



**PASSWORD
DEPOT**
BY AceBIT

Password Depot for Android

Quick Start Guide – Android

As of: January 26, 2026

This guide walks you through the most important steps to use Password Depot safely on Android—no technical background required.

Table of Contents

Table of Contents	2
Introduction.....	4
Key Terms	4
Getting Oriented.....	5
Getting Started	9
Install and launch the app	9
Create a new database (recommended).....	11
Open an existing database	13
Import a database or key file.....	15
App Settings.....	16
General	16
Storage.....	17
Biometrics.....	17
Appearance.....	17
Security	18
Search	18
Managing Key Files	19
Core Features	20
Create and edit entries/folders	20
Link entries	24
Use the password generator	25
Store and copy 2FA codes (TOTP)	26
Sign in securely: built-in browser and auto-complete	28
Favorites, search, and sorting	30
Protecting and Managing Your Database.....	34
Syncing and Access on the Go	36
Connect a cloud service.....	36
Enterprise Server (business).....	39
Find and restore backups	40
Tips	41
Everyday security checklist.....	41
Extra protection: Second password.....	41

Quick fixes for common problems	43
Help & Support	44

Introduction

Password Depot is a password manager. You store your credentials—such as passwords or credit card details—in an encrypted database and can securely access them from anywhere.

- Technical requirements: Android 12 or later is required.
- The Android app is available for free—no license is required.

IMPORTANT: Without your database master password, your data cannot be recovered. Choose a strong password and keep it safe.

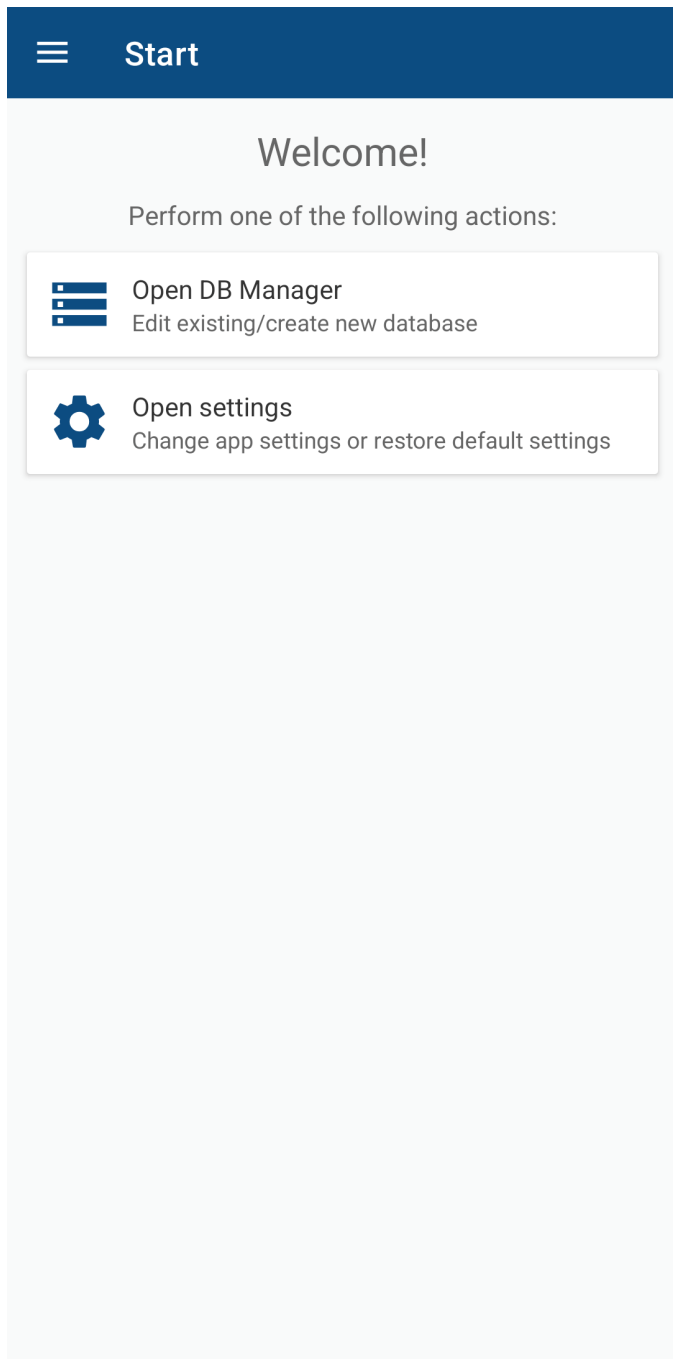
Key Terms

- **Database:** Your encrypted file containing all entries (e.g., “Private.psw”).
- **Master password:** The main 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., a password, credit card, or identity.
- **Folder:** Folders let you group entries as you like (e.g., “Work”, “Personal”).
- **Favorites:** Favorites give you quick access to frequently used entries.
- **TOTP:** A time-based one-time code for 2FA logins.

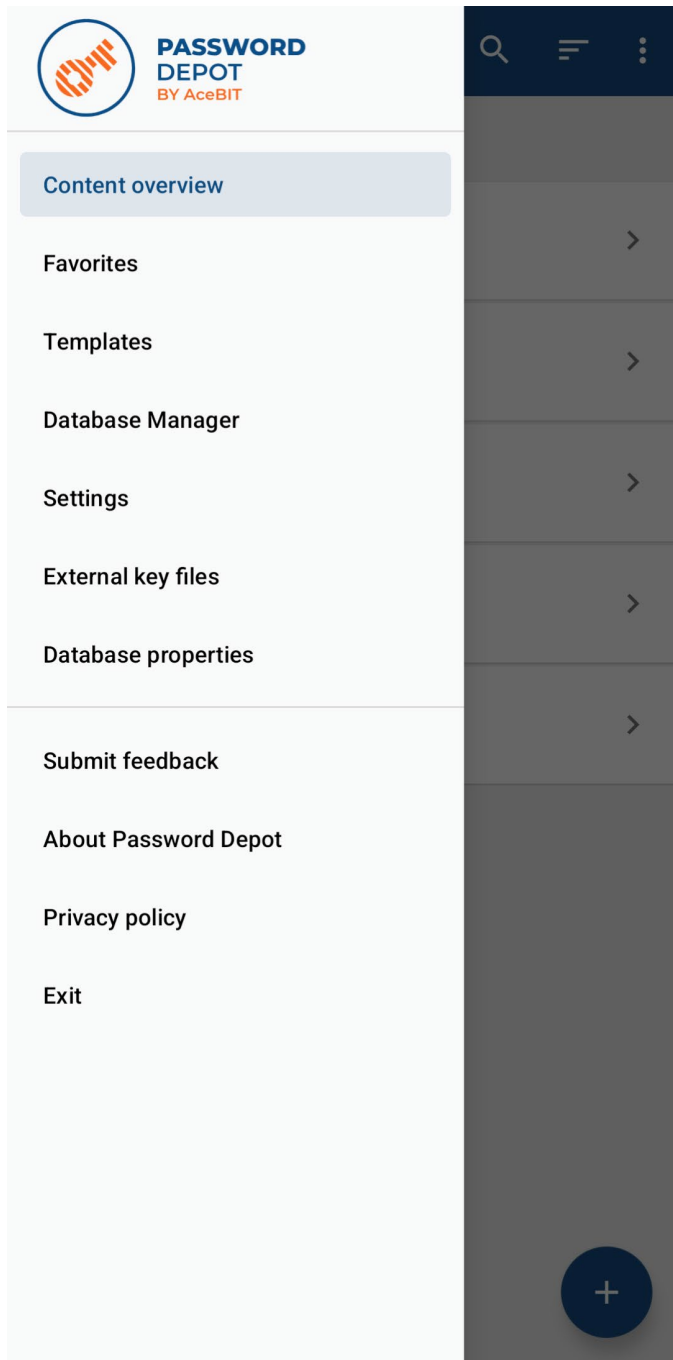
Getting Oriented

The app is structured around these main areas:

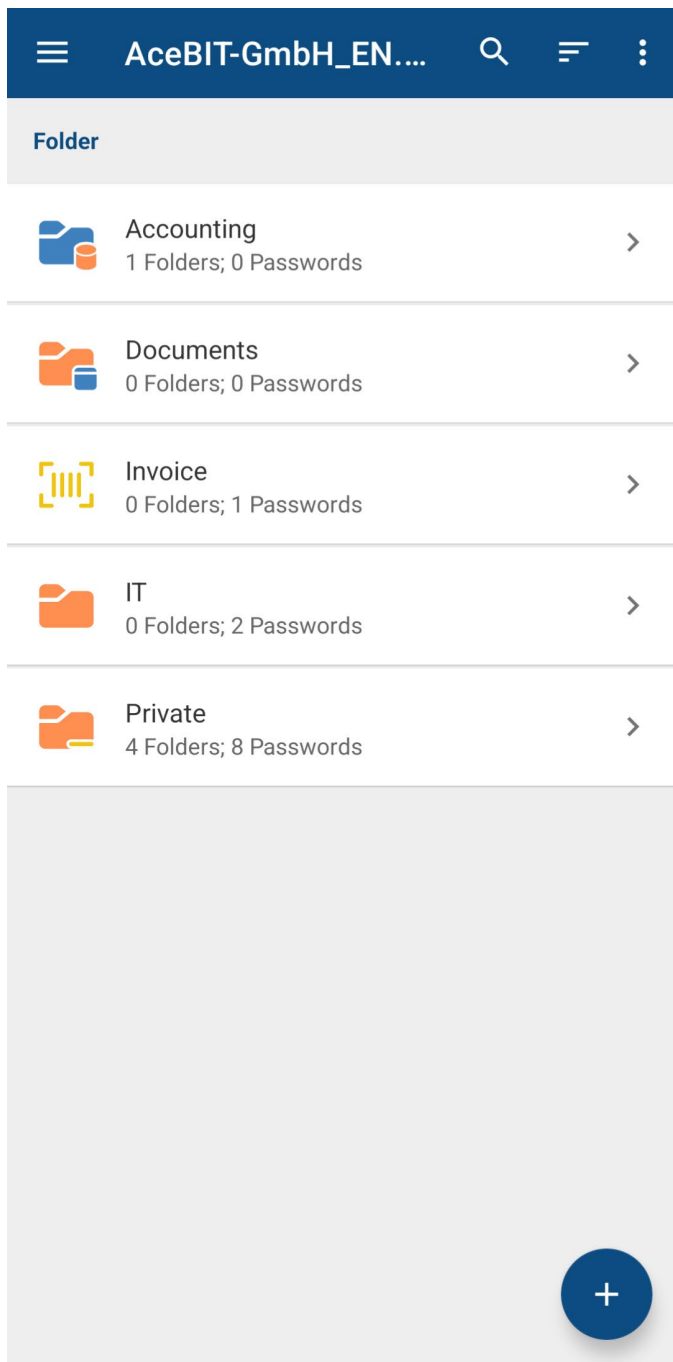
- **Home screen:** Quick actions and recently used databases.



