Enpass User Manual - Android

Release 6.3.0

Sinew Software Systems Pvt Ltd

Nov 19, 2019

CONTENTS

Enpass Version– 6.3.0

Welcome to the Enpass user manual for Android. 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.

CHAPTER

ONE

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.

CHAPTER

TWO

PREREQUISITES

From version 6.3.0 onwards, Enpass requires Android 5.0 or later.

CHAPTER

THREE

GETTING STARTED

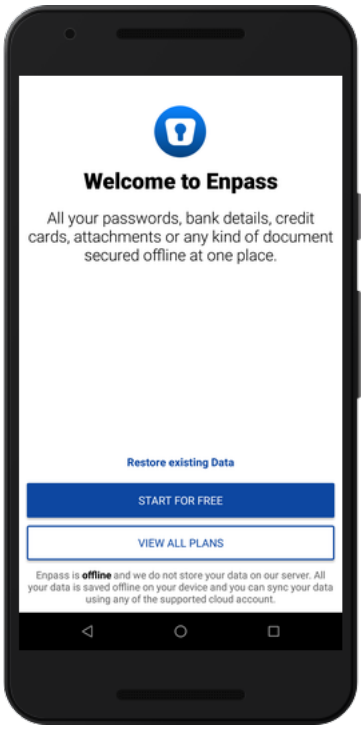
You can start using Enpass either as a new user or as an existing user.

3.1 As a new user

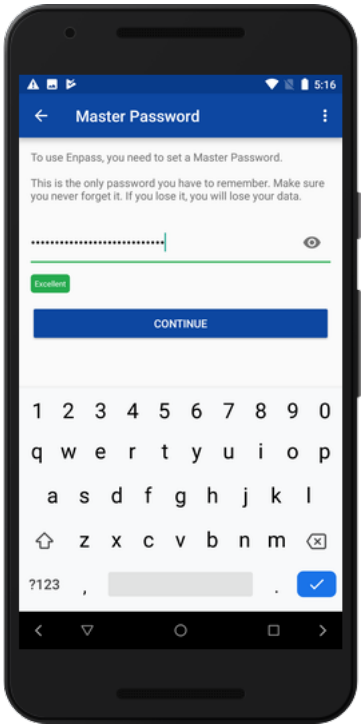
If you're a new user, you first need to set up a master password before adding any items. Enpass encrypts all your data with the master password. Read more about *master passwords*.

To create a master password, follow these steps:

1. On the Welcome screen of Enpass, tap **Start for free**.



2. Create your master password and tap **Continue**.



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 can select a few settings here for a quick setup.

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

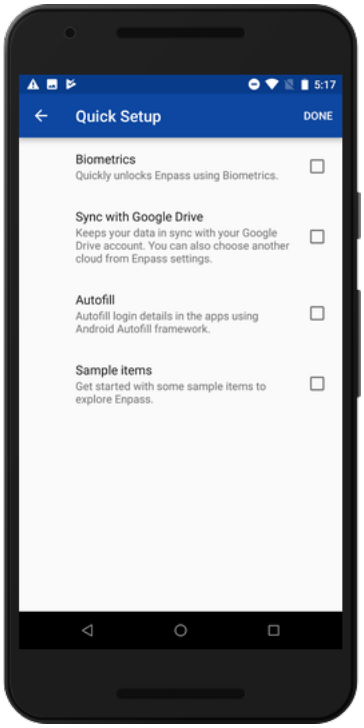
By *registering*, you can remove this limit.

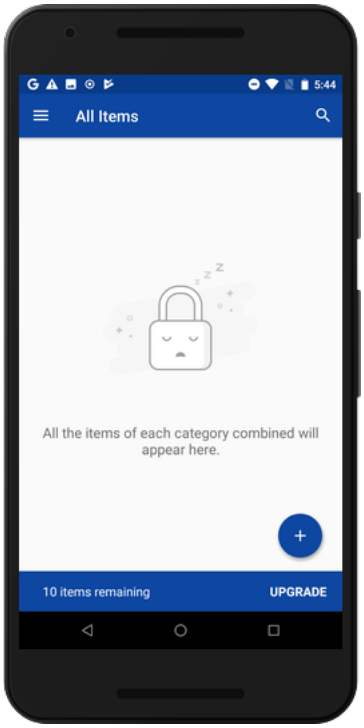
3.2 As an existing user

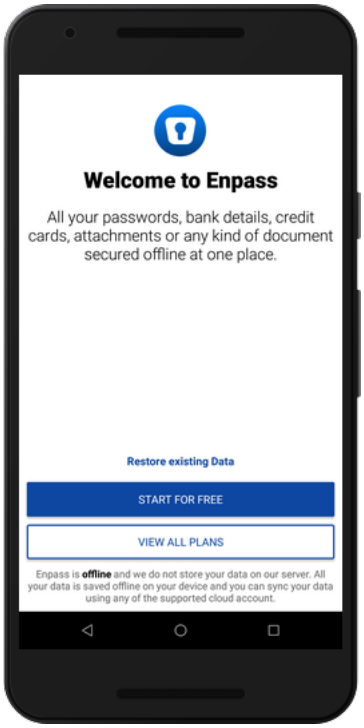
If you are an existing user of Enpass, you would be having your data somewhere, either on any cloud where you have synced before or a local backup of data. You can directly restore that data from a *Backup File* or from a *cloud*.

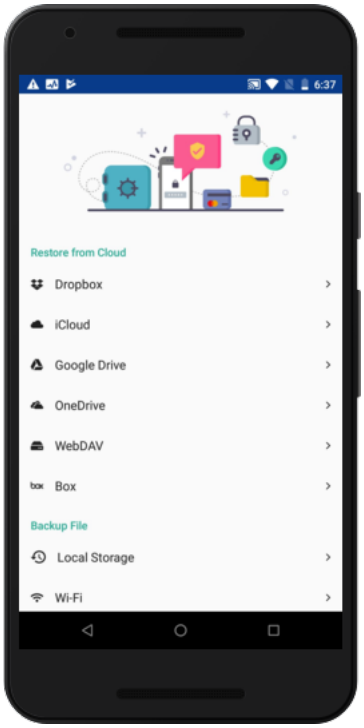
- Open Enpass. On the Welcome screen you can see the option, **Restore existing data**. Tap to continue.

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


5:17
Quick Setup
DONE
Biometrics
Quickly unlocks Enpass using Biometrics.
Sync with Google Drive
Keeps your data in sync with your Google Drive account. You can also choose another cloud from Enpass settings.
Autofill
Autofill login details in the apps using Android Autofill framework.
Sample items
Get started with some sample items to explore Enpass.


5:44
All Items
All the items of each category combined will appear here.
10 items remaining
UPGRADE


Welcome to Enpass
All your passwords, bank details, credit cards, attachments or any kind of document secured offline at one place.
Restore existing Data
START FOR FREE
VIEW ALL PLANS
Enpass is offline and we do not store your data on our server. All your data is saved offline on your device and you can sync your data using any of the supported cloud account.


6:37
Restore from Cloud
Dropbox
iCloud
Google Drive
OneDrive
WebDAV
Box
Backup File
Local Storage
Wi-Fi

CHAPTER

FOUR

MASTER PASSWORD

Enpass encrypts all your data using the master password. You also unlock the app with it. Make the masterpassword strong. If you lose it, we cannot help you recover it. Write it down 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.

4.1 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 android device you need to:

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

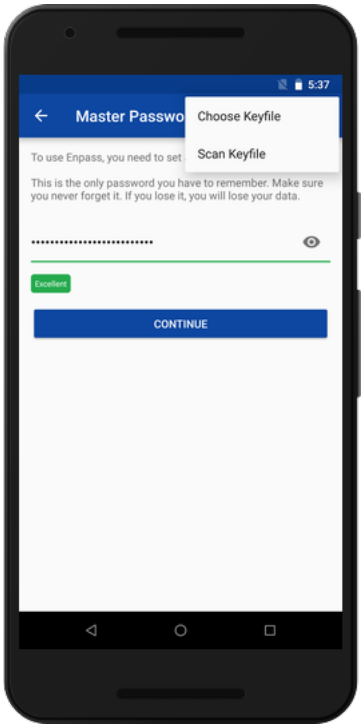
4.2 Generating the keyfile

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

4.3 Adding the keyfile

To add a keyfile, follow these steps:

1. From Enpass on your android device, tap **Settings > Security > Change master password**.
2. In the **Change password** screen, tap the **More options** button at the top right (The **More options** menu button will display only if the vault has a keyfile).
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.

4.4 Removing keyfiles

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

CHAPTER

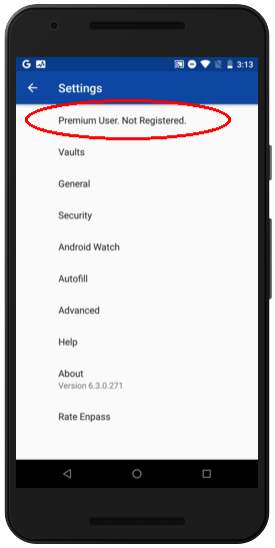
FIVE

REGISTRATION

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

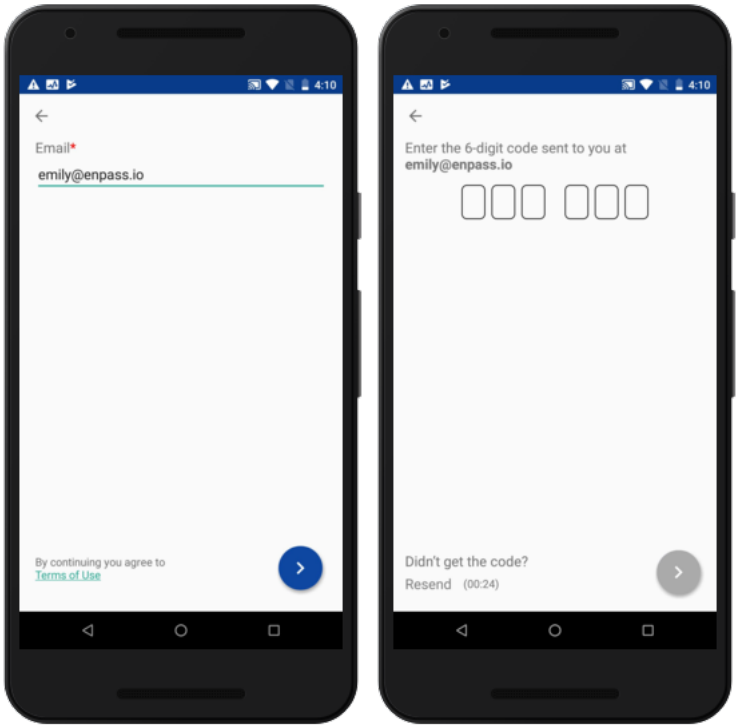
To register your purchase, follow these steps:

- 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 Google 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're 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 data remains offline on your device as earlier.

CHAPTER

SIX

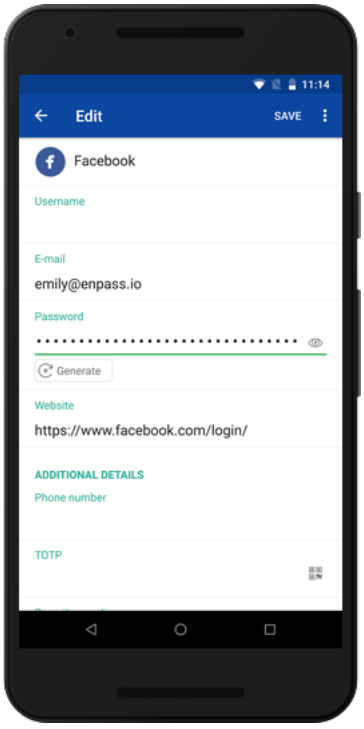
ADDING AND MANAGING ITEMS

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

6.1 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** or **Category** page, 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.

6.2 Adding TOTP

In Enpass you can store the Time-based one-time passwords using the following steps.

- Select the item in which you want to add TOTP.
- Tap on the `Edit` button. If the item is of login type there is a default field of *TOTP* 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 customized field of type *TOTP*.
- Drag the scanner over the QR code on the website from which you are adding TOTP, 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.

6.3 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.

6.3.1 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 option menu (3 dots) → Attach Photo → Select Source → Capture photo or select from device → Crop the photo → Tap *Done* → Add a Filename → Save the photo and done.

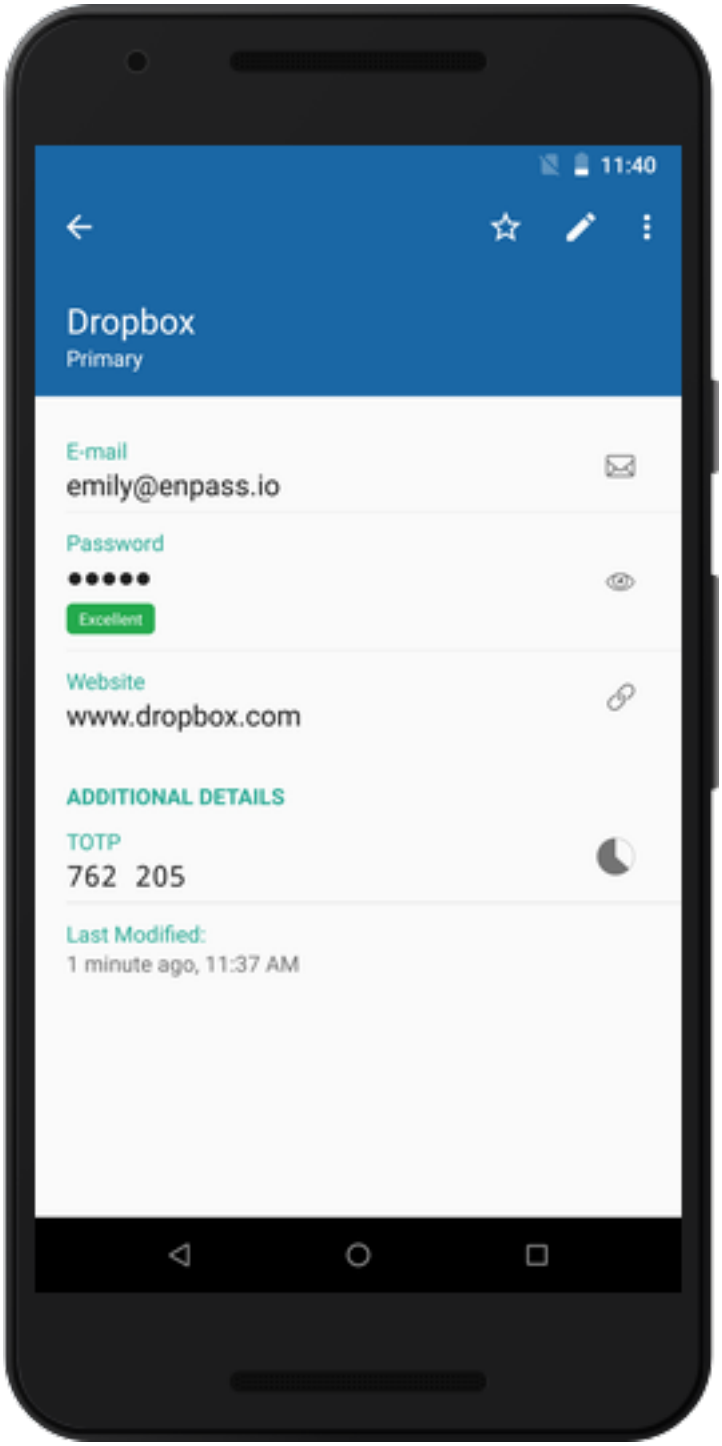
6.3.2 Attach file

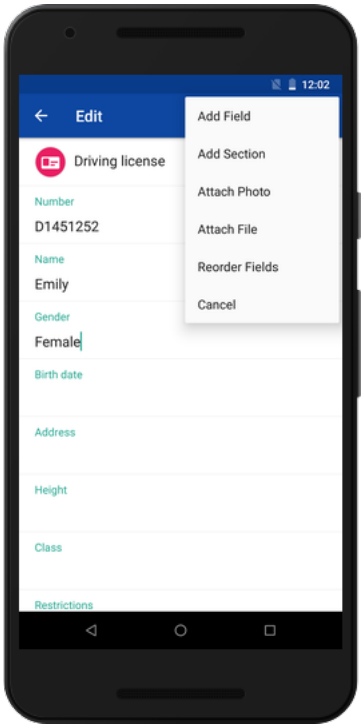
Same way, you can attach a file saved in your device as an attachment. Simply `Edit` item → Tap on option menu (3 dots) → Attach File → Choose a file from your device → Tap on *Save* to finally save the item.

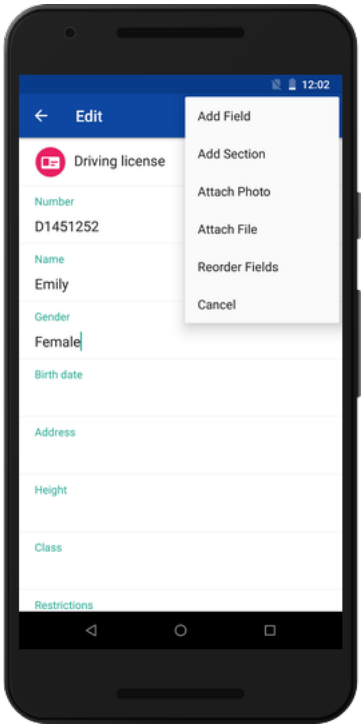
Note: All the items having attachments are directly accessible from the sidebar –> Attachments.

6.3.3 View Attachment

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

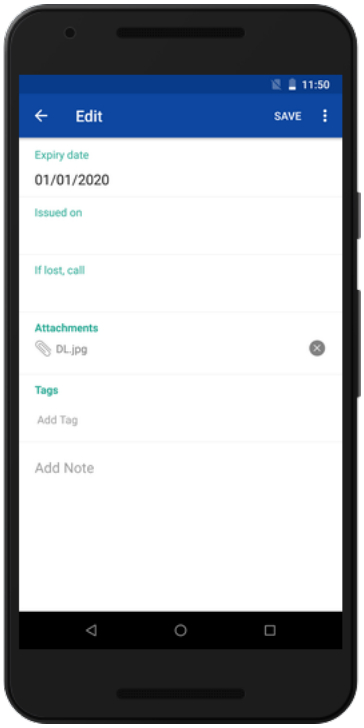

11:40
Dropbox
Primary
E-mail
emily@enpass.io
Password
Excellent
Website
www.dropbox.com
ADDITIONAL DETAILS
TOTP
762 205
Last Modified:
1 minute ago, 11:37 AM


12:02
Edit
Add Field
Add Section
Attach Photo
Attach File
Reorder Fields
Cancel
Driving license
Number
D1451252
Name
Emily
Gender
Female
Birth date
Address
Height
Class
Restrictions


12:02
Edit
Add Field
Add Section
Attach Photo
Attach File
Reorder Fields
Cancel
Driving license
Number
D1451252
Name
Emily
Gender
Female
Birth date
Address
Height
Class
Restrictions

6.3.4 Delete Attachment

To delete an attachment, `Edit` the item and scroll down to the *Attachments* section. Tap on right next to attachment name to delete it. A warning message will appear, tap on *Delete* to continue. To pertain the changes, you need to **save** the item as well.



