



**PASSWORD
DEPOT**
BY AceBIT

Password Depot for iOS

Quick Start Guide – iOS

As of: January 26, 2026

This guide shows the most important steps to use Password Depot on iOS securely—without any technical prior knowledge.

Table of Contents

Table of Contents	2
Introduction.....	4
Key terms.....	4
Getting started	5
Start the app and find your way around	5
Open or create a database	7
Open an existing database	8
Create a new database.....	9
Unlock a database	10
Quickly open recently used databases.....	11
Configure security and convenience settings.....	12
General	13
Storage	17
Biometrics.....	17
Appearance	18
Security.....	18
Search	18
Use key files.....	19
Create a key file	19
Back up or share an existing key file	20
Use a key file in a database	21
Core functions	22
Content overview: folders, search, sorting and favorites	22
Create and organize folders	23
Search	24
Sort and group.....	26
Use favorites.....	27
Delete entries and select multiple items	28
Create entries	29
Edit entries and important fields.....	31
Categories, tags and expiration date.....	32
Password Generator.....	33
URL and integrated web browser.....	34
Auto-fill in the integrated web browser.....	35

TOTP: Generate one-time codes in the app.....	37
Manage TAN list	39
Add custom fields.....	40
Store certificates/key files in entries.....	41
Links: reference an entry instead of duplicating it.....	42
Second password: extra protection for sensitive entries.....	43
Templates and custom entries.....	44
Manage templates	44
Create a custom entry	45
Use entries day to day.....	46
Copy user name and password	46
Open documents	47
Open links	48
Protect and manage the database	49
Save	50
Create and restore backups	50
Lock and unlock	51
Refresh	51
Change the master password.....	51
Export	52
Close database	53
Database properties.....	53
Storage locations and synchronization	54
Connect and disconnect cloud storage	54
FTP and WebDAV Servers.....	55
Enterprise Server (company).....	56
Tips	58
Secure on the go: the most important rules	58
Organization: find faster instead of searching	58
Quickly solve common problems	58
Help and Support.....	58

Introduction

With Password Depot, you store passwords and other confidential information in an encrypted database that you can access from anywhere. You open this database with your master password – optionally also with a key file (two-factor authentication).

IMPORTANT: Without your database master password, your data cannot be recovered. Choose a strong password that you can keep safe.

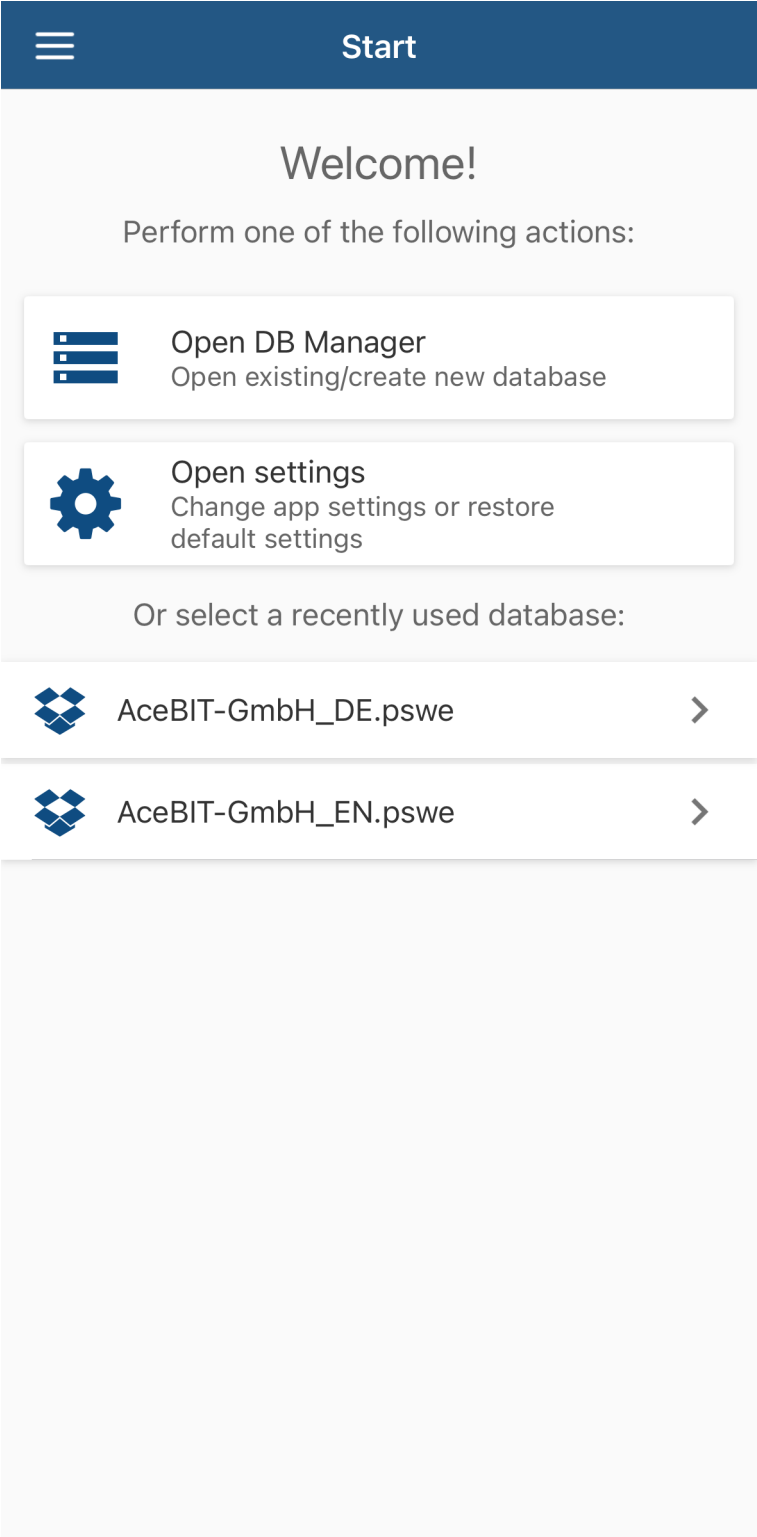
Key terms

- **Database:** Your encrypted file containing all entries (e.g., "Private.psw").
- **Master password:** The primary password used to open the database.
- **Key file:** An additional file used as a second factor to open the database (2FA = two-factor authentication).
- **Entry:** A stored item, e.g., password, credit card or identity.
- **Folder:** Allows you to group entries (e.g., "Work", "Private").
- **Favorites:** Provide quick access to frequently used entries.
- **TOTP:** A time-based one-time code for 2FA logins.

Getting started

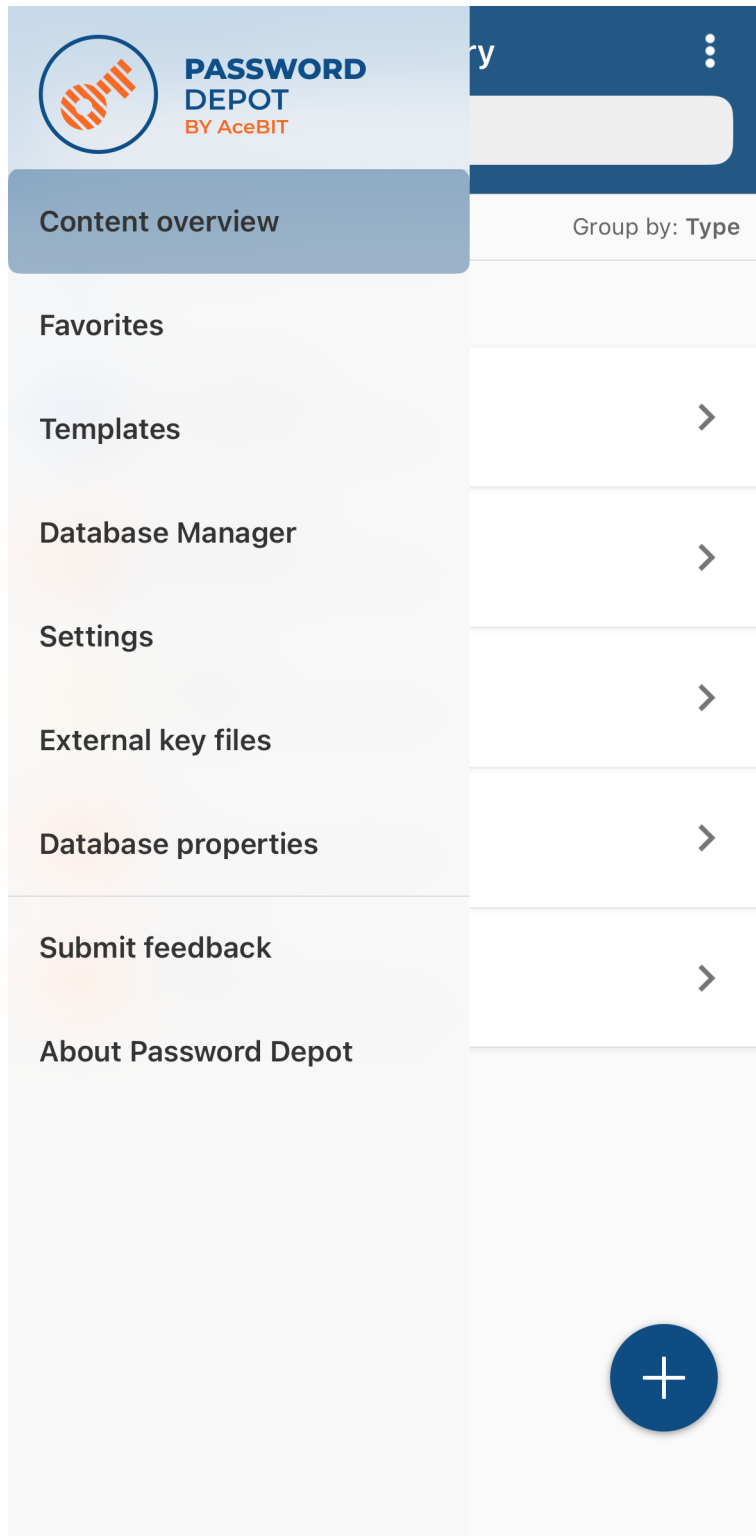
Start the app and find your way around

After launching, you will see the "Welcome!" screen. From here, you can open recently used databases or switch to the **Database Manager** (via **Open DB Manager**).



How to open the side menu:

- Tap the menu icon (☰) in the top-left.
- Select the desired area, e.g., **Content overview** or **Settings**.

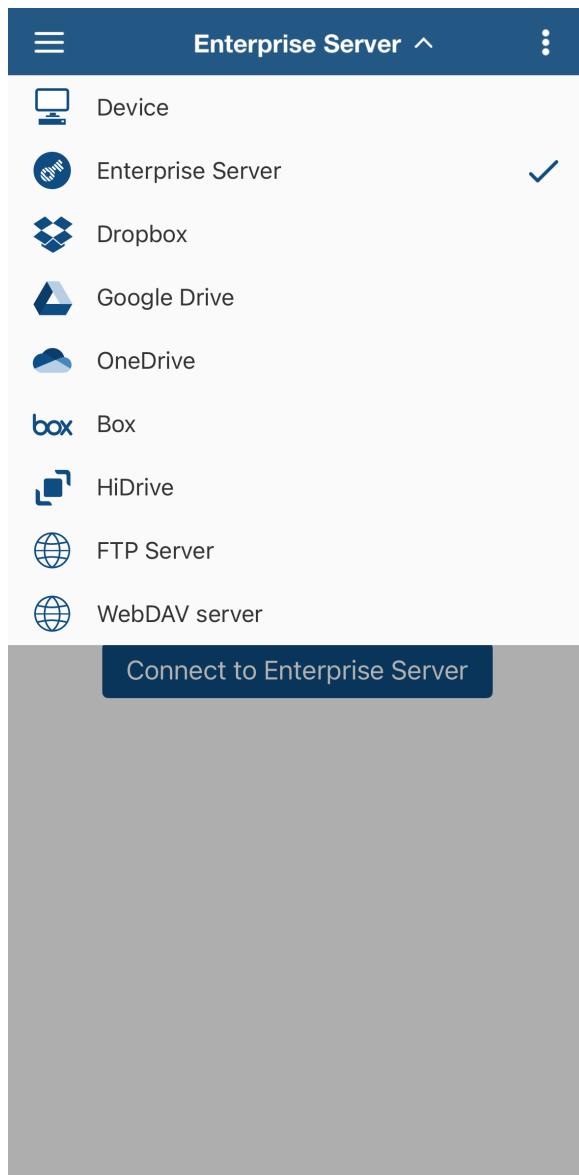


Key sections in the menu:

- **Start** – Takes you back to the "Welcome" screen.
- **Content overview** – Shows folders and entries for the currently opened database.
- **Favorites** – Shows your most important entries in one place.
- **Templates** – Manage custom entry templates.
- **Database Manager** – Open or create databases on the device, in the cloud or on the Enterprise Server.
- **Settings** – Security and convenience settings.
- **External key files** – Manage key files (if used).
- **Database properties** – Settings for the currently opened database (e.g., enabling a second password).

Open or create a database

In the **Database Manager**, first select the desired storage location using the down arrow in the top bar. You will then see the available databases or can create a new one.



Available storage locations:

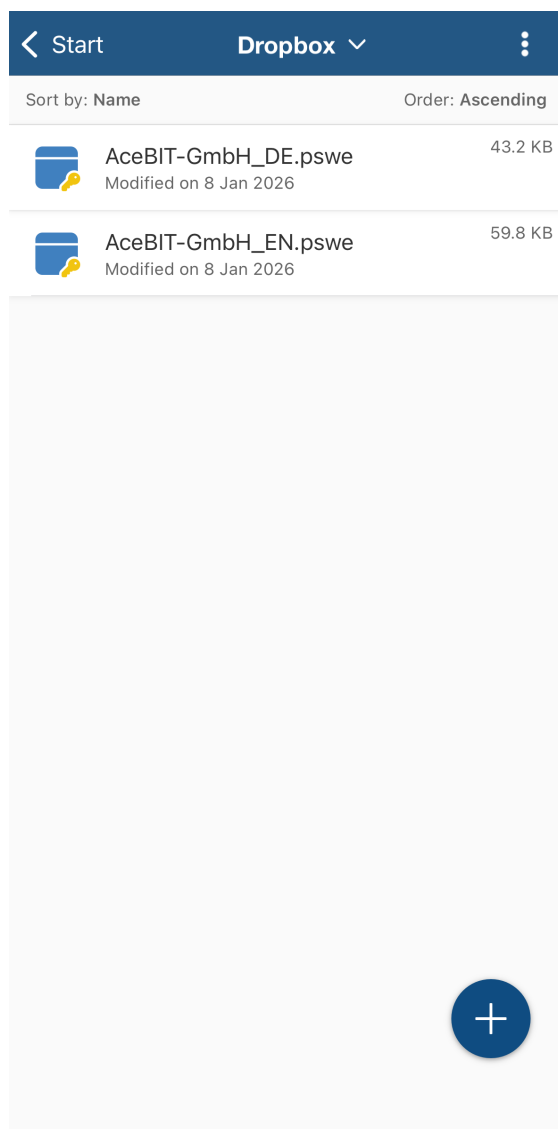
- **Device** – Databases stored directly on your iPhone/iPad.
- **Dropbox / Google Drive / OneDrive / Box / HiDrive** – Databases in your chosen cloud.
- **FTP Server (FTP) / WebDAV Server (WebDAV)** – Databases on a server in the network/Internet.
- **Enterprise Server** – If your company uses Password Depot, databases can be stored centrally on the Enterprise Server and shared with you.

TIP: If you are new, start with the storage location **Device**. You can copy or sync your database to another location at any time later.

Open an existing database

To open an existing database:

- Open **Menu (☰)** → **Database Manager**.
- Select the storage location at the top (e.g., "Device" or "Dropbox").
- If needed: Tap **Connect** and sign in to the provider.
- Tap the desired database file.



Create a new database

To create a new database:

- Open **Menu** (☰) → **Database Manager**.
- Use the down arrow in the top bar to select the storage location where the new database should be stored.
- Tap **Create** (white plus on a blue background in the bottom-right).
- Enter a file name.
- Set the master password – optionally also a key file if you select this authentication method.
- Tap **Done** to create the database.

The screenshot shows the 'Create database' screen. At the top, there is a dark blue header with a back arrow, the text 'Create database', and a 'Done' button. Below the header, there are three input fields: 'Name', 'PSWE', and 'Master password'. The 'Master password' field has a dropdown arrow. Below the 'Master password' field, there is a section titled 'The master password must be longer' with three checked items: 'At least 15 characters long', 'The following character types must be used:', and 'Numbers'. There is also a link 'Check in Pwned password list'. Below this are fields for 'Password' and 'Confirm password', both with eye icons. At the bottom is a 'Hint' field and a 'Storage location' section with 'Dropbox' selected.

IMPORTANT: Choose a strong master password. Ideally it should be at least 12 characters long and used only once. If needed, use **Check in Pwned password list** to automatically check whether your chosen password appears in known data leaks.

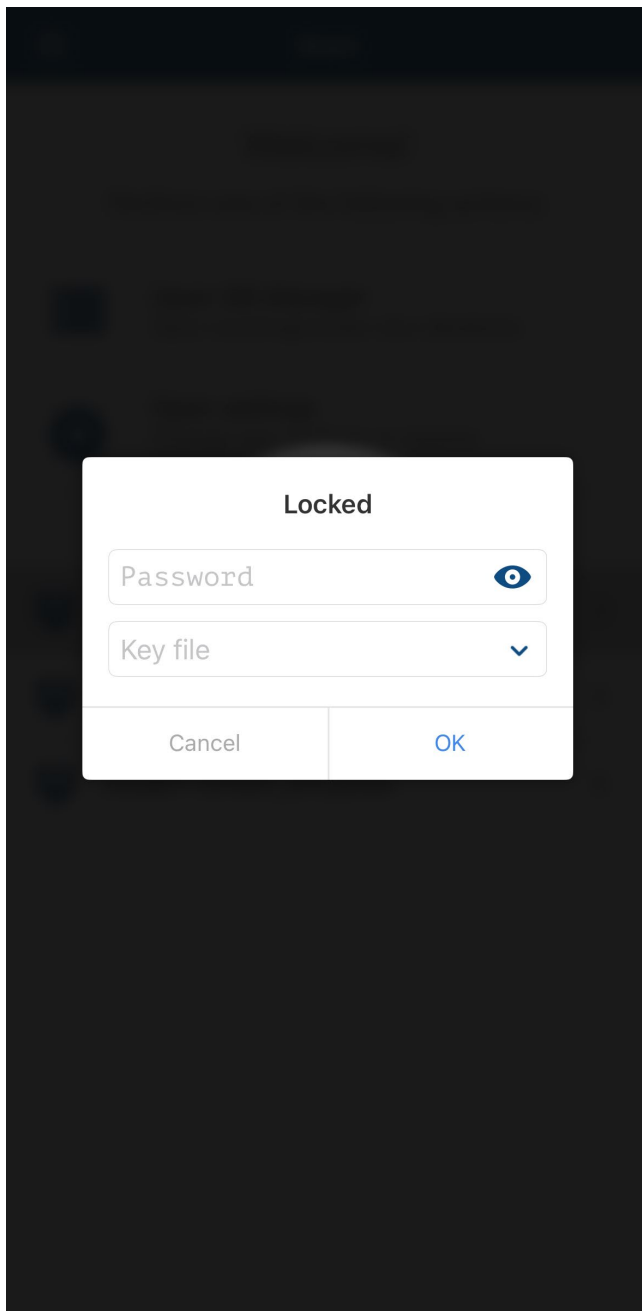
Unlock a database

When opening an existing database, an unlock dialog appears. Depending on protection, you need:

- only the master password,
- only the key file, or
- master password and key file together.