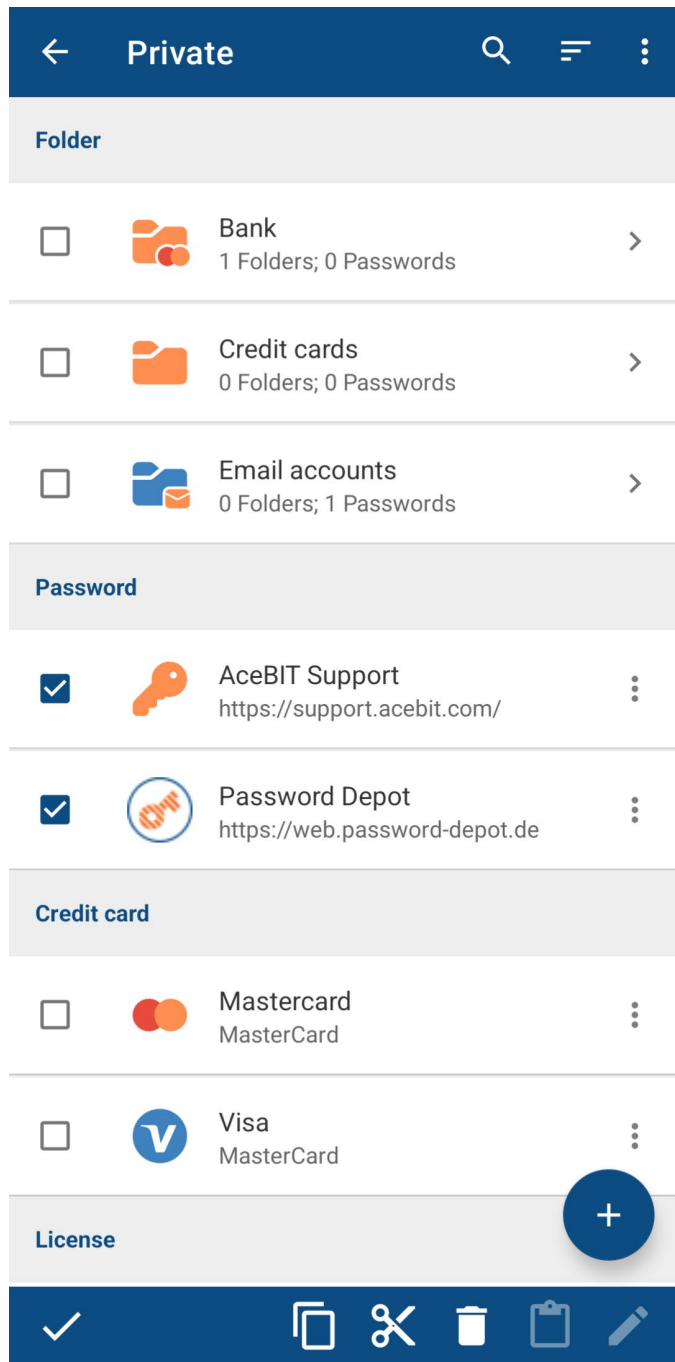
- **Navigation menu** (top-left): Switch to Database Manager, Favorites, Settings, etc.



- **Top action bar** (e.g., Search, Sort, 3-dot menu): Actions for the current view.



- **Bottom context bar:** Appears after long-pressing a database, folder, or entry (multi-select possible).




Getting Started

Install and launch the app

- Install Password Depot from the Google Play Store.

←

⋮

 **Password Depot for Android**
AceBIT

4.5 ★
3K reviews ⓘ

500K+
Downloads

3
PEGI 3 ⓘ

Install ▾

Install on phone.

Sync and access your vault from multiple devices

Access your vault with your fingerprint

Keep all of your private info encrypted in one place

Quickly auto-fill logins

About this app →

Password Depot for Android is an easy-to-use and powerful password manager.

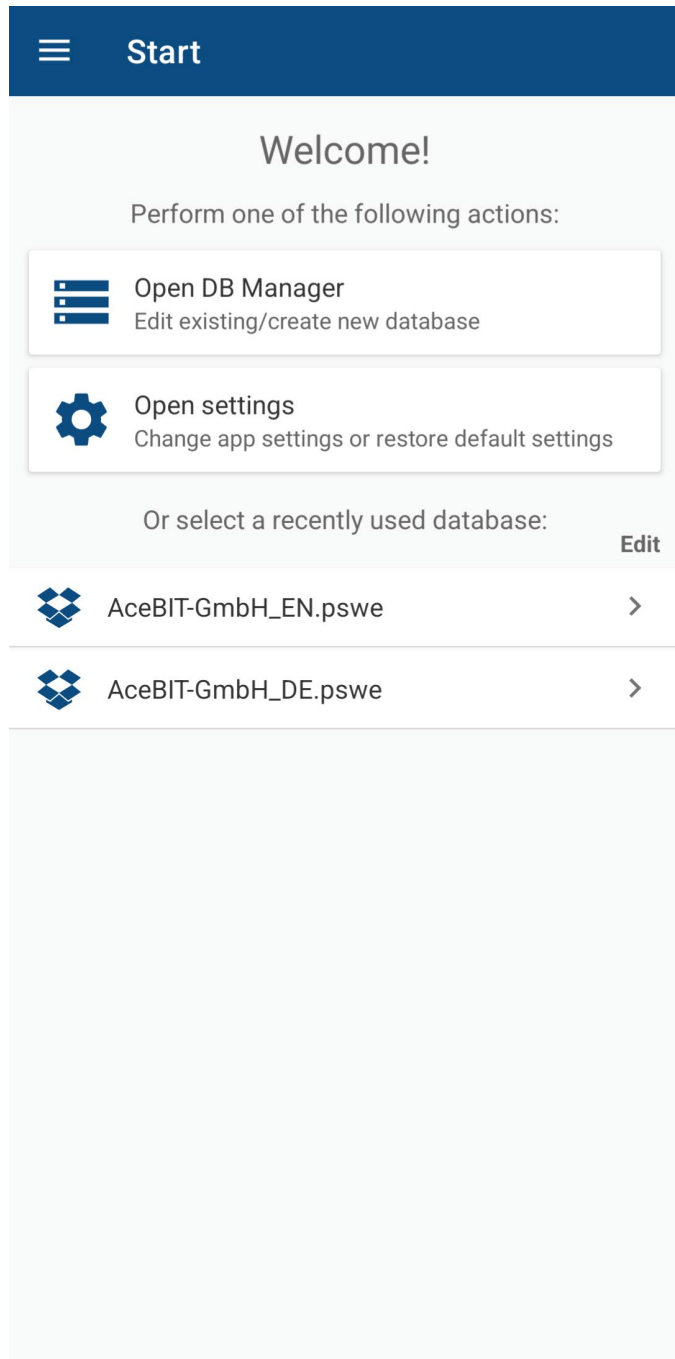
Tools Password

Data safety →

Safety starts with understanding how developers collect

Games Apps **Search** Books

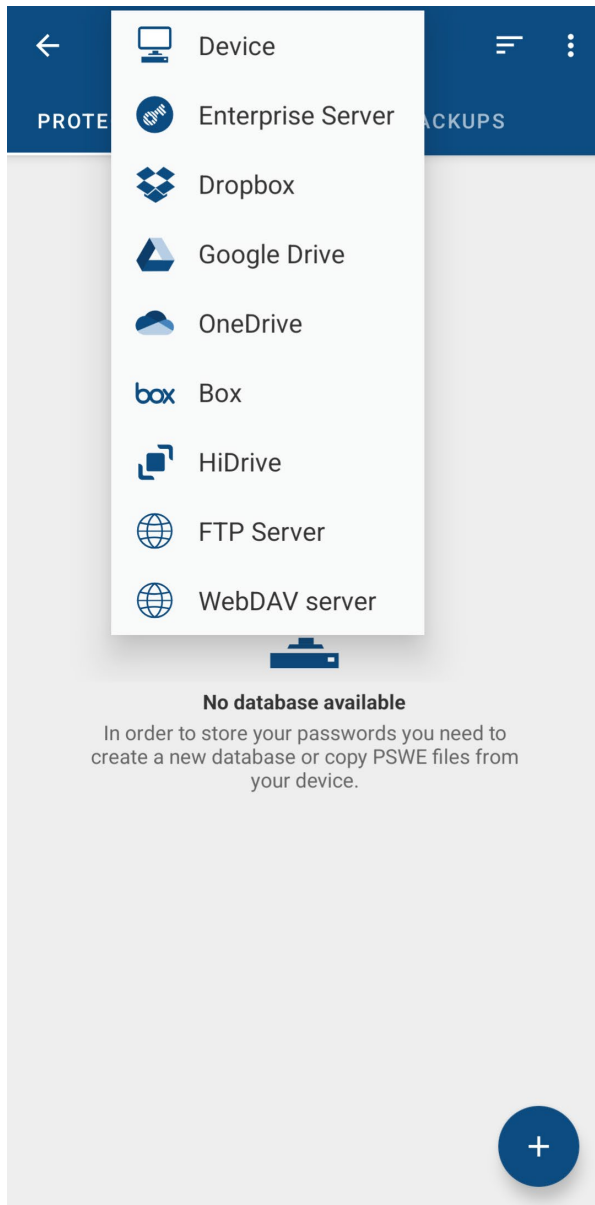
- Open the app. On the home screen you'll see quick actions and recently used databases.



Create a new database (recommended)

Create a new database if you're starting fresh or want a clean structure.

- Tap **Open DB Manager** to open the Database Manager.
- Select where you want to store/open the database (tap the small down arrow at the top). Available locations: **Device**, Enterprise Server, Dropbox, Google Drive, OneDrive, Box, HiDrive, FTP Server, WebDAV Server. If you select Device, the database is stored in **Protected Storage** by default for maximum security.



- To create a database under **Device**, tap the button in the bottom-right corner (white plus on blue). Enter a name and choose **PSWE** as the format (recommended).
- Choose the authentication method:
 - • **Master password** (standard)
 - • **Master password + key file** (most secure)
 - • **Key file only** (not recommended)
- Enter your master password and/or select the key file. You can also add a hint to help you remember the password.
- Tap **Create database** to finish.