6.4 Tags

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

6.4.1 Tagging items

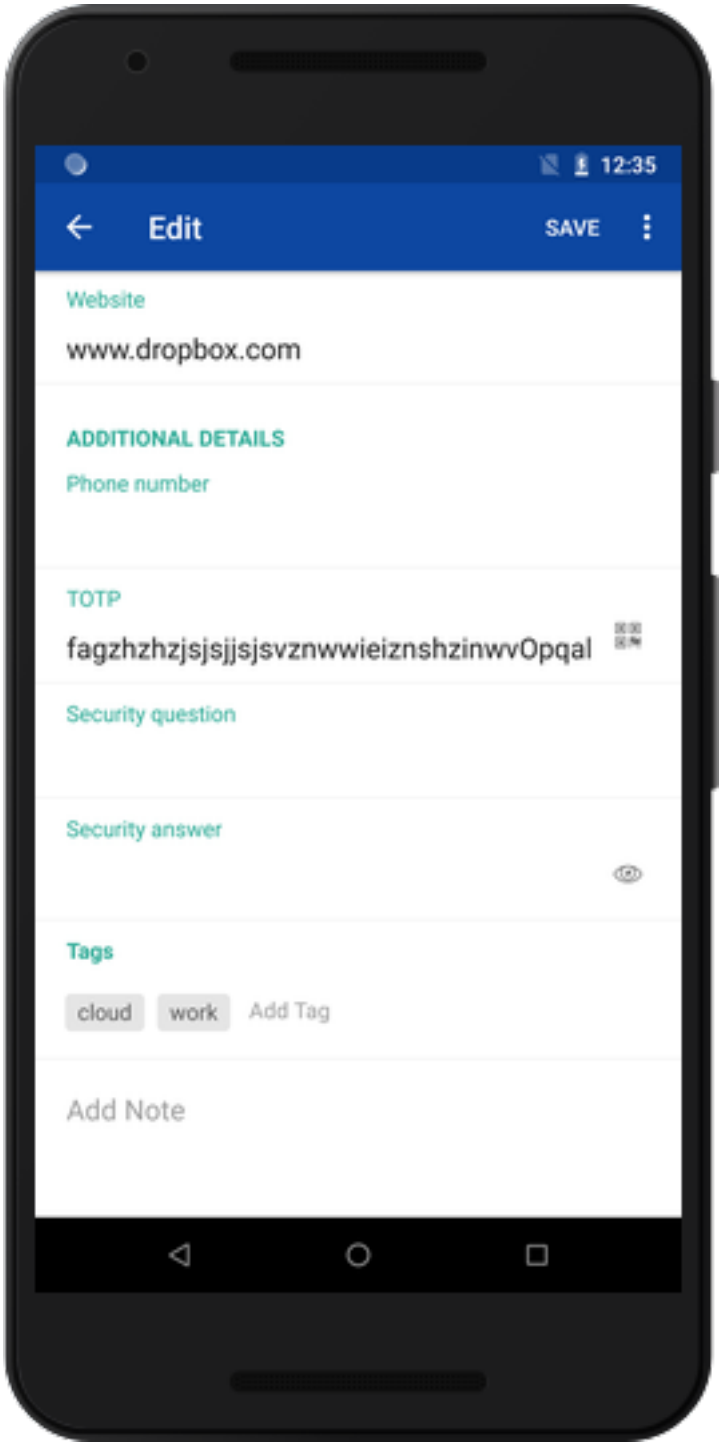
The following steps will guide you to add tags to your items.

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 sidebar. Just tap on Tags from the sidebar, and you'll be presented with the list of all the existing tags in Enpass.


12:35
Edit
SAVE
Website
www.dropbox.com
ADDITIONAL DETAILS
Phone number
TOTP
fagzhzhzjsjsjjsjsvznwwieiznshzinwvOpqal
Security question
Security answer
Tags
cloud
work
Add Tag
Add Note

From Sidebar

You can also create tags from tag-listing in sidebar 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 → Add item details → Tap *Save*

Add existing Items under a tag

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

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

6.4.2 Nested Tags

You can add the sub-tags in an existing tag in Enpass. To add a sub-tag, Select the *Tag* in sidebar 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.

6.4.3 Editing Tags

Select **Tags** from the sidebar. Tap on the option menu (3-dots) and tap *Edit* → edit tag name → Save and done. On the same screen, you can also delete the tag by tapping the *delete* icon.

6.4.4 Untag an Item

To untag an item, Select **Tags** from the sidebar → Select the tag → Tap on the options menu (3 dots) on the item and tap on *Untag*.

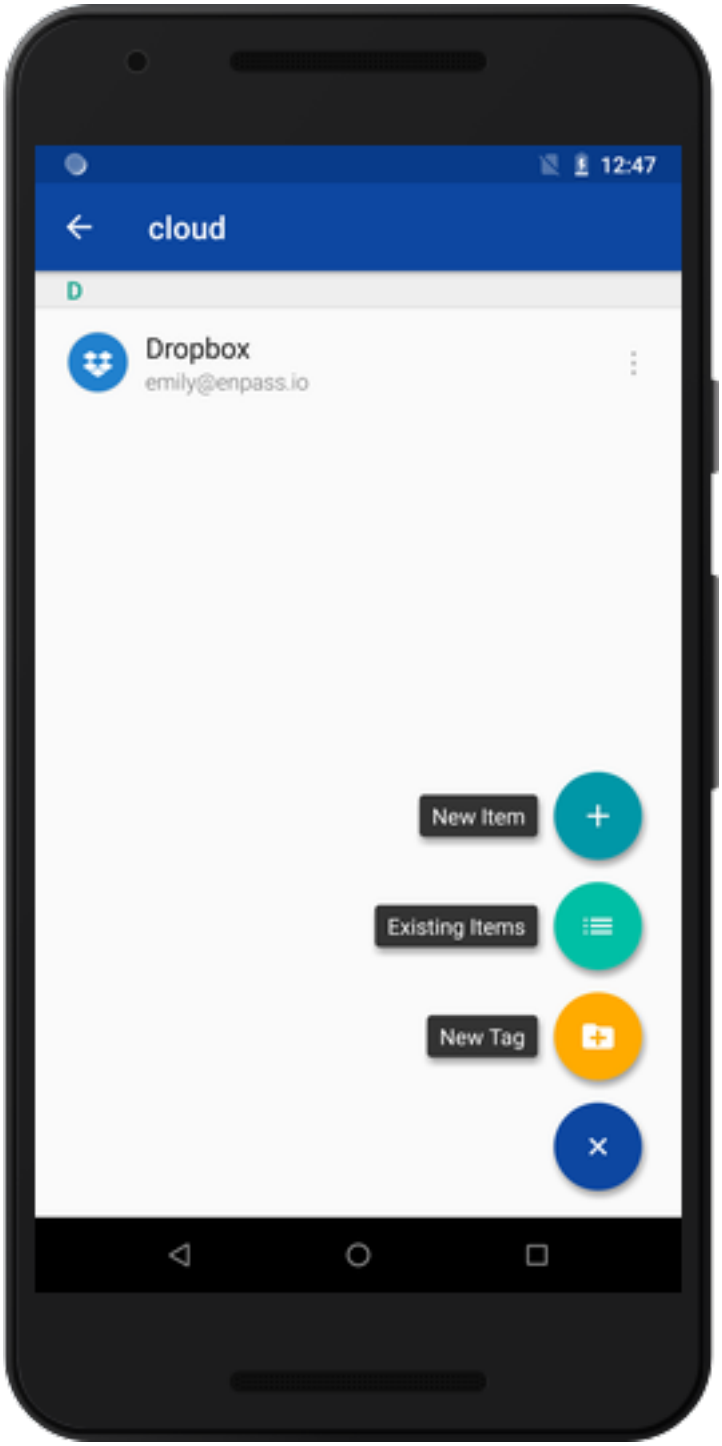
6.5 Deleting and Archiving

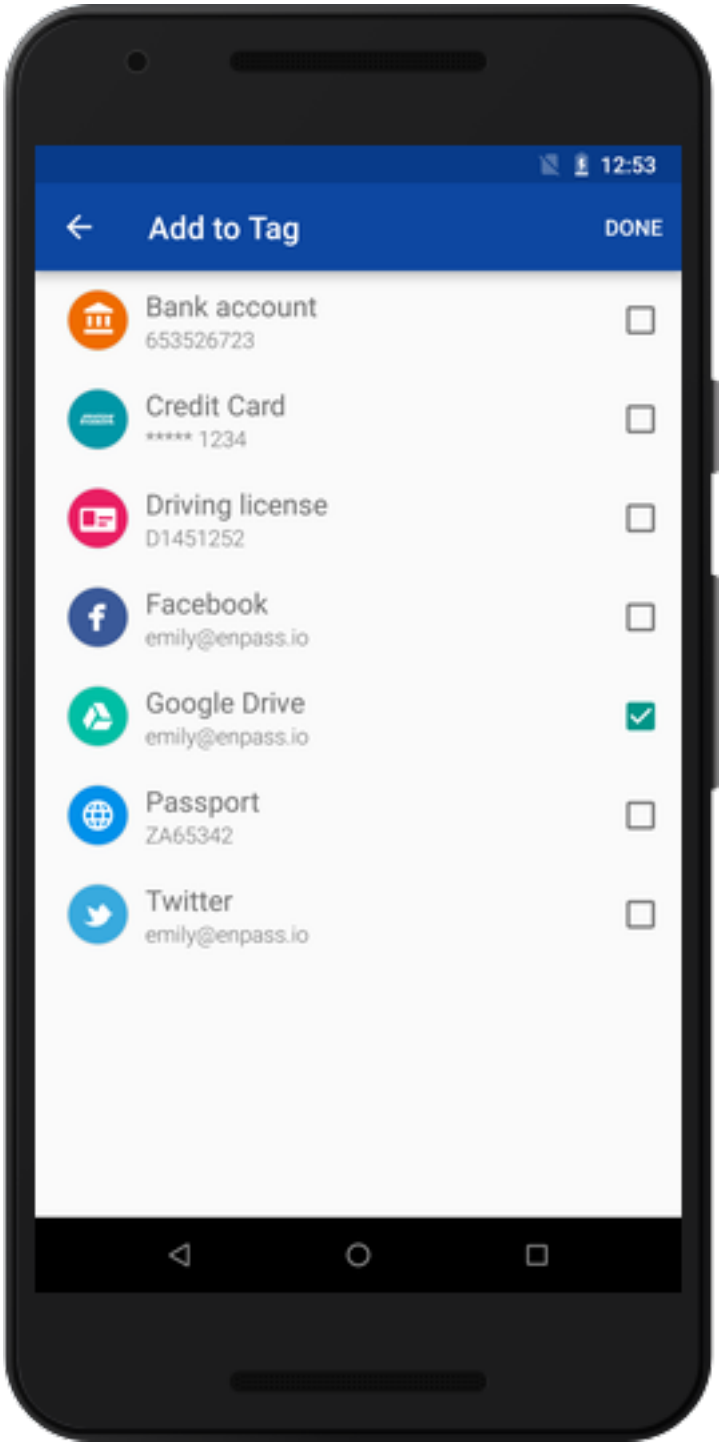
You can move items to *Trash* which are no longer in use and from there you can permanently delete them. Also, Enpass lets you *Archive* items which you don't want to trash.

6.5.1 Trash

- To move an item to Trash, tap on the item > Tap on the 3-dots > *Move to Trash*.
- To restore an item from Trash, tap on *Trashed* under *Others* in the sidebar > Tap on the 3-dots of the item > Tap *Restore*.
- If you want to delete the item permanently, delete it from the *Trashed* under *Others* in the sidebar.

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


12:47
cloud
D
Dropbox
emily@enpass.io
New Item
Existing Items
New Tag


12:53
Add to Tag
DONE
Bank account
653526723
Credit Card
***** 1234
Driving license
D1451252
Facebook
emily@enpass.io
Google Drive
emily@enpass.io
Passport
ZA65342
Twitter
emily@enpass.io

6.5.2 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 the 3-dots > Archive.

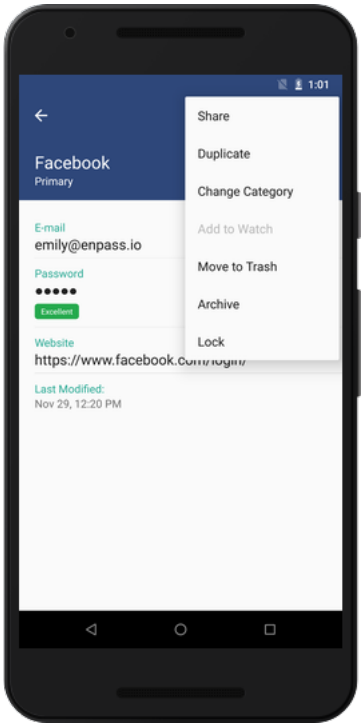
Note: The Archived item will remain in Enpass but will not appear in the search results.

- To unarchive an item, tap on *Archived* under *Others* in the sidebar > Tap on the 3-dots of the item > Tap *Restore*.

6.6 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 the options menu (3-dots) > Duplicate.



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

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

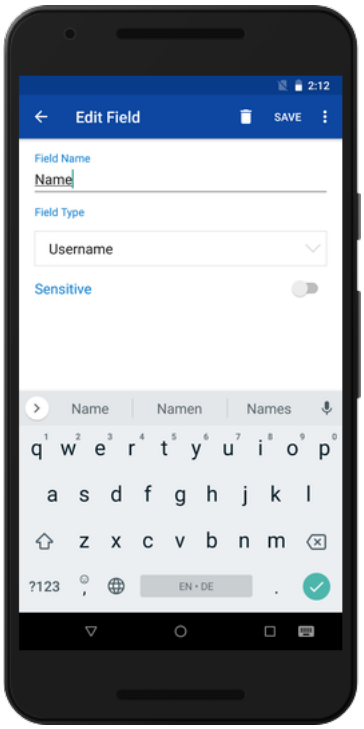
6.7 Customizing Fields

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

6.7.1 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 **Save** after making the changes.

6.7.2 Adding fields

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

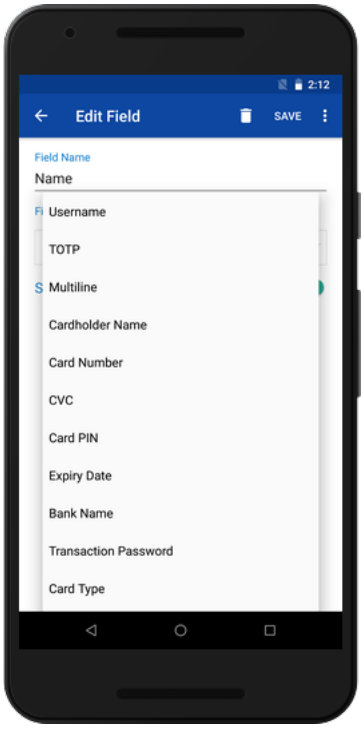
- While you are at the Edit screen, from the action bar menu, select *Add Field*.
- Enter the new field's name and choose the appropriate type. You can also mark the field type to be as *Sensitive*.
- Finally **Save** the item to pertain the changes.

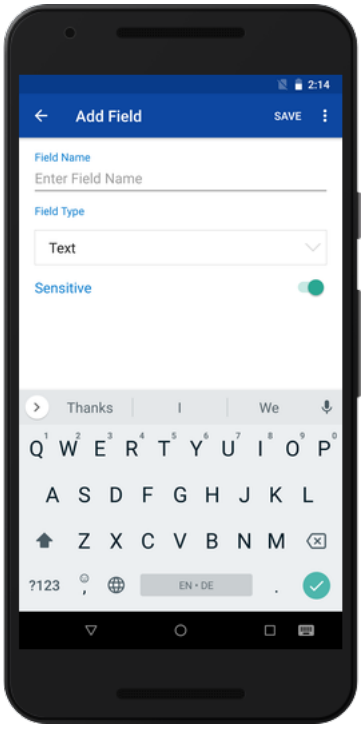
Important: We recommend that you keep the **Sensitive** mode ON for passwords or security answers. This way your passwords, PINs and other similar texts would stay safe from shoulder surfers when you use the app in public places.

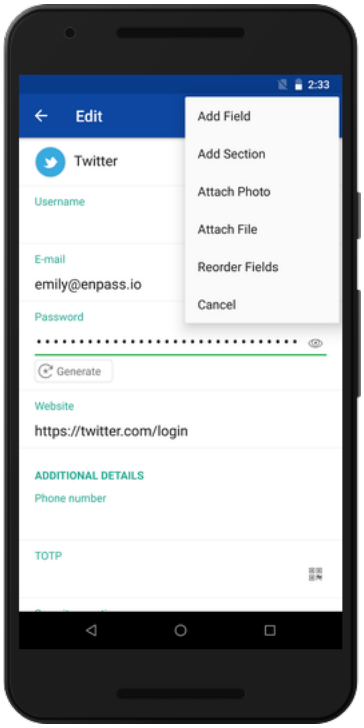
6.7.3 Re-ordering Fields

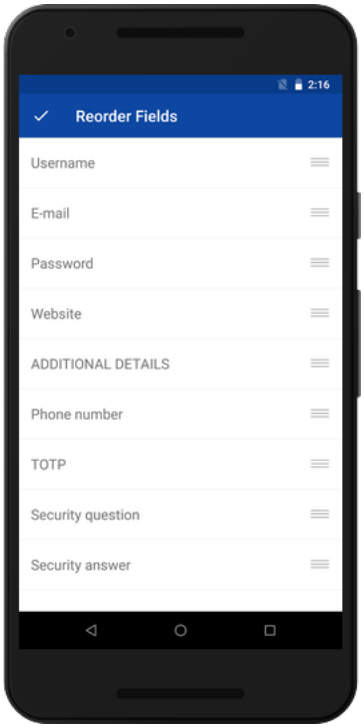
You can also re-arrange the order of the fields in an item. * From the action bar menu on Edit screen, select *Reorder Fields*.

- Hold and drag the fields to Re-arrange them and *Save* the changes.


2:12
Edit Field
SAVE
Field Name
Name
Username
TOTP
Multiline
Cardholder Name
Card Number
CVC
Card PIN
Expiry Date
Bank Name
Transaction Password
Card Type

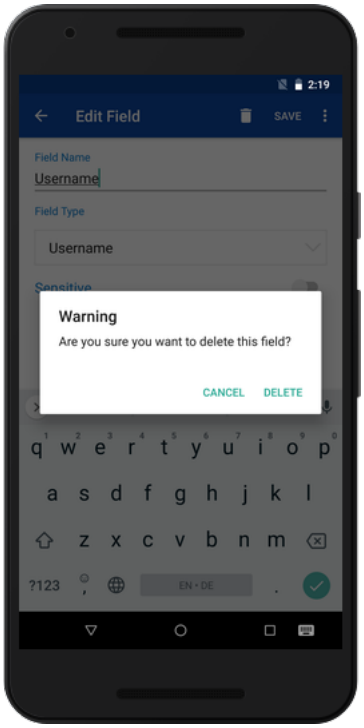

2:14
Add Field
SAVE
Field Name
Enter Field Name
Field Type
Text
Sensitive
Thanks
I
We
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
?123
EN • DE


2:33
Edit
Add Field
Add Section
Attach Photo
Attach File
Reorder Fields
Cancel
Twitter
Username
E-mail
emily@enpass.io
Password
Generate
Website
https://twitter.com/login
ADDITIONAL DETAILS
Phone number
TOTP


2:16
Reorder Fields
Username
E-mail
Password
Website
ADDITIONAL DETAILS
Phone number
TOTP
Security question
Security answer

6.7.4 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. You will see a *Delete* icon. Tap that. A warning message will be displayed for confirmation of deletion. Tap **Delete** to remove that field. To pertain the changes finally, you need to **Save** the item as well.