To unlock:

- Enter the master password.
- If needed, select a key file.
- Tap **Open**.

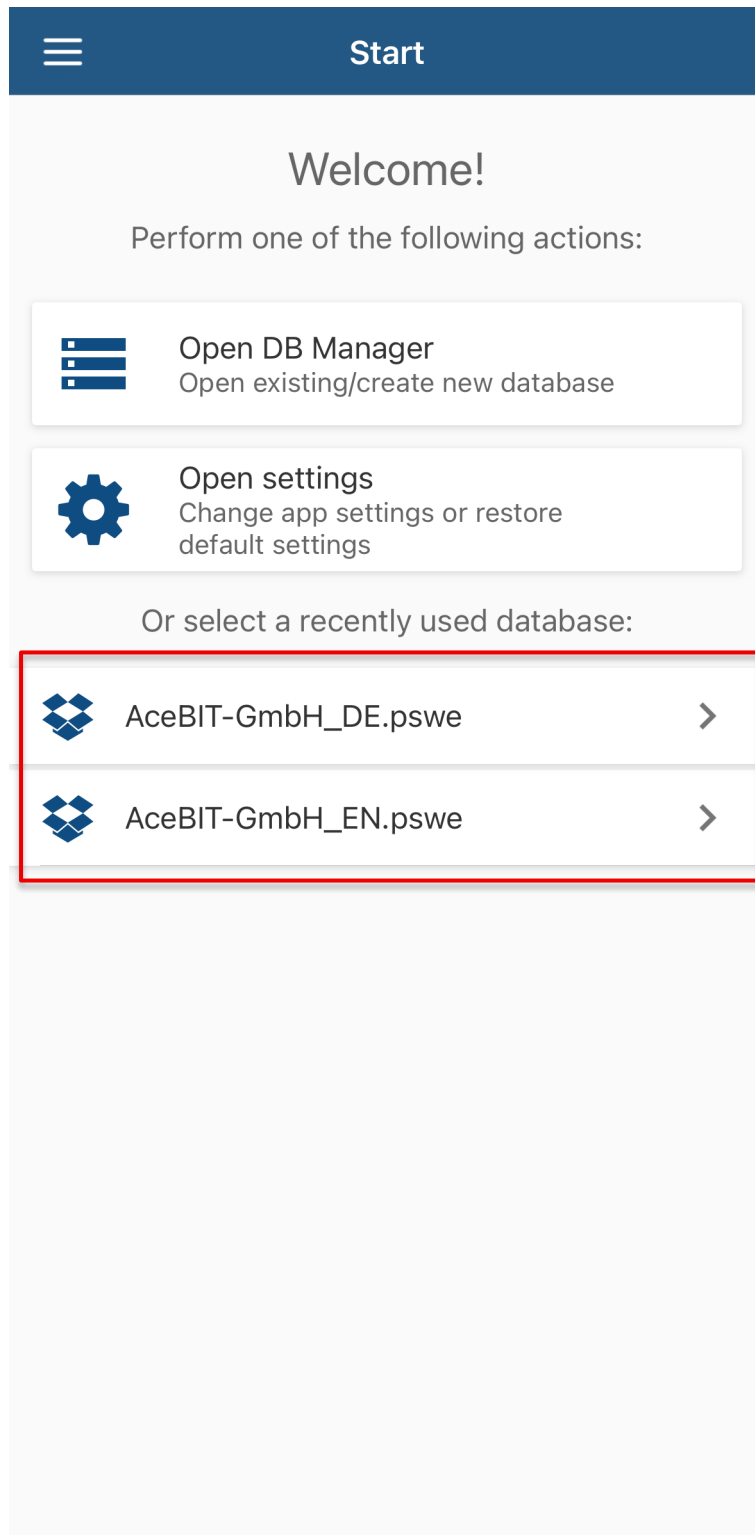


TIP: In the unlock dialog, tap **Show hint** (if you saved a hint for the master password) to help you remember it without revealing the password itself.

Quickly open recently used databases

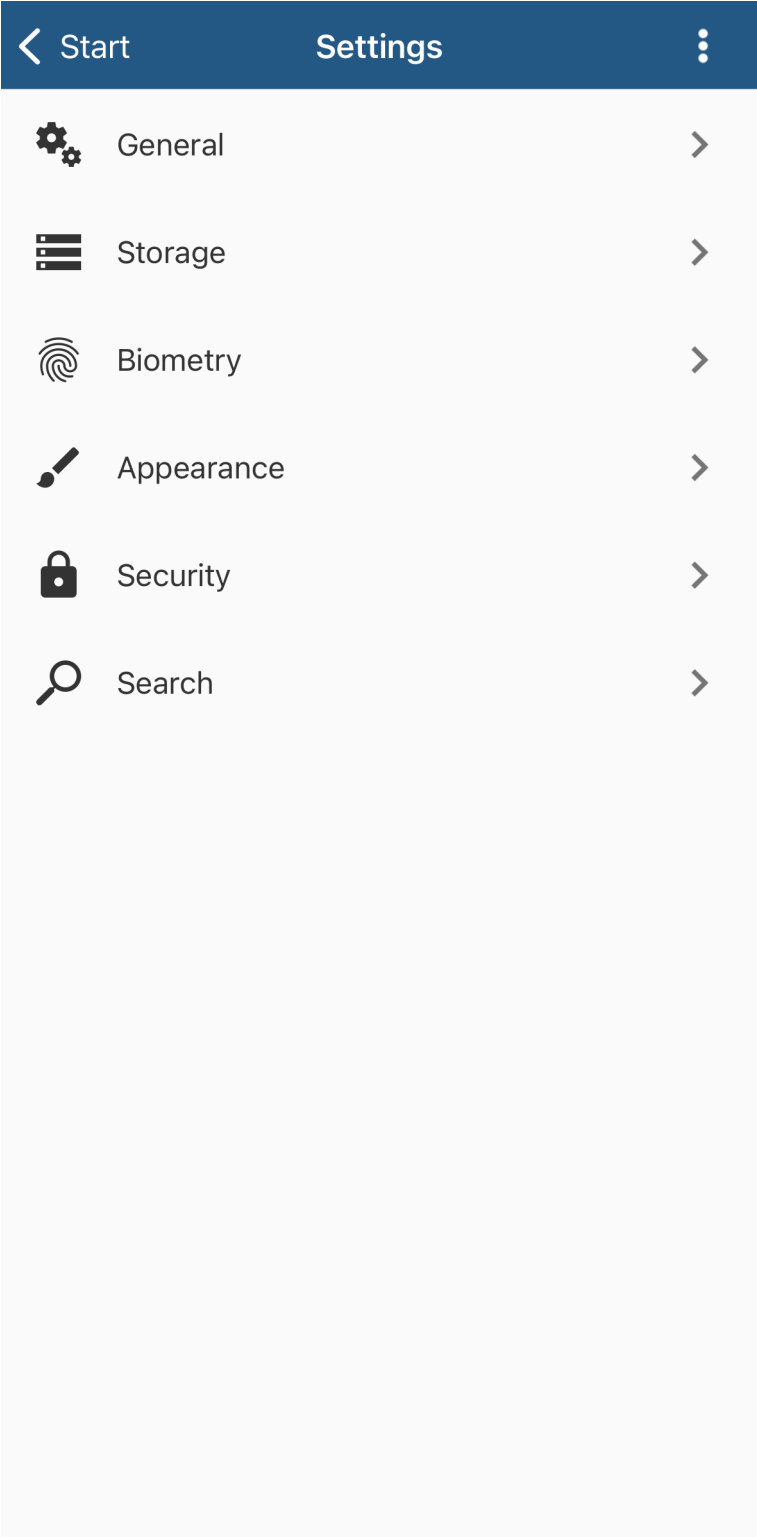
If you have opened a database before, it appears on the "Welcome" screen under **Recently used databases**.

- Open the **Start** area.
- Tap the desired database under **Recently used databases**.
- Unlock the database as usual.



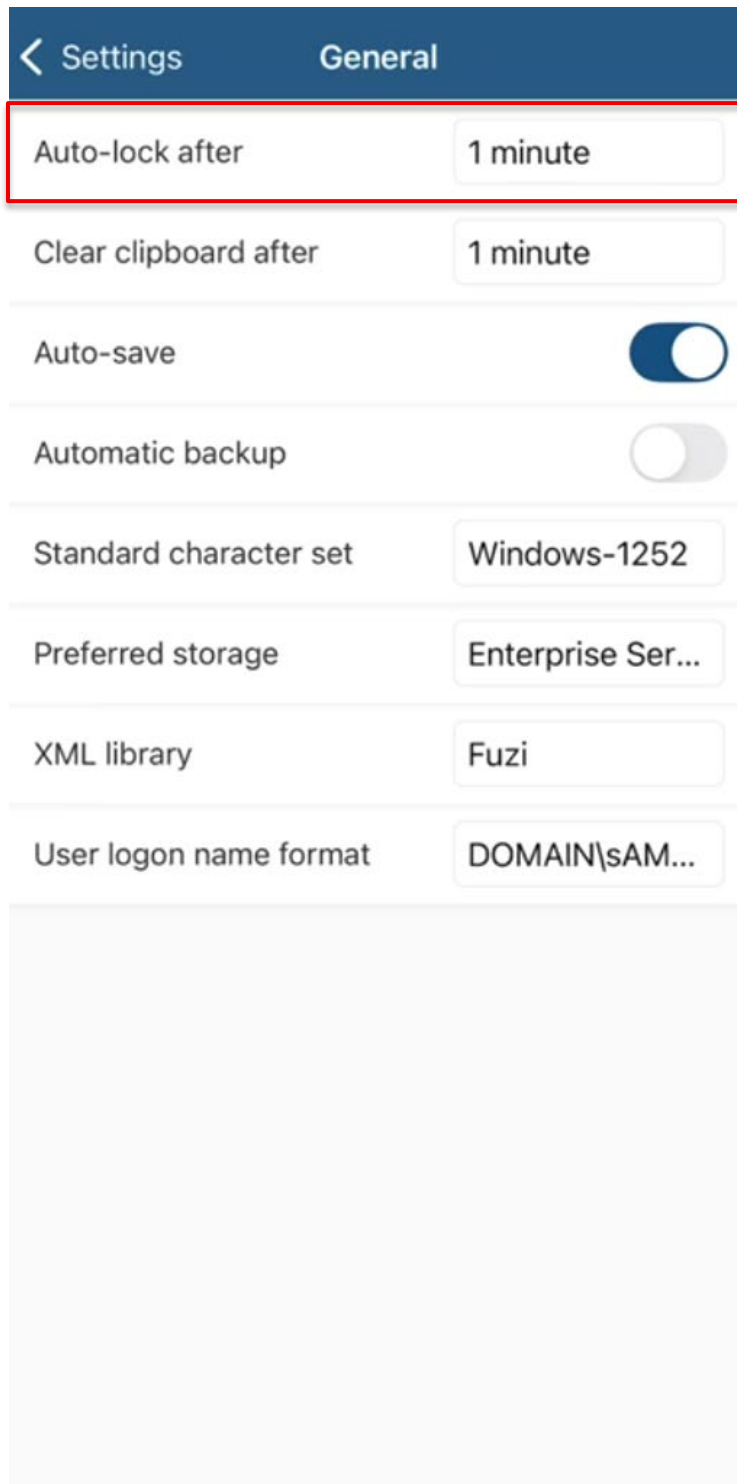
Configure security and convenience settings

In the app settings, you can define various security and convenience settings. You can find them under **Menu** (☰) → **Settings**.



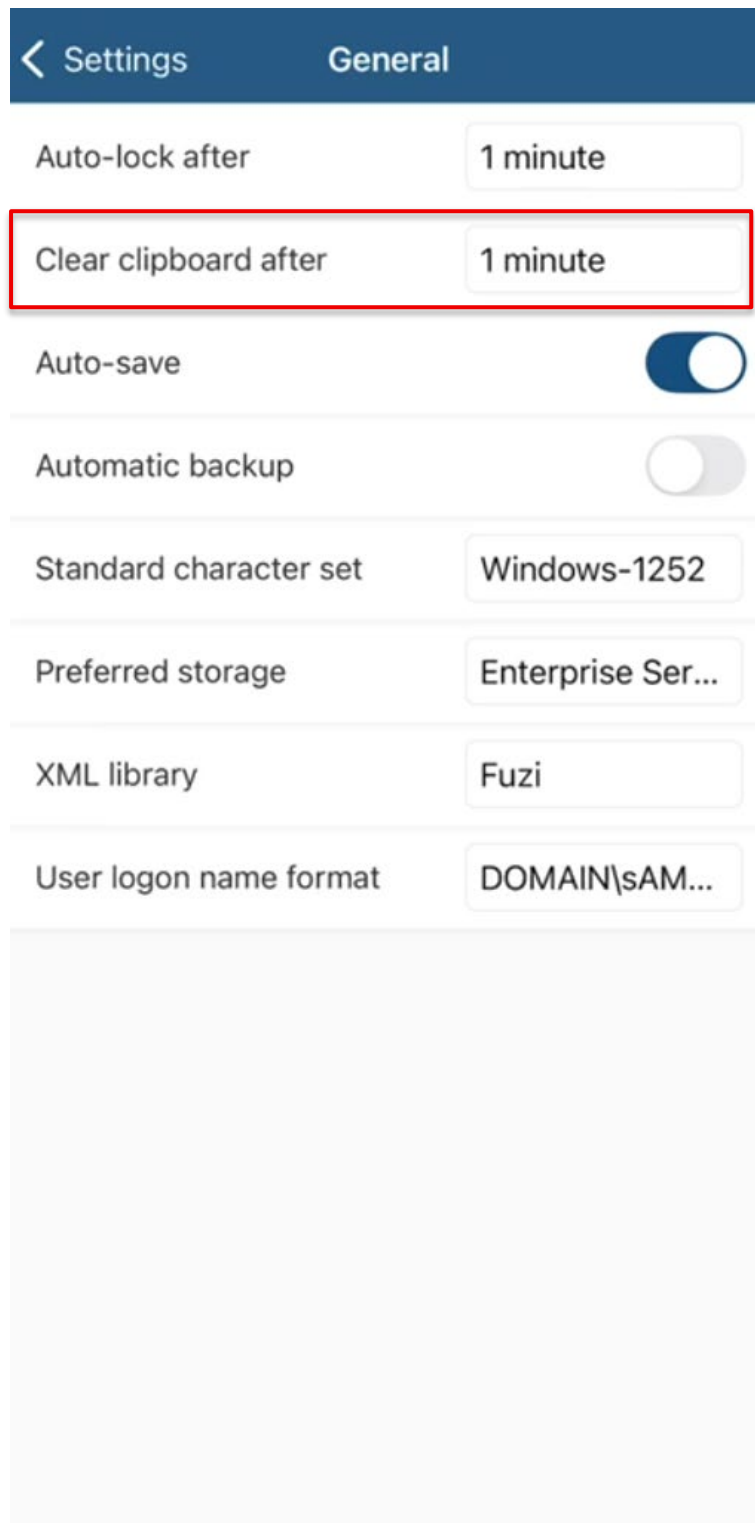
General

- **Auto-lock after:** Set a short value, e.g., 1 minute. Your database will then be locked automatically after the selected time and is protected against unauthorized access. To unlock, enter the master password and/or key file again.



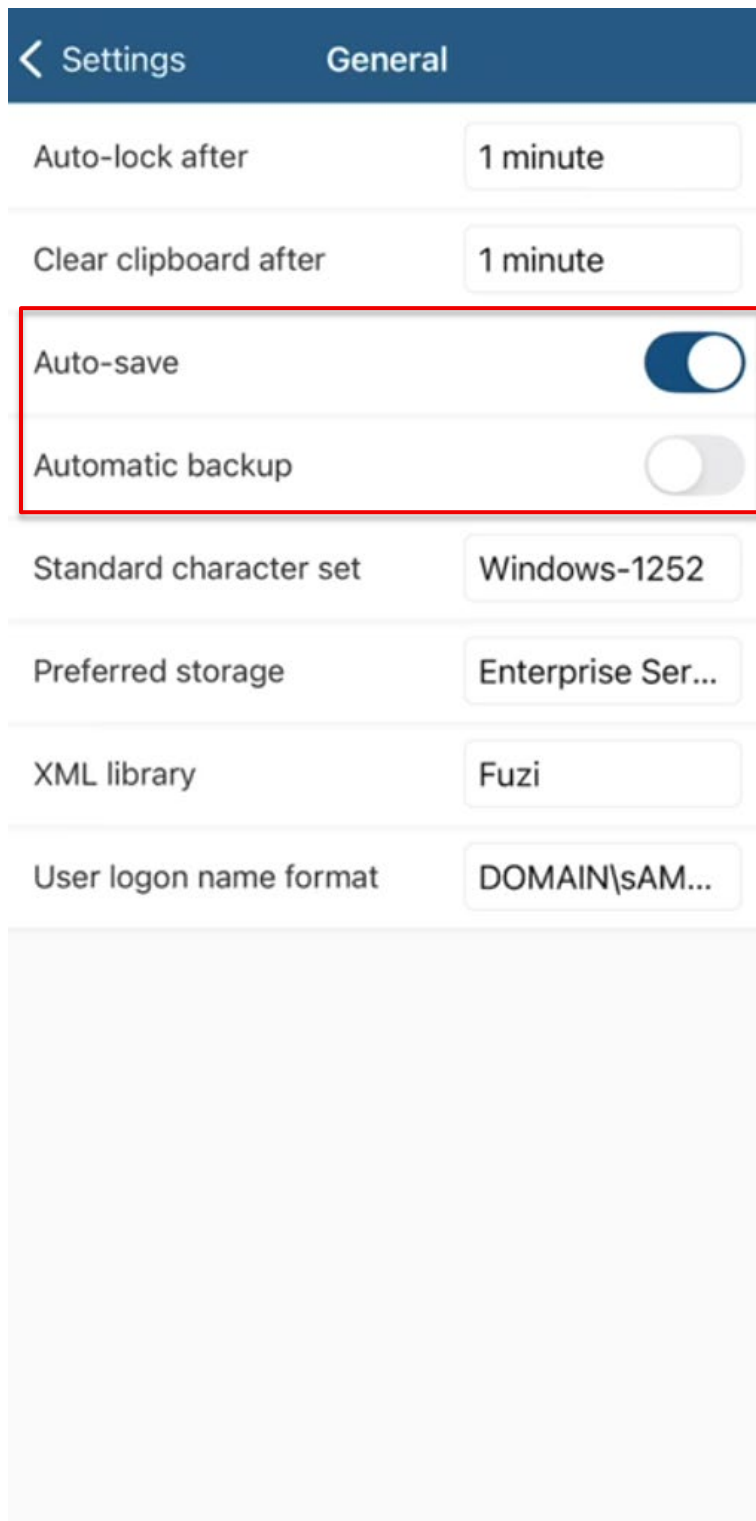
Settings		General
Auto-lock after	1 minute	
Clear clipboard after	1 minute	
Auto-save	<input checked="" type="checkbox"/>	
Automatic backup	<input type="checkbox"/>	
Standard character set	Windows-1252	
Preferred storage	Enterprise Ser...	
XML library	Fuze	
User logon name format	DOMAIN\sAM...	