← Create database

Name PSWE

Authentication by
Master password and key file

15+ Length A Uppercase a Lowercase 0-9 Numbers

CHECK IN PWNEED PASSWORD LIST

Password

Confirm password

Key file
No key file available +

Hint

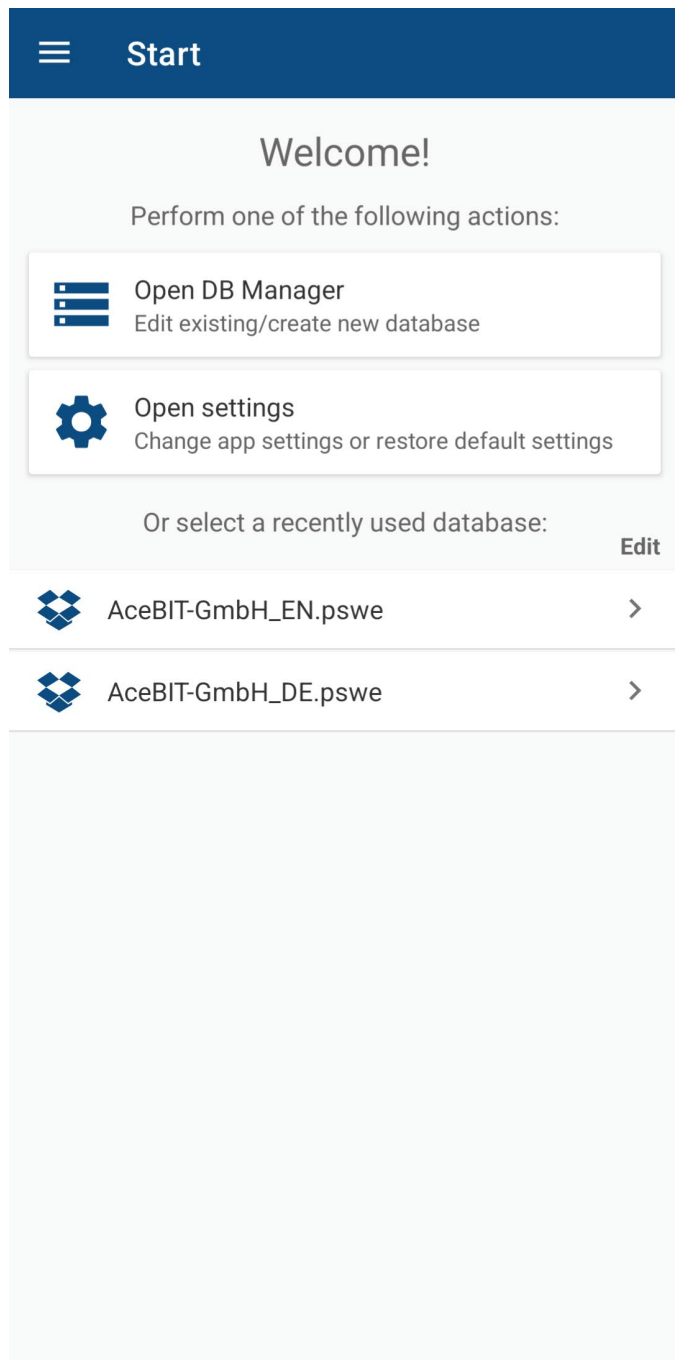
Storage location Protected storage

CREATE DATABASE

TIP: Use a key file as an additional factor and store it separately from the database (e.g., in a different cloud service or another secure location).

Open an existing database

- From the home screen under **Recently used databases**, tap the database, or open the Database Manager and select the file there.



- Enter your master password. If you use a key file, select the correct key file as well.
- Optional: Tap **Show hint** if you saved a password hint.



To unlock "DB.psw" please enter your password and select the key file.

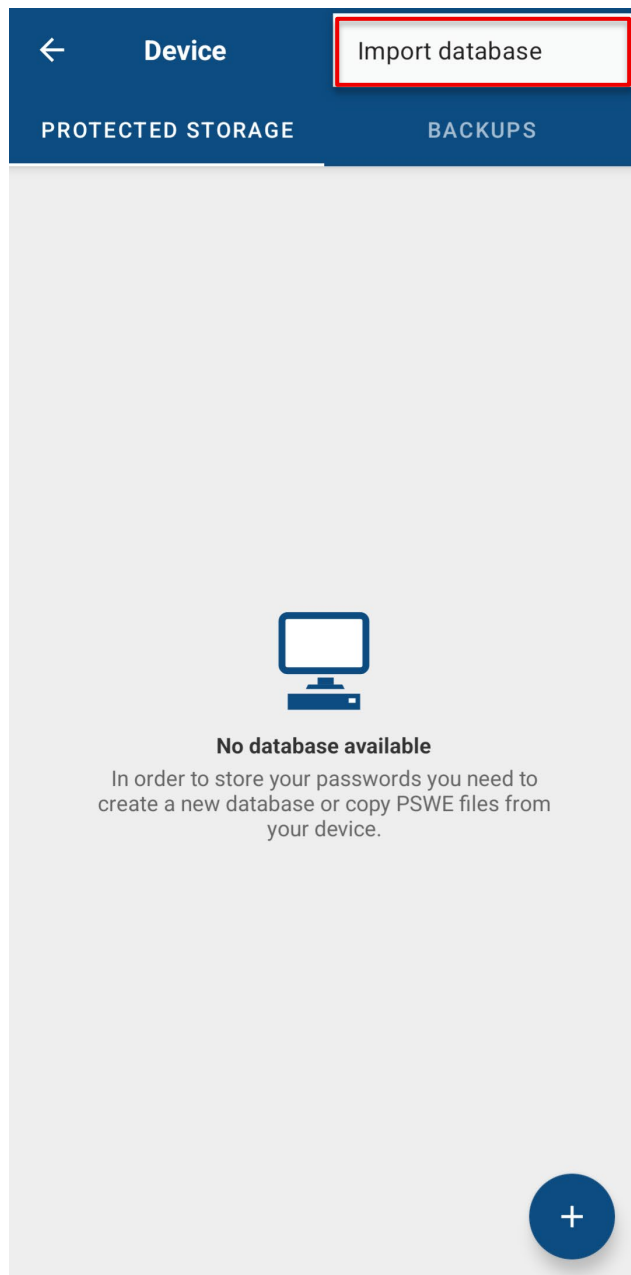
Import a database or key file

Import existing database files (e.g., created in Password Depot for Windows or on another device) so you can open them in the Android app.

- Open the **Database Manager**.
- Tap the three dots (top-right) and select **Import database**.
- Select the file (.pswe/.pswd or a key file). The app copies it into Protected Storage.

IMPORTANT: Keep databases in Protected Storage whenever possible. Files in publicly accessible folders are easier to attack.

CAUTION: Databases in Protected Storage belong to the app. If you uninstall the app, these files are deleted. Create backups (ideally outside the app).

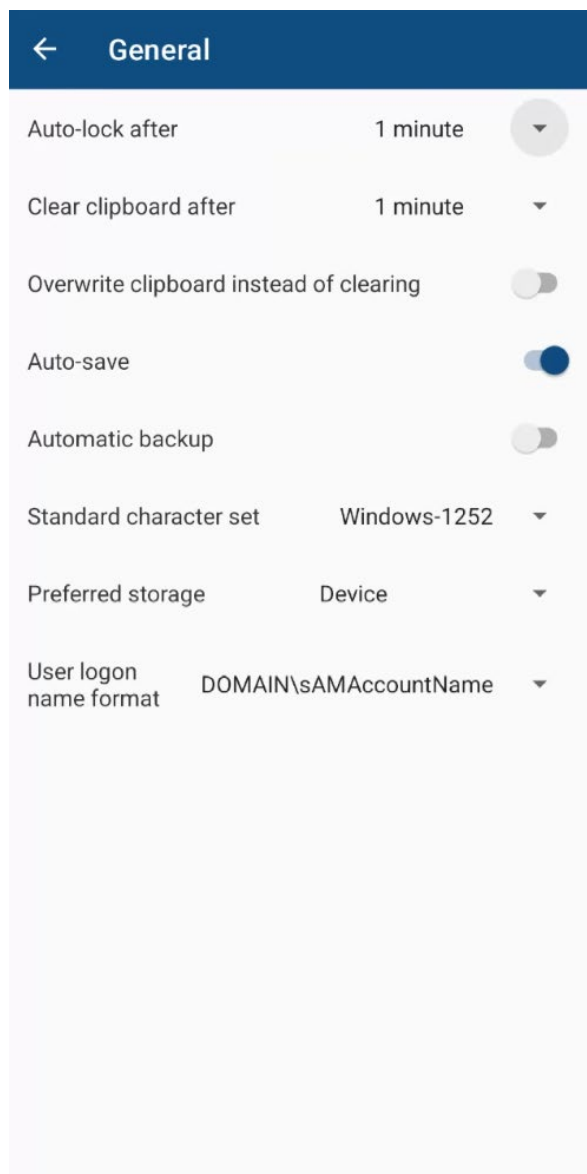


App Settings

- **Open settings** from the home screen (Open settings) or via the menu (top-left) and then Settings/**Options**.

General

- **Auto-lock after:** For better security, set a short auto-lock time (e.g., 1–2 minutes). After that, you must unlock again with the master password and/or key file.
- **Clear clipboard after:** Enable automatic clipboard clearing after a set time.
- **Overwrite clipboard instead of clearing:** Increases security.
- **Auto-save:** Automatically saves the database when you make changes.
- **Automatic backup:** Automatically creates backup files.
- **Standard character set:** Adjust the character set if needed.
- **Preferred storage:** Choose which location is shown first (Device, Enterprise Server, Dropbox, Google Drive, OneDrive, Box, HiDrive, FTP Server, WebDAV Server).
- **User logon name format:** Choose between Simple, DOMAIN\sAMAccountName and UPN.



Storage

Enterprise Server

- **Enable SSL/TLS:** Relevant only for Enterprise Server version 17.
- **Save local copy of databases:** Enables offline usage where permitted.

OneDrive

- **Use an alternative storage method:** Helpful if you run into OneDrive storage issues.

WebDAV server

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

Biometrics

- If supported and set up on your device, you can enable biometrics here as an unlock method.

Appearance

- **Color scheme:** System default, Light, or Dark.
- **Show launch animation:** Choose whether the animation plays on startup.
- **Show database name in title:** Choose whether the database name appears at the top.

Security

- Define rules for your master password: set a minimum length and require uppercase/lowercase letters, numbers, and/or special characters.

