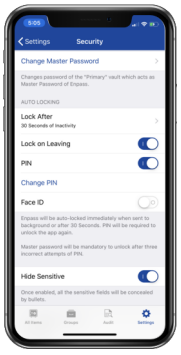
The master password is set as the default authentication requirement. You can avoid entering your master password altogether by using a PIN Code.



Once enabled, you'll be asked to enter the PIN to unlock the app every time. Although, after an unsuccessful attempt, you again have to enter the master password to open the app.

Change PIN

- Tap **Change PIN** button, enter the new PIN and confirm it. Tap on done, and this will change your PIN.



Touch ID/Face ID

Enpass supports the built-in Touch/Face ID sensor. That means you can use your fingerprint instead of passwords to unlock Enpass.

Using Touch/Face ID has two significant benefits:

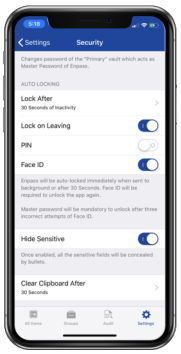
- It is quicker than entering a password.
- It saves your password from unwanted attention.

While unlocking, after three unsuccessful attempts with Biometrics, Enpass asks for the master password to proceed.

> ***Note***
>
> You cannot use Fingerprint and PIN together.

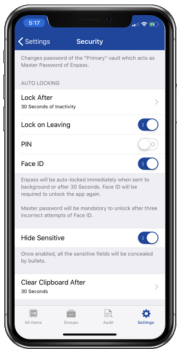
Hide Sensitive

Enable this setting to conceal all sensitive fields by bullets.



Clear Clipboard

When you copy any data from Enpass, it gets stored on your device's clipboard. You can choose when to clear this data from the clipboard. By default, it is set to **After 30 seconds**.



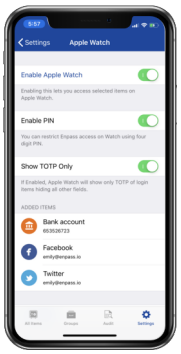
Enpass for Apple Watch

Enpass for Apple Watch lets you access your frequently required items directly from your wrist.

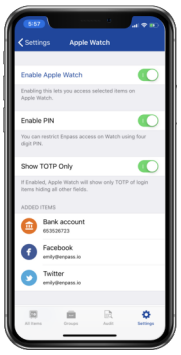
Enabling Enpass for Apple Watch

For setting Enpass for Apple Watch all you need is Enpass App installed on your device (with iOS 8 or above) and an Apple Watch. Also ensure that your device is protected by passcode as you cannot use Enpass for Apple Watch without having that enabled.

- Pair your Apple Watch with your iPhone → Open Enpass on your iPhone. Go to Enpass Settings and select **Apple Watch** → Enable Apple Watch →



- Enable PIN code (optional) and use it to unlock Enpass on Apple Watch.



> ***Note***
>
> For security reasons, we strongly recommend you to create a PIN to unlock Enpass App on Apple Watch.

- Enable *Show One-time password Only* and Apple Watch will show the One-time password of the item, hiding all other fields.

Installing Enpass on Apple Watch

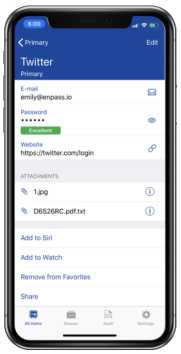
Follow the steps below to install/show Enpass on Apple Watch.

- Open *Apple Watch* app on your iPhone and go to **My Watch** → Scroll down till you see the Enpass app → Tap on Enpass and Enable *Show App on Apple Watch*

Look at your Apple Watch and you will see Enpass being installed.

Adding items

- To add an item to Android Watch, go to the details screen of item → Tap `Add to Watch`.



- You can access all the items added to watch from Settings → `Apple watch`.

Security

Apple Watch works through the iPhone to which it is paired. It communicates securely only with that device over Bluetooth using Apple Watchkit.

Only those items are accessible on Watch which you added to `Apple Watch` for sharing. These shared items are not as secured as rest of the items as your master password is no more protecting them. They are stored in the watch itself, which is protected by your watch os. However, these items do not leave the watch in any case; neither during the backup of iTunes nor of iCloud Keychain.

For extra security, you should enable the PIN code for Watch. Otherwise, if anyone gets access to your watch, will be able to see the items stored on it. So one should use Apple watch with great attention and care.

Note

For better security of your data while using Apple Watch, it is advised to

1. Use an excellent Device Passcode.
2. Use a good Enpass Watch PIN Code.
3. Be careful what you store for the watch — only the frequently used short items like locker code etc.