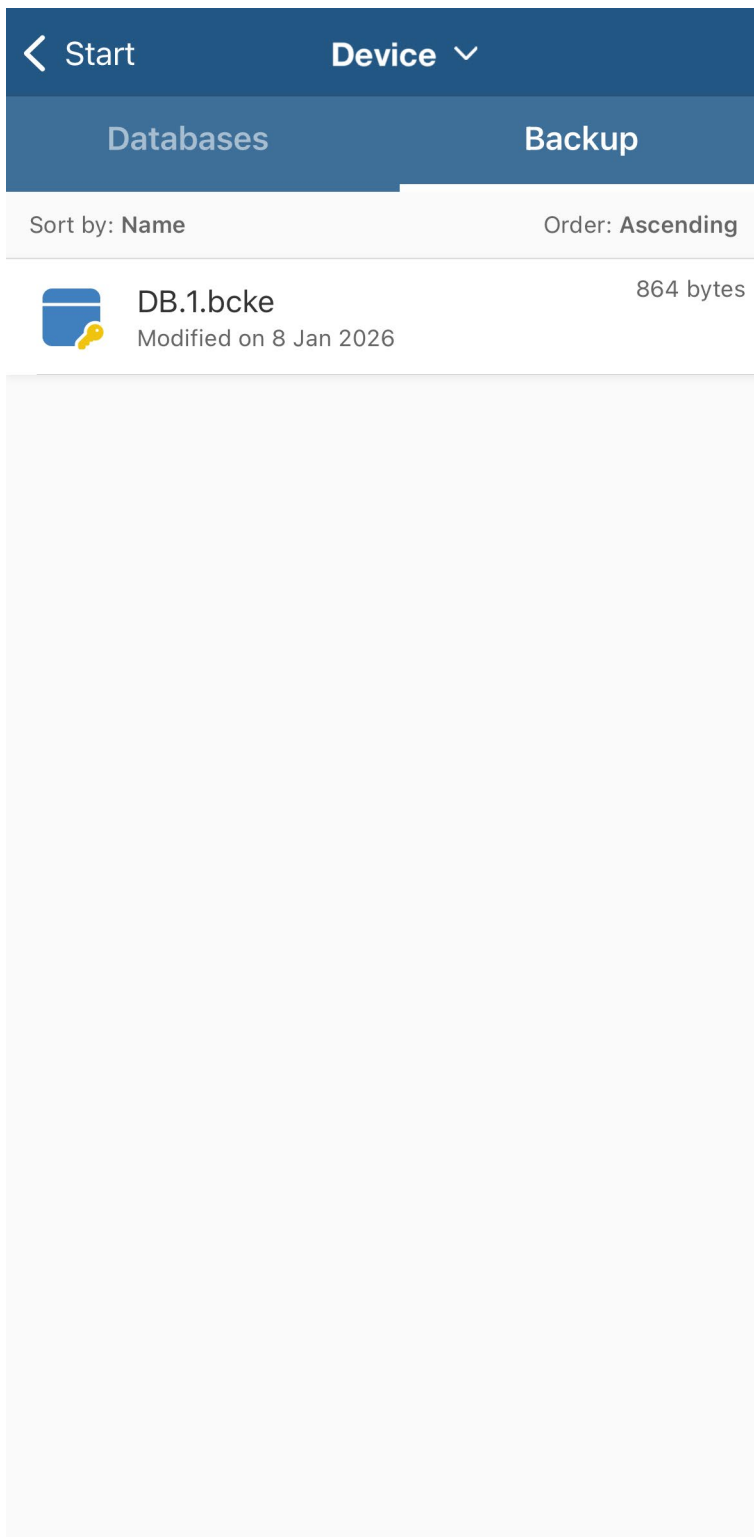
- **Clear clipboard after:** Enable automatic clipboard clearing after a set time. A short value is recommended here as well.



IMPORTANT: Copy passwords only when you will paste them immediately. Avoid unnecessary clipboard usage.

- **Auto-save:** If enabled, the database is saved automatically when you make changes.
- **Automatic backup:** If enabled, backup files of your database are created automatically. You can find backups in the **Database Manager** under **Device** → **Backup** tab.





- **Standard character set:** Adjust the character set used.
- **Preferred storage:** Choose which storage location should be shown by default. Options include Device, Enterprise Server, Dropbox, Google Drive, OneDrive, Box, HiDrive, FTP Server and WebDAV Server.
- **XML library:** Change the XML library used. This can help if you experience memory issues. Options: Fuzi and AEXML.
- **User logon name format:** Choose between Simple, DOMAIN\sAMAccountName and UPN.

Storage

Enterprise Server

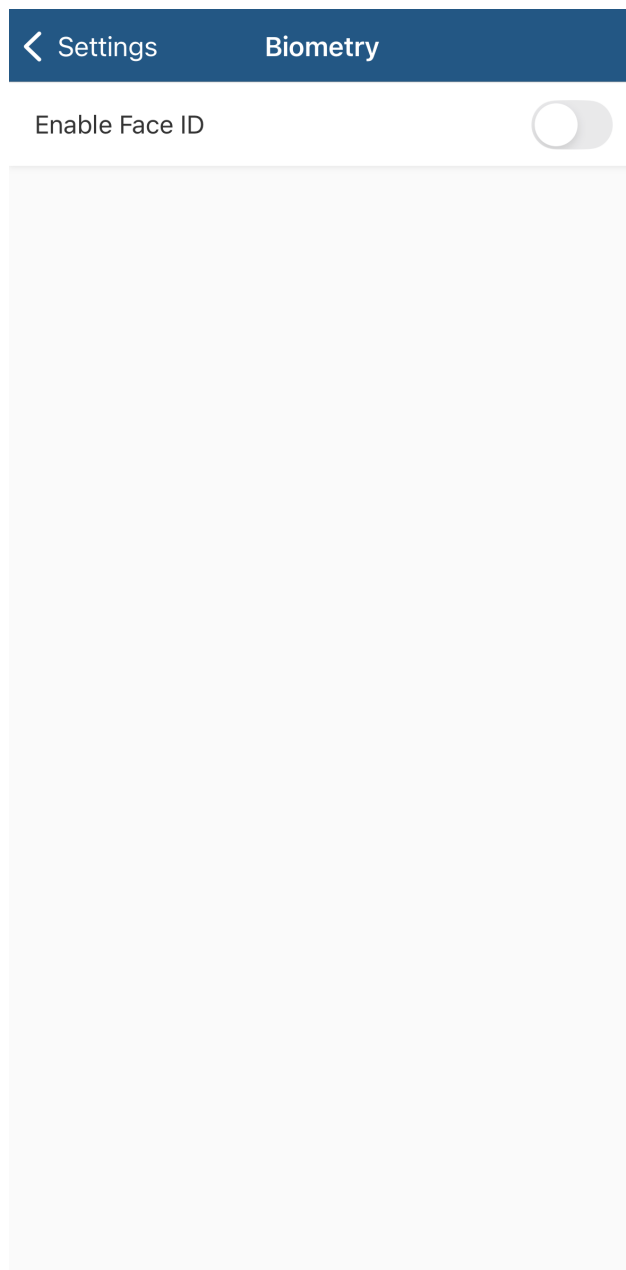
- **Enable SSL/TLS:** This setting is only relevant for Enterprise Server users of version 17.
- **Save a local copy of databases:** Allows a local copy of the server database to be stored.

WebDAV Server

- **Connection timeout (seconds):** If you connect to a WebDAV server, you can set a connection timeout here.

Biometrics

- **Enable Touch ID/Face ID:** To unlock a database faster, you can also use biometrics. The master password remains essential. Enable **Touch ID** or **Face ID** (depending on your device). Then open a database once with the master password and confirm the prompt to allow biometrics for this database.



Appearance

- **Show start animation:** Choose whether an animation is shown when starting the app.

Security

- Define master password policies here. You can set a minimum length and specify whether uppercase letters, lowercase letters, numbers or special characters must be included.

Settings	Security
Minimum length of password	<input type="text" value="15"/>
Uppercase letters required	<input checked="" type="checkbox"/>
Lowercase letters required	<input checked="" type="checkbox"/>
Numbers required	<input checked="" type="checkbox"/>
Special characters required	<input type="checkbox"/>

Search

- **Automatically start quick search when typing:** If enabled, the search starts automatically while you type.

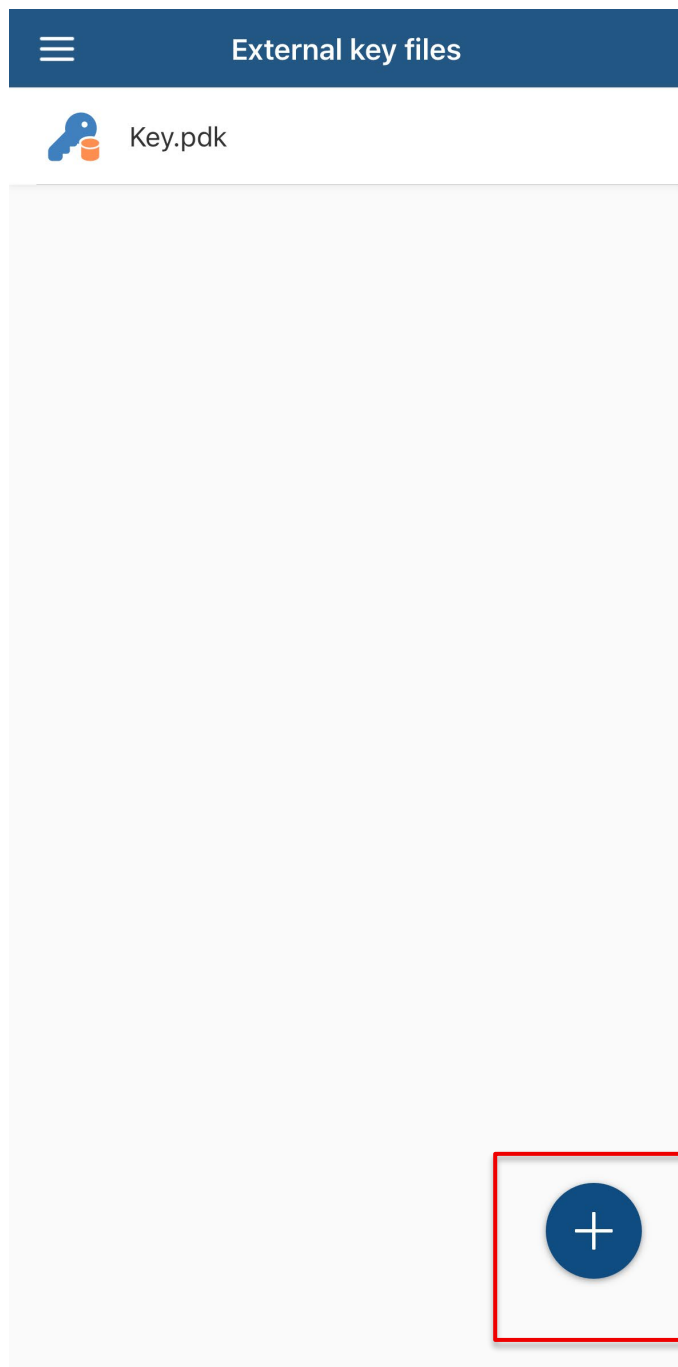
Use key files

A key file complements your master password. The database can then only be opened if both are present: the correct master password and the associated key file.

IMPORTANT: Keep the key file separate from the master password. If you lose the key file, you also lose access to the database protected by it.

Create a key file

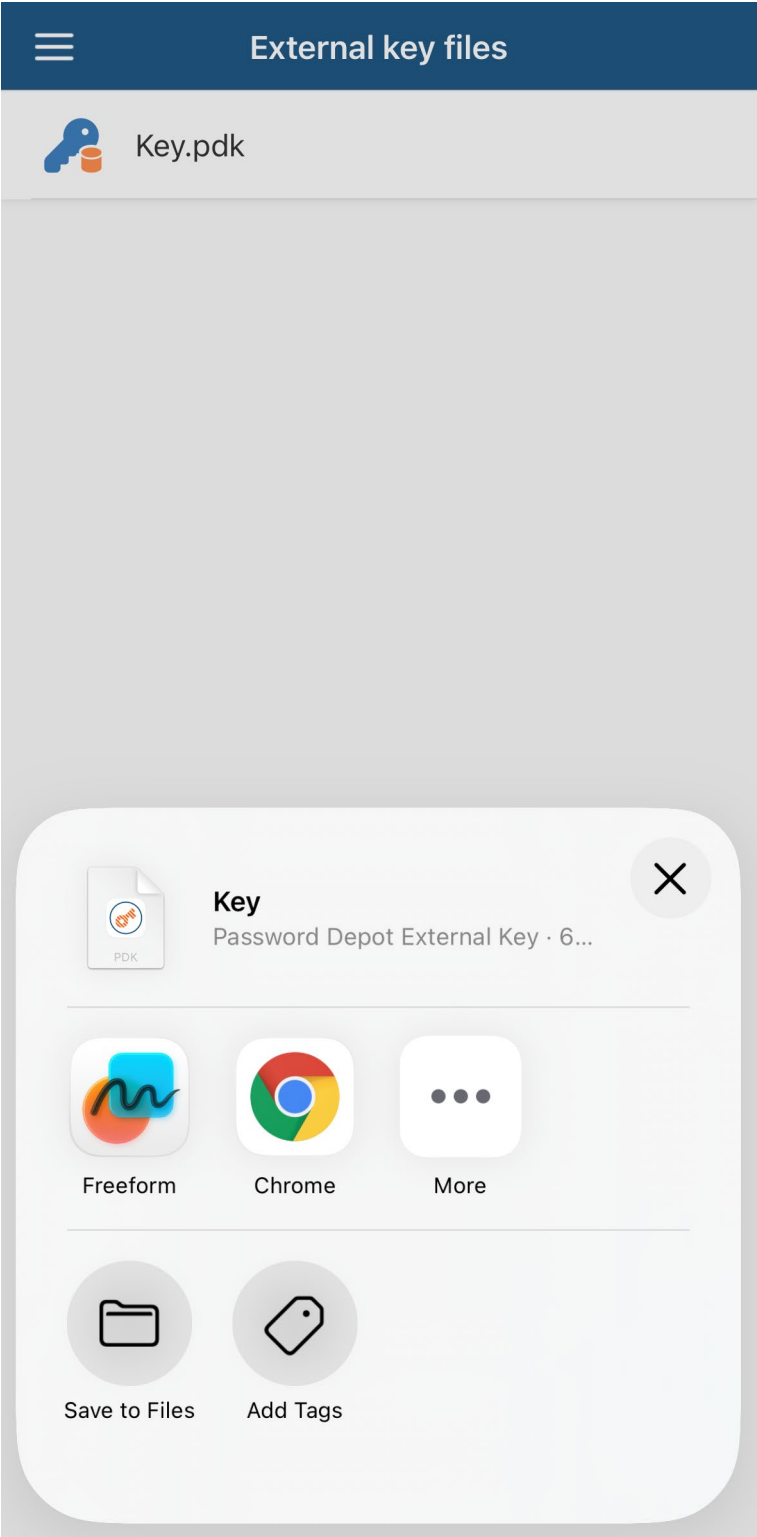
- Open **Menu** (☰) → **External key files**.
- Tap **Create external key file** (white plus on a blue background in the bottom-right).
- Give the key file a clear name (e.g., "PD-Key-iPhone").



Back up or share an existing key file

You can export a key file via the iOS Share menu (e.g., into the Files app).

- Tap the desired key file in the list.
- Choose a secure destination (e.g., Files app).



Use a key file in a database

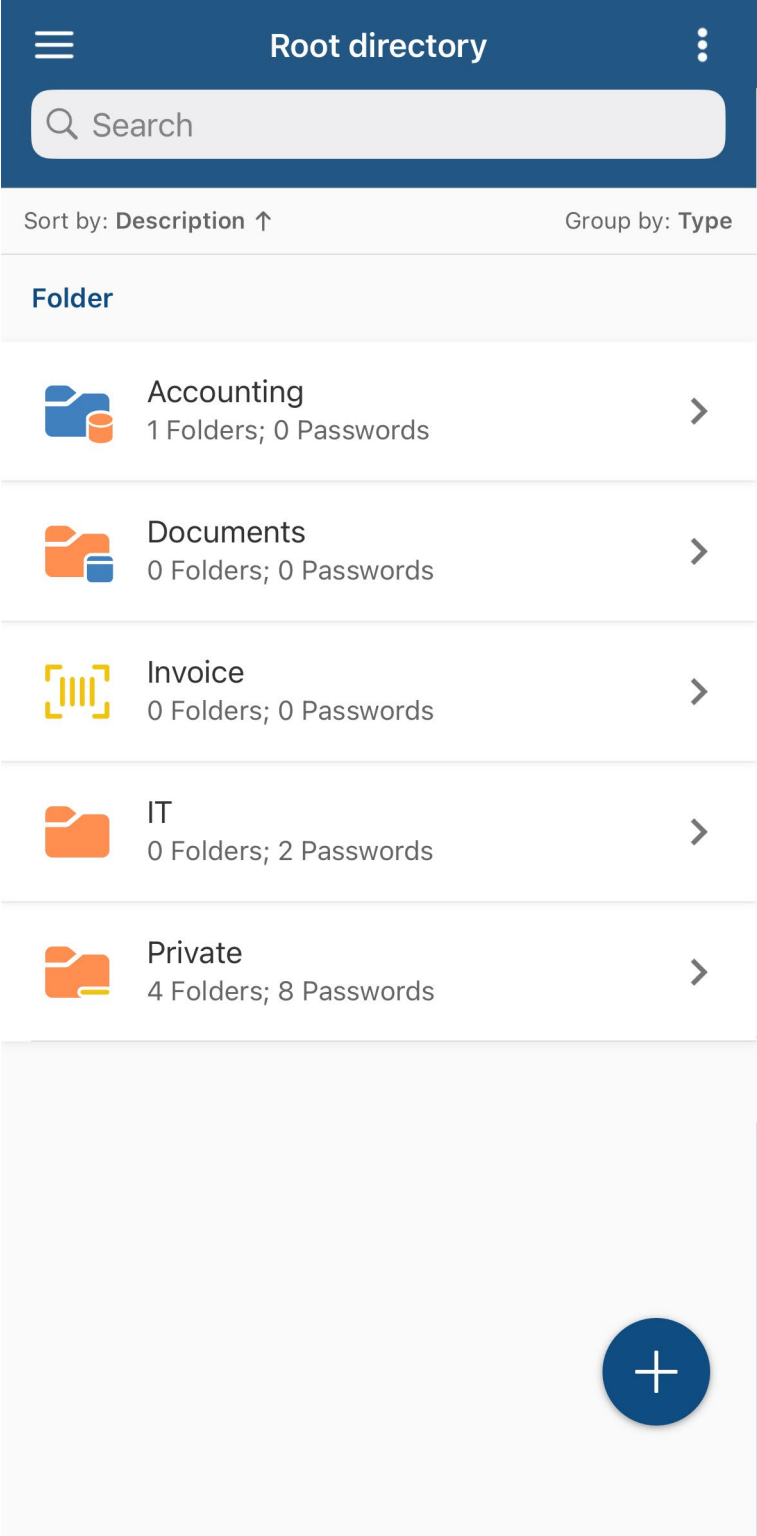
- When creating a database or changing database access, select the authentication method **Master password and key file**.
- When unlocking, select the matching key file in the dialog.