← Security

Master password policy

Minimum length of password Value (1 - 255)

Uppercase letters required

Lowercase letters required

Numbers required

Special characters required

Search

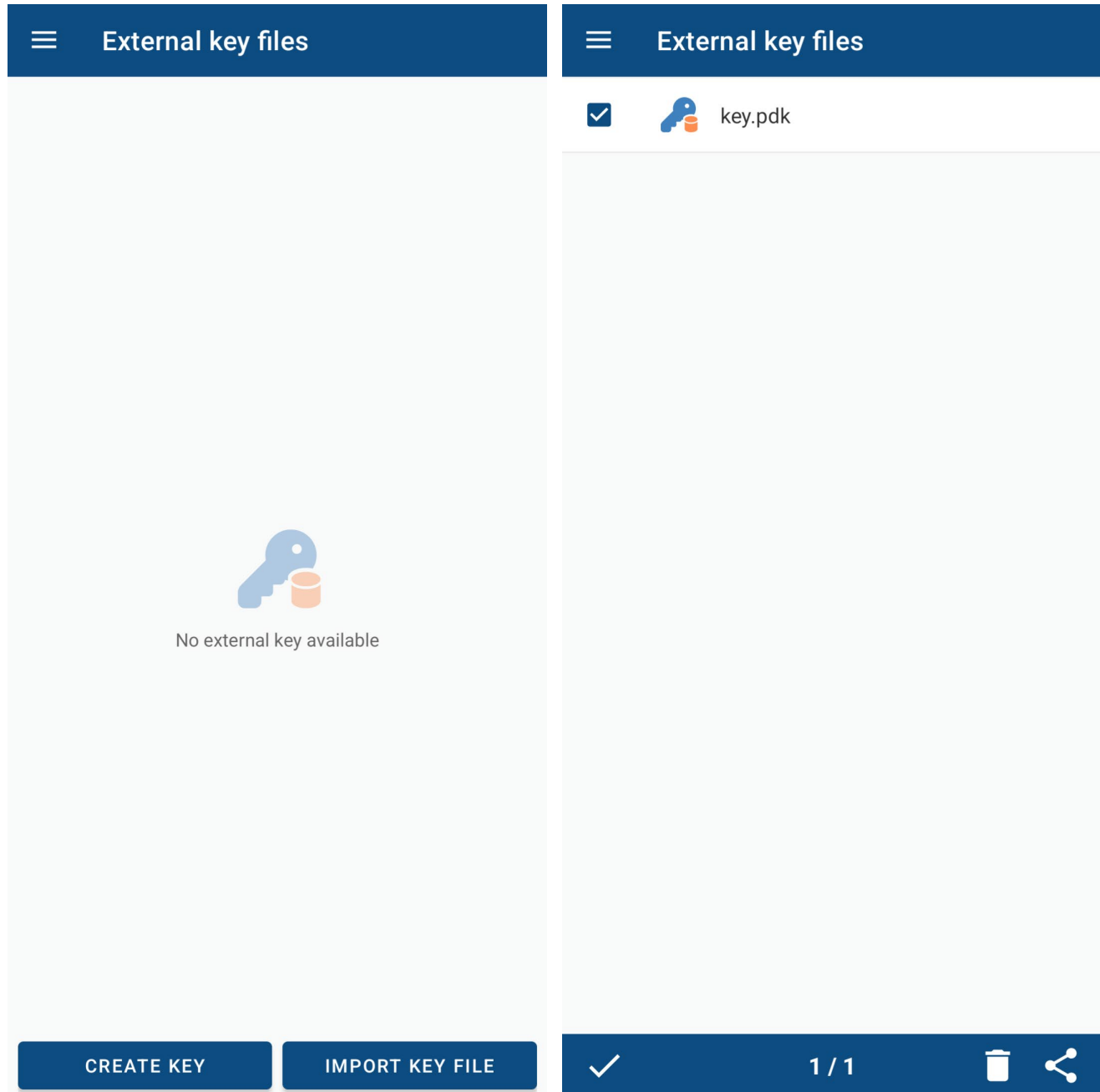
- **Start quick search automatically while typing:** If enabled, the search starts as you type.

Managing Key Files

If you authenticate with master password + key file, you manage key files centrally in the app.

- Open the menu (top-left) and select **External key files**.
- Tap **Create key file** to generate a new one, or **Import key file** to add an existing one.
- Use **Share** to move the key file to a secure location (e.g., a secure cloud). Select the key file from the list and then tap **Share** (bottom-right).

IMPORTANT: Store the database and the key file separately. Anyone who has both can more easily gain unauthorized access to your data.

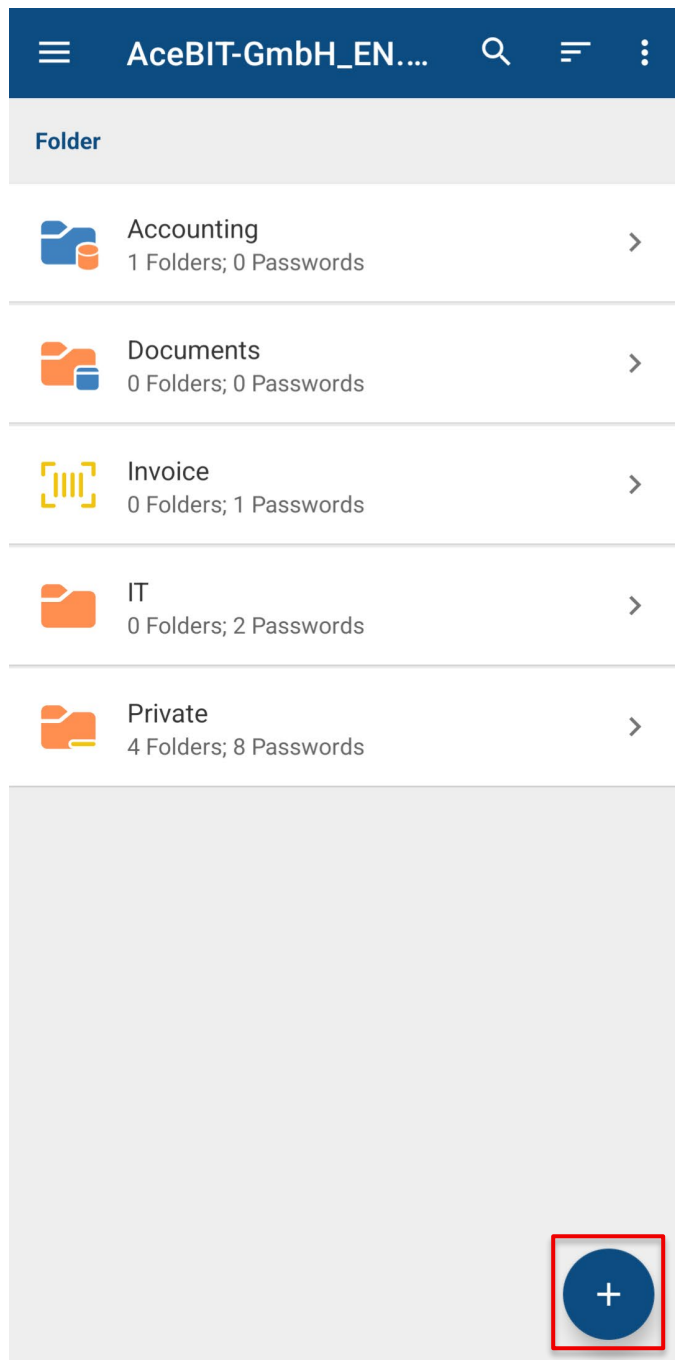


Core Features

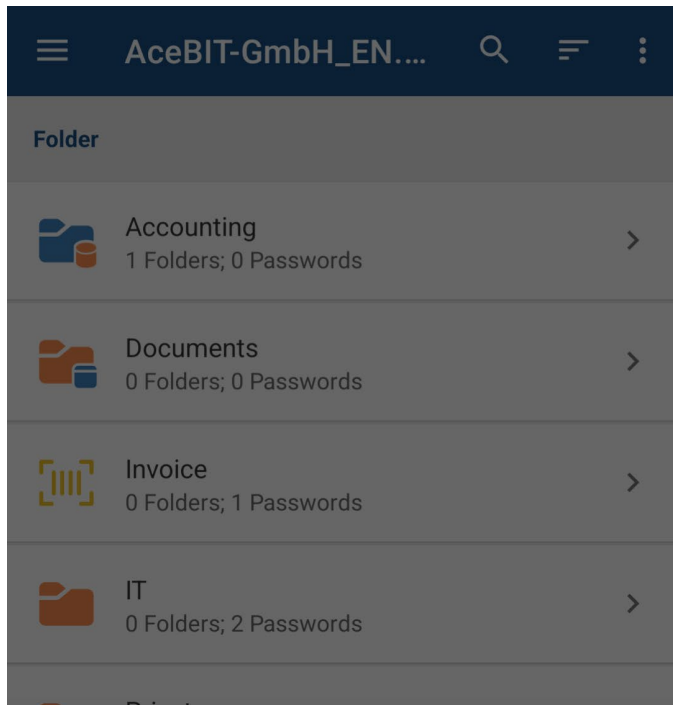
Create and edit entries/folders

To create your first password entry:

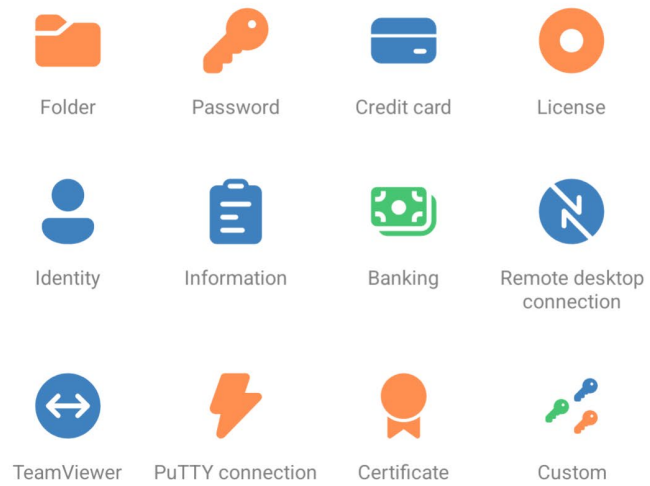
- Open an existing database.
- Tap + (white plus on blue) in the bottom-right corner.



- Select the entry type (e.g., **Password**).



New entry



- Fill in at least the **Description** field. Optional fields: **Category, User, Password, URL, Importance, Expiration date, Tags, Notes.**

The screenshot shows a mobile application interface for creating a new password entry. The title bar is dark blue with a back arrow on the left, the text 'New password' in the center, and a white checkmark on the right. Below the title bar is a horizontal menu with five tabs: 'GENERAL', 'ADDITIONAL', 'SECURITY', 'FIELDS', and 'T'. The 'GENERAL' tab is currently selected. The main content area is white and contains several input fields:

- Description:** A text input field with an orange key icon to its right.
- Category:** A dropdown menu with a downward arrow.
- User:** A text input field.
- Password:** A text input field with an eye icon (to toggle visibility) and a pencil icon (to edit) to its right.
- URL:** A text input field with a share icon to its right.
- Importance:** A dropdown menu with 'Medium' selected and a downward arrow.
- Expiration date:** A date input field showing '1/14/26' and a toggle switch to its right.
- Tags:** A text input field.
- Notes:** A text input field.