6.7.5 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 the options menu (3-dots) > tap on *History*.

6.7.6 Customizing Password Fields

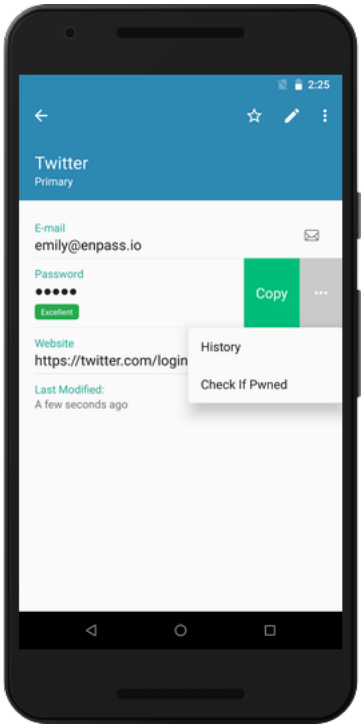
Unlike other field types, password field has additional options which allow you to set an expiry date to that particular password and exclude the password from the *password audit*.

6.7.7 Exclude from Audit

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

6.7.8 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 Password Audit* option is unchecked.

6.7.9 Sensitive

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

6.8 Adding Section

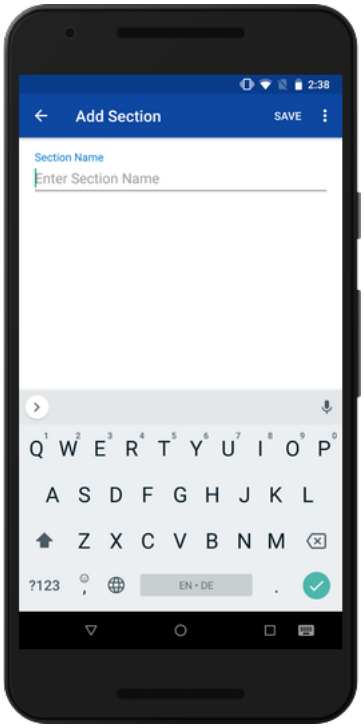
Follow the steps below to add sections in the item:

- Go to the edit screen of the item. From the action bar select *Add Section*.
- Enter Section Name.
- Finally *Save* the item to pertain the changes.

6.9 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*



6.9.1 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

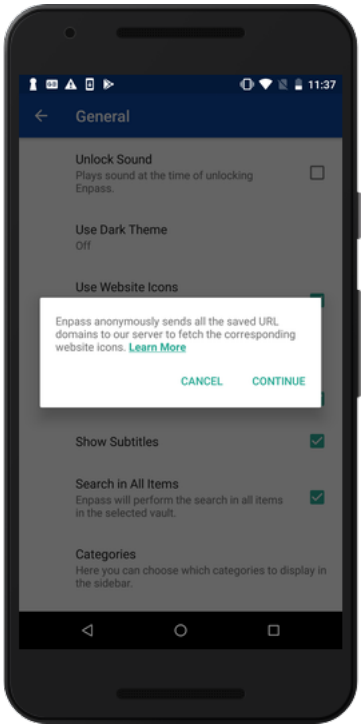
Tap the **Menu icon** → **Settings** → **General** → Select the **Use Website Icons** check box → **Continue**.

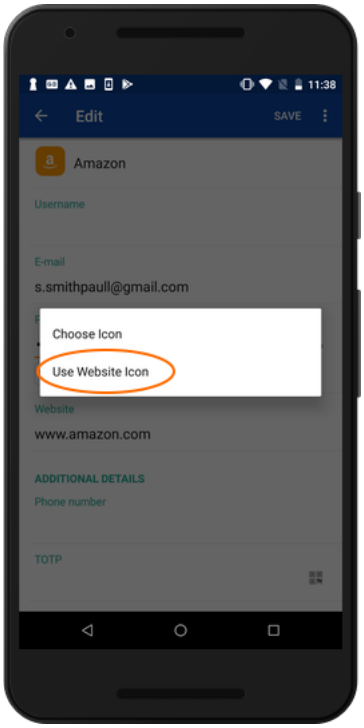
6.9.2 Enabling website icons for a particular site:

1. Open the item from the main screen and tap the **Edit** button.
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.

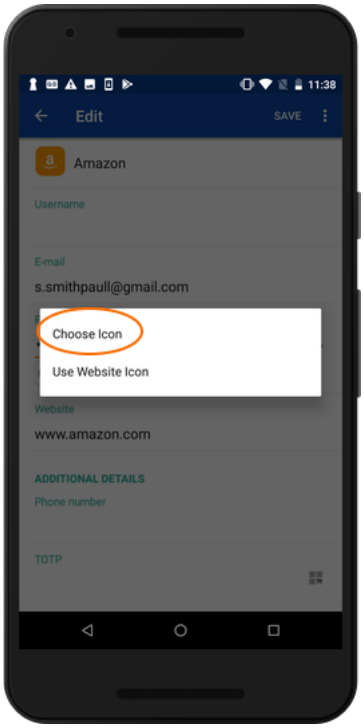

11:37
General
Unlock Sound
Plays sound at the time of unlocking Enpass.
Use Dark Theme
Off
Use Website Icons
Enpass anonymously sends all the saved URL domains to our server to fetch the corresponding website icons. Learn More
CANCEL
CONTINUE
Show Subtitles
Search in All Items
Enpass will perform the search in all items in the selected vault.
Categories
Here you can choose which categories to display in the sidebar.


11:38
Edit
SAVE
Amazon
Username
E-mail
s.smithpaull@gmail.com
Choose Icon
Use Website Icon
Website
www.amazon.com
ADDITIONAL DETAILS
Phone number
TOTP

6.9.3 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 screen.
2. Tap the **Edit** button.
3. Tap the icon of the item.
4. Select **Choose Icon**. Enpass displays a collection of icons from which you can select your icon for the item.



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

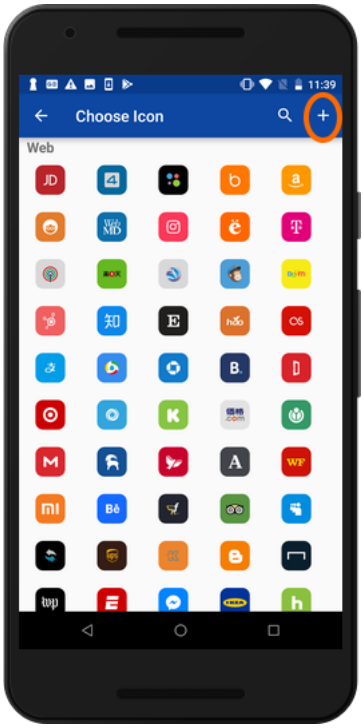
1. Tap **+** at the top right corner of the screen.

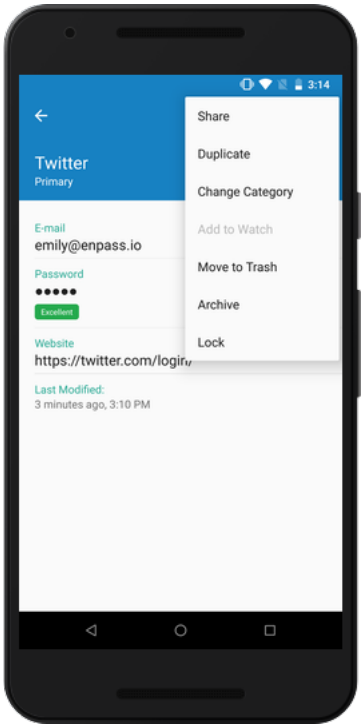
2. Select **Allow Enpass to capture images and record audio and video**.
3. Locate the image in your phone; resize it if necessary.
4. Tap **Done**.

6.10 Changing Category

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

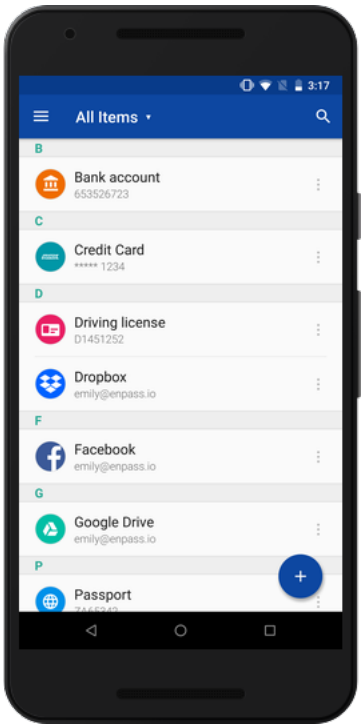
- Open the item and from the action bar menu, tap on **Change Category** > Select the the category you want to set for the item.


11:39
Choose Icon
Web


3:14
Share
Duplicate
Change Category
Add to Watch
Move to Trash
Archive
Lock
Twitter
Primary
E-mail
emily@enpass.io
Password
Excellent
Website
Last Modified:
3 minutes ago, 3:10 PM

6.11 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.

6.11.1 Sort By

You can use this option to arrange the items systematically in a sequence ordered specific criterion.

6.11.2 Title

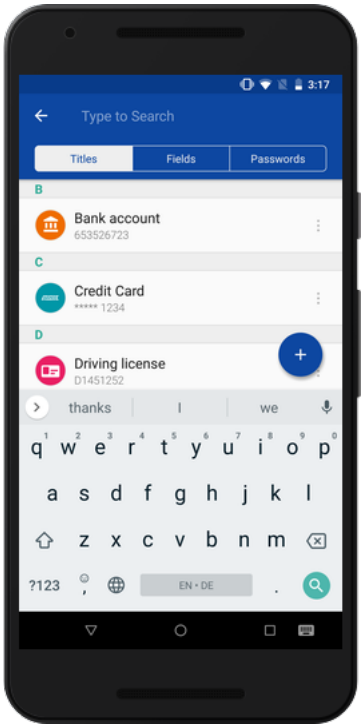
Use this option to arrange your items in the ascending alphabetical order.

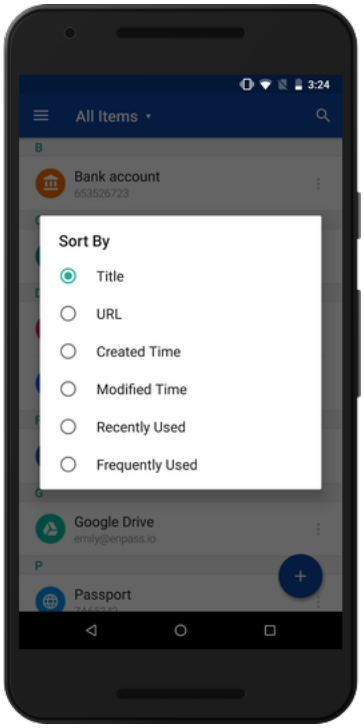
6.11.3 Url

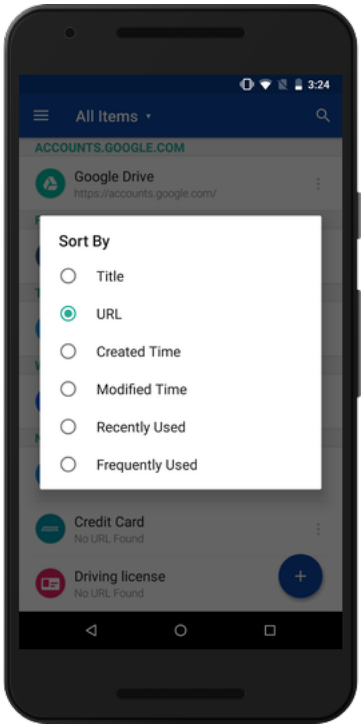
This option will arrange your items by ascending alphabetical order of the URL, making the items with no URLs appear in the last.

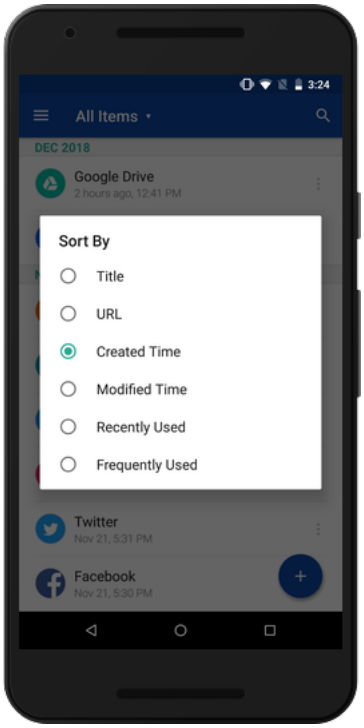
6.11.4 Created Date

Use this option to sort your items according to the date of creation. The latest created items will appear first.


3:17
Type to Search
Titles
Fields
Passwords
B
Bank account
653526723
C
Credit Card
***** 1234
D
Driving license
D1451252
thanks
I
we
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
?123
EN • DE


3:24
All Items
Bank account
653526723
Sort By
Title
URL
Created Time
Modified Time
Recently Used
Frequently Used
Google Drive
P
Passport

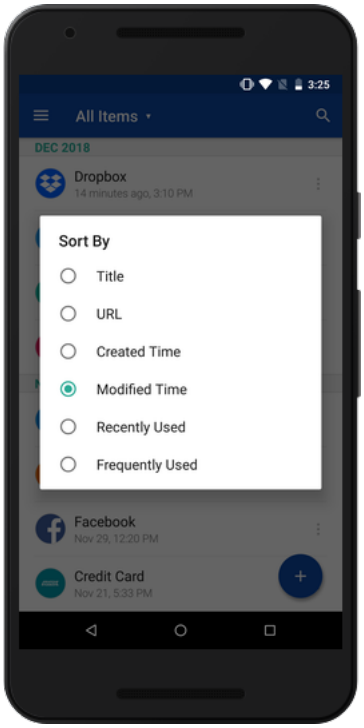

3:24
All Items
ACCOUNTS.GOOGLE.COM
Google Drive
https://accounts.google.com/
Sort By
Title
URL
Created Time
Modified Time
Recently Used
Frequently Used
Credit Card
No URL Found
Driving license
No URL Found


3:24
All Items
DEC 2018
Google Drive
2 hours ago, 12:41 PM
Sort By
Title
URL
Created Time
Modified Time
Recently Used
Frequently Used
Twitter
Nov 21, 5:31 PM
Facebook
Nov 21, 5:30 PM

Note: Any item that you've duplicated or copied from other vaults will act as a newly created item, and will appear in the search results accordingly.

6.11.5 Modified Time

Use this arrangement of items to sort the list by their modification time. The item with the latest modification time will appear first.



Note: Any item will be treated as modified when you actually change any of its property, favorite/unfavorite it, change its category, and will appear in the search results accordingly.

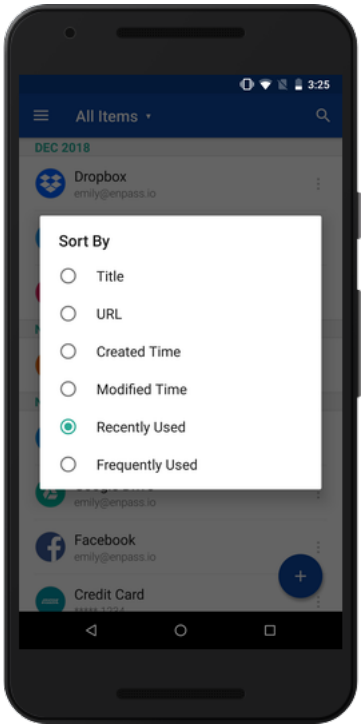
6.11.6 Recently Used

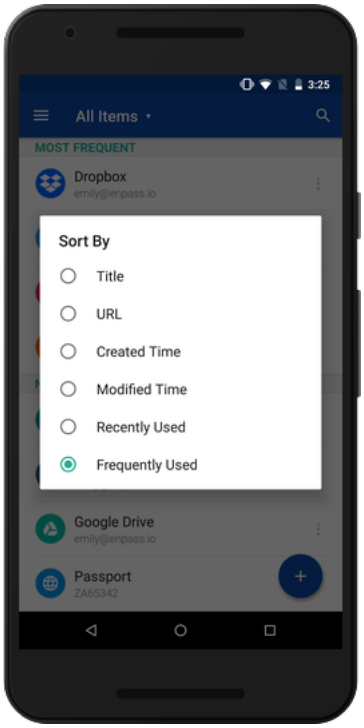
This will sort the items by their usage. The most recently used items will appear first, and the items that have never been used will appear last in the list.

The items you've used for autofill or else copied any field value will be considered in the recently used sorting.

6.11.7 Frequently Used

Use this feature to arrange the items according to their usage. The most frequently used items will appear first, then the rarely used items, and at last will appear the items that you've never used.


3:25
All Items
DEC 2018
Dropbox
emily@enpass.io
Sort By
Title
URL
Created Time
Modified Time
Recently Used
Frequently Used
Facebook
emily@enpass.io
Credit Card


3:25
All Items
MOST FREQUENT
Dropbox
emily@enpass.io
Sort By
Title
URL
Created Time
Modified Time
Recently Used
Frequently Used
Google Drive
emily@enpass.io
Passport
ZA65342

6.12 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.

6.13 Check Pwned passwords

Enpass lets you check your passwords against the list of breached passwords managed by Troy Hunt. It's a trustworthy procedure, ensuring that your passwords are safe in Enpass and never sent to the internet. Here's how you can check your leaked password within Enpass-

1. From the detail screen of your item, tap on the password field → Choose option menu (3 dots) → click on the `Check if Pwned` in the context menu.
2. On the next screen, you'll see a message to validate the operation. Click *Continue*.
3. You will now see the results.

Note: You can also check all the items found with pwned passwords in the Weak passwords list under Password Audit.

6.13.1 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.

Tip: Desktop version of Enpass, lets run the check for all of passwords at once.

CHAPTER

SEVEN

ORGANIZATION

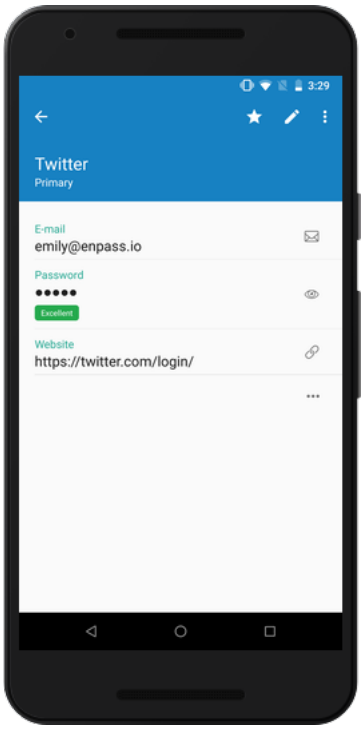
In Enpass, you can efficiently organize your credential using the following ways:

7.1 Marking Favorites

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

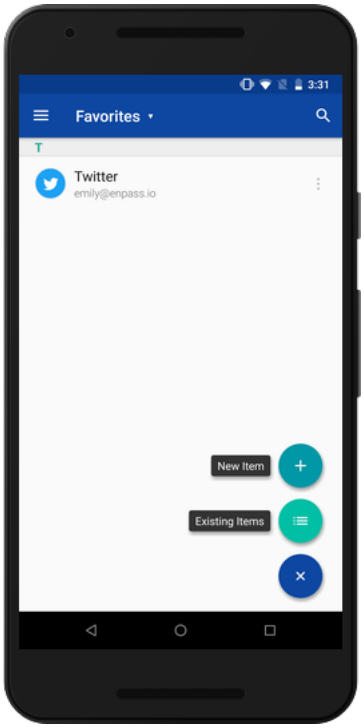
7.1.1 From detail screen

- Tap the **Star** icon on the detail screen of the item.