The screenshot shows a mobile application interface for creating a database. At the top, there is a dark blue header with a back arrow, the text 'Create database', and a 'Done' button. Below the header are two input fields: 'Name' and 'PSWE'. A red rectangular box highlights a dropdown menu that is currently set to 'Master password and key file'. Below this menu, there are several options and checkboxes: 'The master password must be longer' (checked), 'At least 15 characters long' (checked), 'The following character types must be used:' (checked), 'Uppercase' (checked), 'Lowercase' (checked), and 'Numbers' (checked). There is also a checkbox for 'Check in Pwned password list'. Below these are two password input fields: 'Password' and 'Confirm password', each with an eye icon for visibility. There is also a 'Key file' dropdown menu with a plus sign button next to it, and a 'Hint' input field. At the bottom of the main form area, there are two options: 'Storage location' and 'Protected storage'. Below this is a section for 'Authentication by' with a 'Done' button. At the very bottom, there is a grey overlay with three options: 'Master password', 'Key file', and 'Master password and key file', with the latter being highlighted in a darker grey.

Core functions

Content overview: folders, search, sorting and favorites

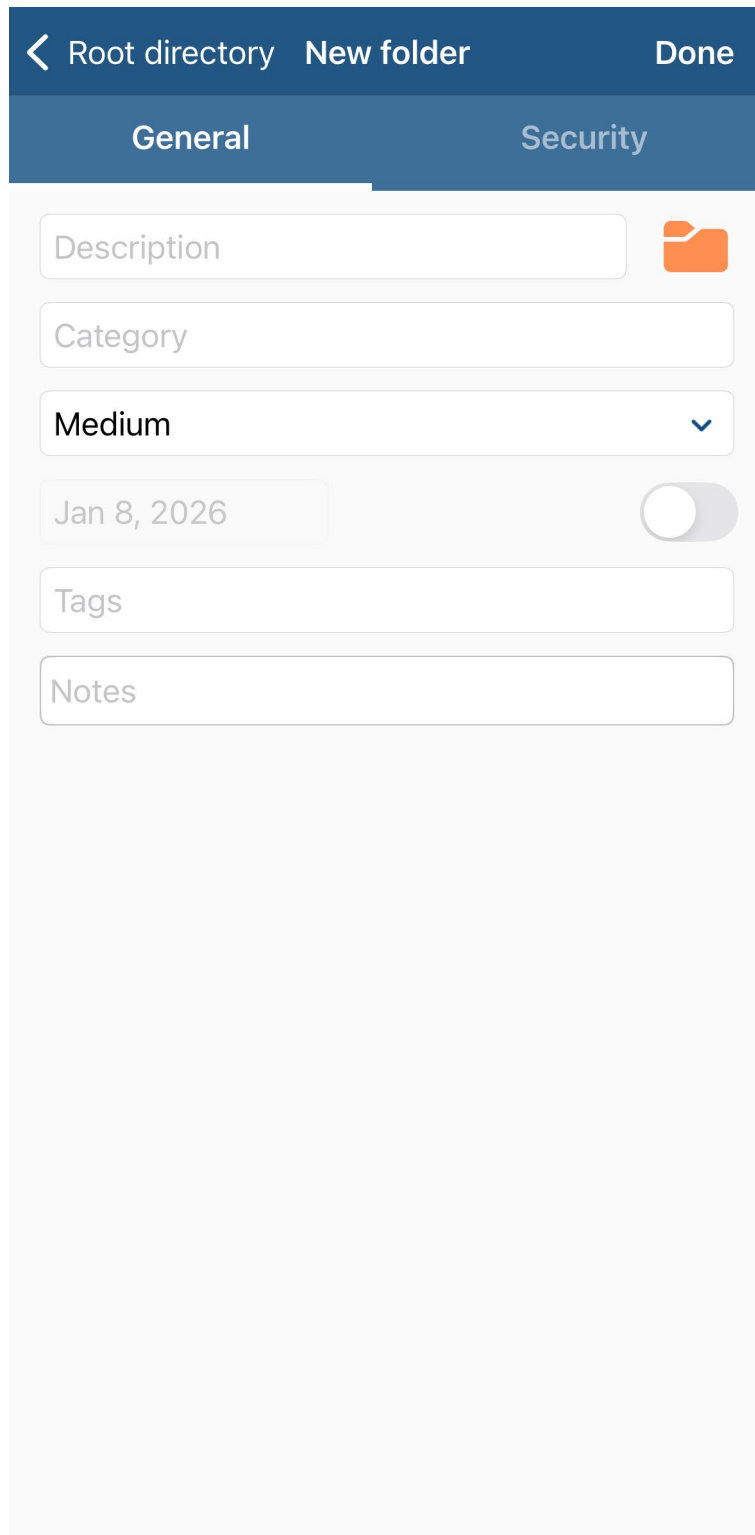
After opening a database, you will see the **content overview**. Folders and entries are listed here.



Create and organize folders

Folders help you structure entries and keep things clear. To create a folder:

- Tap the + (Create) in the bottom-right.
- Select **Folder**.
- Enter a name and save.

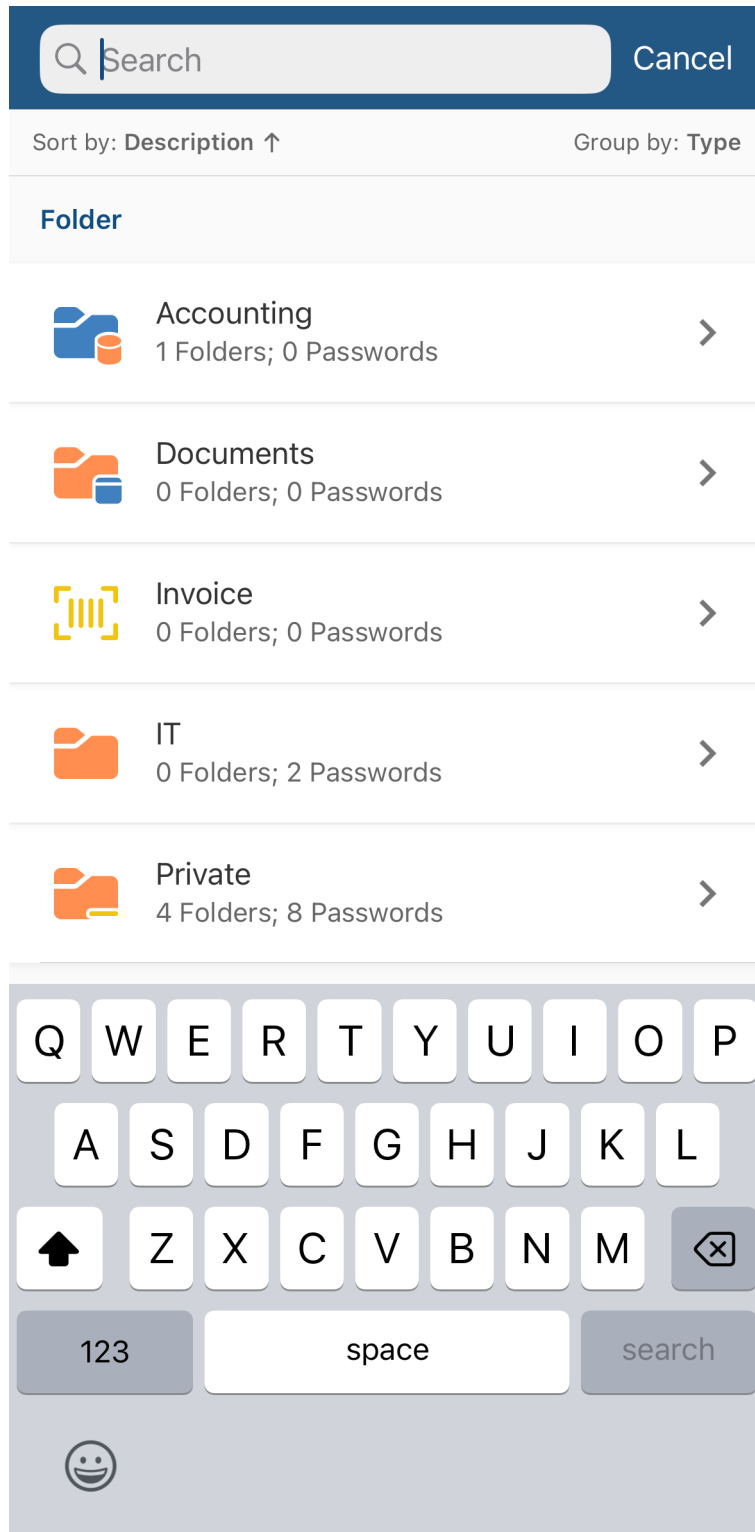


The screenshot displays a mobile application interface for creating a new folder. At the top, there is a dark blue header bar with a back arrow, the text 'Root directory', 'New folder', and 'Done'. Below the header, there are two tabs: 'General' (selected) and 'Security'. The main content area contains several input fields and a toggle switch:

- Description:** A text input field with a folder icon to its right.
- Category:** A text input field.
- Medium:** A dropdown menu currently showing 'Medium' with a downward arrow.
- Date:** A date input field showing 'Jan 8, 2026' and a toggle switch to its right.
- Tags:** A text input field.
- Notes:** A text input field.

Search

- Tap the search field at the top.
- Enter a search term (e.g., website, username, category).
- End the search using **Cancel** to return to the normal view.



Optionally, you can enable Quick search so the app searches immediately across multiple fields while you type:

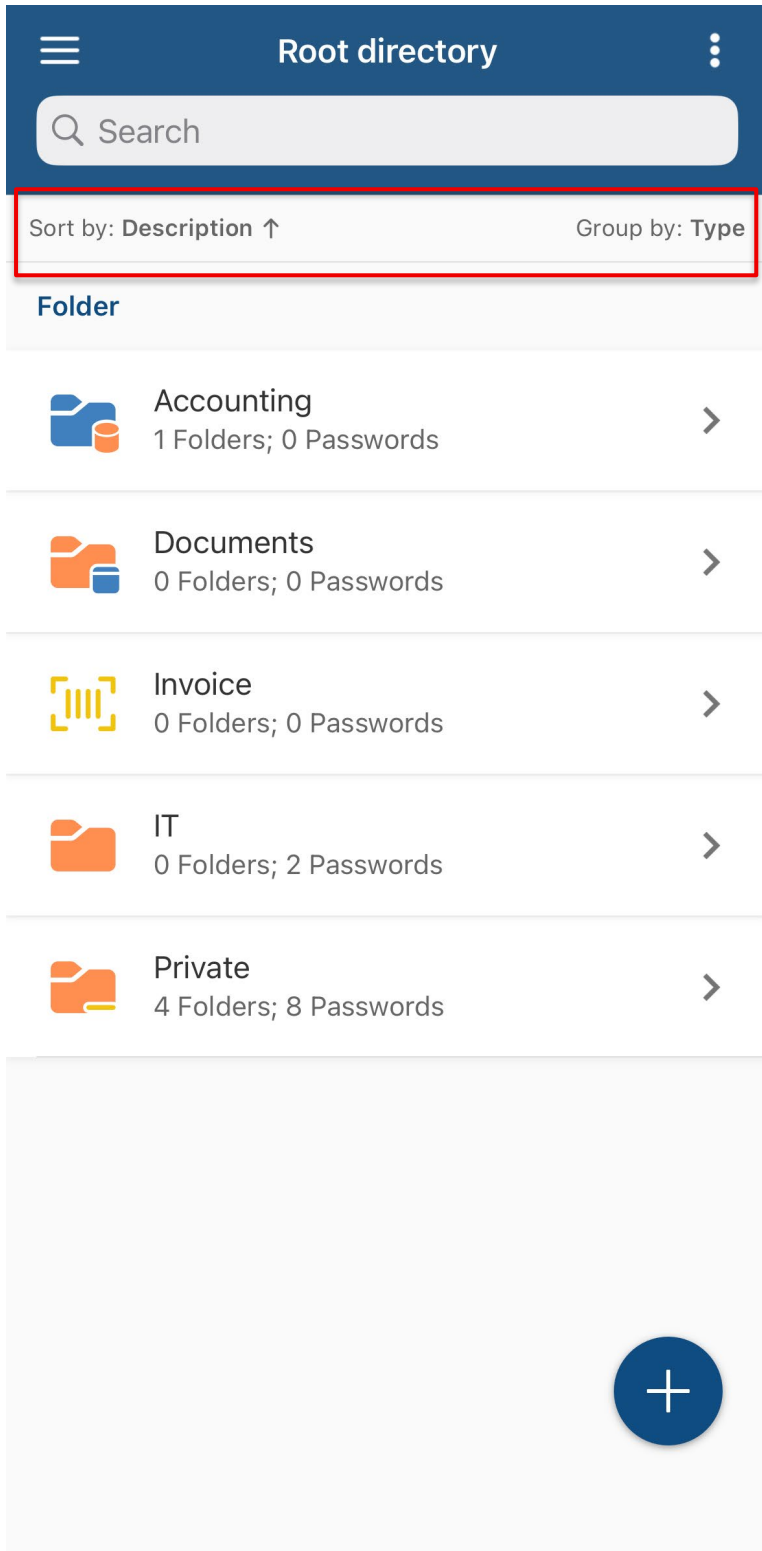
- Open **Menu (☰)** → **Settings** → **Search**.
- Enable **Automatically start quick search when typing**.



Sort and group

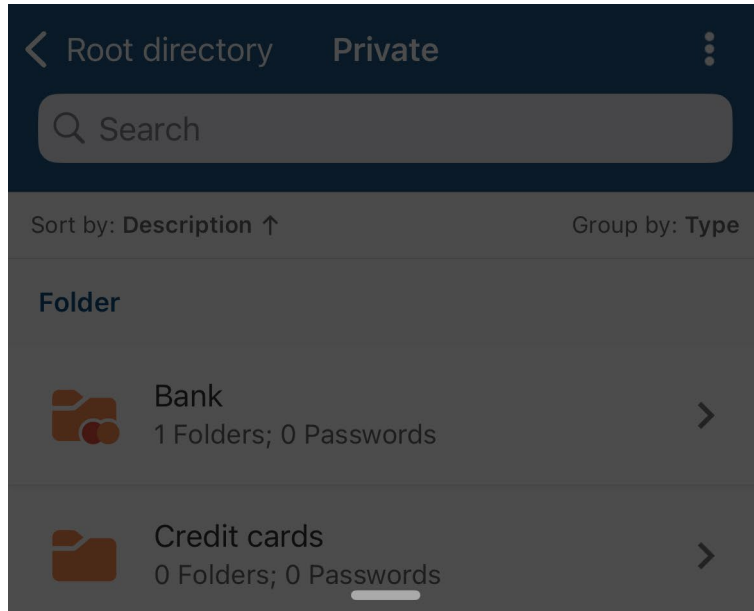
Adjust the view, e.g., by category or type. This makes it easier to navigate and find entries faster.

- In the content overview, tap the sort/group options (top of the list).
- Choose **Sort by** and/or **Group by**.
- Also choose the sort order (ascending/descending).



Use favorites

- Open an entry's actions by tapping the entry.
- Tap **Add to favorites**.
- Open **Menu (☰)** → **Favorites** to see a list of all favorites.



 Details

 Edit

 Add to Favorites




 Copy user name

 Copy password

 Copy TOTP code

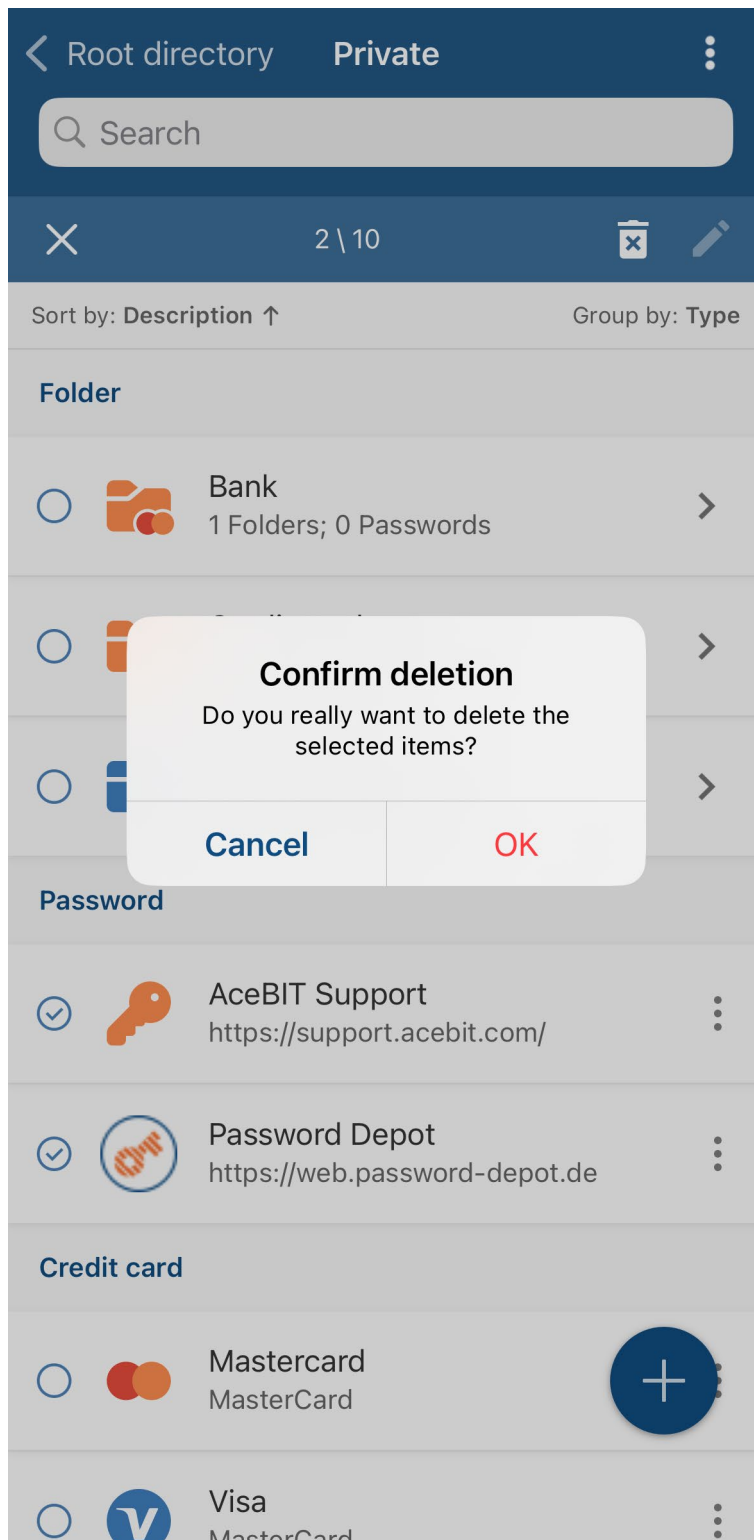
 Open URL

 Create linked entry

Delete entries and select multiple items

To delete entries or folders:

- Press and hold an entry/folder to start selection mode.
- Select additional items if needed.
- Tap **Delete** (trash icon) and confirm.