- Tap **Save** (checkmark in the top-right).
- Additional tabs may be available depending on the entry type: **Additional, Security, Fields, TAN, Conditional access.**
- To edit an existing entry, tap the three dots next to it and choose **Edit**. The same screen opens as when creating an entry; update fields and save.

To create a folder:

- Tap **+** and choose **Folder**.
- Enter a name and save.
- Editing a folder works the same way as editing an entry.

The screenshot shows the 'New folder' screen in a mobile application. The header is dark blue with a back arrow on the left, the text 'New folder' in the center, and a checkmark on the right. Below the header are two tabs: 'GENERAL' (selected) and 'SECURITY'. The main content area is white and contains several input fields: 'Description' with a folder icon, 'Category' with a dropdown arrow, 'Importance' with 'Medium' selected and a dropdown arrow, 'Expiration date' with '1/14/26' and a toggle switch, 'Tags', and 'Notes'.

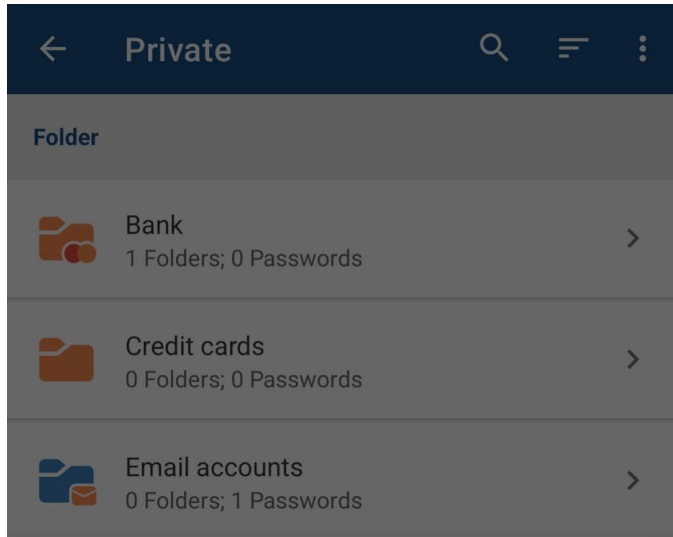
In addition to **Password**, other entry types include:

- **Credit card**: Card data for online payments.
- **Identity**: Personal data (name, address, email).
- **License**: Software license keys.
- **Information**: Free-text note (e.g., Wi-Fi password).









Link entries

Use linked entries if you want to reuse the same credentials in multiple places. Changes to the original will automatically apply to the links.

- Open the actions for an entry by tapping the three dots next to it.
- Select **Create linked entry**. The linked entry is created automatically.



Actions

-  Details
-  Edit
-  Add to Favorites
-  Copy user name
-  Copy password
-  Copy TOTP code
-  Open URL
-  **Create linked entry**

Use the password generator

Generate strong passwords right in the entry.

- When creating or editing an entry, tap the pencil icon in the Password field.
- Set the desired length and character types.
- Tap **Generate** and accept the password.

TIP: Use at least 12 characters; for important entries, 16+.

The screenshot shows the 'Password generator' interface. At the top, there is a dark blue header with a back arrow on the left, the text 'Password generator' in the center, and a checkmark on the right. Below the header is a text input field containing the placeholder text 'Generated password'. Underneath the input field are two buttons: a dark blue 'GENERATE' button, which is highlighted with a red rectangular box, and a light gray 'COPY' button. Below the buttons is a section titled 'Generator settings'. This section includes four settings, each with a toggle switch: 'Password length' is set to '10'; 'Uppercase' is turned on (blue toggle); 'Lowercase' is turned on (blue toggle); 'Special characters' is turned off (gray toggle); and 'Numbers' is turned on (blue toggle).

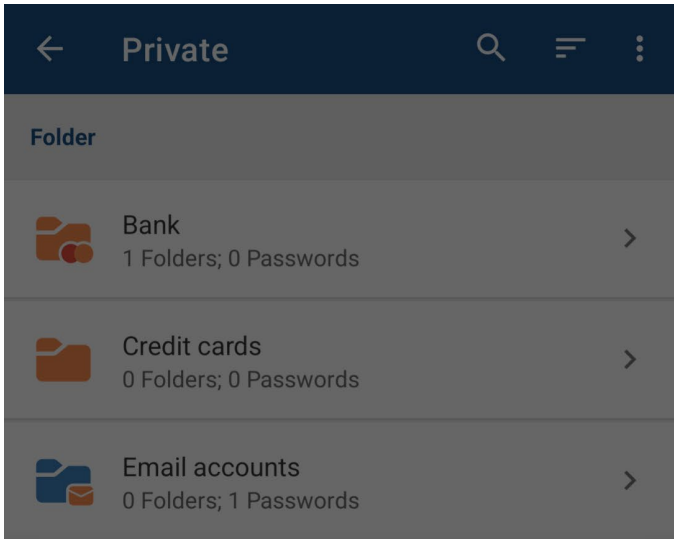
Store and copy 2FA codes (TOTP)

If a service requires a one-time code, you can store the secret in the entry and copy the code directly.









- Open a password entry, tap the three dots, and choose **Edit**.
- In the **Additional** tab, enter the 2FA/TOTP secret.
- Save (checkmark, top-right).
- Copy the current code via the entry actions (three dots) → **Copy TOTP code**, then paste it into the login field.

The screenshot shows the 'Edit password' interface with the 'Additional' tab selected. The fields are as follows:

- Command line parameters:** An empty text input field.
- Auto-complete:** A dropdown menu showing '<USER><TAB><PASS><ENTER>' with a small edit icon to its right.
- 2FA Secret:** A text input field containing five dots, with an eye icon to its right for toggling visibility.
- TOTP:** A text input field containing the number '403872'. To its right is a blue 'COPY' button and a circular refresh icon containing the number '25'.



Actions

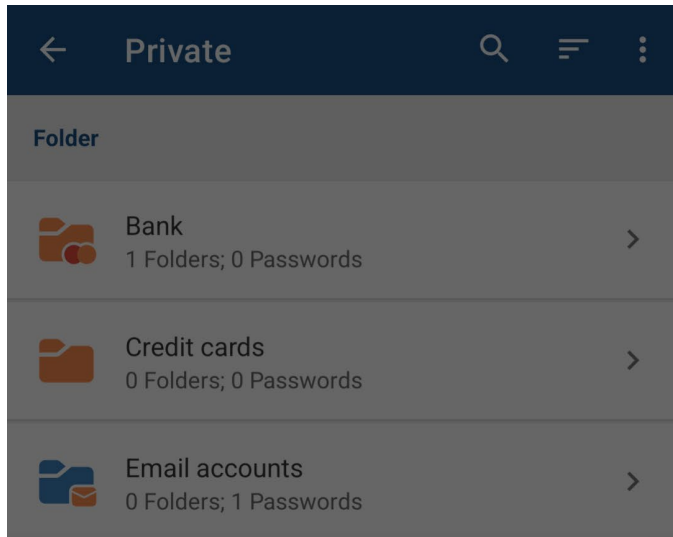
-  Details
-  Edit
-  Add to Favorites
-  Copy user name
-  Copy password
-  Copy TOTP code
-  Open URL
-  Create linked entry

Sign in securely: built-in browser and auto-complete









You can open a saved URL directly in the built-in browser and have login details filled in automatically.

- Open a password entry.
- Select **Open URL** to open the site in the built-in browser.
- Tap the field on the website and choose **Auto-complete** or, if available, the individual items Username, Password, and TOTP.

TIP: If auto-complete does not work for a website, adjust the auto-complete sequence: open the entry in the app, go to the **Additional** tab, and edit the **Auto-complete** field (pencil icon). You can also add delays.



Actions

-  Details
-  Edit
-  Add to Favorites
-  Copy user name
-  Copy password
-  Copy TOTP code
-  Open URL
-  Create linked entry

Navigation icons: back, refresh, left arrow, right arrow, expand/collapse.


AUTO-COMPLETE (highlighted with a red border)


User name: AceBIT


Password:


Logo: PASSWORD DEPOT BY AceBIT


Flags: UK, ? (help), ⚙️ (settings)

Server Address*: 127.0.0.1 

Port*: 8714 

Authentication Method: Standard Authentication 

Username*: AceBIT 

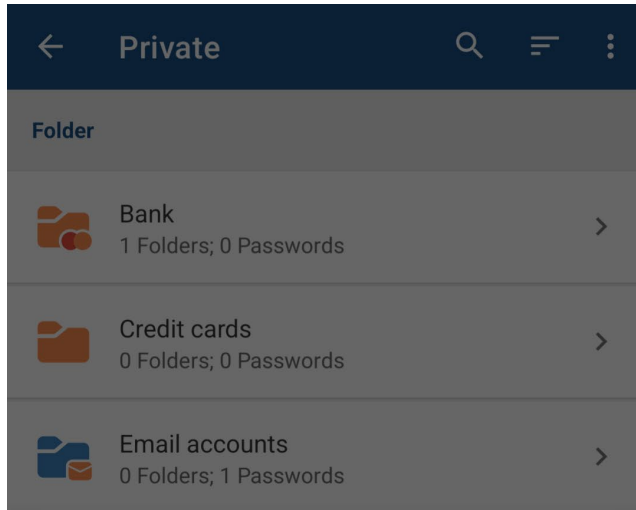
Password*: 

Sign in









Favorites, search, and sorting

Setting favorites makes it easier to quickly find entries again. Search and sorting also help you structure your database and find entries fast.