7.1.2 From favorite list

- Go to the Favorites list in the sidebar and tap the **+** sign. Select from the pre-existing items or create new ones to add to Favorites.



7.2 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 the sidebar.

7.3 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.

7.3.1 Hide Category

You can hide the categories from sidebar from the Enpass settings. *Tap here* to see the steps.

7.3.2 Change Category

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

7.3.3 Add custom categories and templates

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

7.4 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*.

CHAPTER

EIGHT

VAULTS IN ENPASS

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.

8.1 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.

8.2 Multiple Vaults

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

8.2.1 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*.

8.2.2 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 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.

8.2.3 Sharing a Vault

Once you have set up multiple vaults in Enpass, you can easily share any vault with your family, friends or colleagues using cloud synchronization. See how.

Just set up sync with the supported cloud account, and then share the login details of this cloud account and the vault password of Enpass with the intended person so that they can create a new vault in their Enpass by restoring data from the cloud. There are a few points that you must keep in mind before sharing a vault:

- You need to share the Master Password.
- You'd have to share the login details of cloud account with each member with whom you want to share the vault.
- Every person having the access to the vault has full permissions to read, write (delete) any item from the vault, or even change the Master password of the vault as you can't set any sharing attributes or access permissions.

8.2.4 Adding the shared vault

Once you know the cloud account details and the vault password of the <shared vault>, you just have to restore the data from the cloud using <these simple steps>. There are a few important points you need to keep in mind before adding the shared vault:

- Any change in the data on the shared vault will get reflected on all the other synced devices.
- Change in the vault password will get updated automatically on the synced cloud account and a sync error will occur on the other synced devices.

8.2.5 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 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, you can see the password of the vault.

CHAPTER

NINE

SYNCING DATA

Enpass lets you sync your data with other devices through any of the supported clouds. Syncing across Enpass is very secure as all your data is transmitted in encrypted format, and cryptography is always performed locally on the device only.

9.1 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.

9.2 Supported clouds

Currently, Enpass supports syncing of data across devices through your own account on following clouds where we do not store any of your data on our server.

- Dropbox
- Google Drive
- OneDrive
- iCloud
- WebDAV

9.3 Setup 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.

9.4 Folder Sync

Enpass lets you sync with any folder, accessible on your device or on the network.

9.4.1 Set up Folder Sync

To set up set up folder sync, refer to the *sync settings* in Enpass.

9.4.2 Sync Timings

- Every time you unlock Enpass, 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 make any change in data, Enpass waits for 5 secs and initiates an auto-sync.

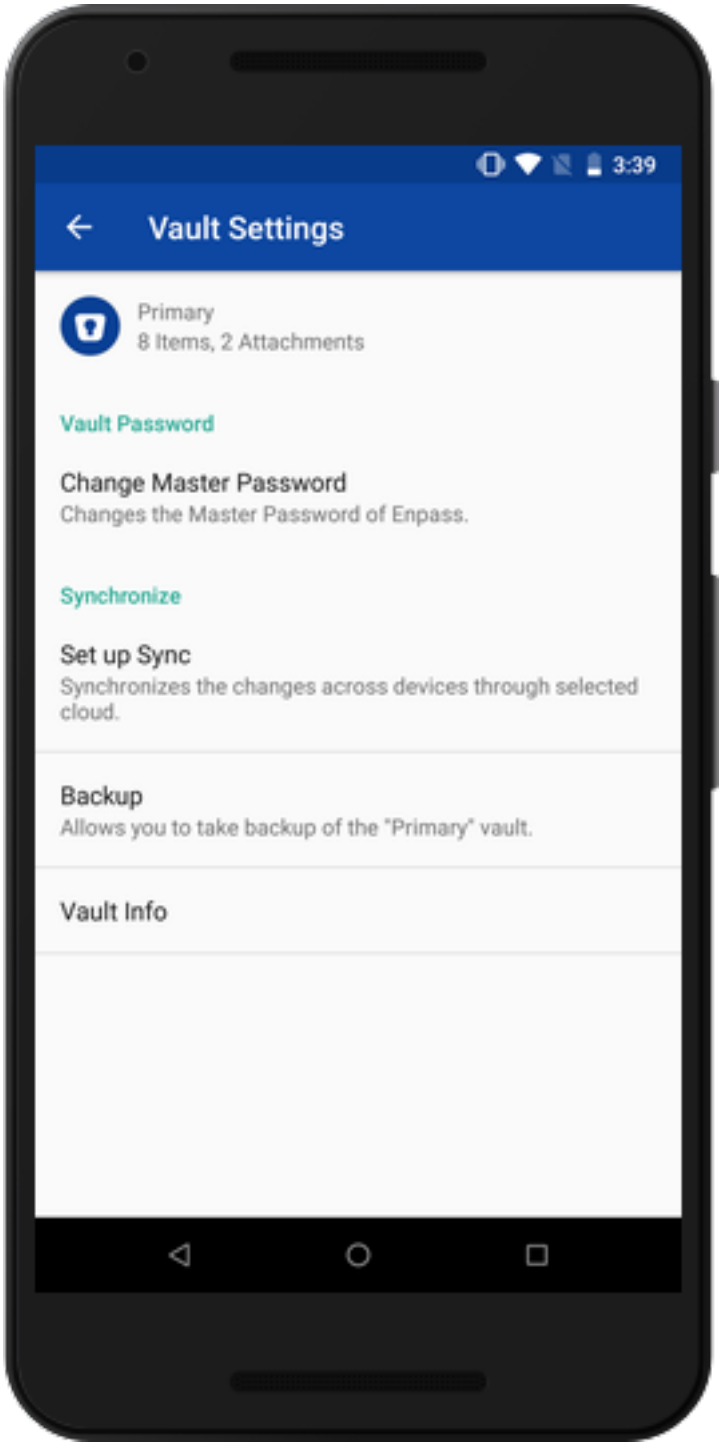
9.4.3 Time Stamps

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).


3:39
Vault Settings
Primary
8 Items, 2 Attachments
Vault Password
Change Master Password
Changes the Master Password of Enpass.
Synchronize
Set up Sync
Synchronizes the changes across devices through selected cloud.
Backup
Allows you to take backup of the "Primary" vault.
Vault Info

CHAPTER

TEN

BACKUP AND RESTORE

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

10.1 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.

10.2 Restoring backup

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

10.2.1 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:

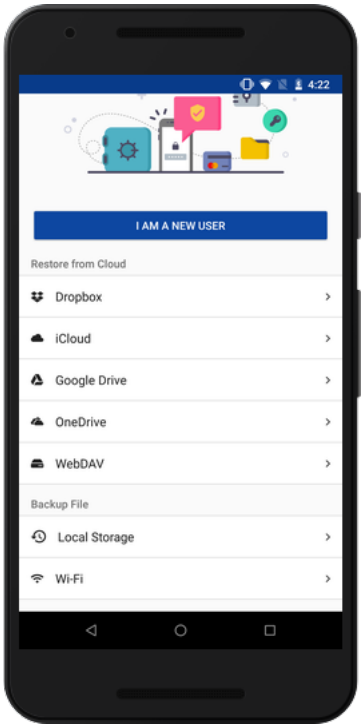
- Using a browser on other system, navigate to the IP address visible in the *Restore over Wi-Fi* screen in your Mobile device.
- Tap **Choose File** on your system and navigate to the backup file's location. Tap on Submit. Now you'll be asked to enter the password of the file in your device.

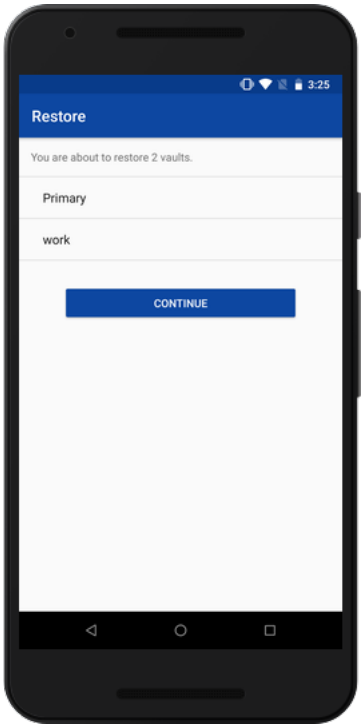
Note: While restoring data in secondary vault, you have to choose the vault you need to restore. In case if your backup contain multiple vaults and you restore all of them, you need to *Erase everything* and start over by restoring data from backup file.

10.2.2 From local storage

Tap on the Local Storage and select the file from the device. After selecting the file, 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.

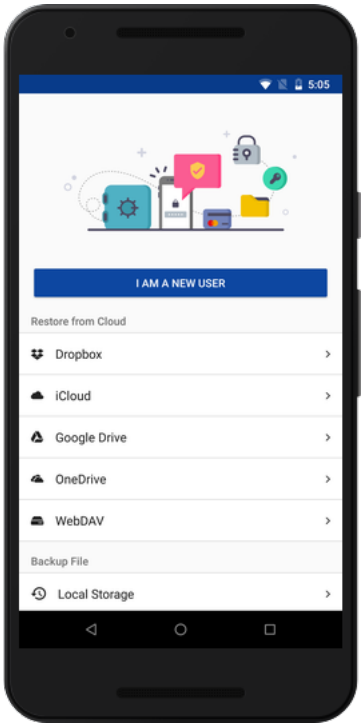

4:22
I AM A NEW USER
Restore from Cloud
Dropbox
iCloud
Google Drive
OneDrive
WebDAV
Backup File
Local Storage
Wi-Fi


3:25
Restore
You are about to restore 2 vaults.
Primary
work
CONTINUE

10.3 Restore from Cloud

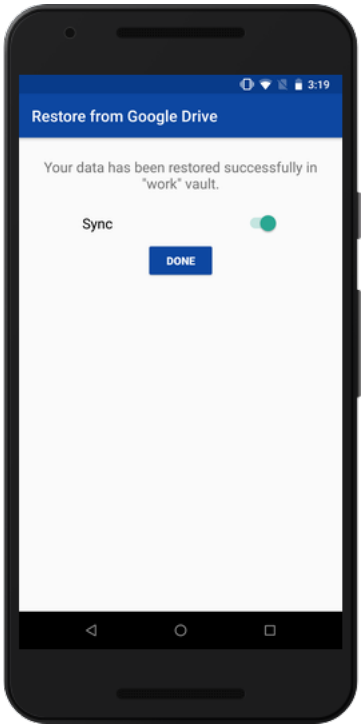
Following steps review the process of restoring from cloud:

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.


3:19
Restore from Google Drive
Your data has been restored successfully in "work" vault.
Sync
DONE

CHAPTER

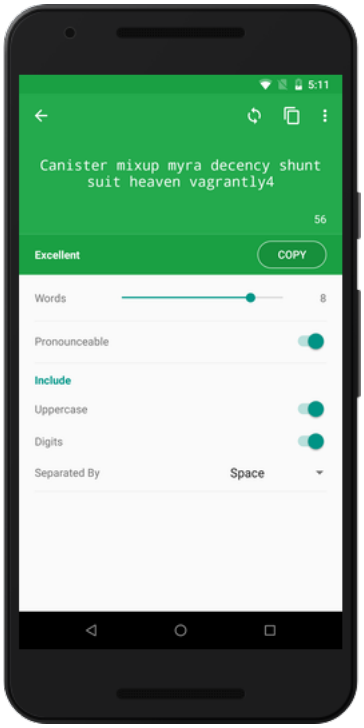
ELEVEN

PASSWORD GENERATOR

Enpass has a built-in password generator to help you in creating unique and robust passwords whenever you need.

11.1 Generating Passwords

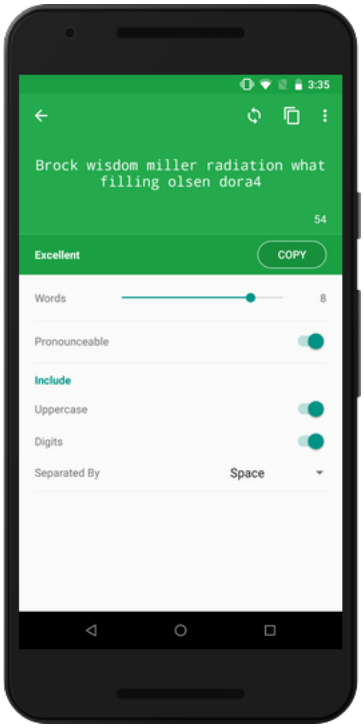
You can generate password from `Edit` page of any item by tapping the *Generate* button right next to password field, or you can go to the sidebar and tap on *Generator* icon.



The password's complexity can be altered using the various controls provided on generator. You can create pronounceable as well as random passwords.

11.1.1 Pronounceable passwords

Pronounceable passwords are created with Diceware methodology using 14400 English dictionary words. You can set the number of words, include the uppercase, digits, and symbols as separators (dollar, hyphen, comma, space, period, underscore or hash).



11.1.2 Random passwords

While generating **Random passwords**, you can decide the total length of the password, the number of minimum or exactly uppercase, digits, and symbols. Also, you can specify the symbols you want to exclude while generating the password.

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*).

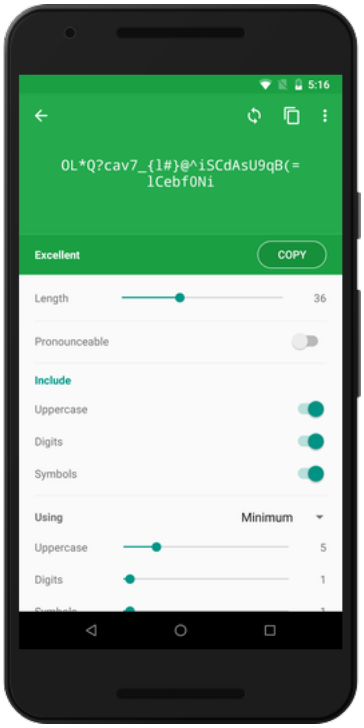
Note: Enpass uses zxcbvn algorithm to give you a realistic estimation of password strength.

11.2 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



11.3 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.

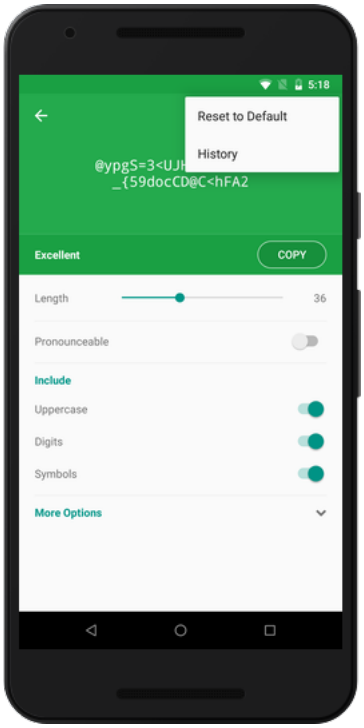
11.3.1 Password history of an item

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 Pwned* option. Select `History` to see the previously used passwords.

11.3.2 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.


5:18
Reset to Default
History
@ypgS=3<UJ
_{59docCD@C<hFA2
Excellent
COPY
Length
36
Pronounceable
Include
Uppercase
Digits
Symbols
More Options

CHAPTER

TWELVE

AUTOFILL

With Enpass, you don't need to manually copy and paste your passwords in the apps and browsers as it can securely autofill the login and credit card details in apps and supported browsers.

Enpass in Android uses the following three approches to do the autofilling, and for better experience you can enable all of them at a time.

1. Android Autofill Framework
2. Notifications through Android Accessibility
3. Enpass Keyboard

Depending on the Android version on your device, the Autofill options might look different. For help in activating and using Autofill on your device, please have a look here.

The following table gives you quick glance over the ways you can use to autofill on different Android versions:

Android OS	**Autofills using**		
	Autofill Framework	**Notifications**	**Enpass Keyboard**
Android 9.x	✓ *Supported apps & browsers*	✓ *Supported apps & browsers*	✓
Android 8.x	✓ `Supported apps only`	✓ *Supported apps & browsers*	✓
Pre Android 8		✓ *Supported apps & browsers*	✓

CHAPTER

THIRTEEN

ENPASS FOR CHROMEBOOKS

Enpass is entirely integrated with the Chrome Operating System running on Chromebooks. The contemporary Enpass App for Android also works with those Chromebooks which supports the Apps from Google Play Store. The process of setting up Enpass on Chromebook is same as setting up Enpass on Android devices.

13.1 Autofilling in Chromebooks

One of the best assistance that Enpass provides is the freedom to Auto-fill your information with just a single click. No speculation, no typing, no copy/paste required- Enpass does it all for you.

Enpass extension for Chromebook is the same extension used for the Chrome browser in the desktops, and in Chromebooks, it only works with the supported versions.

13.1.1 Installing Enpass Extension

Installing Enpass extension for Chrome browser in Chromebook is same as installing it for the Chrome in desktops.

- Visit the Chrome Web Store to add the extension to Chrome browser.
- Click on *Add to Chrome* and a pop-up will appear prompting you to add the extension to the browser.
- Click on *Add extension* to add the extension to Chrome browser. Once securely installed, you will see an Enpass icon at the top-right corner of your browser.