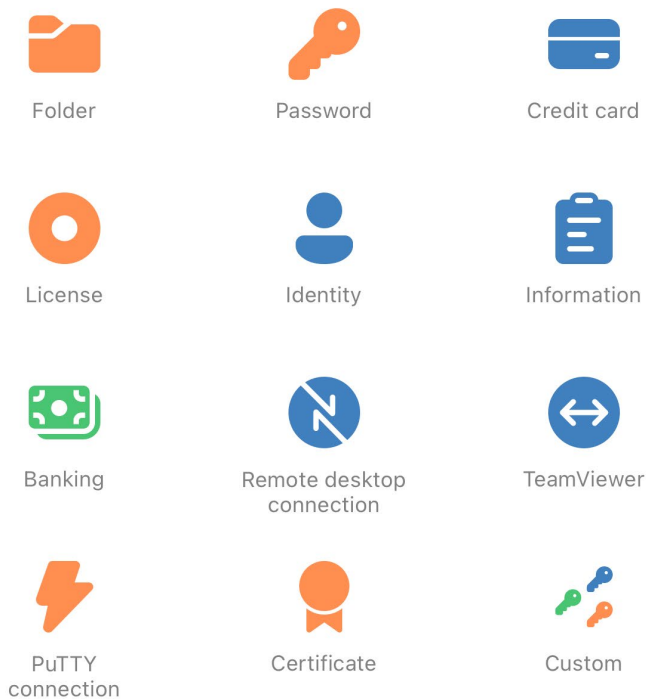
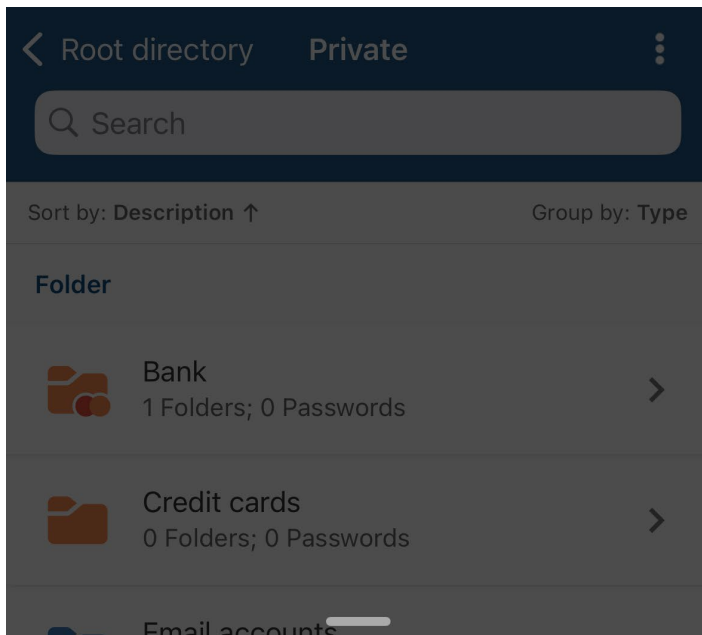
IMPORTANT: Deleted entries are generally not recoverable. If you are unsure, create a backup first.

Create entries

Entries are your stored information – e.g., passwords, website logins, credit cards or licenses.

To create a new entry:

- Open the target folder in the content overview.
- Tap the + (Create) in the bottom-right.
- Select the desired entry type.
- Fill in at least **Description**. Optional fields include **Category**, **Username**, **Password**, **URL**, **Importance**, **Expiration date**, **Tags** and **Notes**. Then tap Save.



Different entry types are available for storing different kinds of information:

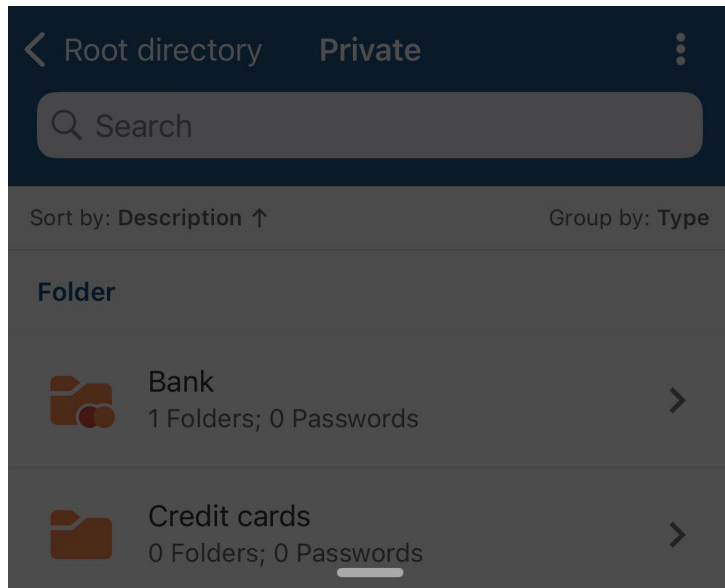
Type	Best for	Typical fields
Password	Website/app login, device access	Username, Password, URL, TOTP (one-time code)
Credit card	Securely store card data	Card number, Expiration date, Cardholder, PIN
License	Software licenses	License key, Product, Version
Identity	Personal data	Name, Address, Phone number, Notes
Information	Free-text notes	Title, Content/Note
Banking	Bank/card information	Card number, Account/Bank, PIN, Notes
Remote Desktop connection	Server/PC access	Computer/Host, User, Password, Command line
TeamViewer	Remote support access	ID, Password, Notes
PuTTY connection	SSH/terminal access	Host, Username, Password/Key info, Command line
Certificate	Certificates/key files	Public/Private key, Password, Expiration date
Custom	Your own forms	Fields based on a template (templates)

WARNING: Depending on the database (e.g., databases stored on the Enterprise Server) and your assigned rights, entry types may be restricted. Some types (e.g., Document or Passkey) may exist without being creatable on iOS.

Edit entries and important fields

You can edit entries at any time. Open an entry's actions via the three dots to the right of the entry and select **Edit**.

- In the content overview, tap an entry.
- Select **Edit**.
- Add or update fields and tap Save. In addition to General, other tabs may be available depending on the entry type. For a Password entry, these can include **Additional**, **Security**, **Fields**, **TAN** and **Conditional access**.



 Details

 Edit

 Add to Favorites

 Copy user name

 Copy password

 Copy TOTP code

 Open URL

 Create linked entry

Categories, tags and expiration date

Use metadata to stay organized and reduce risk. Under **General** in an entry's properties, you can set:

- **Category** – groups entries by topic.
- **Tags** – freely assigned keywords for flexible searching.
- **Expiration date** – reminds you about expiring passwords, cards or certificates.
- **Importance** – helps prioritize (e.g., "high" for admin access).

The screenshot shows a mobile application interface for editing a password entry. At the top, there is a dark blue header with a back arrow, the text "Private", the title "Edit password", and a "Done" button. Below the header is a tabbed interface with four tabs: "General" (selected), "Additional", "Security", and "Fields". The main content area is a light gray form with several input fields and controls:

- A text field containing "Password Depot" with a circular icon to its right.
- A text field labeled "Category".
- A text field containing "AceBIT".
- A text field containing a complex password "\$_eRj>Rj^5Thi|Z/;&&(+bzPY" with an eye icon for visibility and a pencil icon for editing.
- A text field containing the URL "https://web.password-depot.de" with a right-pointing arrow icon.
- A dropdown menu showing "Medium" with a downward arrow.
- A date field showing "Jan 8, 2026" and a toggle switch.
- A text field labeled "Tags".
- A text field labeled "Notes".

Password Generator

Instead of creating passwords yourself, you can use the Password Generator to automatically create secure passwords.

- Open an entry with a password field (e.g., Password, License or Banking).
- In the password field, tap the pencil icon.
- Select length and character types, then tap Generate. Tap **Done**; the generated password is applied to the entry automatically.

Generated password

Generate Copy

Generator settings

Password length

Uppercase

Lowercase

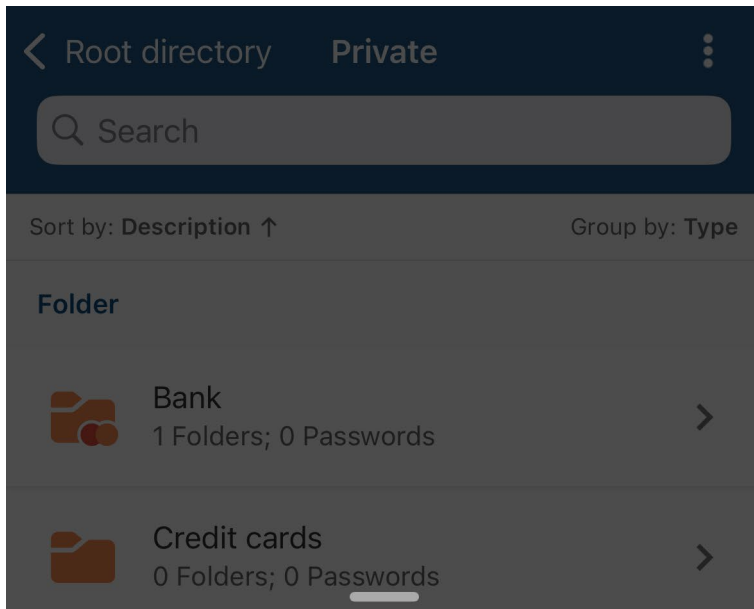
Special characters


Numbers


URL and integrated web browser


If a URL is stored in the URL field of an entry, you can open it directly.


- Open the actions for an entry.
- Tap **Open URL**.





-  Details


-  Edit


-  Add to Favorites

-  Copy user name

-  Copy password

-  Copy TOTP code

-  **Open URL**

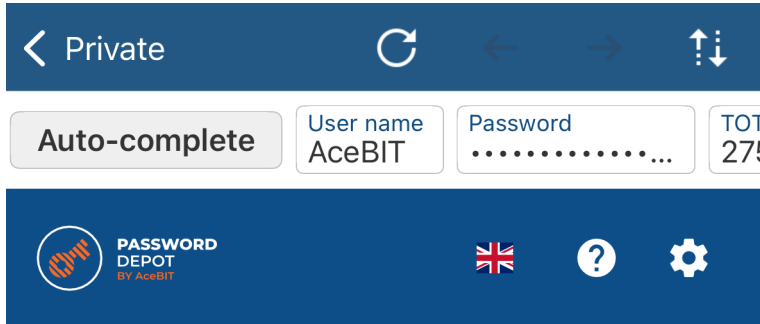
-  Create linked entry


TIP: For maximum security, verify the URL before filling any data. Use HTTPS whenever possible (encrypted website connection).


Auto-fill in the integrated web browser


In the integrated web browser, you can fill fields automatically. Password Depot uses an auto-complete sequence (a sequence of steps).


- Open an entry and choose **Open URL**.
- Show the button bar (toggle button in the navigation bar).
- Tap **Auto-complete** to run the saved sequence.




Server Address* 

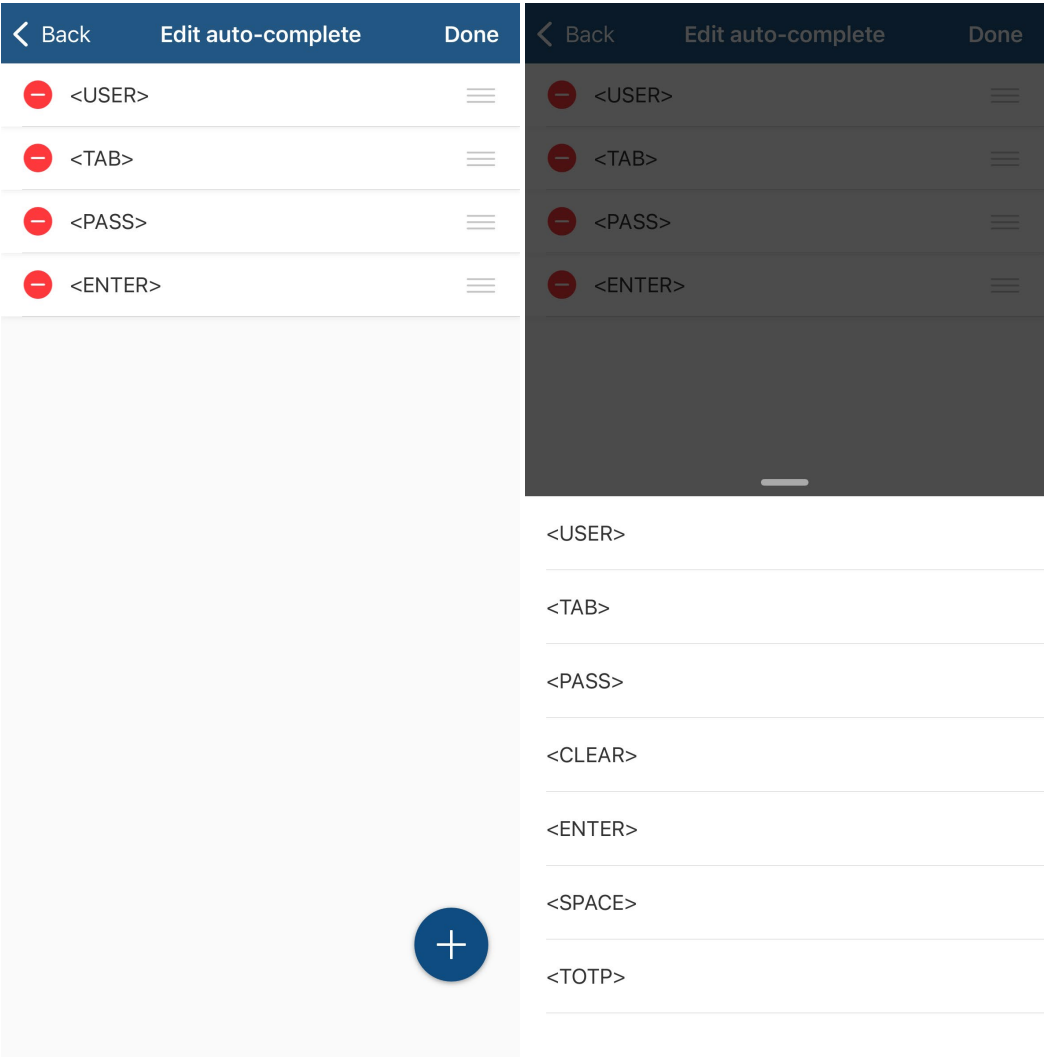
Port* 

Authentication Method 

Username* 

Password* 

If auto-fill causes problems on a website, you can adjust the sequence: open the entry, go to the **Additional** tab, and under **Auto-complete** tap the pencil icon to compose your own sequence. You can also add delays.

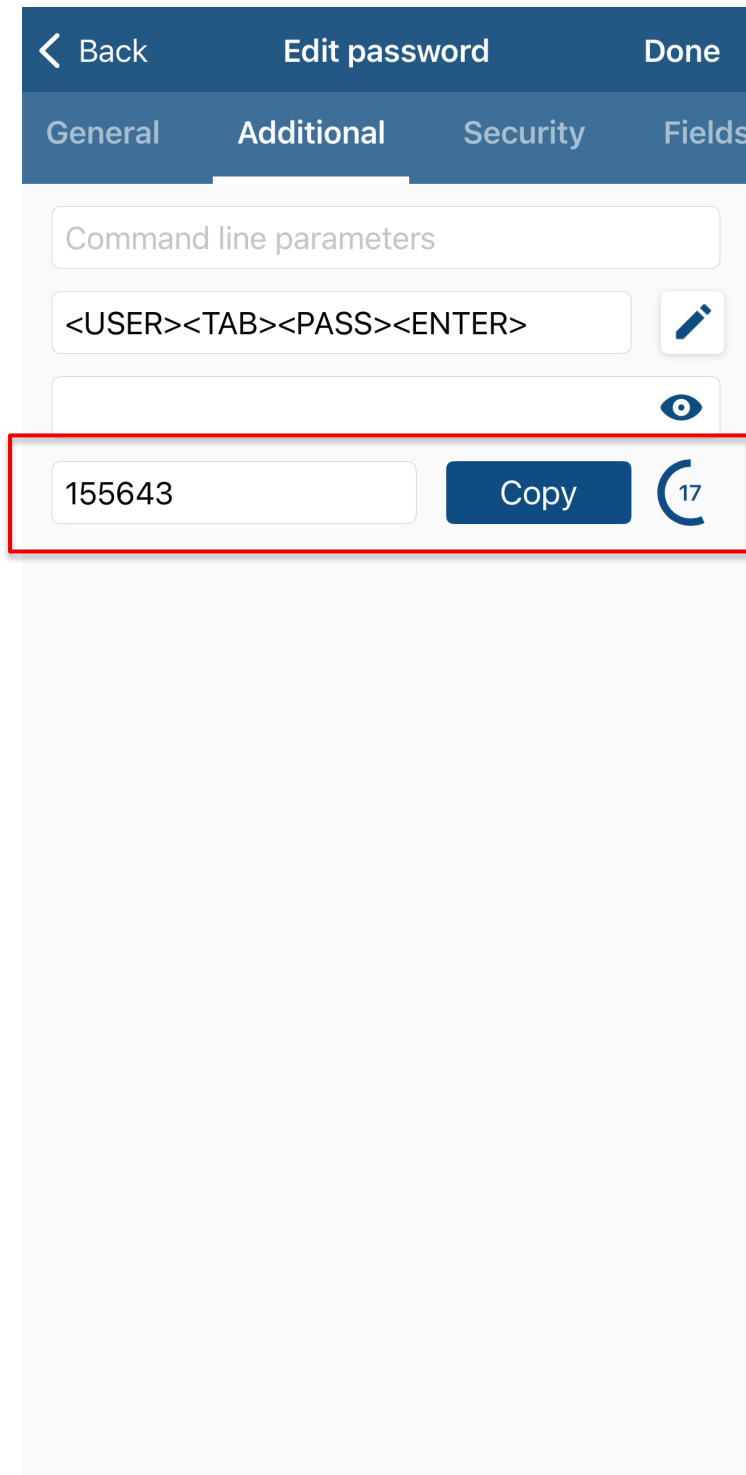


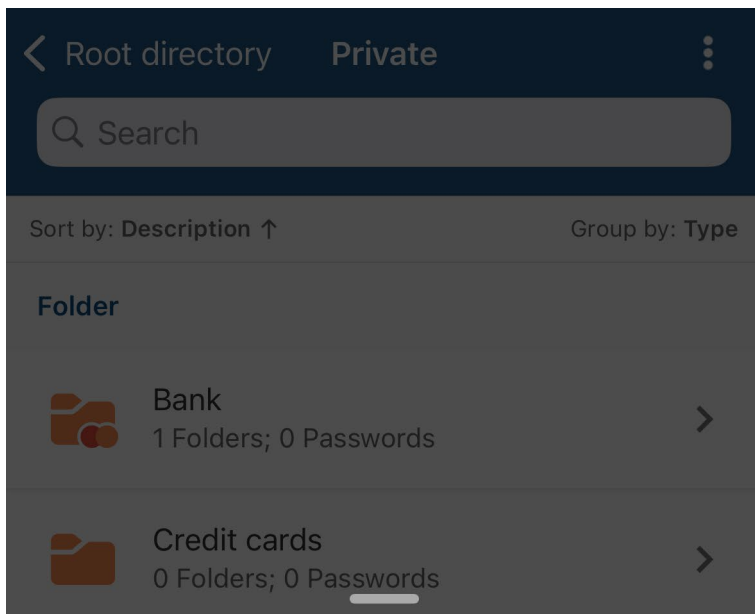
TIP: Auto-fill supports typical steps such as username, password, tab and submit. Not all special keys are supported.