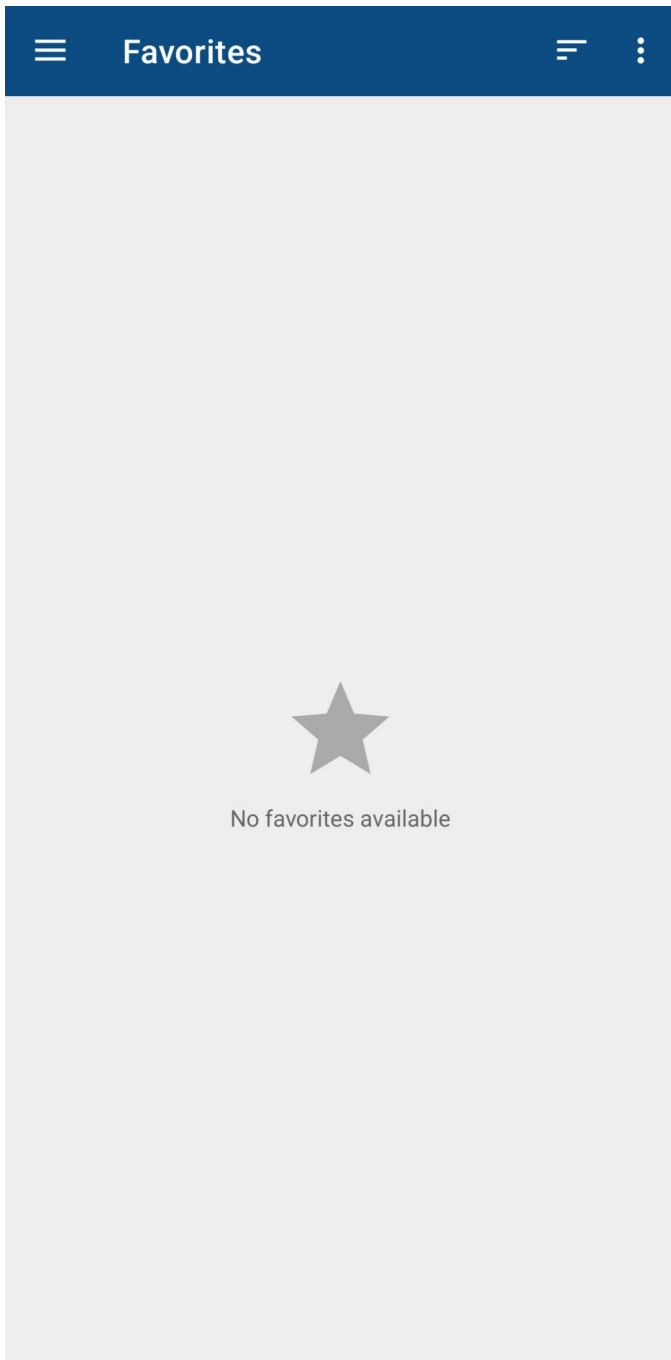
- **Set favorite:** Open entry actions and tap **Add to Favorites** (star).



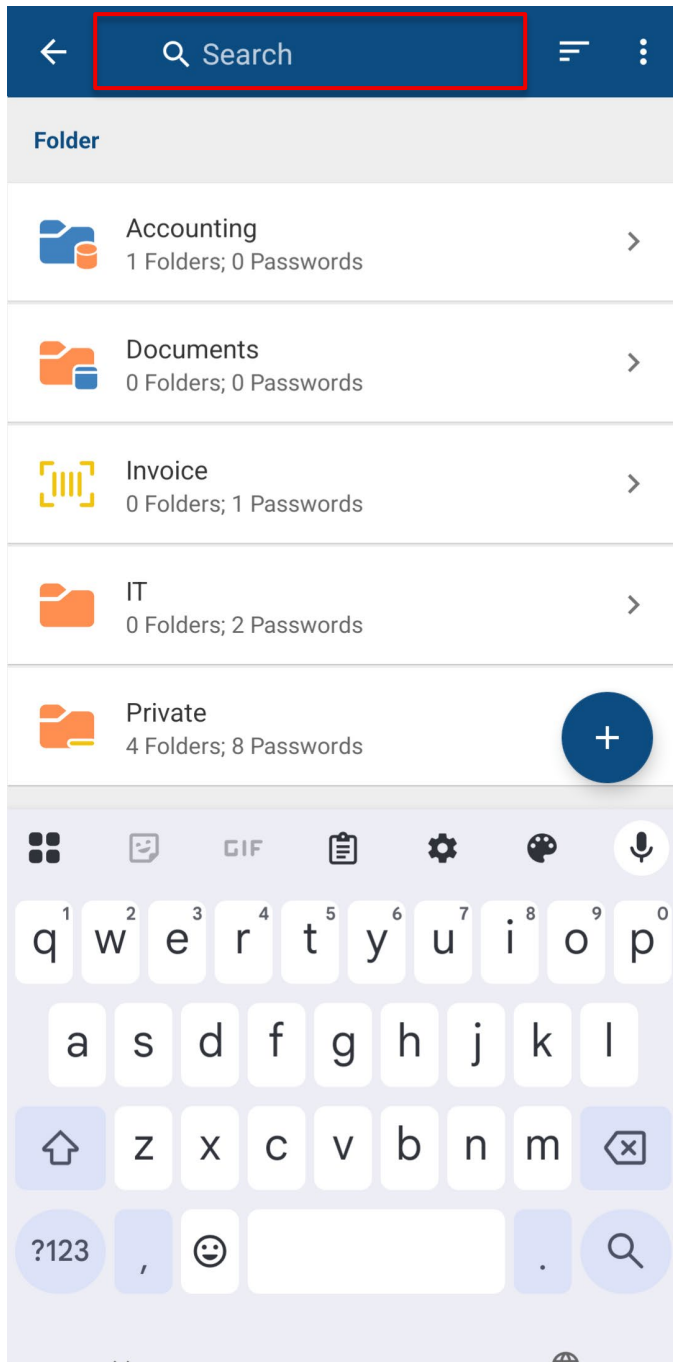
Actions

-  Details
-  Edit
-  Add to Favorites
-  Copy user name
-  Copy password
-  Copy TOTP code
-  Open URL
-  Create linked entry

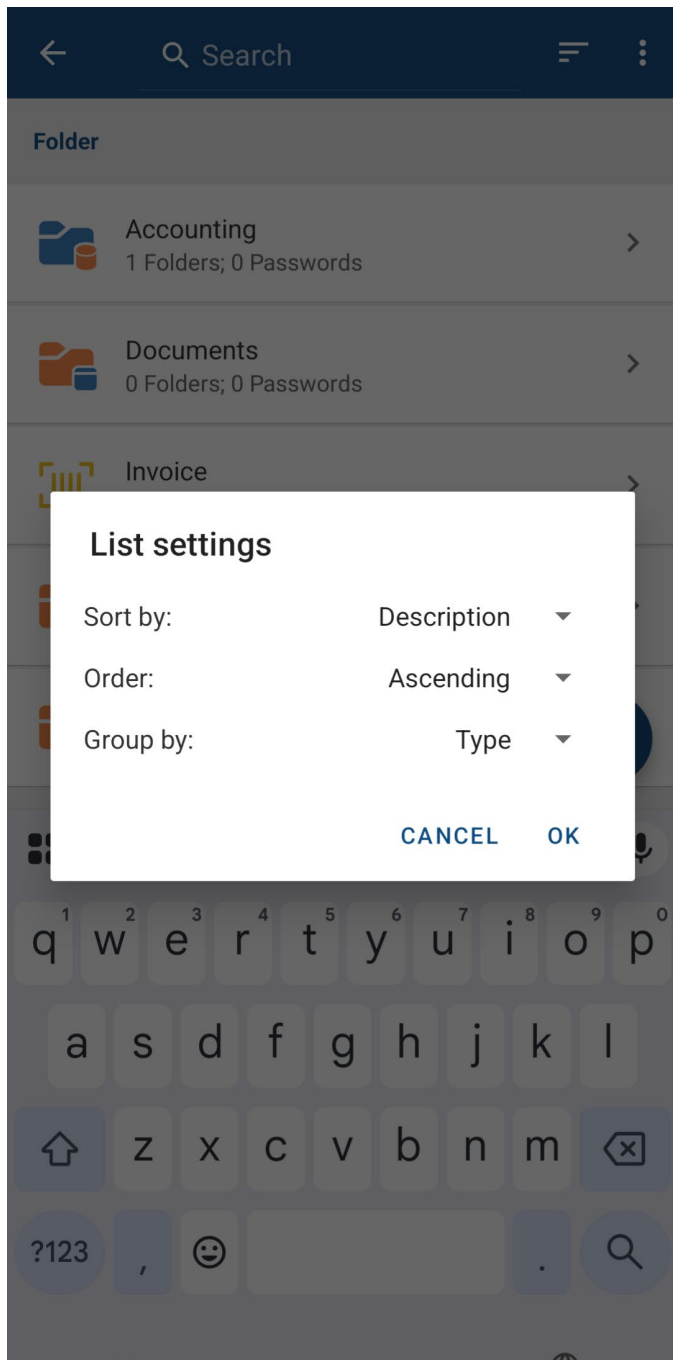
- **Open favorites:** Open the menu (top-left) and select **Favorites**.



- **Search:** Tap the search icon (magnifier) and enter a term. Password Depot lists matching entries.



- **Sort/Group:** Tap the sort/view icon near the search icon and choose criteria (e.g., Description, Category, Type).



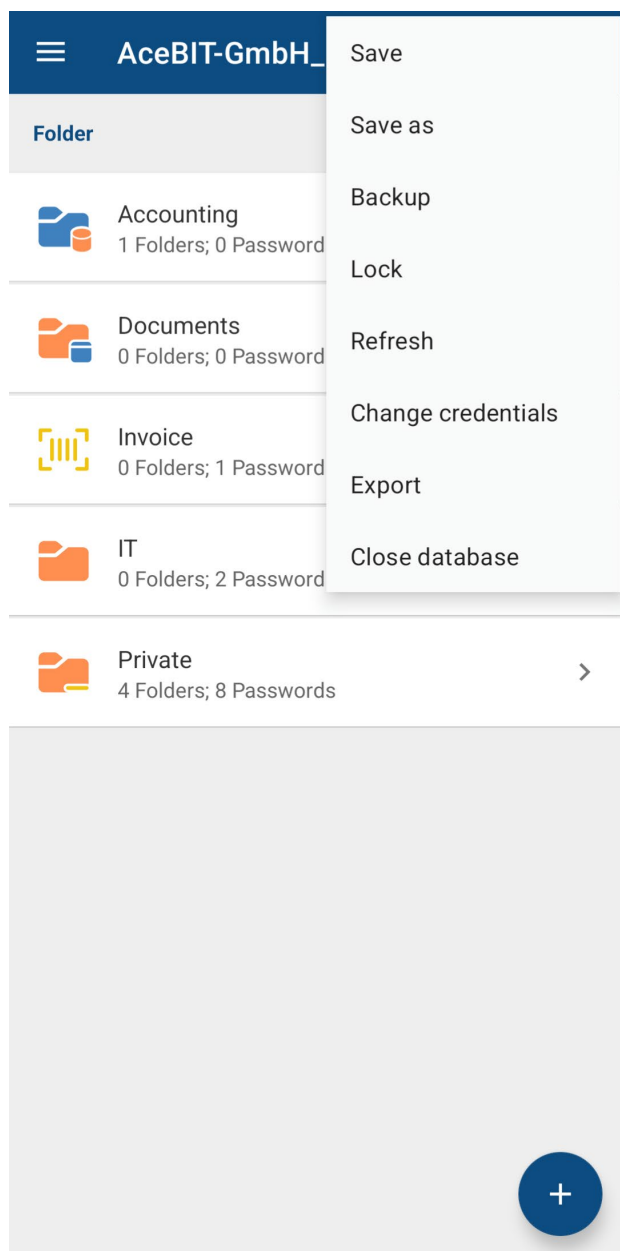
TIP: Favorites are stored on the device. If you use the same database on multiple devices, set favorites separately on each device.