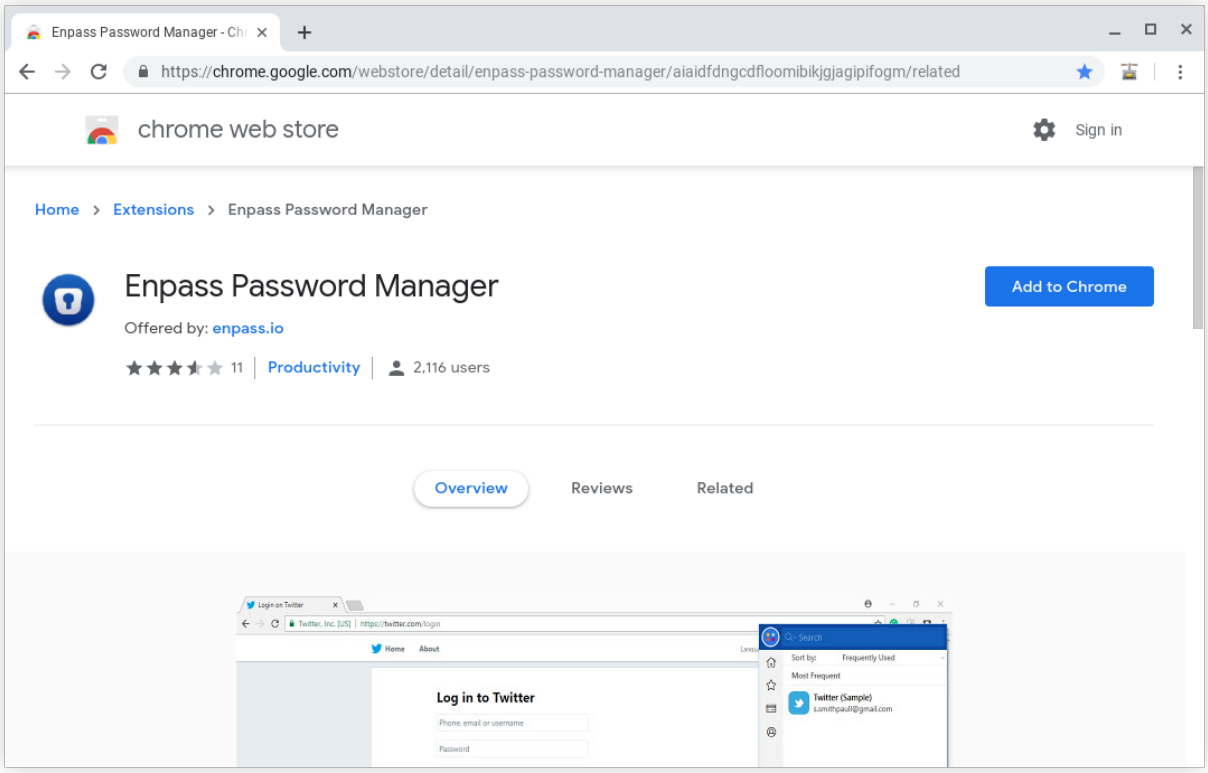
13.1.2 Enable Autofilling

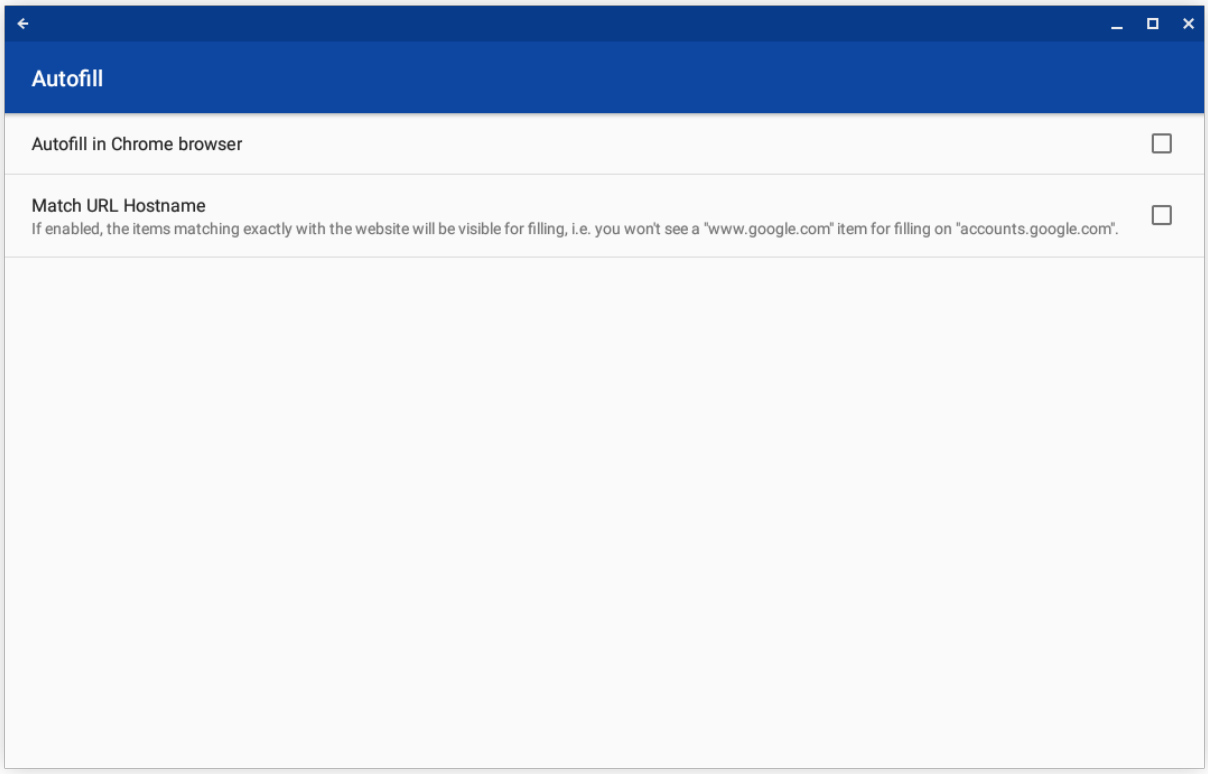
To do the autofilling using Enpass extension in supported Chromebooks, you first need to enable it from Enpass settings.

- Go to Enpass setting and click on *Autofill*.
- It will land you on the *Autofill* page. Enable *Autofill in Chrome browser*, and it will land you on the page where you need to connect the extension with the Enpass app. Once it's done, you can enjoy the seamless autofilling with Enpass on Chromebook.

13.2 Using Enpass Extension

While browsing, Enpass extension does many operations like Autofilling logins and credit cards, updating and saving new logins, etc.; thus giving a smooth browsing experience in an easy way.

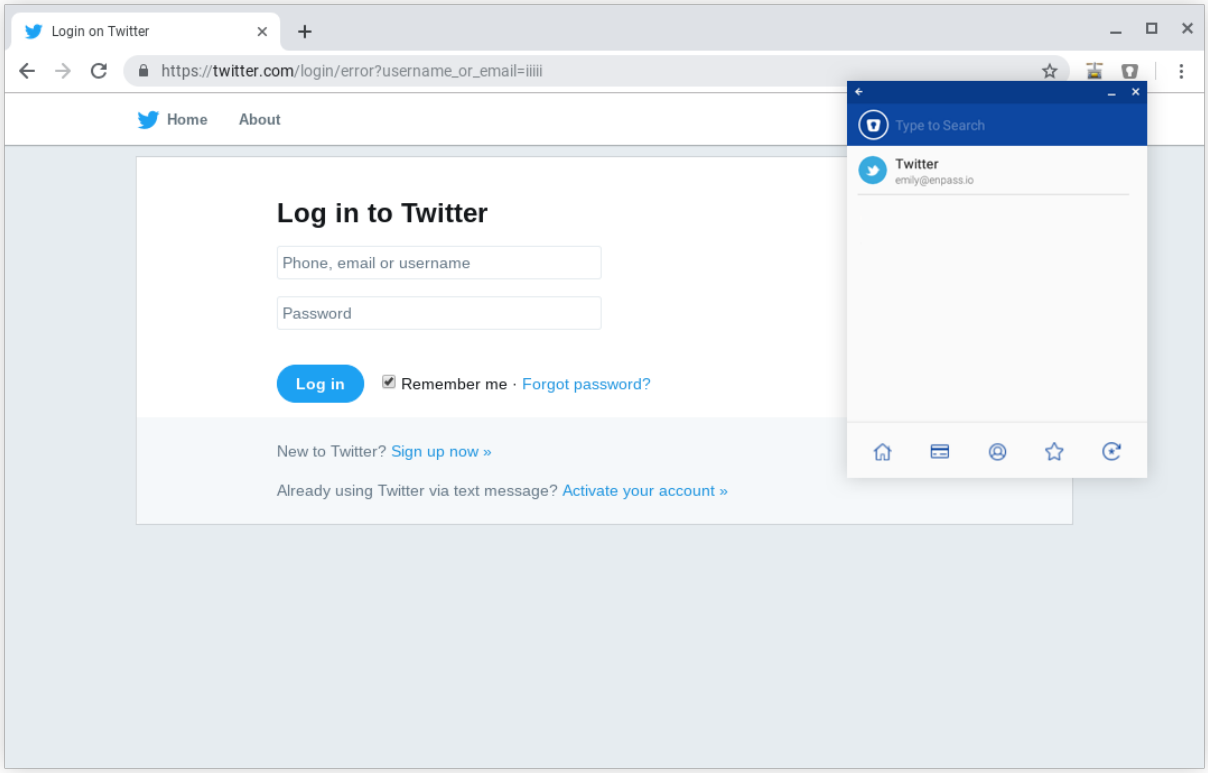

Enpass Password Manager - Ch
https://chrome.google.com/webstore/detail/enpass-password-manager/aiaidfdngcdfloomibikjgjagipifogm/related
chrome web store
Sign in
Home
Extensions
Enpass Password Manager
Enpass Password Manager
Offered by: enpass.io
11
Productivity
2,116 users
Add to Chrome
Overview
Reviews
Related
Log in to Twitter
Phone, email or username
Password
Sort by:
Frequently Used
Most Frequent
Twitter (Sample)


Autofill
Autofill in Chrome browser
Match URL Hostname
If enabled, the items matching exactly with the website will be visible for filling, i.e. you won't see a "www.google.com" item for filling on "accounts.google.com".

13.2.1 Autofilling Logins

The Enpass extension detects logins forms on the fly, and the desired information is fetched securely from Enpass database.

- Click the Enpass icon to launch Enpass extensiom from your browser when you reach a login page.



- Enpass will show you a list of all matching login items (already saved) for that domain. Select the one you want to sign in with..
- Login details will be filled-in automatically.

13.2.2 Autofilling Credit Cards

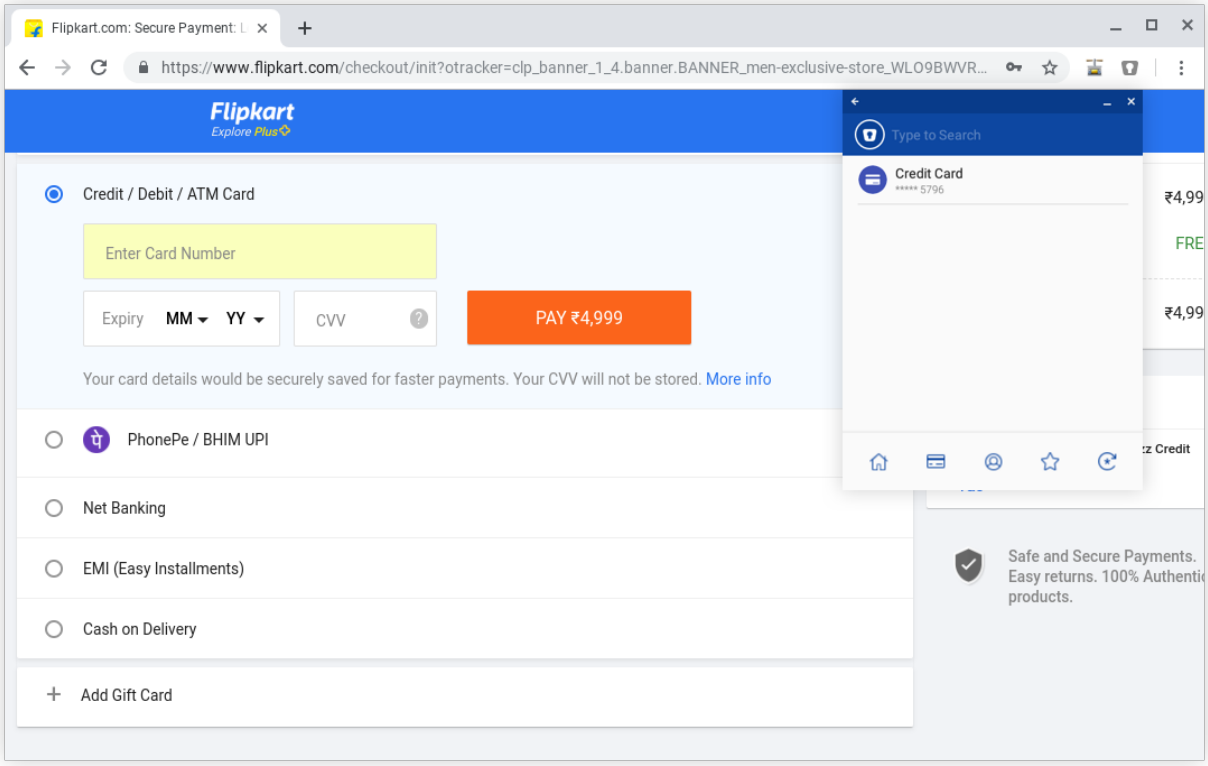
Similar to logins, Enpass also detects the credit cards forms on pages those ask for credit-card information.

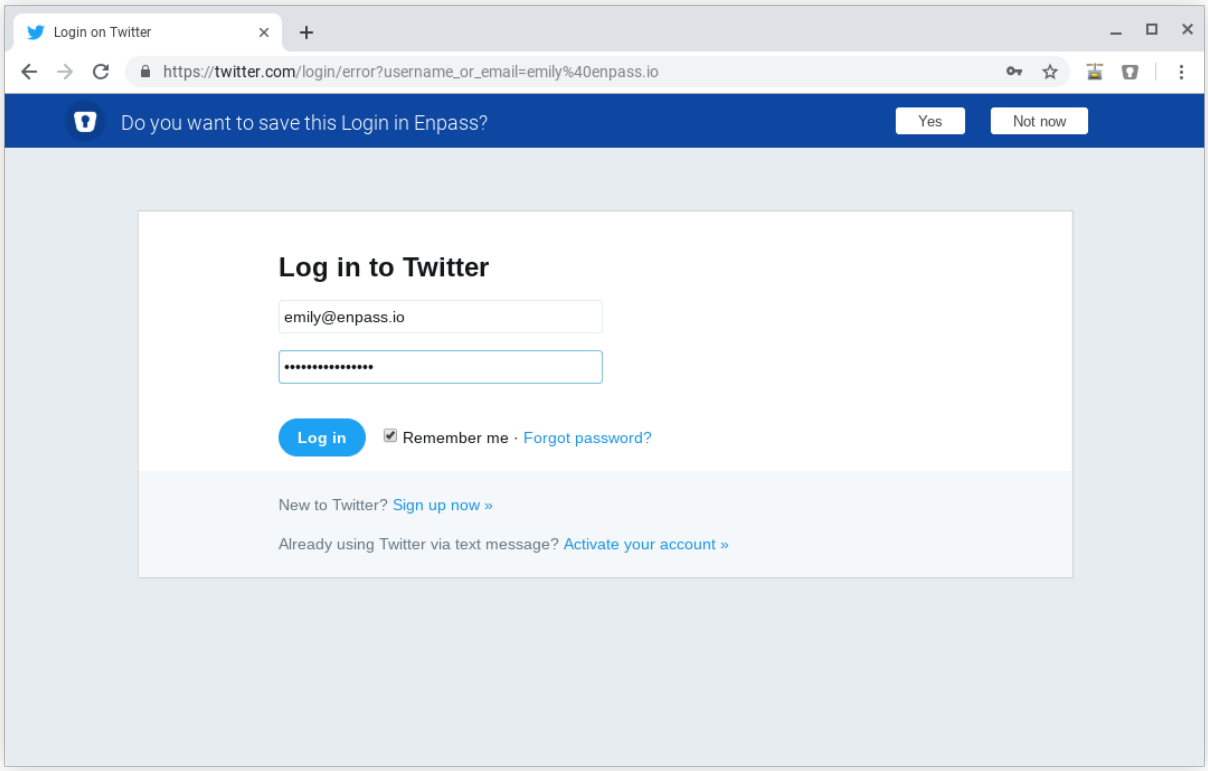
- Click the Enpass icon on browser to launch Enpass extension and it will show the list of saved credit cards.
- Select the card you want to fill with and Enpass will automatically fill the details.

Important: Credit card information will be filled only if the credit card form is in the visible area on the screen. Otherwise, You'll have to scroll the form into visible area to autofill the fields.

13.2.3 Saving New Logins

When you log into any web-page with new information (not saved in Enpass database), Enpass automatically detects the attempt and prompts you to save the information as a new login, and all this without switching to Enpass App.

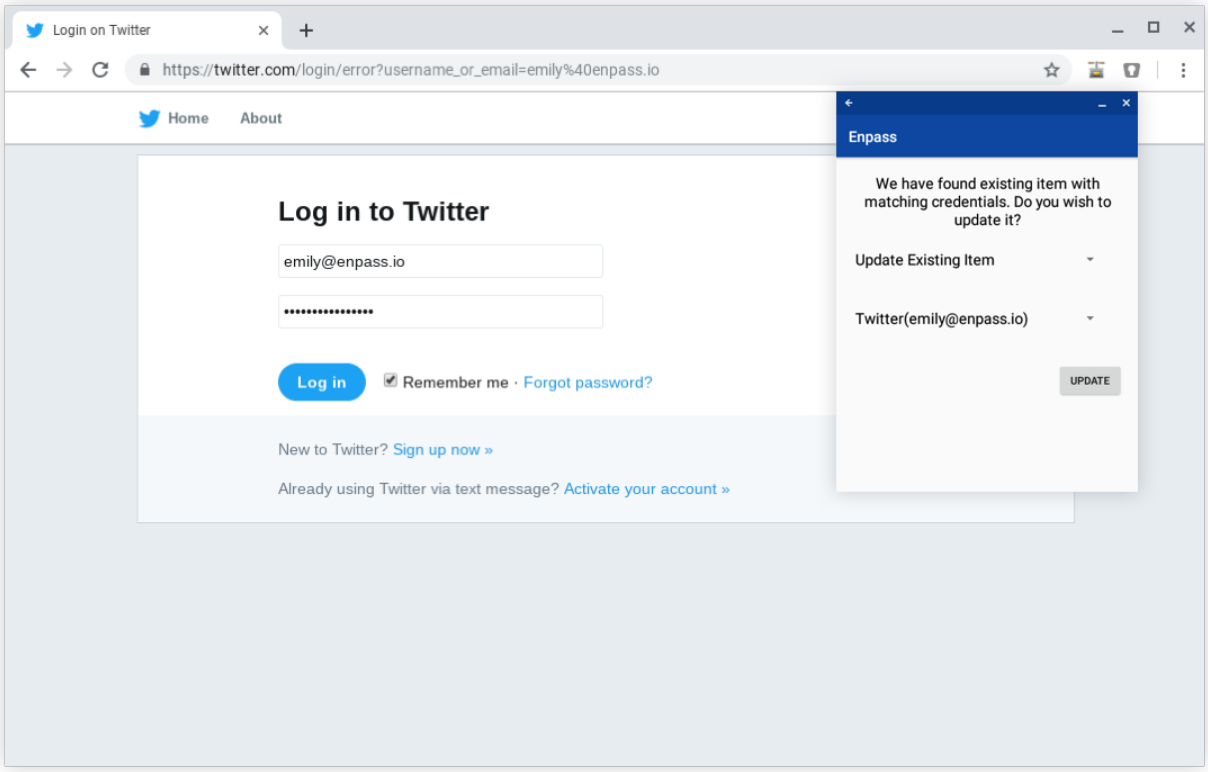

Flipkart.com: Secure Payment:
https://www.flipkart.com/checkout/init?otracker=clp_banner_1_4.banner.BANNER_men-exclusive-store_WLO9BWVR...
Flipkart
Explore Plus
Credit / Debit / ATM Card
Enter Card Number
Expiry MM YY
CVV
PAY ₹4,999
Your card details would be securely saved for faster payments. Your CVV will not be stored. More info
PhonePe / BHIM UPI
Net Banking
EMI (Easy Installments)
Cash on Delivery
Add Gift Card
Type to Search
Credit Card
₹4,99
FRE
₹4,99
Safe and Secure Payments.
Easy returns. 100% Authenti
products.


Login on Twitter
https://twitter.com/login/error?username_or_email=emily%40enpass.io
Do you want to save this Login in Enpass?
Yes
Not now
Log in to Twitter
emily@enpass.io
Log in
Remember me · Forgot password?
New to Twitter? Sign up now »
Already using Twitter via text message? Activate your account »

- Click *Yes* and you'll be prompted to unlock *Enpass extension*.
- Unlock the Enpass extension and click *Save* to save it as a new item in Enpass.