TOTP: Generate one-time codes in the app

Many services use a one-time code (TOTP) in addition to the password. Password Depot supports these codes.

- Open an entry and switch to the **Additional** tab.
- Enter the received code under **2FA secret**.
- Save the entry.
- Later, copy the TOTP via the **Copy TOTP code** action when selecting the entry, or directly in the **Additional** tab.






 Details

 Edit


 Add to Favorites

 Copy user name

 Copy password

 Copy TOTP code

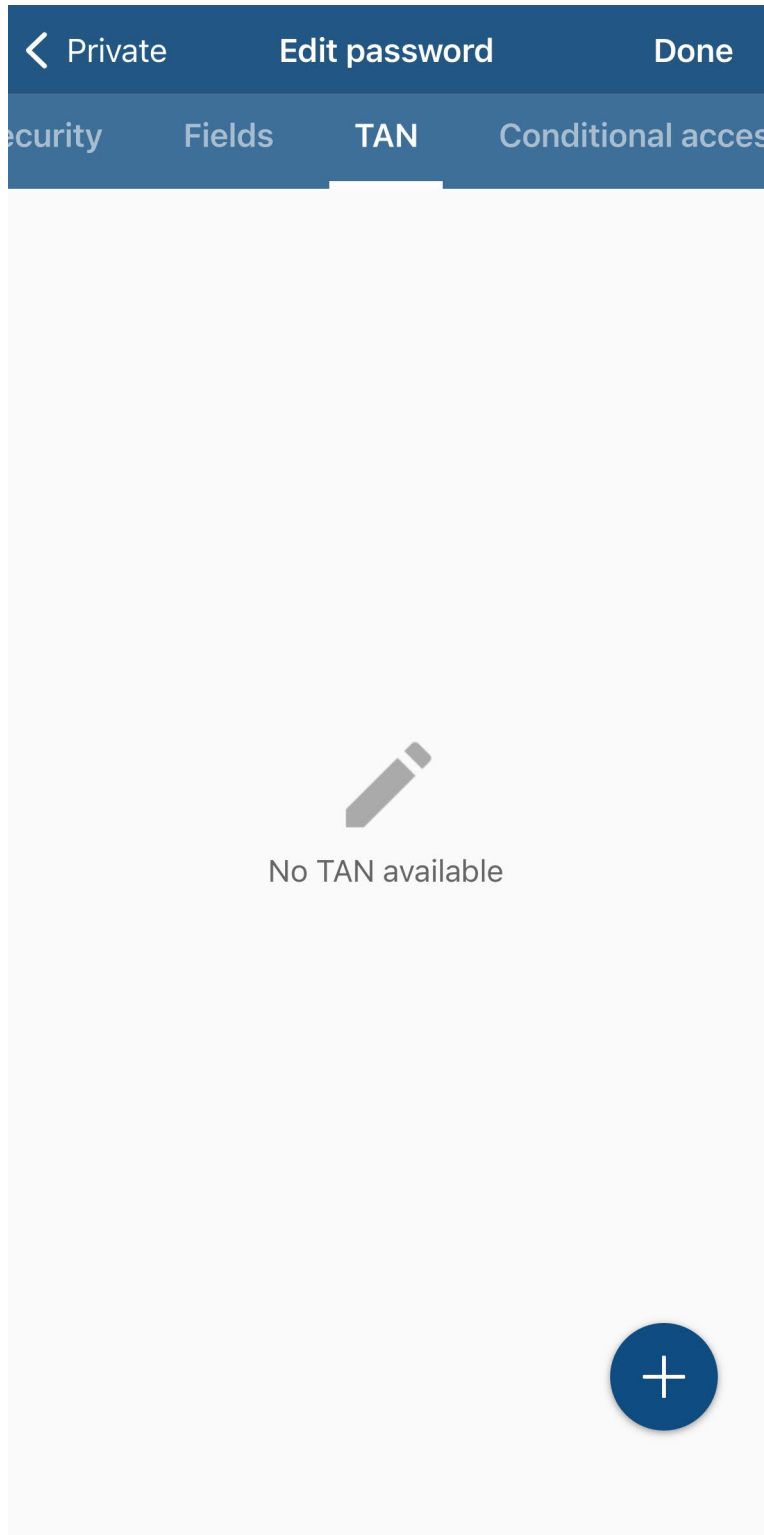
 Open URL

 Create linked entry

Manage TAN list

For certain banking/transaction methods, you can store TANs (transaction numbers) as a list.

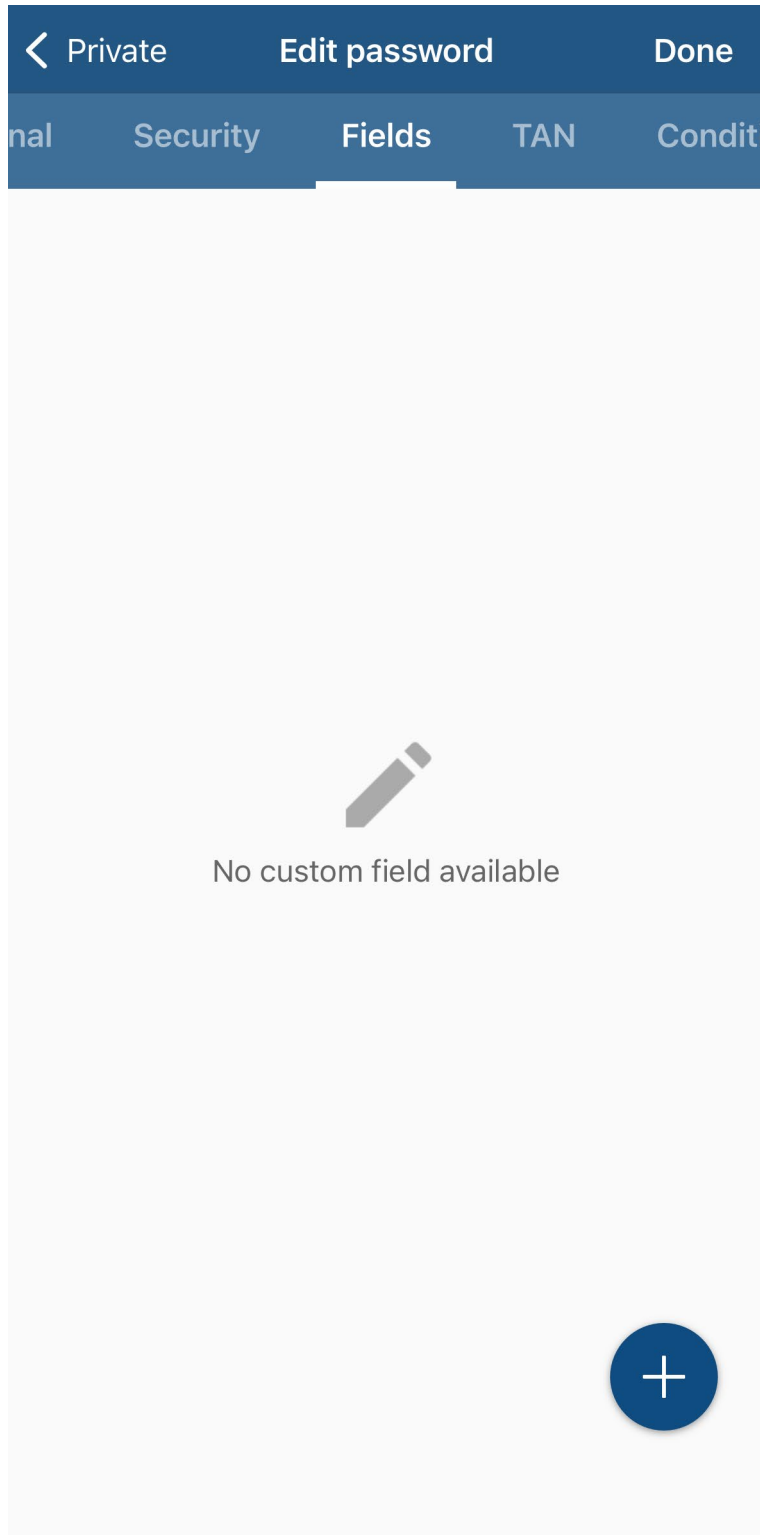
- Open an entry and select the **TAN** tab.
- Add a TAN via the +.
- Save the entry.



Add custom fields

You can add your own fields – e.g., "Customer number", "PIN2" or "Security question".

- Open an entry and switch to the **Fields** tab.
- Tap + to create an additional field.
- Select the field type (text/password/... if offered) and save.




Store certificates/key files in entries

For Certificate entries, you can add files and export them later.



- Create an entry of type **Certificate** or open an existing one.
- In **Edit**, select the public and/or private key.
- Save the entry.
- Use the Share function in the entry (to the right of the public/private key fields) if you need to export a certificate.



← Private New certificate Done


General Security Conditional access


Description 


Category

Public key  

Private key  

Password 

Medium 

Jan 9, 2026 

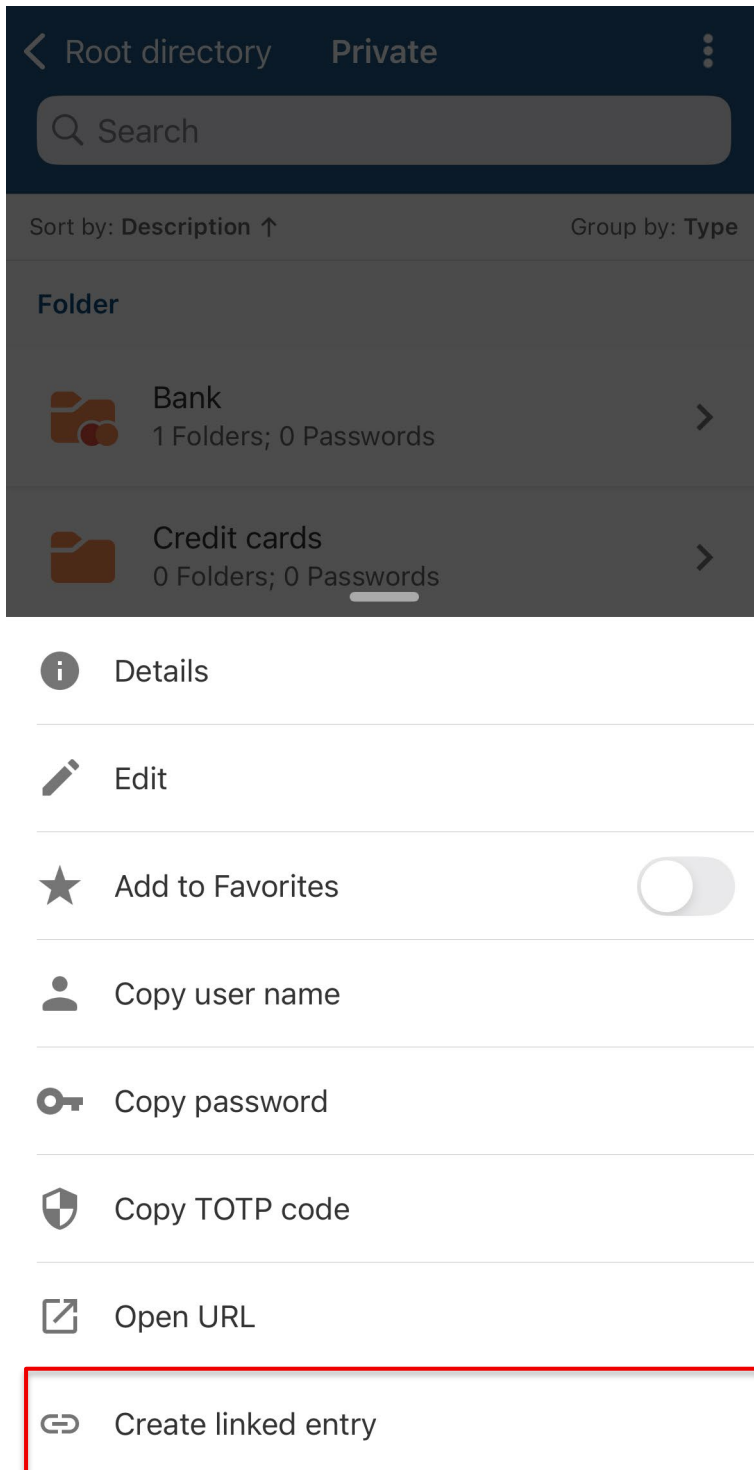
Tags

Notes

Links: reference an entry instead of duplicating it

With **Create linked entry**, you create a reference to an existing entry. Changes to the original are automatically reflected in all links.

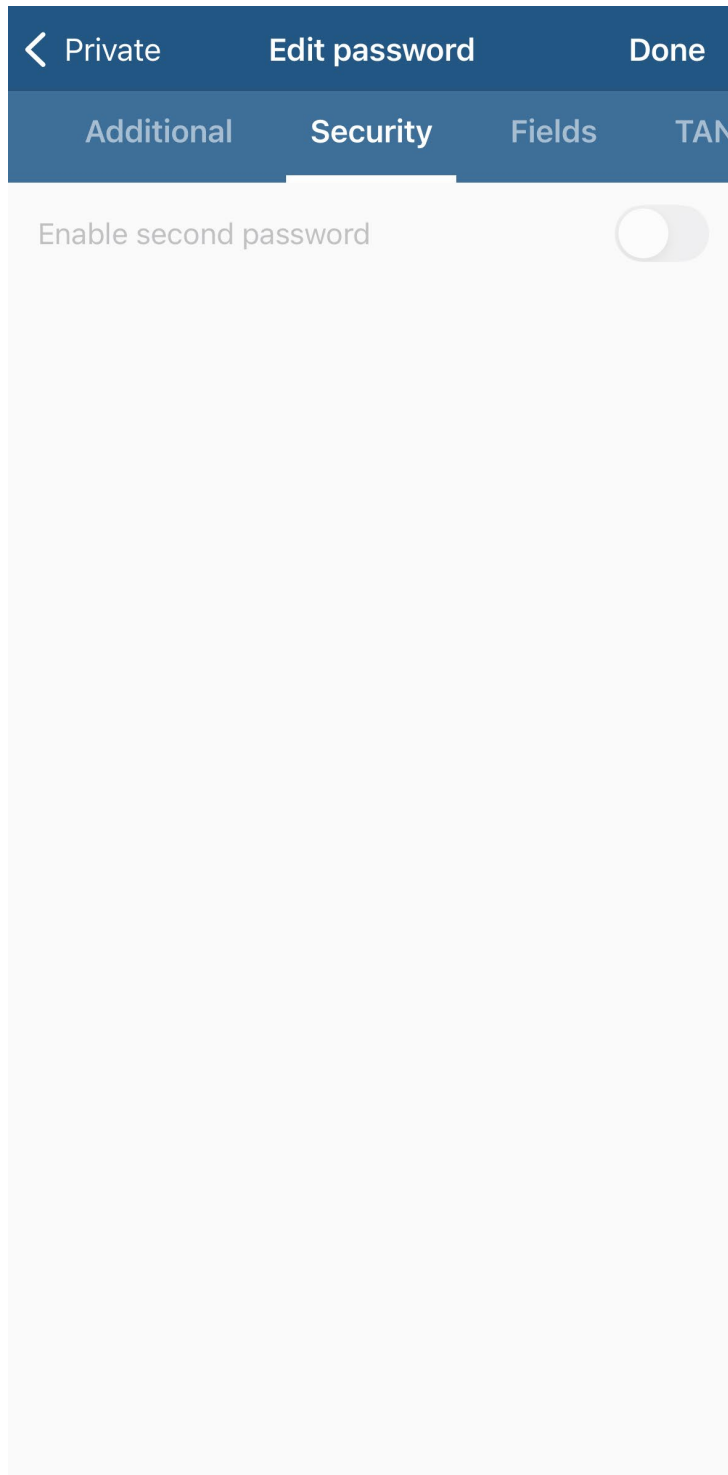
- Open an entry's actions.
- Tap **Create linked entry**.
- A linked copy is created in the current folder.



Second password: extra protection for sensitive entries

A second password protects particularly sensitive areas. When accessing them, you must enter this second password in addition to the master password.

- Open an entry or folder via **Edit**.
- Switch to the **Security** tab.
- Activate **Enable second password** and set a second password.