Protecting and Managing Your Database

Key security and management functions are in the 3-dot menu (top-right) when a database is open.

- **Save:** Saves the current database file.
- **Save as:** Saves the database under a new name in a new file.
- **Backup:** Creates a manual backup. The first time, you can choose the storage location on your device.
- **Lock:** Locks the database so you must enter the master password again to access entries.
- **Refresh:** Updates the database to the latest version.
- **Change credentials:** Change master password and/or key file (you must enter current credentials first).
- **Export:** Export data (XML, CSV, TXT). The export wizards opens (see below).
- **Close database:** Close the current database.

CAUTION: Export files contain your data unencrypted. Store them only briefly and delete them afterward.



Target file options

Password Depot XML (*.xml) ▼

BACK

NEXT

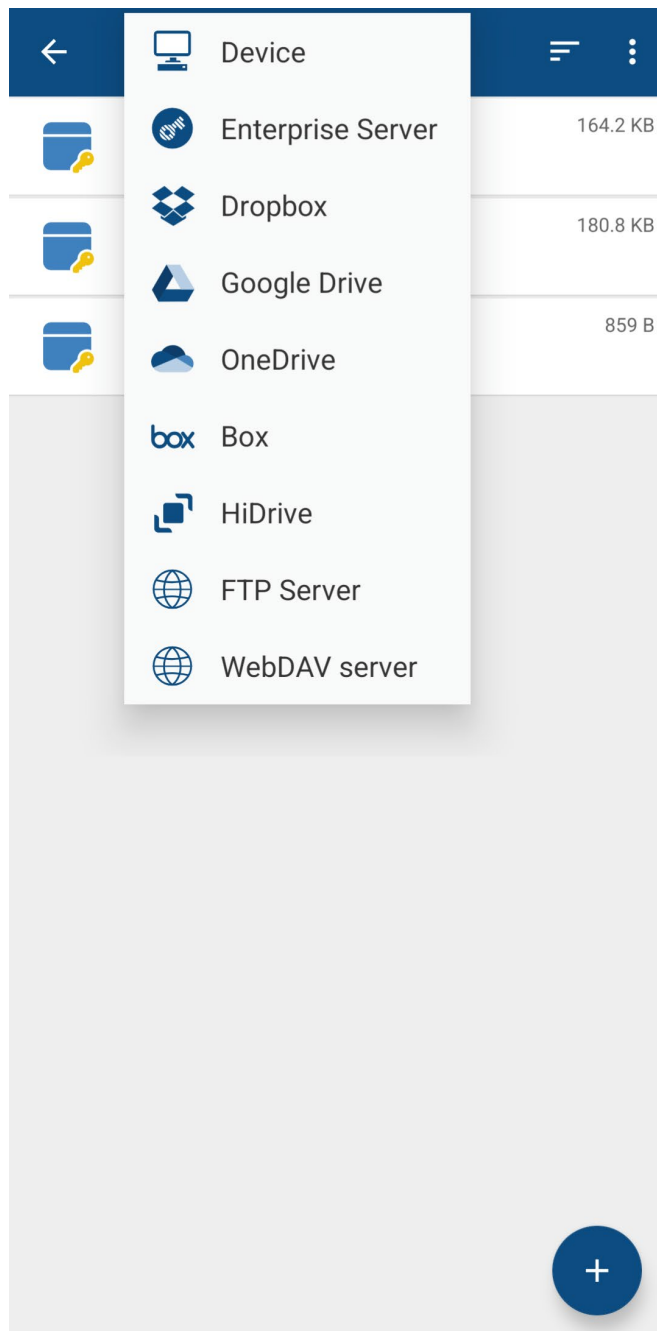
Syncing and Access on the Go

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

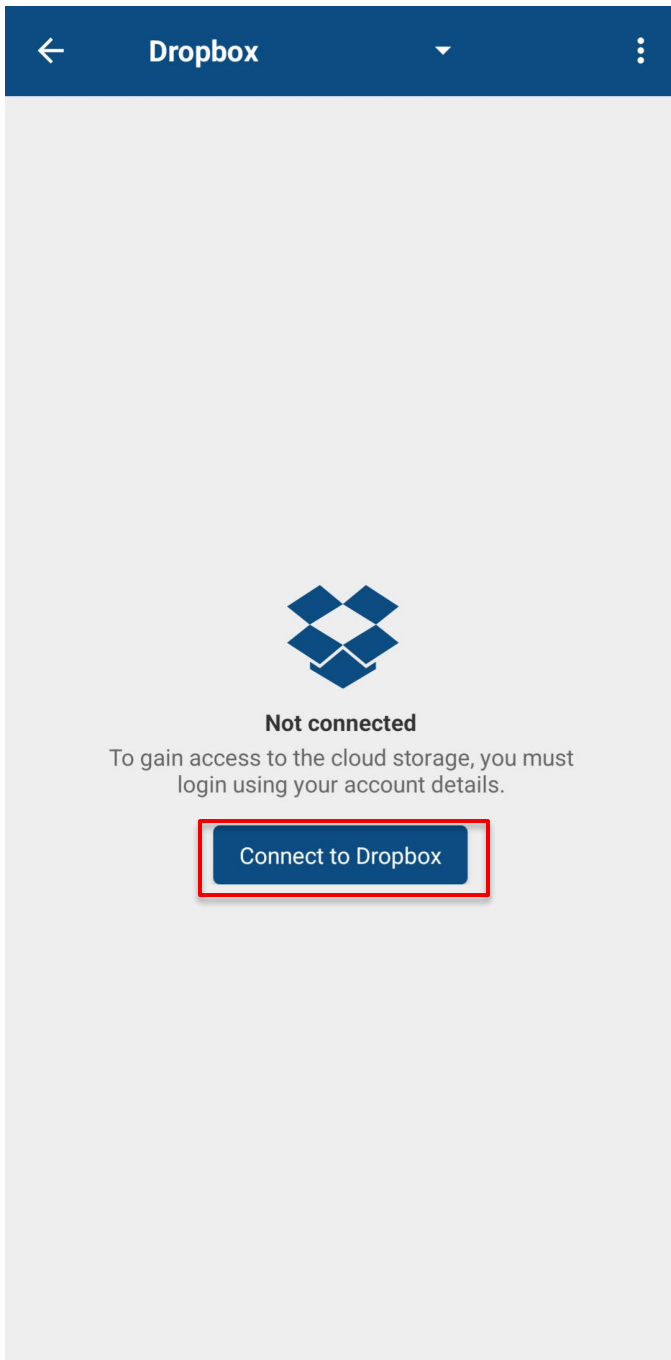
TIP: Before switching devices, always **Save** (3-dot menu → Save) and use **Refresh** to avoid conflicts.

Connect a cloud service

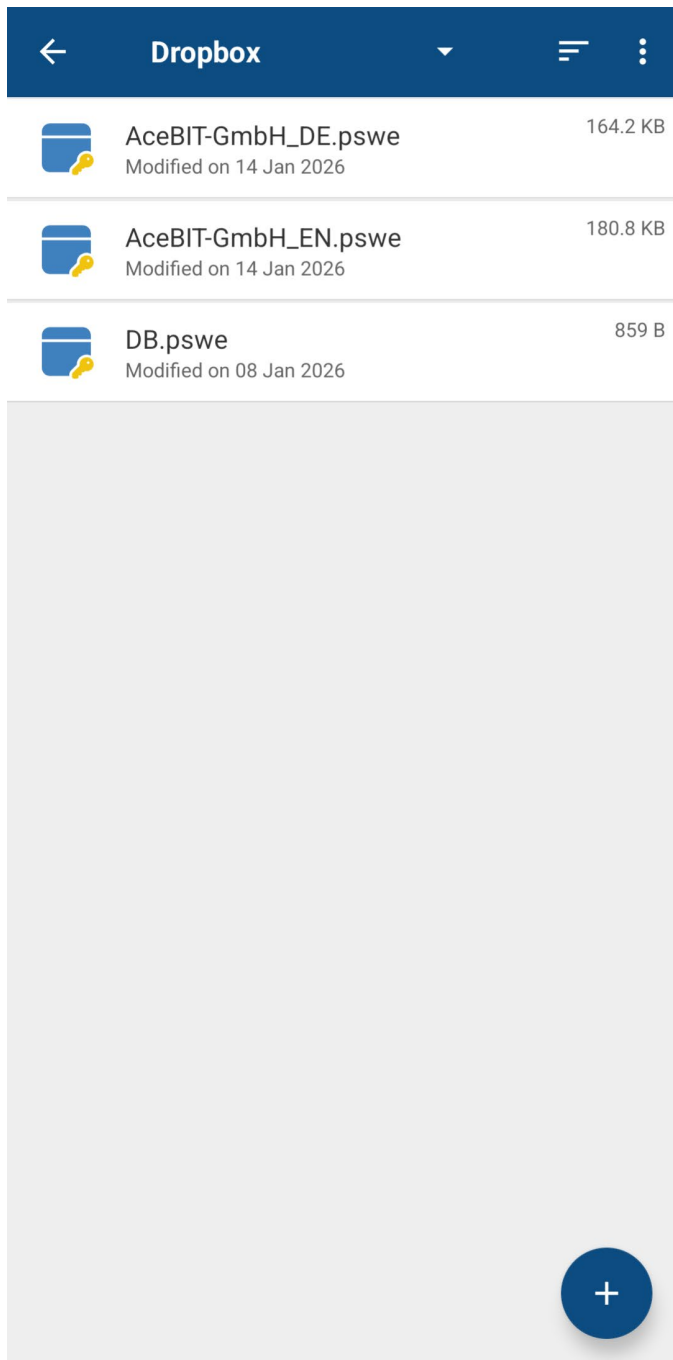
- Open the menu (top-left) and select **Database Manager**.
- From the list at the top (down arrow), choose the cloud service (Dropbox, Google Drive, OneDrive, Box, or HiDrive).



- Tap **Connect** and sign in to your cloud service.



- Open the database from the cloud as usual.