13.2.4 Updating Existing Logins

When you log in to an existing webpage (saved in Enpass database) with a new password, Enpass detects the changes and prompts to update the information. See how:



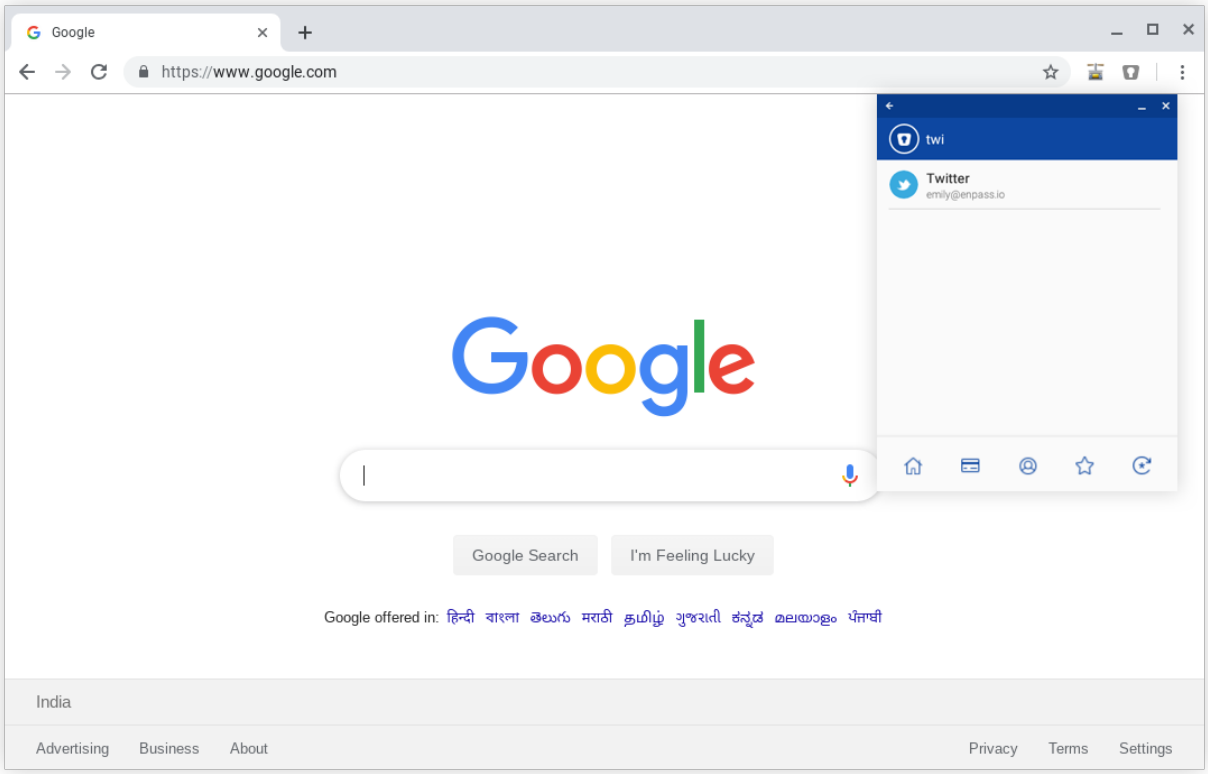
- Go to the login page and fill the login details.
- Click login and a pop-up will appear asking to update the existing item.
- Click *Yes* and you'll be prompted to unlock *Enpass extension*.
- Unlock the Enpass extension and click *Update* to update the item in the Enpass database.
- You can also save this as a new item by selecting the *Save as new item* from the dropdown list in the extension.

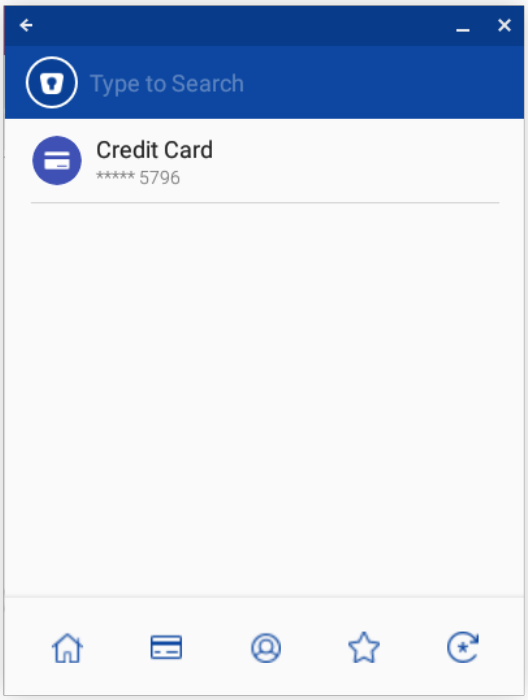
13.2.5 Searching items

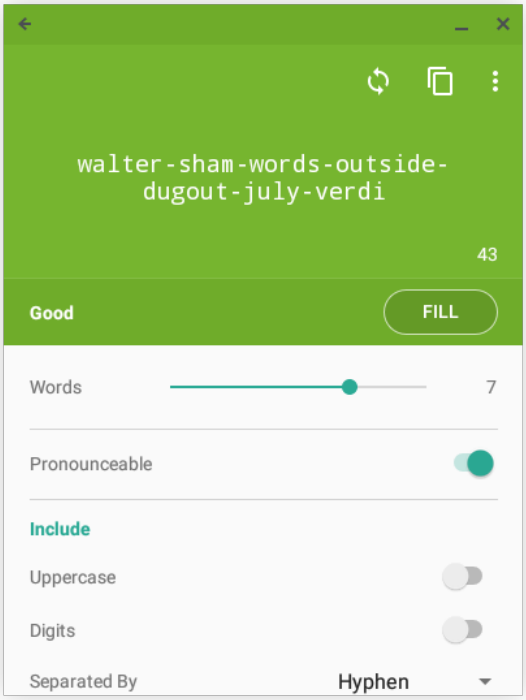
Just click on the Search Bar, and start typing the text you are looking for. Enpass will search in the currently selected vault and will refine the results as you type. You can search the items saved in Enpass database and also sign-in to the web-page using the extension.

13.2.6 Generating Passwords

You can create robust and unique passwords by just clicking on the *Password Generator* icon.


Google
https://www.google.com
twi
Twitter
emily@enpass.io
Google
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
India
Advertising
Business
About
Privacy
Terms
Settings


Type to Search
Credit Card
***** 5796


walter-sham-words-outside-dugout-july-verdi
43
Good
FILL
Words
7
Pronounceable
Include
Uppercase
Digits
Separated By
Hyphen

The password generator in Chromebooks works the same way as the password generator in Android, read more.

CHAPTER

FOURTEEN

SHARE

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

14.1 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.

14.1.1 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.

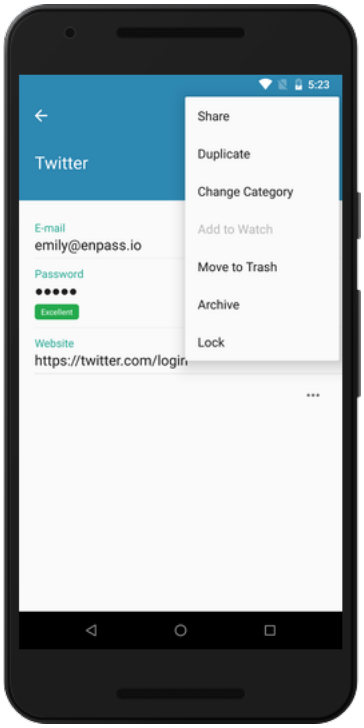
- Open the item which you want to share. Tap on the options menu (3-dots) > Tap on share. An alert with a warning message will appear, tap on *I Understand* > Choose the fields which you want to share > Tap on *Share Button* > Choose the medium to share your item, and finally you can share the item.

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.

14.1.2 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 the menu > Select *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:

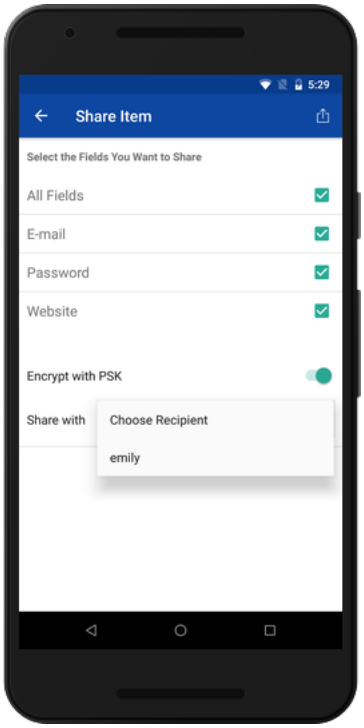
- Always use a secure channel/medium for sharing. i.e., No one must listen in on or temper with the medium.
- Double check that you are sending it to the correct person.
- Delete the shared text after being sent and ask the recipient to delete the same as well after importing the item in their Enpass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

14.2 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.

14.3 Adding by opening link

If the shared item (in scrambled form) is detected as a link, directly tapping 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.

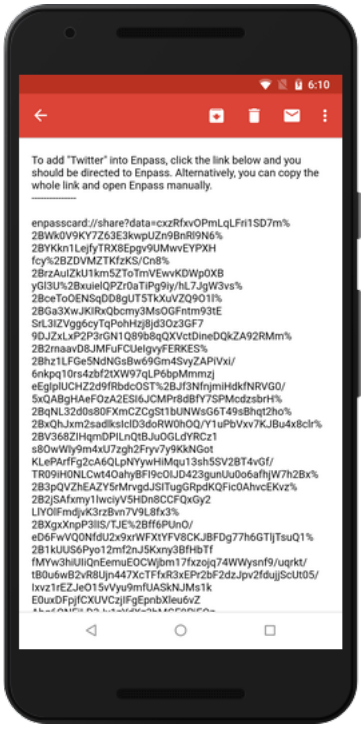
Note: Attachments in the shared item will only be added to Enpass if the item is encrypted with a PSK. Otherwise, only the fields will be added.

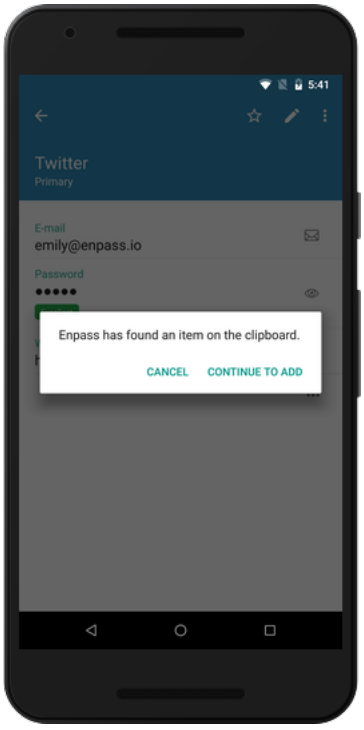
14.4 Adding through clipboard

- Copy the whole shared link on clipboard.
- When you come to the main screen (with the data on clipboard) of Enpass, it automatically detects the information on the clipboard and asks you to add the item to the keychain.

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.


6:10
To add "Twitter" into Enpass, click the link below and you should be directed to Enpass. Alternatively, you can copy the whole link and open Enpass manually.
enpasscard://share?data=cxzRfxvOPmLqLFri1SD7m%
2BWk0V9KY7Z63E3kwpUZn9BnRi9N6%
2BYKkn1LejfyTRX8Epgv9UMwvEYPXH
fcy%2BZDVMZTKfzKS/Cn8%
2BrzAuiZkU1km5ZToTmVEwvKDWp0XB
yGl3U%2BxuielQPZr0aTiPg9ly/hL7JgW3vs%
2BceToOENSqDD8gUT5TkXuVZQ9O1l%
2BGa3XwJKIRxQbcmy3MsOGFntm93tE
SrL3IZVgg6cyTqPohHzj8jd3Oz3GF7
9DJZxLxP2P3rGN1Q89b8qQXVctDineDQkZA92RMm%
2B2rnaavD8JMFuFCUeIgvyFERKES%
2Bhz1LFGe5NdNGsBw69Gm4SvyZAPiVxi/
6nkpq10rs4zbf2tXW97qLP6bgMmmzj
eEglpIUCHZZd9fRbdcOST%2BJf3NfnjmiHdkfNRVG0/
5xQABgHAeFOzA2ESl6JCMPr8dBfY7SPMcdzsbrH%
2BqNL32d0s80FXmCZCgSt1bUNWsG6T49sBhqt2ho%
2BxQhJxm2sadlkskIcID3doRW0hOQ/Y1uPbVxv7KJBu4x8clr%
2BV368ZIHqmDPILnQtBJuOGLdYRCz1
s80wWly9m4xU7zgh2Fryv7y9KkNGot
KLePArfFg2cA6QLpNYywHiMqu13sh5SV2BT4vGf/
TR09iH0NLCwt4OahyBFI9cOIJD423gunUu0o6afhjW7h2Bx%
2B3pQVZhEAZY5rMrvgdJStTugGRpdKQFic0AhvcEKvz%
2B2jSAfxmy1IwciyV5HDn8CCFQxGy2
LIYOlFmdjvK3rzBvn7V9L8fx3%
2BXgxXnpP3lIS/TJE%2Bff6PUnO/
eD6FwVQ0NfdU2x9xrWFXtYFV8CKJBFDg77h6GTIjTsuQ1%
2B1kUUS6Pyo12mf2nJ5Kxny3BfHbTf
fMYw3hiUIiQnEemuEOCWjbm17fxzojq74WWysnf9/uqrkt/
tB0u6wB2vR8Ujn447XcTFfxR3xEPr2bF2dzJpv2fdujjScUt05/
lxvz1rEZJeO15vVyu9mfUASkNJMs1k
E0uxDFpjfCXUVCzjIFgEpnbXleu6vZ


5:41
Twitter
Primary
E-mail
emily@enpass.io
Password
Enpass has found an item on the clipboard.
CANCEL
CONTINUE TO ADD

14.5 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.

- Tap on the attachment you want to share. You will be provided with the preview of the attachment.
- Tap 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.

CHAPTER

FIFTEEN

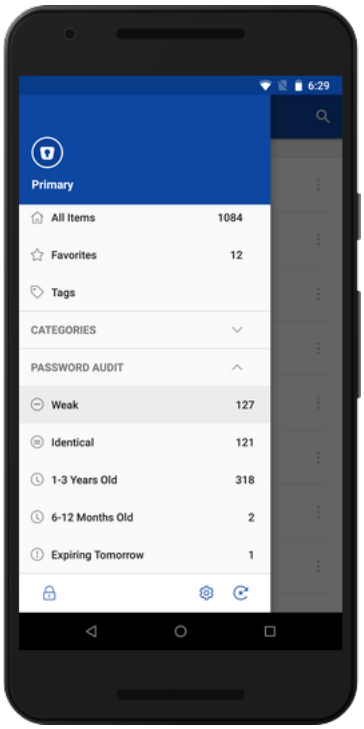
PASSWORD AUDIT

Password Audit in Enpass is a local scanning process to look for weak, identical, expiring and old passwords, and categorizes them accordingly. It helps you keep a regular check on your passwords to avoid any compromise in data security and last moment rush to change expired passwords.

15.1 Weak Passwords

- To check all the weak passwords in Enpass, go to the sidebar > `Password Audit` and tap on *Weak*.

Note: Passwords those found as pwned will also be listed there as weak. Please note that you need to *manually check for pwned passwords* as Enpass will not itself connect to haveibeenpwned.com to check pwnage of your passwords.

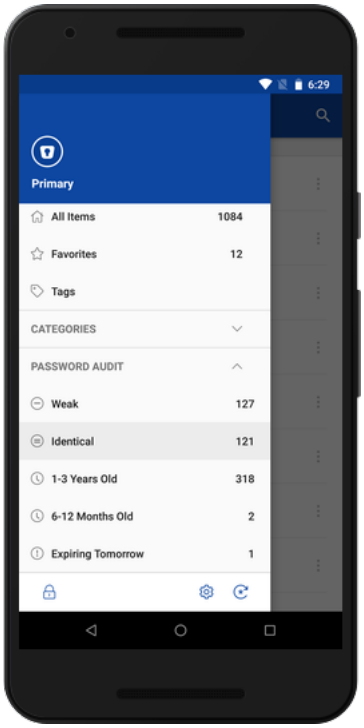


Tip: Enpass lets you mark the items which you want to exclude from Password audit. the *password field* of the item.

15.2 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. Password Audit finds all such items having identical passwords. You can change them to strong and unique passwords using the built-in password generator of Enpass.

- To check all the identical passwords in Enpass, go to the sidebar > `Password Audit` and tap on Identical. You can now see the list containing all the items having matching passwords. All such items will be separated by list headers mentioning first two letters of password and count of such items.



15.3 Old Passwords

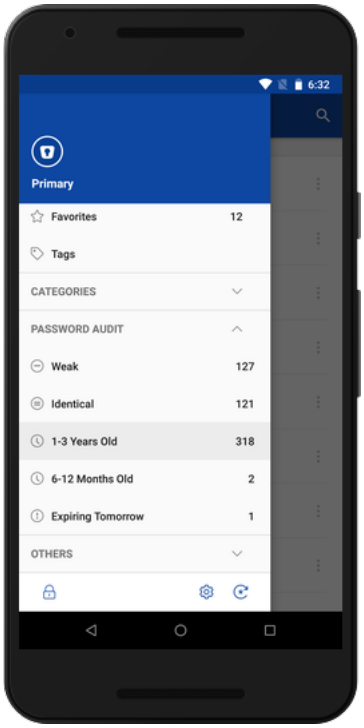
Password Audit in Enpass also categorizes your passwords based on their age in Enpass. They are categorized as

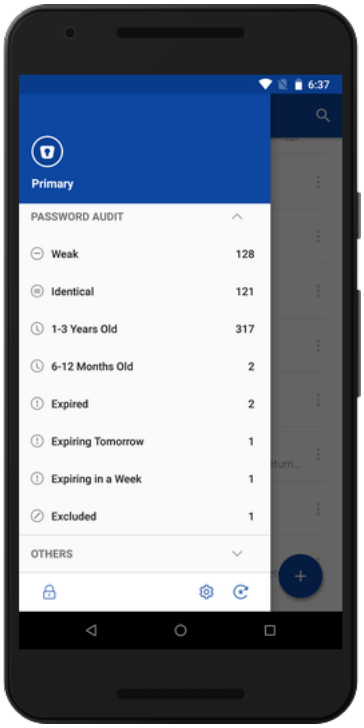
- 3+ years old
- 1-3 years old
- 6-12 months old
- 3-6 months old

15.4 Expiring Passwords

If you have set the *expiry date* to passwords, you'll be able to see the passwords those are expired or expiring in a day, week, or month.

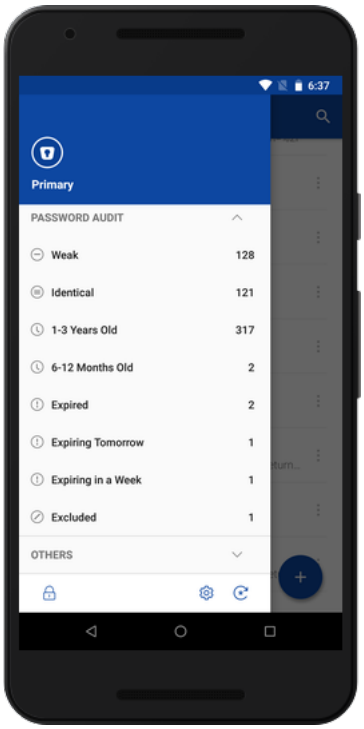
- To check for expiry of passwords in Enpass, go to the sidebar > `Password Audit`. You can now choose any of the expiring password lists.


6:32
Primary
Favorites 12
Tags
CATEGORIES
PASSWORD AUDIT
Weak 127
Identical 121
1-3 Years Old 318
6-12 Months Old 2
Expiring Tomorrow 1
OTHERS


6:37
Primary
PASSWORD AUDIT
Weak 128
Identical 121
1-3 Years Old 317
6-12 Months Old 2
Expired 2
Expiring Tomorrow 1
Expiring in a Week 1
Excluded 1
OTHERS

15.5 Excluded Passwords

Items those you have *excluded* from the Passwords Audit will be listed under a separate list of *Excluded Passwords*.