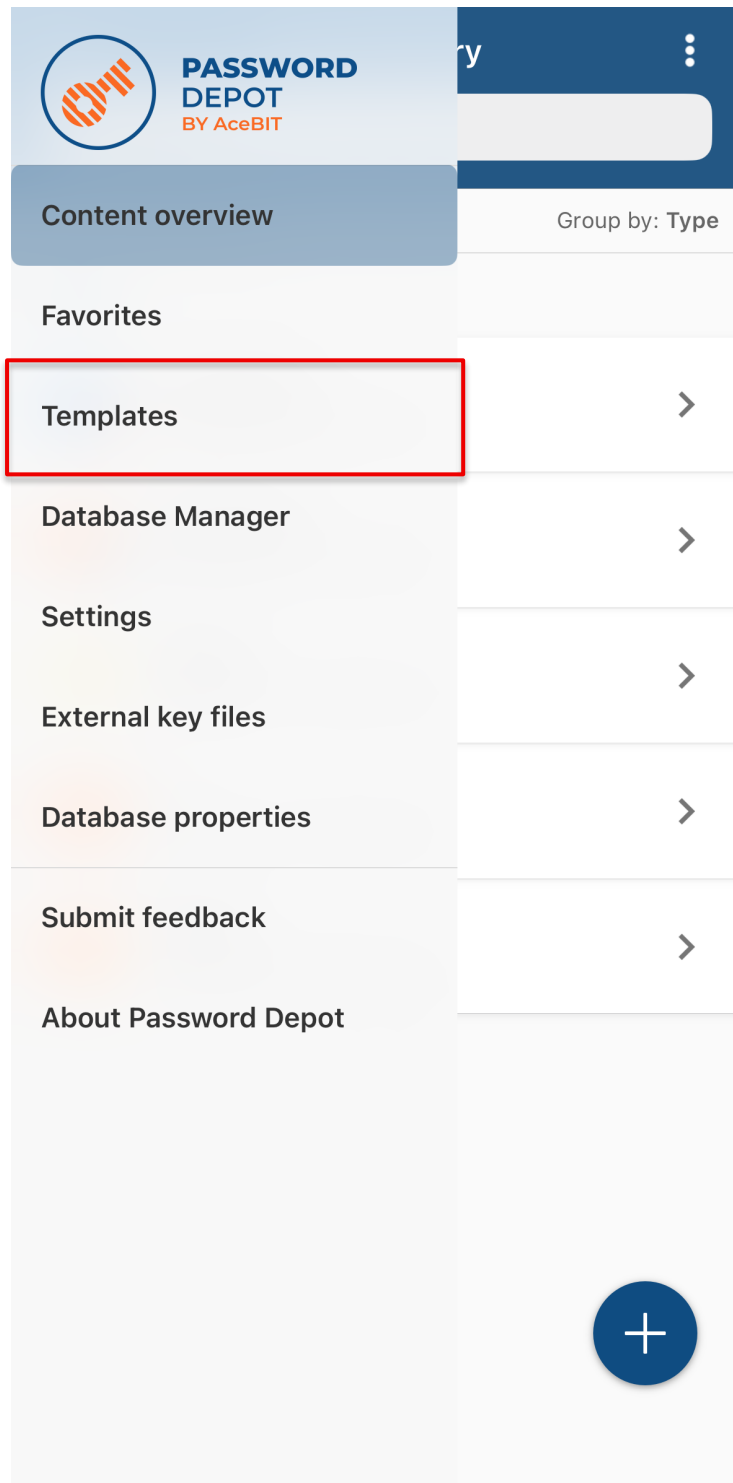
IMPORTANT: Make sure you reliably remember the second password as well. Without it, protected content remains locked.

Templates and custom entries

With templates, you can create custom entries (e.g., for internal processes, projects or special forms).

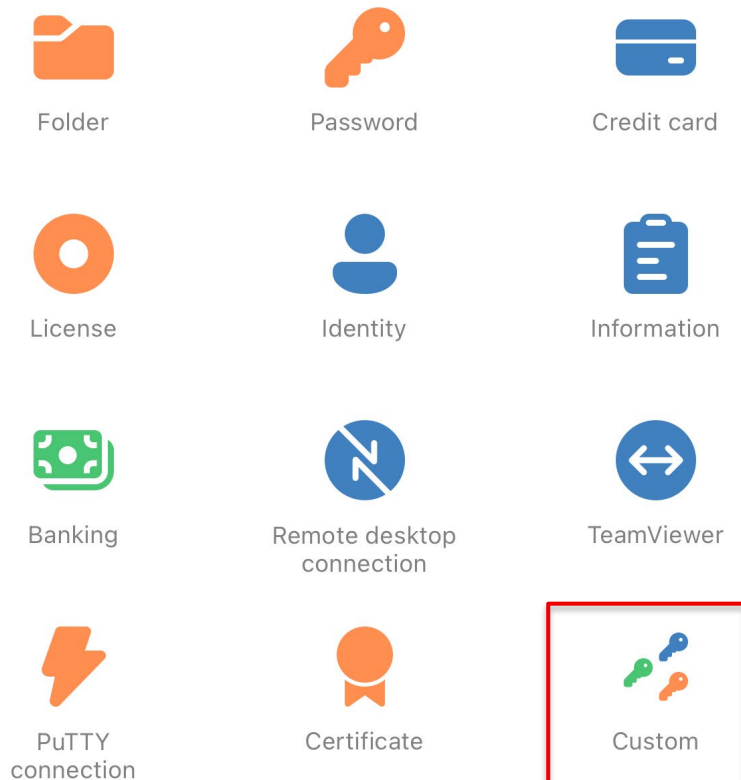
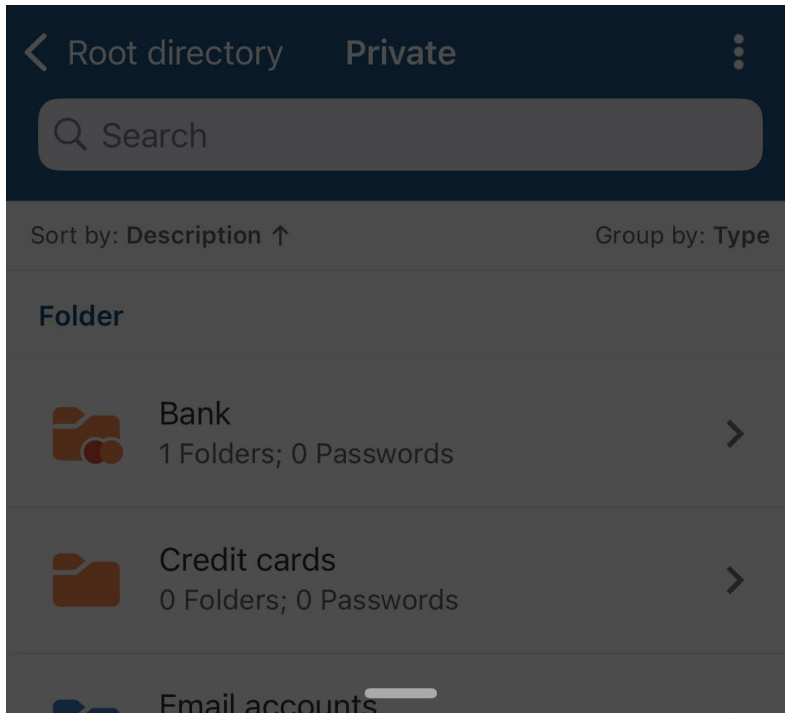
Manage templates

- Open **Menu** (☰) → **Templates**.
- Create a new template via **+** or edit existing ones.
- Define the fields that should appear when creating an entry later.



Create a custom entry

- In the content overview, tap +.
- Select **Custom**.
- Select the desired template.
- Fill in the fields and save.

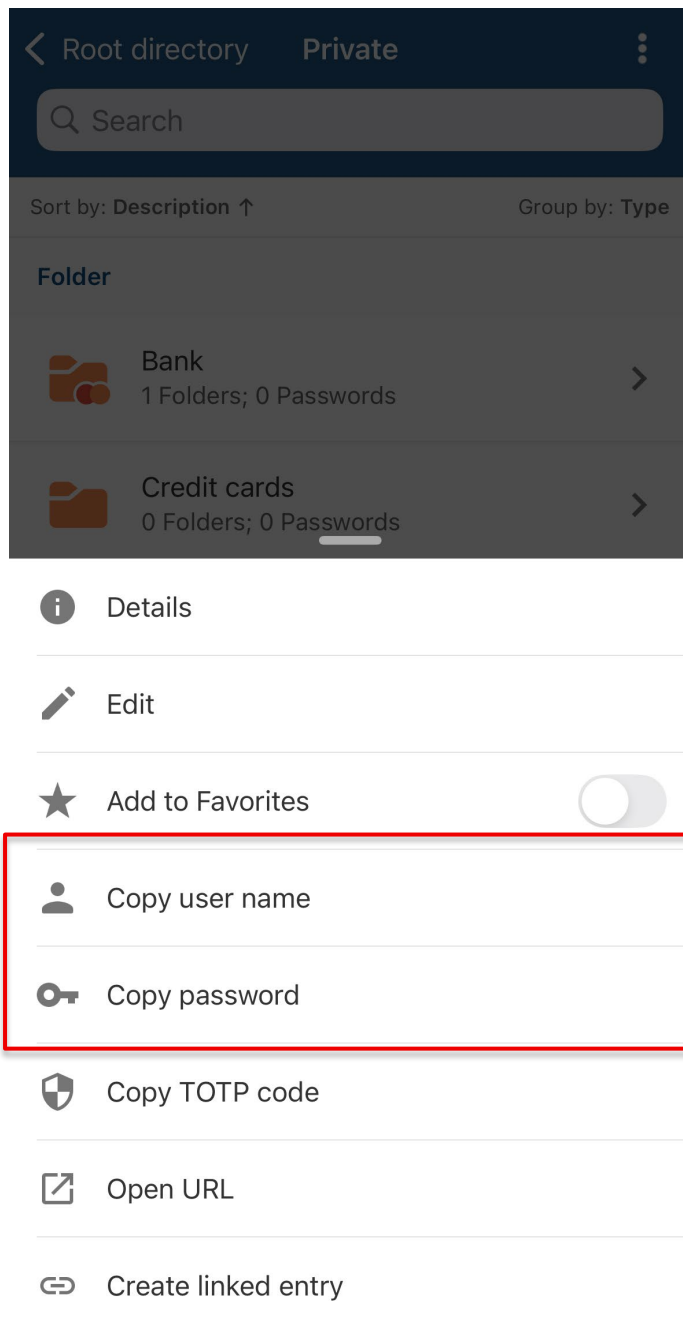


Use entries day to day

Copy user name and password

If you want to paste a password manually into another app:

- Tap the desired entry.
- Tap **Copy user name** or **Copy password**.
- Switch to the target app and paste.

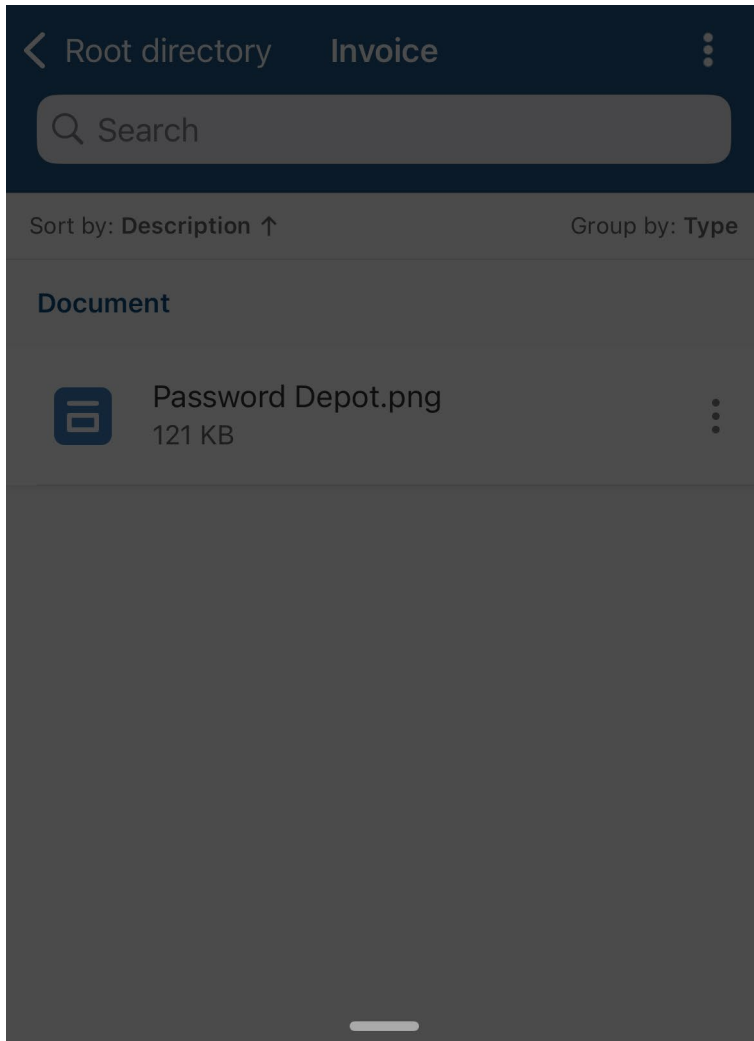


IMPORTANT: Rely on automatic clipboard clearing. If you have disabled it, clear the clipboard manually by copying harmless text.

Open documents

If your database contains Document entries, you can open/share them from within the app.


- Tap a **Document** entry.
- Select **View document**.
- Share or open the document in a suitable app.



 Details

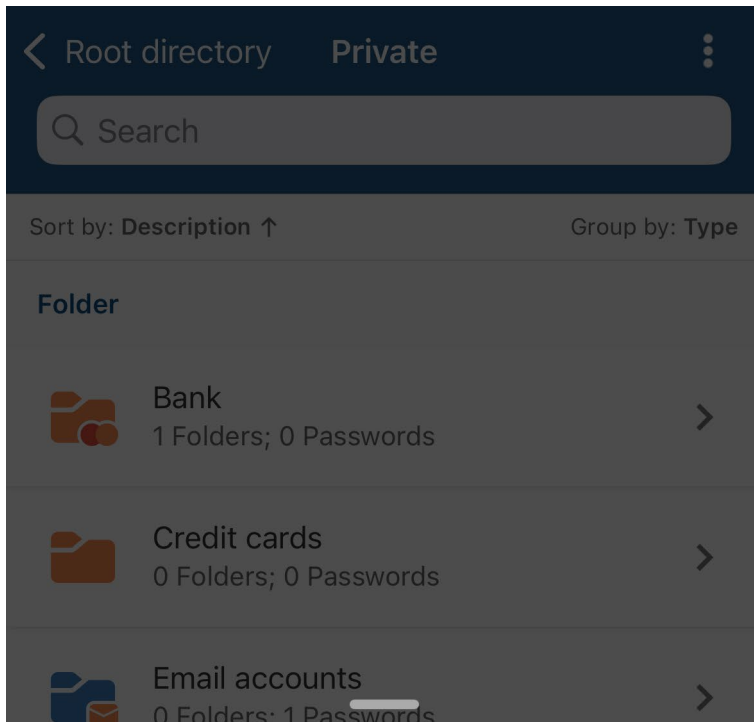
 Edit

 Add to Favorites

 View document

Open links


- Tap a linked entry (link icon).
- Select **Open reference entry** to view the original.




 Details

 Edit

 Add to Favorites

 Copy user name

 Copy password

 Open URL

 Open reference entry

Protect and manage the database

In the content overview, important database functions are available via the menu (three dots in the top-right).

The screenshot shows a mobile application interface for a database. At the top, there is a navigation bar with a back arrow, 'Root directory', and 'Private'. Below this is a search bar with a magnifying glass icon and the text 'Search'. A 'Sort by: Description ↑' option is visible. The main content area is divided into sections: 'Folder', 'Password', and 'Credit card'. Each section contains entries with icons, names, and counts of folders and passwords. A context menu is open over the 'Bank' folder, listing actions: Save, Backup, Lock, Refresh, Change credentials, Export, and Close database. A blue circular button with a white plus sign is located at the bottom right of the interface.

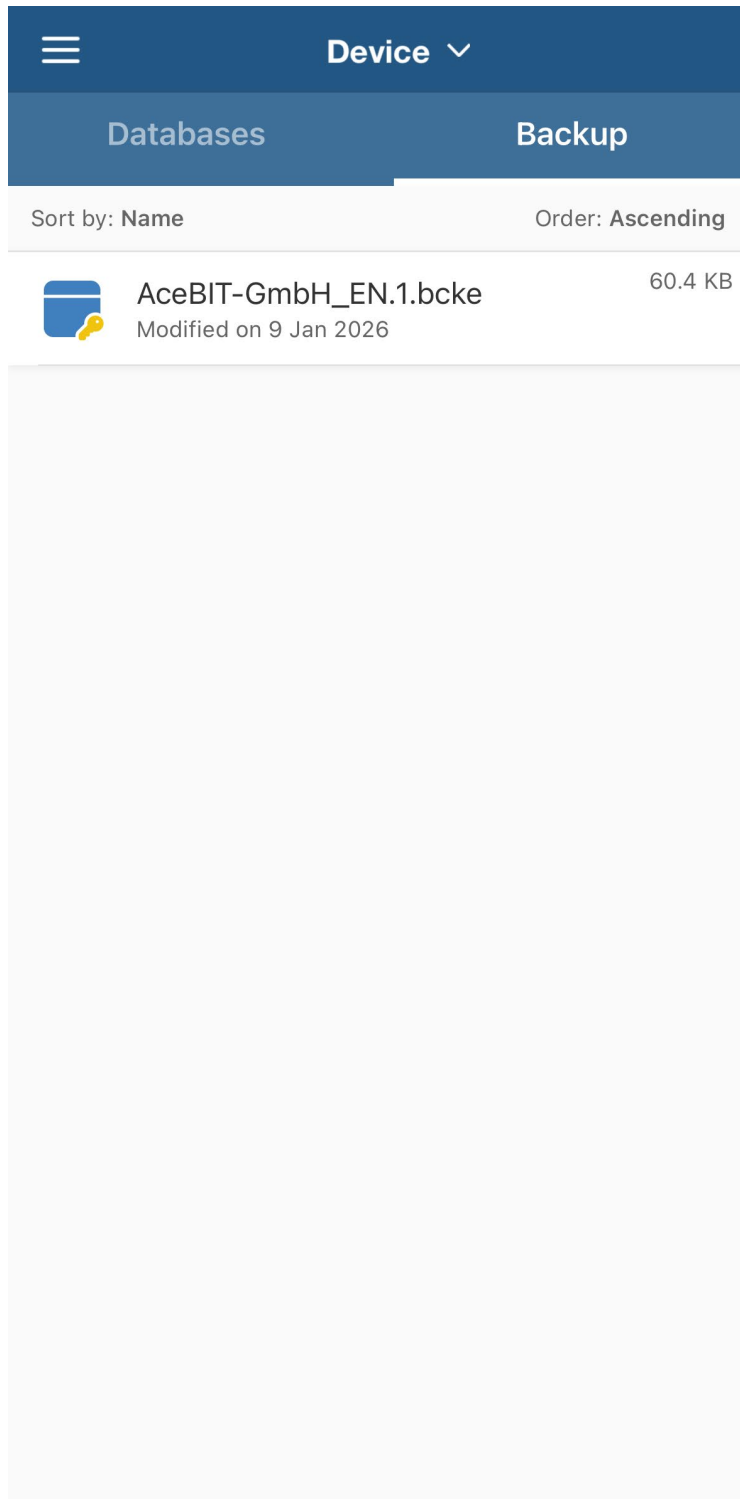
Section	Item Name	Count	Actions
Folder	Bank	1 Folders; 0 Passwords	Save, Backup, Lock, Refresh, Change credentials, Export, Close database
	Credit cards	0 Folders; 0 Passwords	
	Email accounts	0 Folders; 1 Passwords	
Password	AceBIT Support	https://support.acebit.com/	
	Password Depot	https://web.password-depot.de	
Credit card	Mastercard	MasterCard	
	Visa	MasterCard	

Save

- Tap **Save** to commit changes immediately.
- If **Auto-save** is enabled, the app also saves in the background.