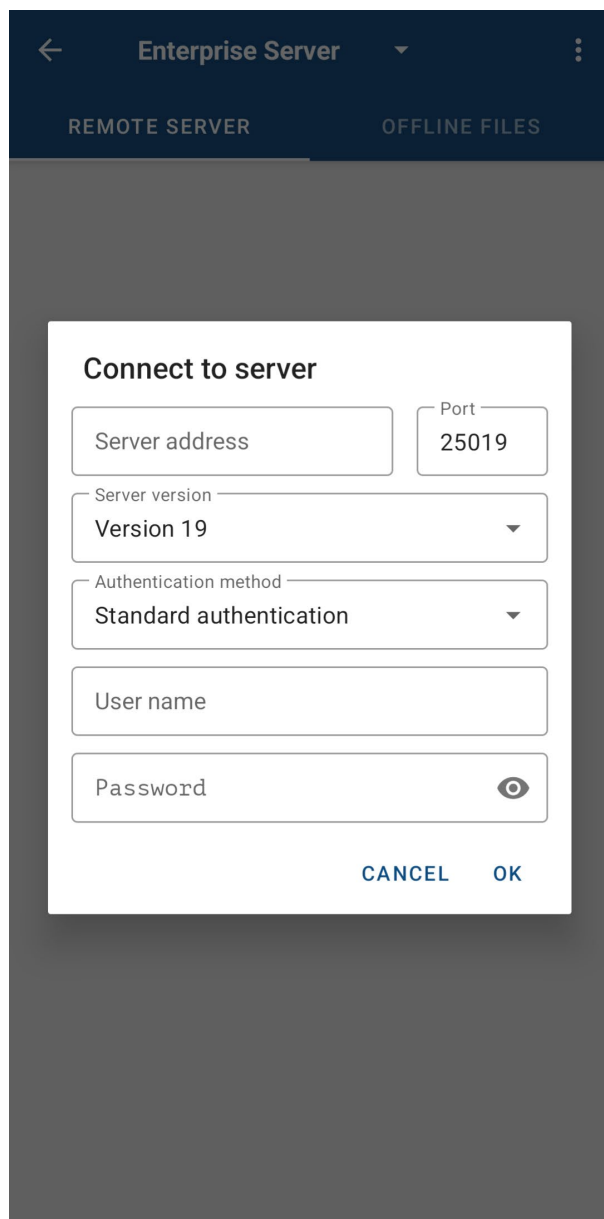
- If needed, use the 3-dot menu → **Disconnect** to end the connection.

Enterprise Server (business)

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

- Open the menu and select **Database Manager**.
- Select **Enterprise Server**.
- Tap **Connect to Enterprise Server** and enter server address, port, server version, username, and password. Depending on your organization's setup, Azure AD authentication, OpenID Connect as well as authentication via Windows Domain Credentials may also be available.
- Open a shared database from the list.

CAUTION: Creating databases on the Enterprise Server is only possible via the server's Server Manager. You can only open server databases if you have access rights granted by your server administrator.



The screenshot shows a mobile application interface for connecting to an Enterprise Server. The top navigation bar is dark blue with a back arrow, the text 'Enterprise Server', and a menu icon. Below the navigation bar are two tabs: 'REMOTE SERVER' (selected) and 'OFFLINE FILES'. The main content area is a white dialog box titled 'Connect to server'. It contains the following fields and controls:

- Server address:** A text input field.
- Port:** A text input field containing the value '25019'.
- Server version:** A dropdown menu with 'Version 19' selected.
- Authentication method:** A dropdown menu with 'Standard authentication' selected.
- User name:** A text input field.
- Password:** A text input field with a toggle icon (an eye) to the right, indicating it can be toggled between visible and hidden.

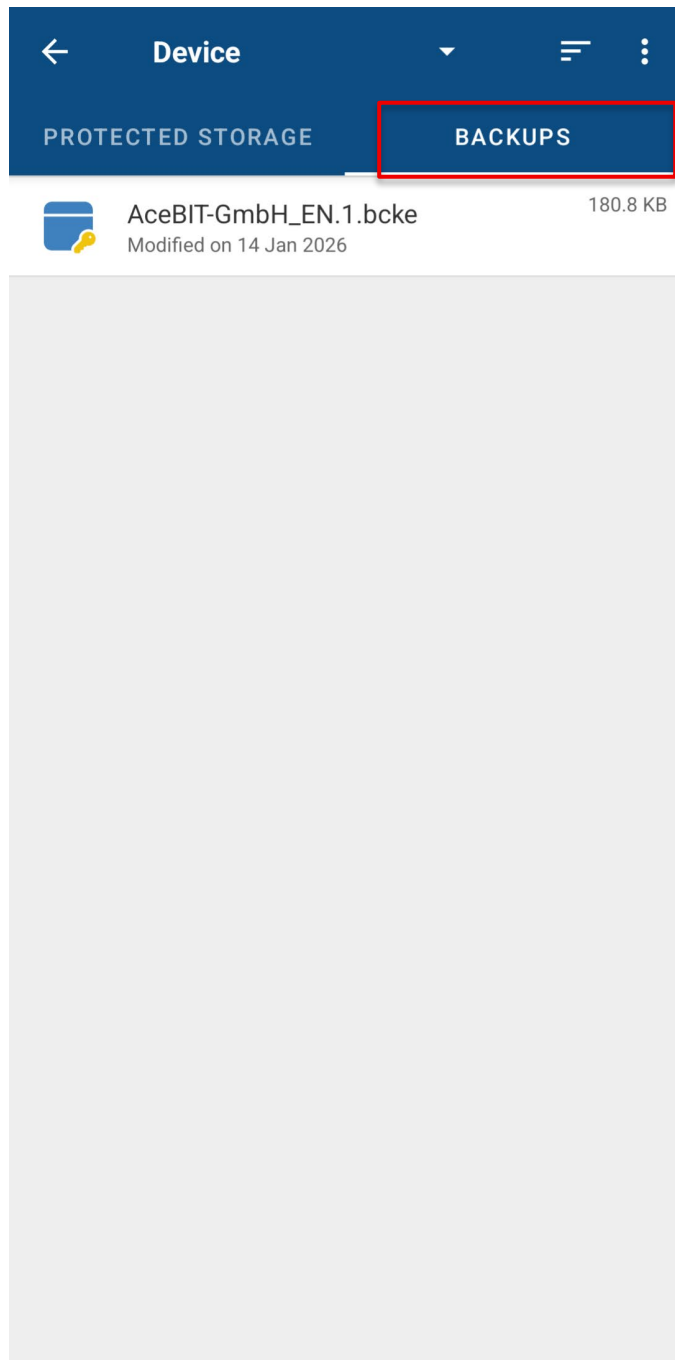
At the bottom of the dialog box are two buttons: 'CANCEL' and 'OK'.

Find and restore backups

Backups help you keep access to your data if a device is lost or a file is damaged.

- In settings (**General**), enable **Automatic backup** (recommended).
- Create a manual backup when needed via the 3-dot menu → **Backup**.
- Open backups via the Database Manager: tap **Backups** and select the backup database from the list.

CAUTION: Treat backups like the original database. Don't share backup files unprotected; use secure storage locations.



Tips

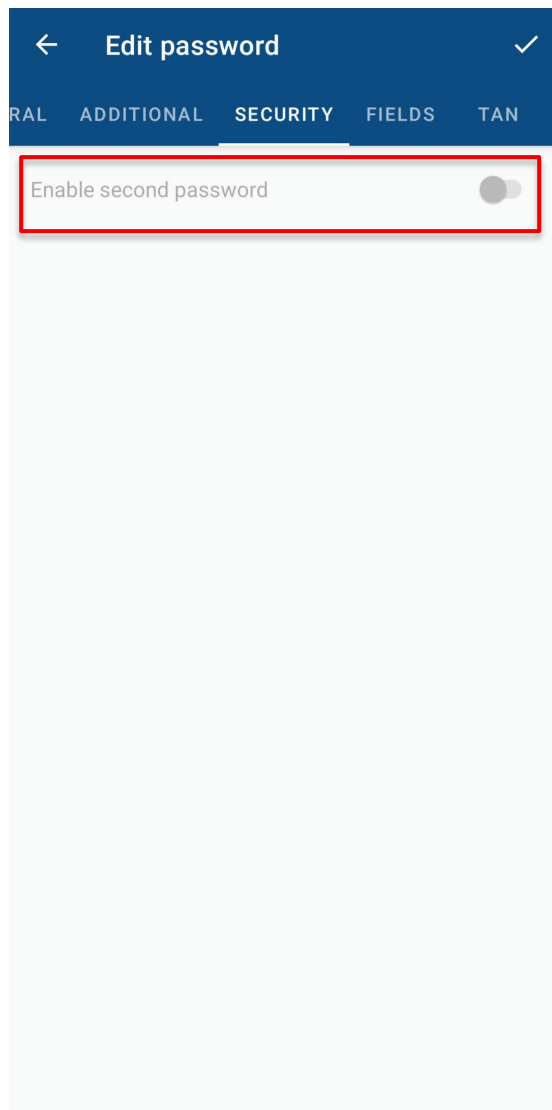
Everyday security checklist

- Use a strong master password and never share it.
- Enable a short auto-lock time and biometrics (if available).
- Automatically clear the clipboard.
- Use a key file as a second factor—and store it separately.
- Create regular backups and store them securely.
- Use a unique, random password per account (use the generator).

Extra protection: Second password

For especially sensitive data, you can set a second password. Then the app requires an additional entry besides the master password.

- For individual entries: Open the entry and go to the **Security** tab to set a second password.



- For folders: Open the folder and go to the **Security** tab.
- For the whole database: Open the menu and select **Database properties**. Here, you can view information on the database (name, location, size, number of folders and entries). Moreover, you can set a second password for the whole database.

Database name: AceBIT-GmbH_EN.psw

Location: Dropbox

Size: 180.8 KB

Contains: 10 Folders; 11 Passwords

Enable database compression

Enable second password

IMPORTANT: This password also cannot be recovered. Only use it if you can store it safely.

Quick fixes for common problems

Database won't open:

- Check capitalization and keyboard layout.
- Make sure you selected the correct key file.
- Use **Show hint** if available.

Biometrics issues:

- Check Android settings for fingerprint/face unlock permissions for apps.
- Disable and re-enable biometrics in the app settings.

Auto-complete doesn't work on a website:

- Use the auto-complete sequence with delays.
- Fill fields individually via Username/Password/TOTP buttons if needed.

Help & Support

If you need further assistance, please contact us:

- Open the menu and select **Submit feedback**. This takes you to the Password Depot website—please choose the **Support** section there.
- Open the menu and select **About Password Depot**. The links also take you to our website where you can select **Support**.