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

CHAPTER

SIXTEEN

SETTINGS OVERVIEW

Following are the settings that you can alter in Enpass.

16.1 Registration status

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

16.2 Lock Now

Tap the lock icon to lock the device immediately.

16.3 Working with vaults

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

16.3.1 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*.

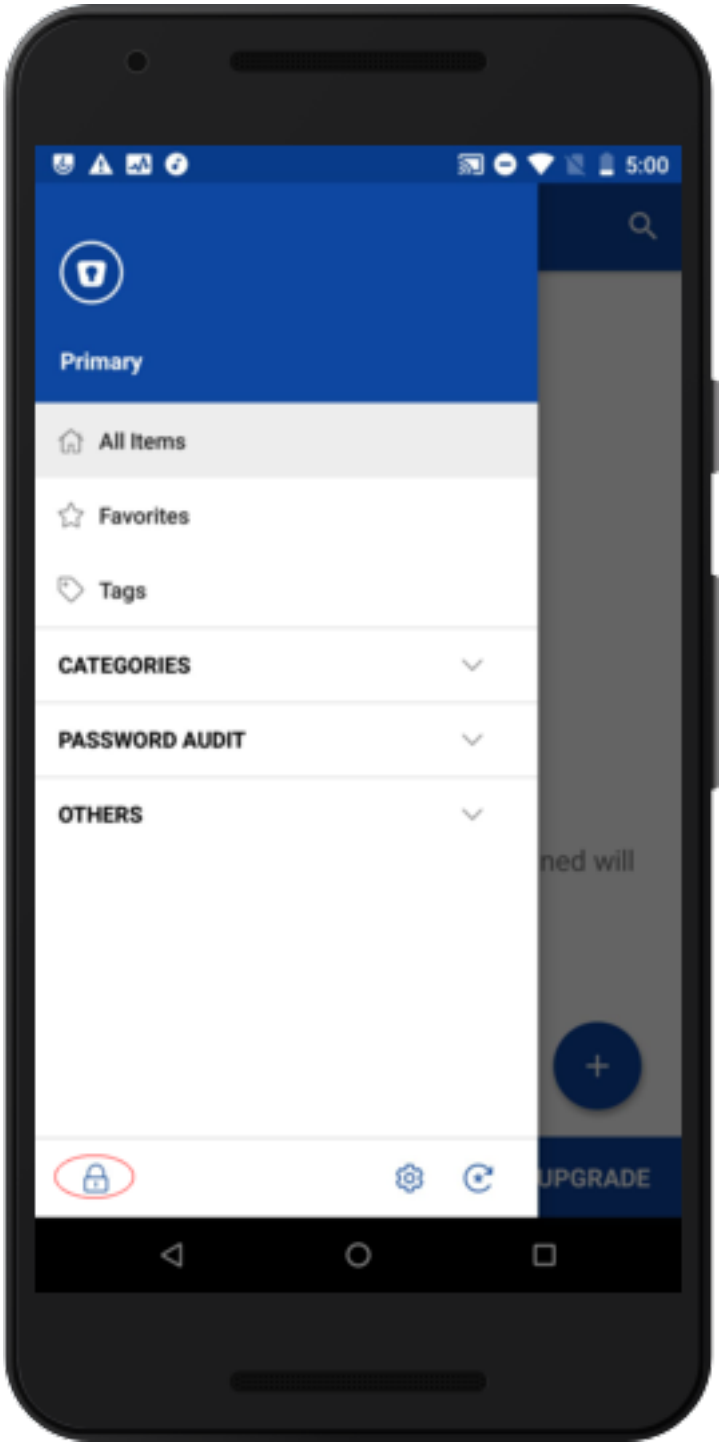
16.3.2 Managing Multiple Vaults

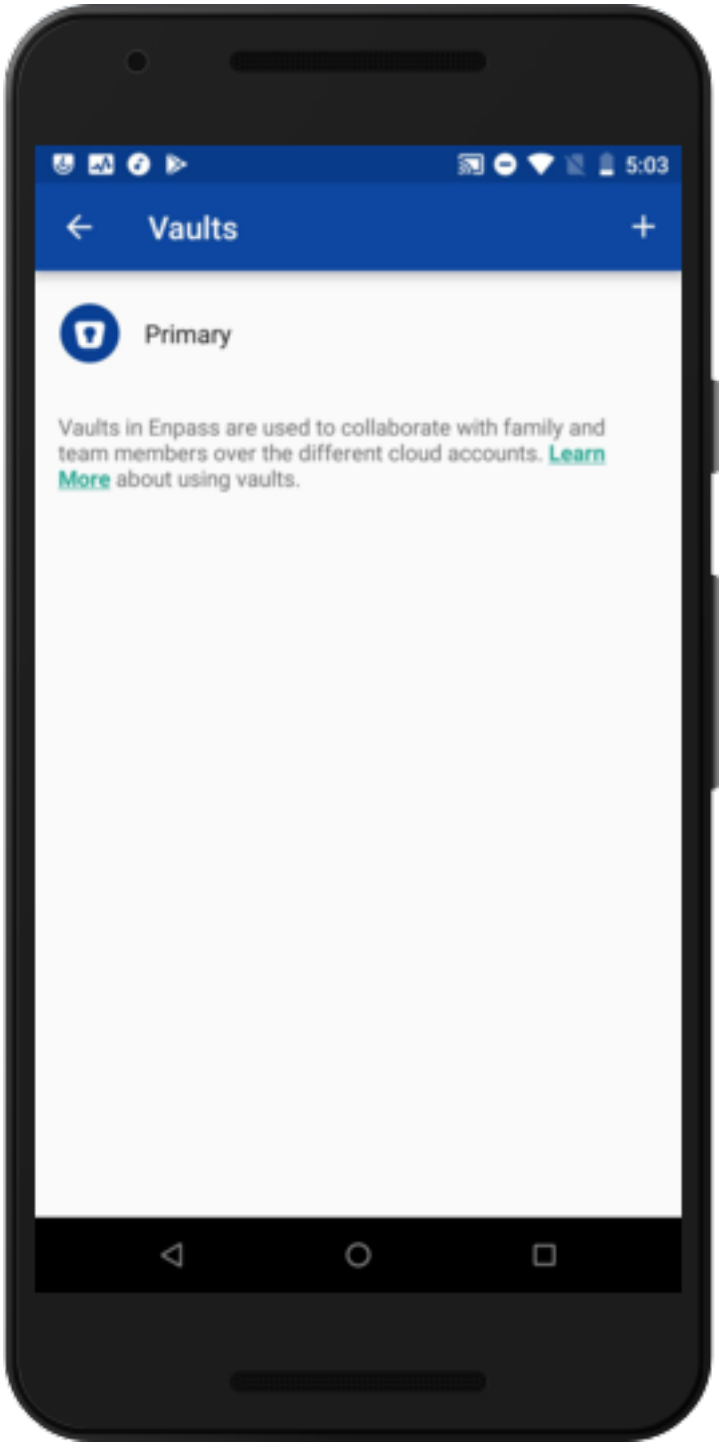
If you created any secondary vault, you will have multiple vaults. The following sections describe the settings for multiple vault users.

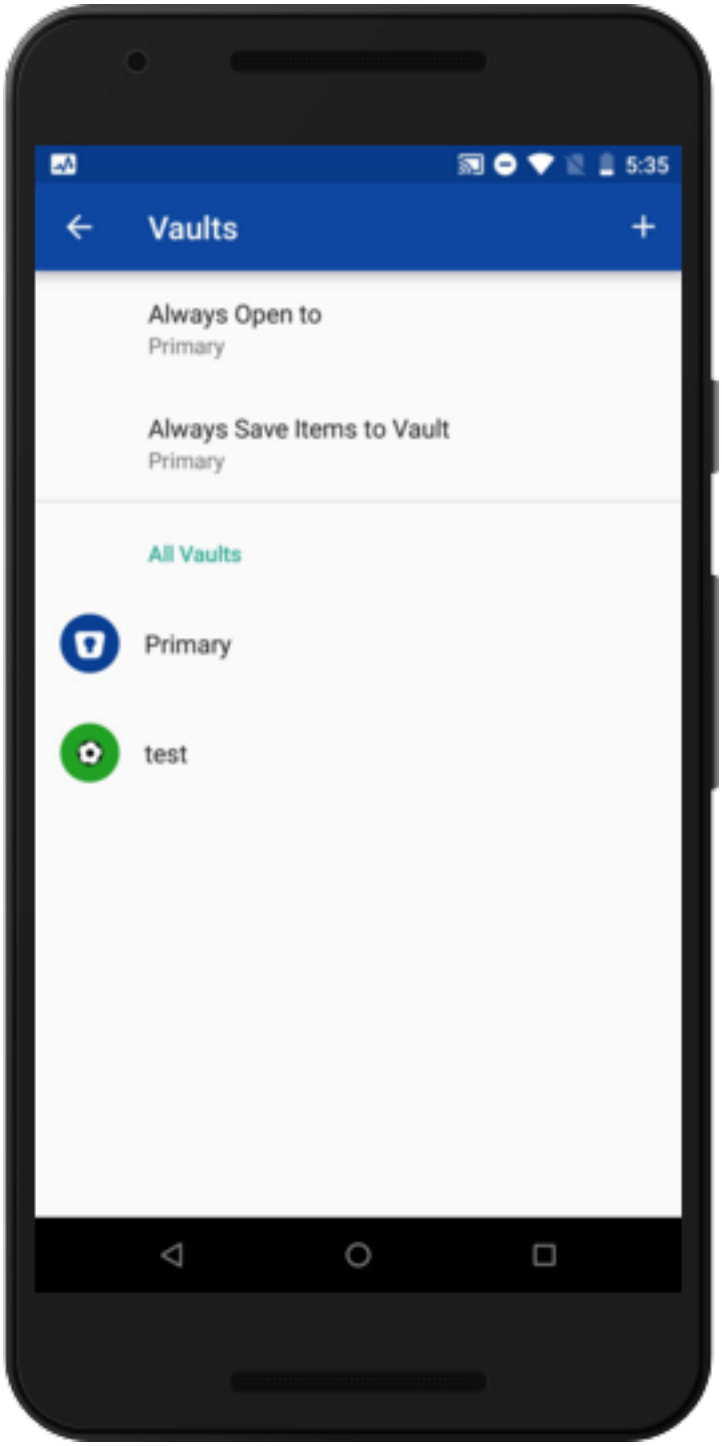
16.3.3 Always Open to

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

1. Go to **Settings**.
2. Tap **Vaults > Always Open to** and choose the vault.


5:00
Primary
All Items
Favorites
Tags
CATEGORIES
PASSWORD AUDIT
OTHERS
ned will
UPGRADE


5:03
Vaults
Primary
Vaults in Enpass are used to collaborate with family and team members over the different cloud accounts. Learn More about using vaults.


5:35
Vaults
Always Open to
Primary
Always Save Items to Vault
Primary
All Vaults
Primary
test

16.3.4 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.

1. Go to **Settings**.
2. Tap **Vaults > Always Save Items to Vault** and choose the vault.

16.3.5 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 > Optionlly you may choose to save this vault password as an item in the Primary vault, otherwise tap *Continue*. Done.

Changing 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.

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 Sync

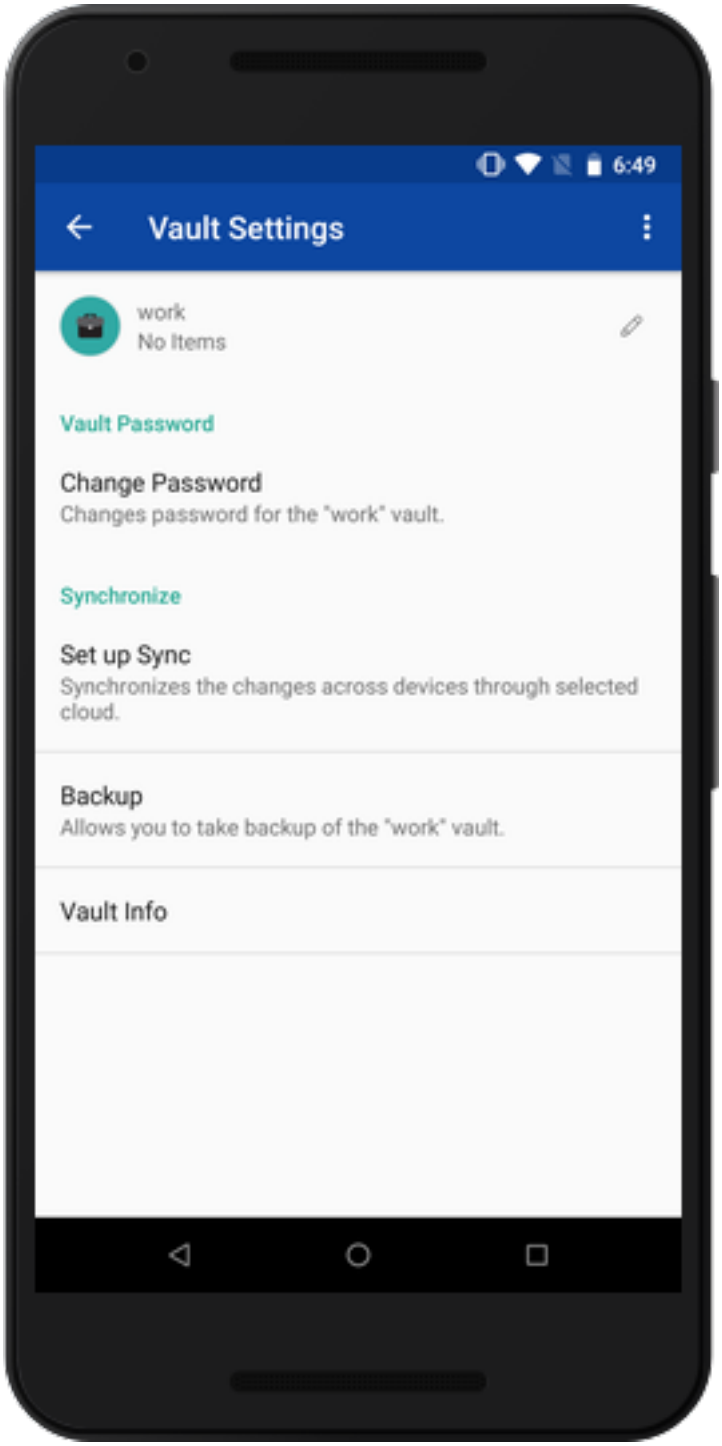
Following steps will guide you through the cloud sync process:

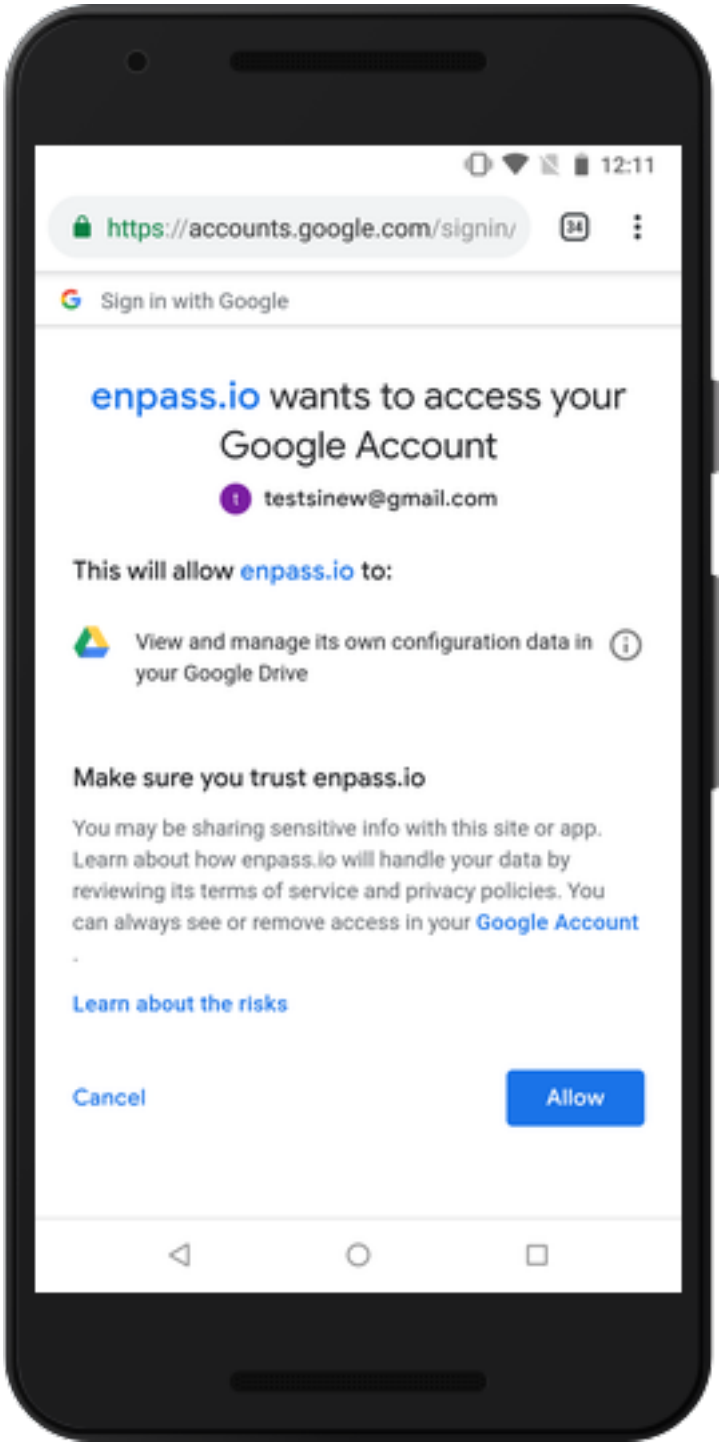
- Select your cloud from the list. You will be directed to the authentication screen of that cloud. Enter your credentials in its login screen. Grant permissions to the cloud to continue with the sync process. Your data will be synced successfully.