Autofill

The settings described below allows you to control the autofilling behavior of Enpass.

Auto-copy One-time password

Enpass will automatically copy the One-time password from the item to the clipboard after autofilling the login details on the webpage. You'll just have to paste the One-time password in the required field and log in. Enpass will also automatically update the One-time password to the clipboard once it gets changed after 30 seconds in the item.

Match URL Hostname

Once enabled, Enpass will only show you the list of items having the same URL hostname to autofill on a login page.

Advanced

This section deals with the Advanced Settings of Enpass.

Sharing

The Enpass version 6 brings secured sharing allowing you to include the attachments with the item and also allow you to encrypt the entire item with a Pre-Shared Key (PSK) before sharing it with anyone.

Add a PSK

Go to Settings > Sharing > Tap on “+” button. Here you can add a key and enter a name to save the PSK.

- Your recently added PSK is added to the list of *Existing PSKs*.

> ***Note***
>
> Once a PSK is added, an additional option to share encrypted item will appear while sharing. You also need to share the PSK with the intended recipient to allow access.

Backup

This feature lets you take backup of your entire Enpass data including all vaults on your desktop over Wi-Fi or locally on your device.

Over Wi-Fi

Follow the steps described here to take the backup of the Enpass data over Wi-Fi.

On Device

Follow the steps described here to take the backup of the Enpass data over on your device.

Universal Clipboard

Disable this, if you don’t want to share content copied from clipboard from Enpass with other supported Apple Devices.

Check Clipboard on Startup

Enabling this explicitly allow Enpass to read the clipboard for shared items on every launch automatically. Once disabled, you will have to then manually add the shared item by selecting **Add an item from clipboard** on the *add item (+)* screen.

Allow Third Party Keyboards

Third party keyboards are capable of monitoring your private data as you type, So, they are disabled by default.

Language

You can set the default language for Enpass from here.

Erase Everything

You can choose this option to erase all your **Enpass data including all vaults and current Enpass settings** from your device.

> ***Tip***
>
> Before erasing everything from the device, you should take a backup of your Enpass data on a cloud or a your dektop.

- Tap on **Erase Everything** and you will see a warning message. Tap *Continue* and now you need to authorize yourself by the master password.

- After the authorization, your data will be deleted and you'll be presented with a welcome screen where you can start over again with Enpass or restore an existing data.

Check for Alerts

If enabled, we will alert you about very important security or Enpass related news. we respect this option and use it when it is highly necessary to notify you about something important. Since this is the only medium to reach you, we recommend you keep it enabled.

Enpass Family Membership

Enpass Family Membership empowers families to help protect their loved ones by providing each person access to the password management service. It helps you add up to five family members and help them manage their passwords, and promote healthier online habits in the cyber world.

You can learn more about the family membership here.

Siri Shortcuts and Quick Actions

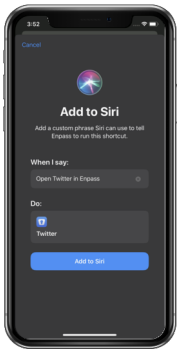
You can create a new item, search in the Enpass keychain or open the list of favorite items, all from your phone's home screen. To do so, just give a firm press on the Enpass icon and choose the action you want to perform.

Siri Shortcuts

In the iOS 12, Apple provided a new Siri Shortcut functionality that allows users to set a voice command to take a specific action in the app. We've also successfully incorporated this feature in the version 5.6.0 allowing you to set a shortcut to access your frequently used items quickly.

Here's How to Set a Shortcut:

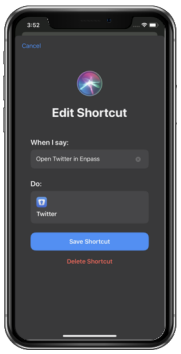
- Open the item you want to set a shortcut for, tap on the *Add to Siri* |rarr| Now record your phrase, and done



- Next time whenever you need to access the item use this command and Siri will open the item for you.

Edit Siri Shortcut

- To edit the existing Siri shortcut, open the item and tap on *Edit Siri Shortcut*. |rarr| To re-record the phrase, tap on *Re-Record Phrase* and continue |rarr| You can delete the existing shortcut by tapping on the *Delete Shortcut* |rarr| You can also delete the Siri shortcut from Device Settings > Siri & Search > My Shortcuts > Right swipe on the shortcut and tap *Delete*.



Note

If you uninstall Enpass or erase all the data from it, all the Siri shortcuts will remain as it is in the Device settings. You need to delete them from there manually.