Create and restore backups

- Tap **Backup** to manually create a backup of your database.
- Then open **Menu (☰) → Database Manager → Device → Backup** to view and, if needed, open the backup.



Lock and unlock

- Tap **Lock** to close/lock the database immediately.
- Afterwards, unlock the database again as usual via master password (and, if applicable, key file/biometrics).

Refresh

Use **Refresh** when the database is in the cloud or on a server and you want to synchronize changes.

Change the master password

- Tap **Change credentials**.
- Enter the current master password and/or current key file.
- Set a new master password and/or a new key file.
- Save to finish.

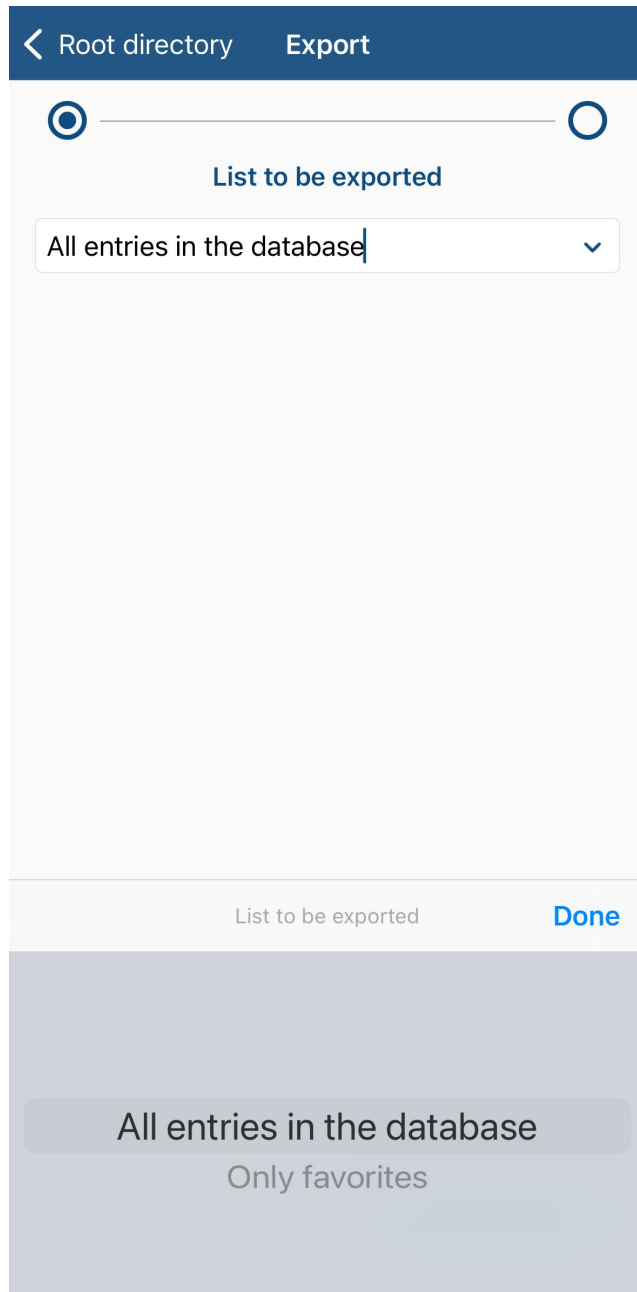
The screenshot shows a mobile application interface for changing credentials. At the top, there is a dark blue header bar with a white back arrow on the left and the text "Change credentials" in white. Below the header, there is a progress indicator consisting of three circles connected by a horizontal line; the first circle on the left is filled with blue, while the other two are empty. Below the progress indicator, the text "Current credentials" is displayed in a dark blue font. Underneath this text is a white text input field with a light blue border, containing the placeholder text "Old password" in a light grey font. To the right of the input field is a small blue eye icon for toggling password visibility. At the bottom of the screen, there are two buttons: a grey button with the text "Back" and a dark blue button with the text "Next".

IMPORTANT: Change a master password only if you are sure you will keep the new password (and, if applicable, the new key file) available long-term.

Export

Export creates an unencrypted file (XML, CSV or TXT). This can be helpful, for example, if you want to use your database on another device.

- Tap **Export**.
- Select the desired content (e.g., **all entries in the database** or **only favorites**) and the desired format (**XML**, **CSV** or **TXT**).
- Save/share the export file only via secure channels.



WARNING: Export files contain your data unencrypted. Store export files only briefly and delete them afterwards.

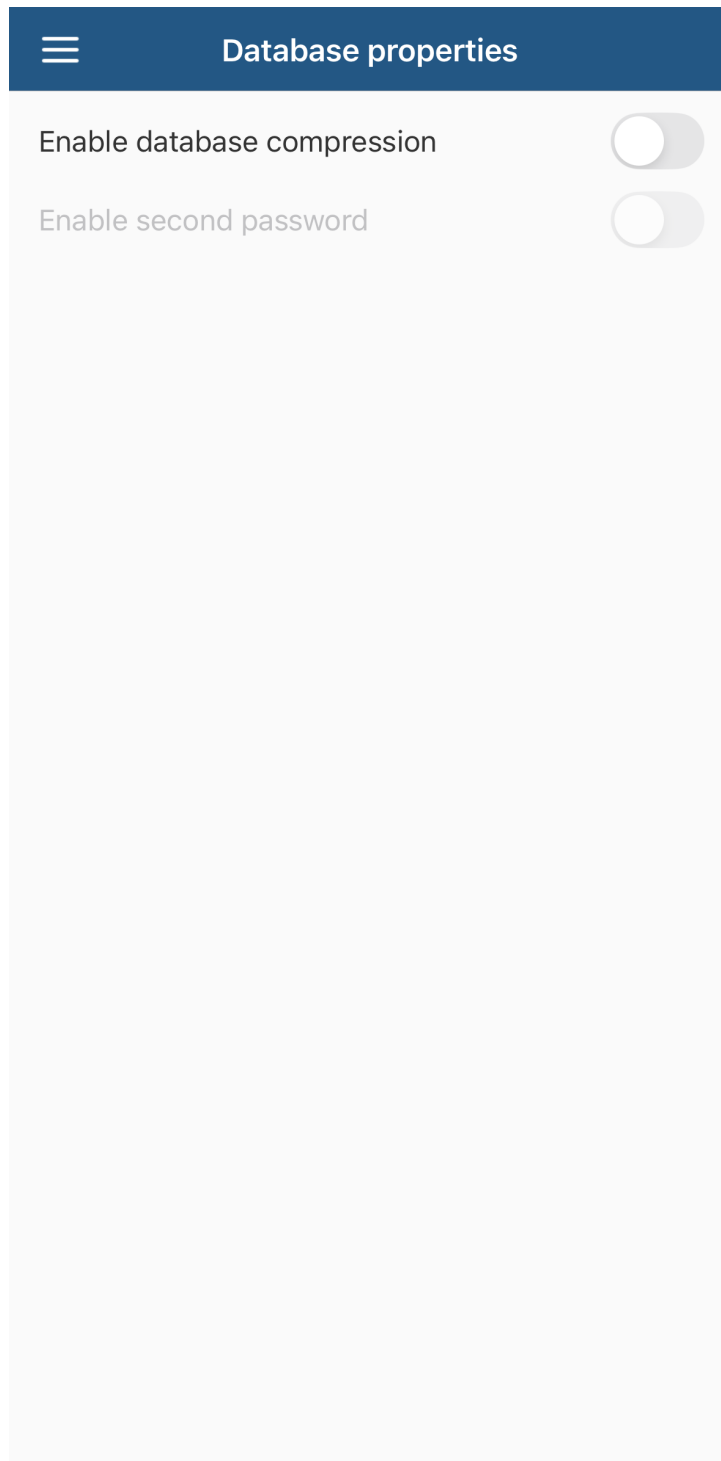
Close database

- Tap **Close database** when you are finished. The database will be locked again.
- Later, open the database again via the Start area or the **Database Manager**.

Database properties

In **Database properties**, you manage settings that belong to the currently opened database.

- Open **Menu (☰)** → **Database properties**.
- If needed, activate **Enable database compression**.
- Manage the database second password here as well (**Enable second password**).



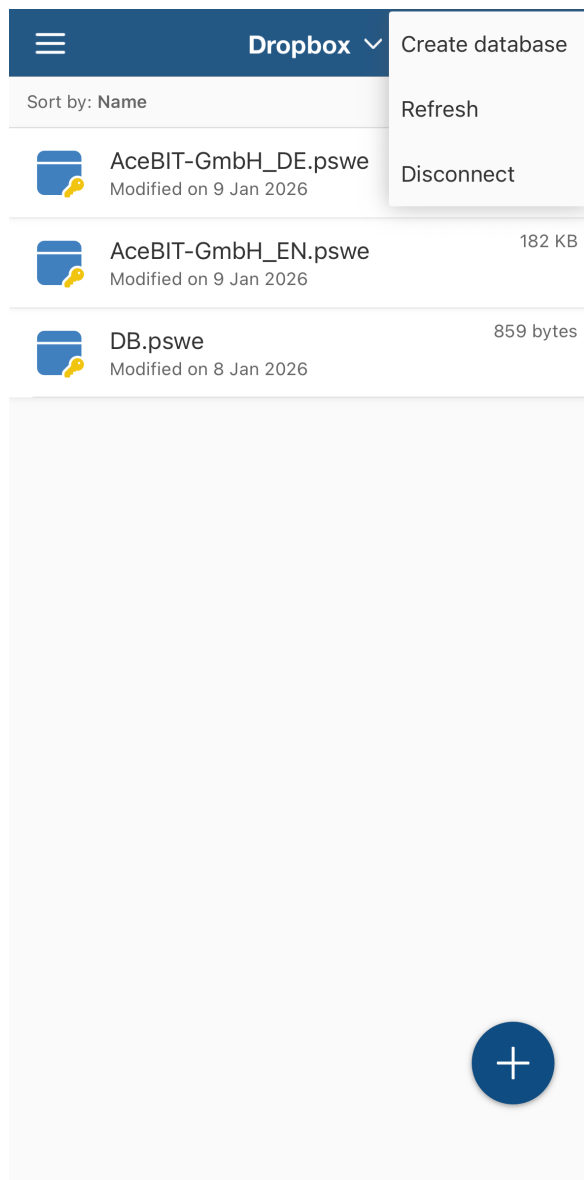
Storage locations and synchronization

Connect and disconnect cloud storage

If you use the same database on multiple devices, store the database in a central location (cloud for private use or Enterprise Server for business customers).

TIP: Before switching devices, always save (three-dot menu top-right → **Save**) and use **Refresh** to avoid conflicts.

- Open **Menu** (☰) → **Database Manager**.
- Select the desired cloud service via the down arrow (**Dropbox, Google Drive, OneDrive, Box or HiDrive**).
- Tap **Connect** and sign in to your cloud service.
- Open the database from the cloud as usual.



- If needed, tap **Disconnect** in the three-dot menu to end the cloud connection.

FTP and WebDAV Servers

For server storage, you typically need address, username and password.

- In the Database Manager, select **FTP Server** or **WebDAV Server**.
- Tap **Connect**.
- Enter the server details and confirm.


Connect to WebDAV server

🌐 Custom ▾

Address

/Password Depot/

User name

Password 

Remember password

Cancel OK

Service Done

Custom

GMX MediaCente

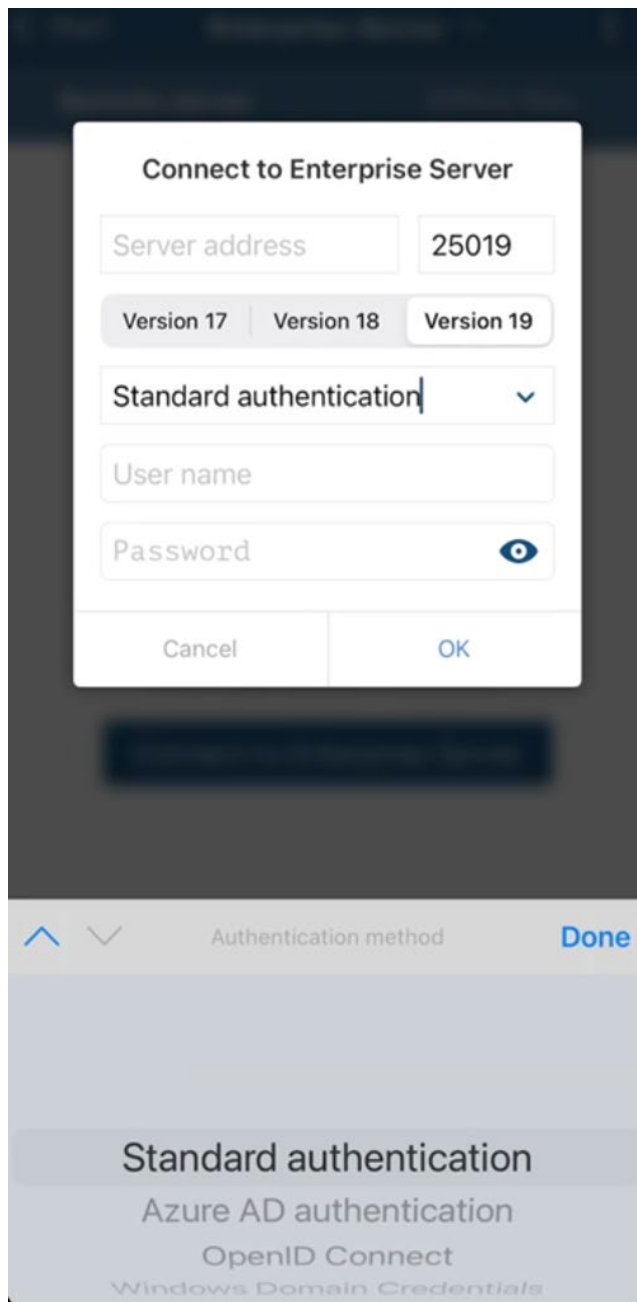
WEB.DE Online-Speicher

MagentaCLOUD

Enterprise Server (company)

If your organization uses a Password Depot Enterprise Server, you will receive the access details from your administrator.

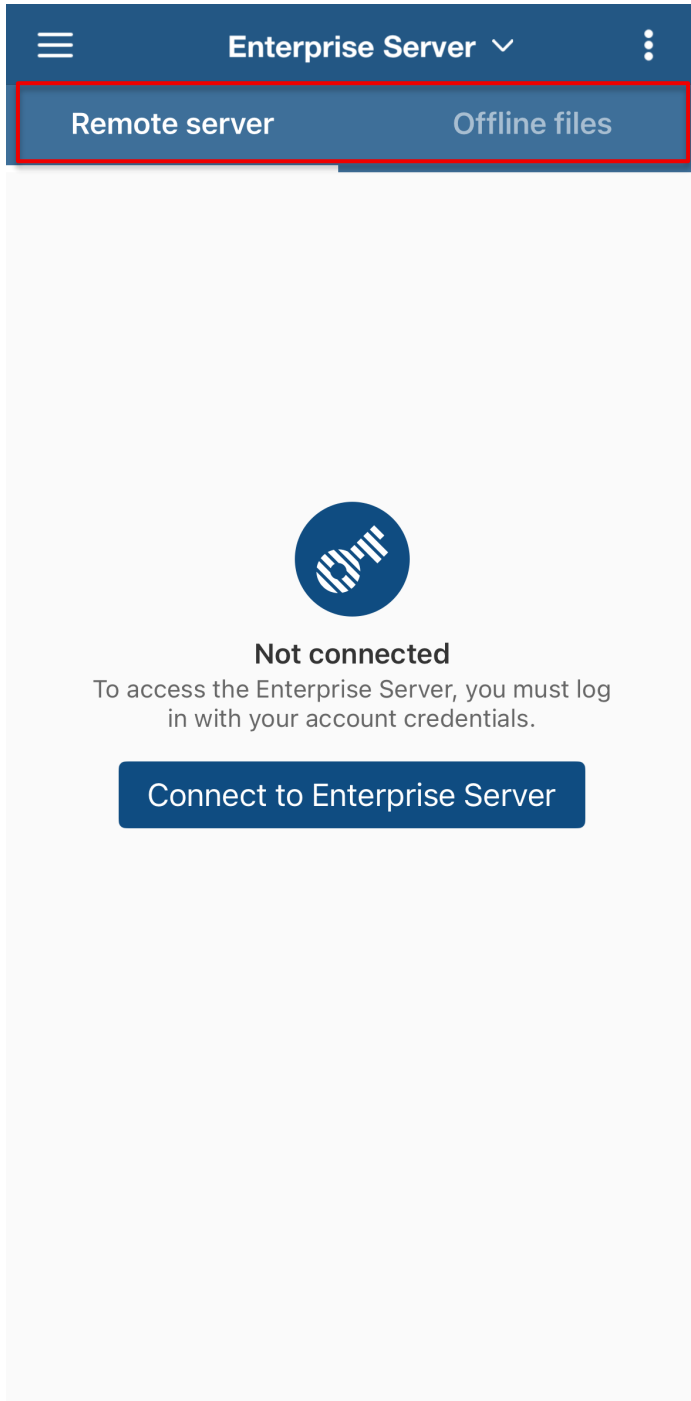
- Open **Menu** (☰) → **Database Manager** and select **Enterprise Server**.
- Tap **Connect to Enterprise Server** and enter server address, port, server version, username and password. In addition to standard authentication, Azure AD authentication, OpenID Connect as well as authentication via Windows Domain Credentials may also be available if configured by your company.
- Open a shared database from the list.



WARNING: Creating databases on the Enterprise Server is done exclusively via the server's Server Manager. You can only open server databases if you have access rights. Access rights are granted by your server administrator.

Offline mode (if enabled))

- If the required permissions have been granted offline files may also be displayed in the Enterprise Server.
- Edit databases offline only if your organization explicitly allows it.
- Afterwards, synchronize when you are online again.



Tips

Secure on the go: the most important rules

- Use a strong master password and never share it.
- Enable a short auto-lock and biometrics (if available).
- Let the clipboard clear automatically.
- Use a key file as a second factor – and store it separately.
- Create regular backups and store them in a secure location.
- Use a unique random password per account, created via the generator.

Organization: find faster instead of searching

- Use folders for clear structures (e.g., "Private", "Work", "Banking").
- Assign categories and tags (keywords) to find entries faster later.
- Mark important entries as favorites.
- Use Sort/Group, e.g., "Group by category".

Quickly solve common problems

The database cannot be opened:

- Check capitalization and the keyboard layout you are using.
- Make sure you selected the correct key file (if used).
- Use **Show hint** (if available) to help you remember the correct master password.

Problems with biometrics:

- Check your iOS device settings to ensure Touch ID/Face ID for apps is enabled.
- Disable biometrics in the app settings and then enable it again.

Auto-fill does not work on a website:

- Use the auto-fill sequence with a delay.
- Fill fields individually using the buttons "Username", "Password" and, if applicable, "TOTP".

Help and Support

If you need further assistance, please contact us:

- Open the menu (top-left) and select **Submit feedback**. You will be taken to the Password Depot website. Please select the Support section there.
- Open the menu (top-left) and select **About Password Depot**. The links also lead to our website where you can choose the Support section.