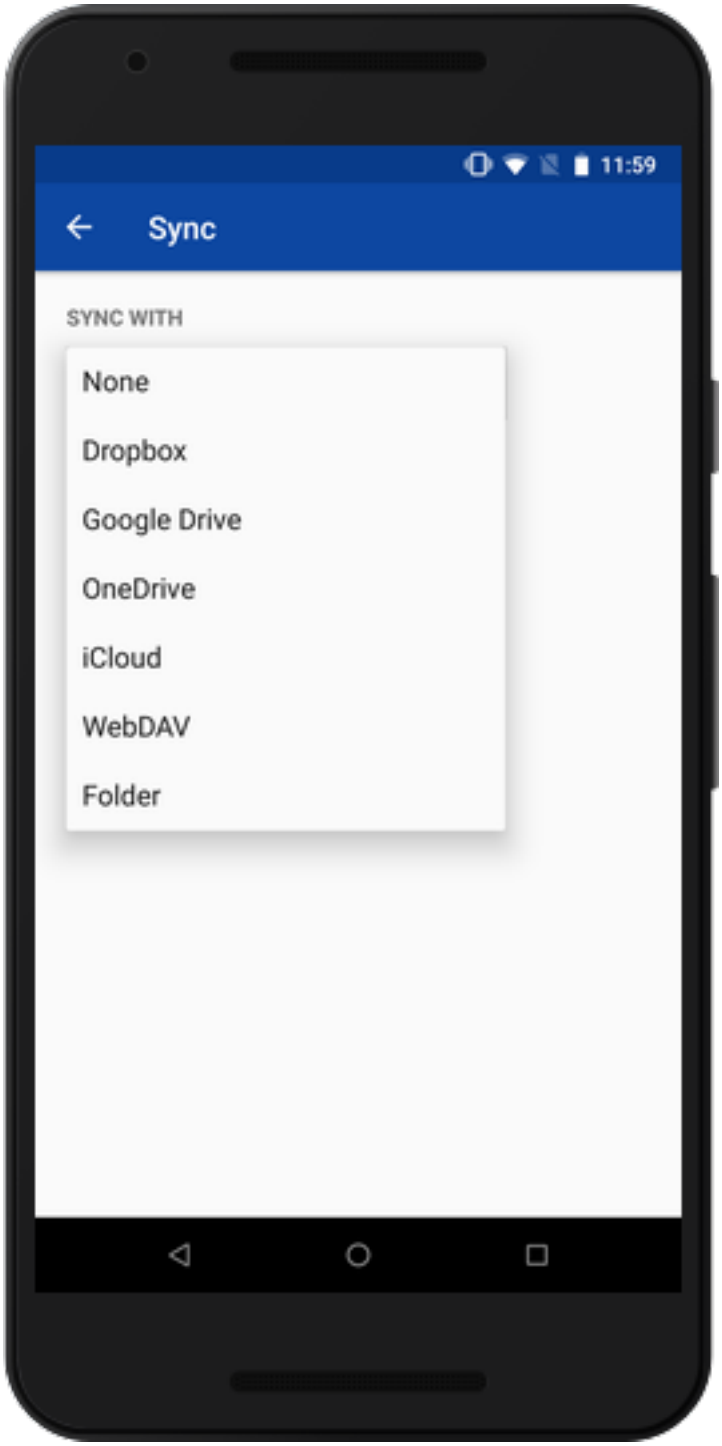
Folder Sync

Enpass provides the ability to sync Enpass data locally to any folder on your device. Just tap on the *SYNC WITH* drop-down bar and select *Folder* from the list. It will open the local storage directory where you can choose any folder of your choice or even create a new one to sync the Enpass data.

Once you've selected the Folder to sync the data, tap on *Done*. It will automatically sync the data and create a *sync_default.walletx* file in that folder.


6:49
Vault Settings
work
No Items
Vault Password
Change Password
Changes password for the "work" vault.
Synchronize
Set up Sync
Synchronizes the changes across devices through selected cloud.
Backup
Allows you to take backup of the "work" vault.
Vault Info


12:11
https://accounts.google.com/signin/
Sign in with Google
enpass.io wants to access your Google Account
testsinew@gmail.com
This will allow enpass.io to:
View and manage its own configuration data in your Google Drive
Make sure you trust enpass.io
You may be sharing sensitive info with this site or app. Learn about how enpass.io will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account .
Learn about the risks
Cancel
Allow


11:59
Sync
SYNC WITH
None
Dropbox
Google Drive
OneDrive
iCloud
WebDAV
Folder

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 device'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. Deselect the option if you don't want to save the password. Tap on *Remove* button, and done.

16.4 General

This section deals with the *General* settings in your Enpass app.

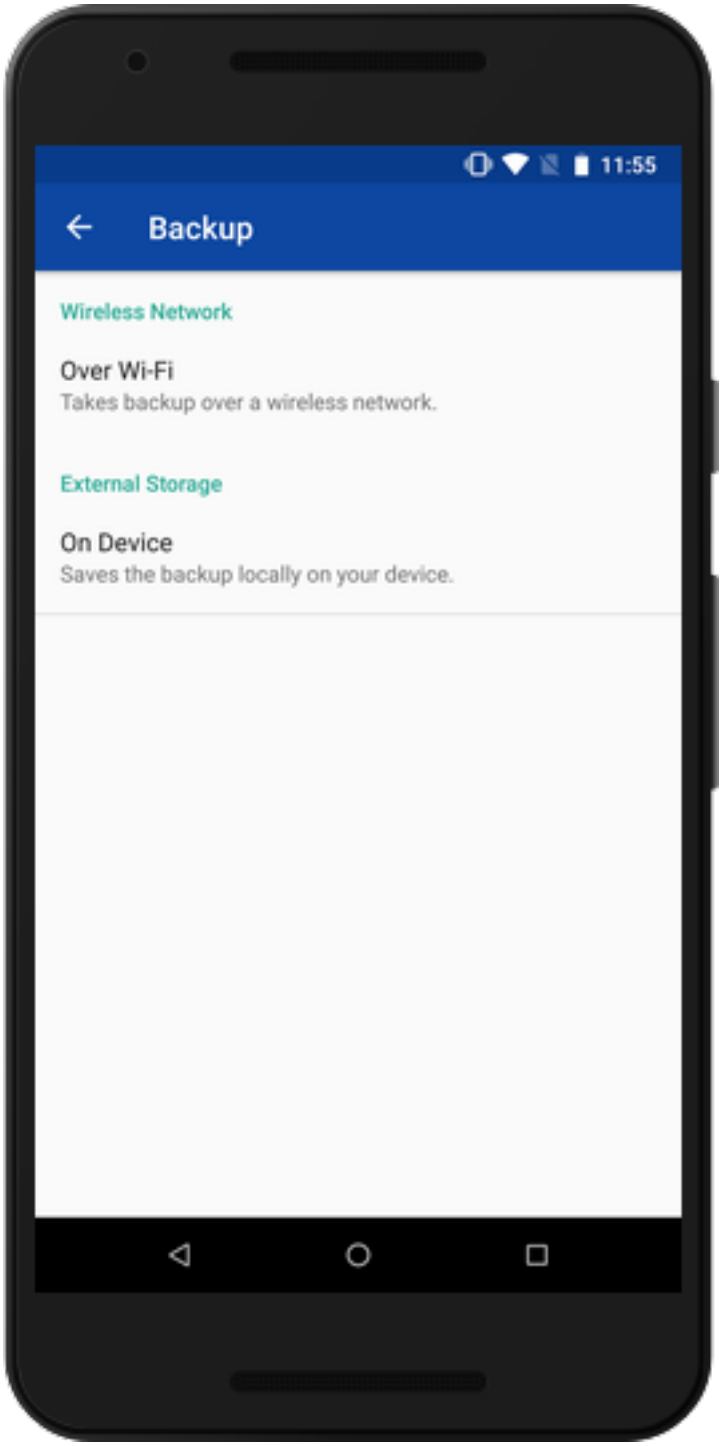
16.4.1 Unlock Sound

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

16.4.2 Use Dark Theme

Tap on *Use Dark Theme* to enable dark theme in Enpass.


11:41
Backup over Wi-Fi
Enpass backup service has been started. Please enter the following address in the browser address bar.
http://105.0.0.103:53036
Remark: Make sure that the Wi-Fi network connected to this device is same as that of the other on which you want to take the backup or restore data from.


11:55
Backup
Wireless Network
Over Wi-Fi
Takes backup over a wireless network.
External Storage
On Device
Saves the backup locally on your device.

16.4.3 Use Website Icons

Please see *Customizing Icons*.

16.4.4 Show Items Count in Sidebar

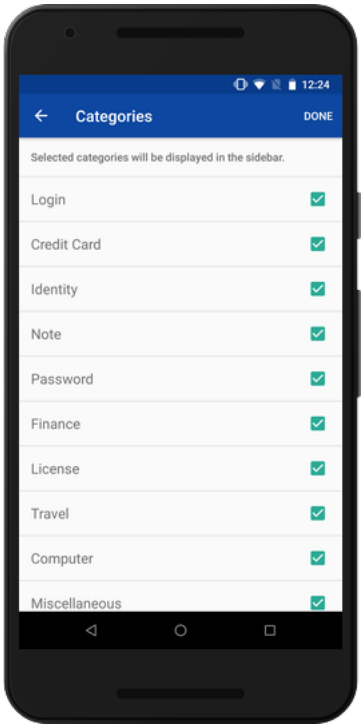
Enabling this will show the total count of items for each category in the sidebar.

16.4.5 Search in All Items

Enabling this will allow Enpass to perform the search in all items in the selected vault.

16.4.6 Hide Categories

Here you can unselect the categories which you want to hide from the sidebar. Tap on *Categories* and unselect the categories you want to hide.

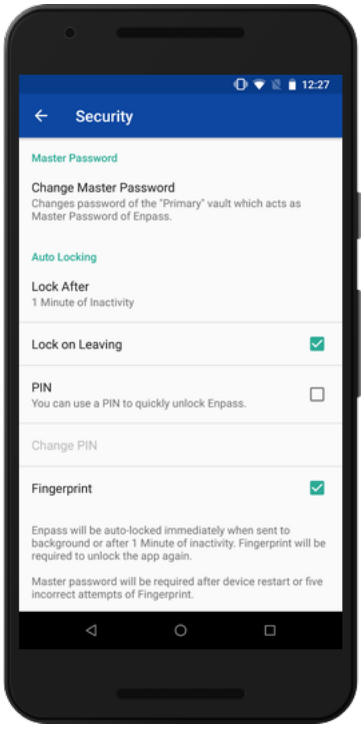


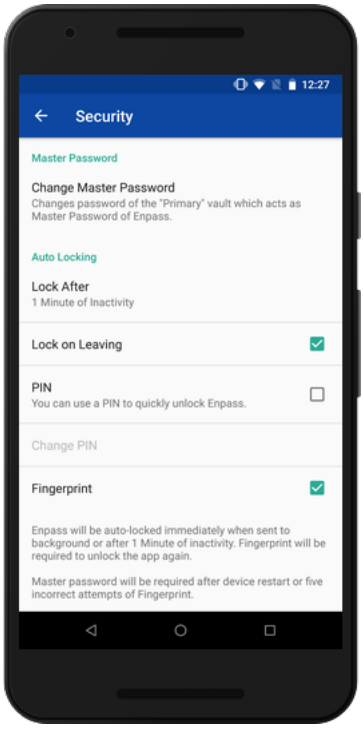
16.5 Security

This section deals with the security settings of Enpass.

16.5.1 Change Master Password

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


12:27
Security
Master Password
Change Master Password
Changes password of the "Primary" vault which acts as Master Password of Enpass.
Auto Locking
Lock After
1 Minute of Inactivity
Lock on Leaving
PIN
You can use a PIN to quickly unlock Enpass.
Change PIN
Fingerprint
Enpass will be auto-locked immediately when sent to background or after 1 Minute of inactivity. Fingerprint will be required to unlock the app again.
Master password will be required after device restart or five incorrect attempts of Fingerprint.


12:27
Security
Master Password
Change Master Password
Changes password of the "Primary" vault which acts as Master Password of Enpass.
Auto Locking
Lock After
1 Minute of Inactivity
Lock on Leaving
PIN
You can use a PIN to quickly unlock Enpass.
Change PIN
Fingerprint
Enpass will be auto-locked immediately when sent to background or after 1 Minute of inactivity. Fingerprint will be required to unlock the app again.
Master password will be required after device restart or five incorrect attempts of Fingerprint.

Note: If you have enabled *sync*, the new master password will be updated to the cloud during next sync operation. Also, other devices syncing with that cloud will ask for this new password.

16.5.2 Auto Locking

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

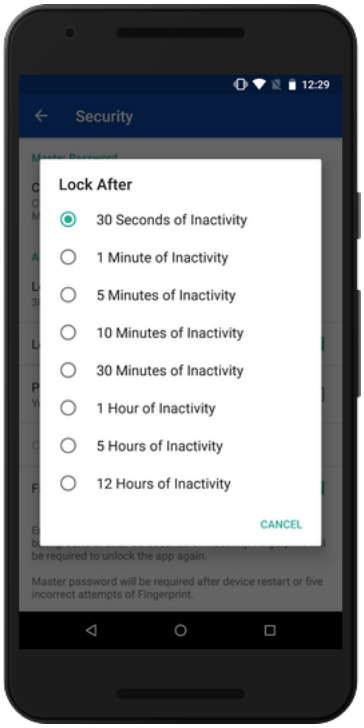
By default, you are supposed to enter the master password for unlocking the app. This could be a tedious process, especially when you have to authenticate every autofill activity while autofilling using your master password.

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

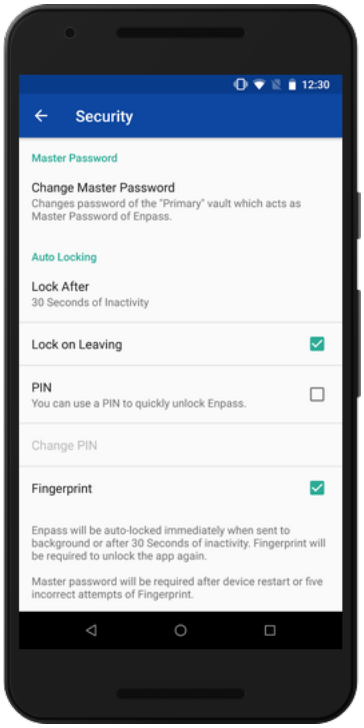
The default setting is **30 Seconds of Inactivity**, which means that Enpass auto locks itself if left unattended for 30 Seconds.



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.



16.5.3 PIN

The master password is set as the default authentication requirement. You can avoid entering your master password altogether by using a 4-10 digit 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.

16.5.4 Fingerprint

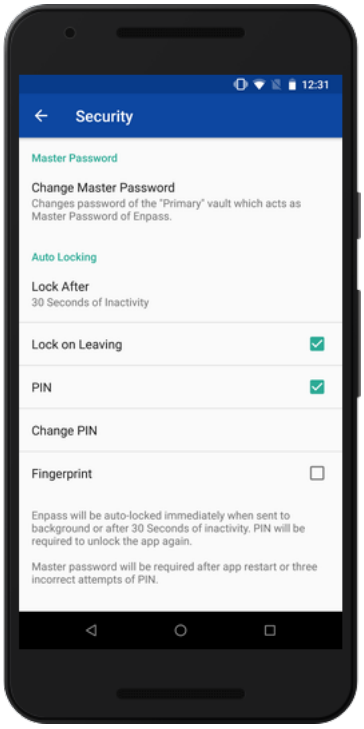
Enpass supports the built-in Fingerprint sensor. That means you can use your fingerprint instead of passwords to unlock Enpass.

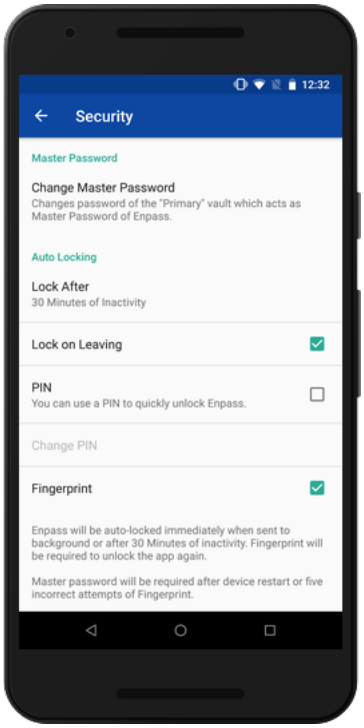
Using Fingerprint has two significant benefits:

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

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

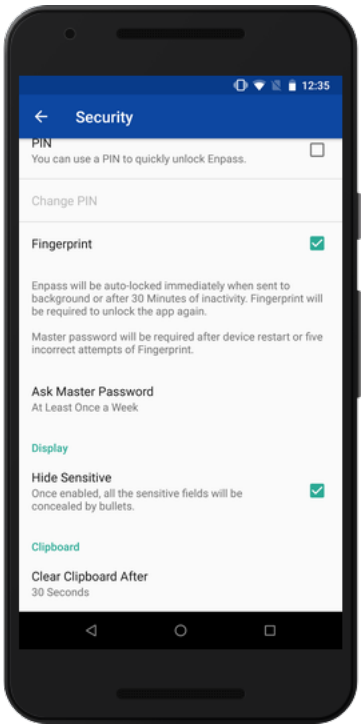
Note: You cannot use Fingerprint and PIN together.


12:31
Security
Master Password
Change Master Password
Changes password of the "Primary" vault which acts as Master Password of Enpass.
Auto Locking
Lock After
30 Seconds of Inactivity
Lock on Leaving
PIN
Change PIN
Fingerprint
Enpass will be auto-locked immediately when sent to background or after 30 Seconds of inactivity. PIN will be required to unlock the app again.
Master password will be required after app restart or three incorrect attempts of PIN.


12:32
Security
Master Password
Change Master Password
Changes password of the "Primary" vault which acts as Master Password of Enpass.
Auto Locking
Lock After
30 Minutes of Inactivity
Lock on Leaving
PIN
You can use a PIN to quickly unlock Enpass.
Change PIN
Fingerprint
Enpass will be auto-locked immediately when sent to background or after 30 Minutes of inactivity. Fingerprint will be required to unlock the app again.
Master password will be required after device restart or five incorrect attempts of Fingerprint.

16.5.5 Hide Sensitive

Enable this setting to conceal all sensitive fields by bullets.



16.5.6 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**.

16.6 Enpass for Android Watch

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

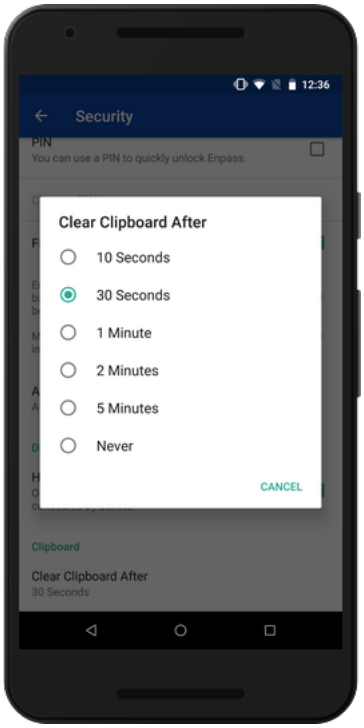
16.6.1 Enabling Enpass for Android Watch

For setting Enpass for Android Watch all you need is Enpass App installed on your device and an Android Watch.

- Pair your Android Watch with your Android Phone → Open Enpass on your Android Phone → Go to Enpass Settings and select **Android Watch** → Enable Android Watch.
- Enable PIN code (optional) and use it to unlock Enpass on Android Watch.

Note: For security reasons we strongly recommend you to create a PIN to unlock Enpass App on Android Watch.

- Enable *Show TOTP Only* and Android Watch will show the TOTP of the item, hiding all other fields.



16.6.2 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 Sidebar → `OTHERS` → `Android watch`.
- All the selected items will be added into the Watch folder and they will be displayed in Enpass for Android Watch.

16.6.3 Security

Android Watch works through the Android Phone to which it is paired. It communicates securely only with that device over bluetooth using Android Wearable Data Layer API.

Only those items are accessible on Watch which you added to `Android Watch` for sharing. These shared items are not as secured as rest of the items as they are no more being protected by your master password. Infact they are stored in watch itself, which is protected by your watch os. However, these items do not leave the watch in any case.

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 Android watch with great attention and care.

16.7 Autofill Settings

Go to *this section* of user-manual to access the Atutofill settings of Enpass.

16.8 Advanced

This section deals with the Advanced Settings of Enpass.

16.8.1 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.

16.8.2 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.

16.8.3 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.

16.8.4 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*.

16.8.5 Allow Screenshots

Enabling this will let you take screenshot and record screen of Enpass. The last accessed screen will also stay visible in the background tasks.

16.8.6 Language

You can set the default language for Enpass from here.

16.8.7 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.