

OBSKURA

INVISIBLE SECURITY FOR YOUR DATA

USER MANUAL

VERSION 0.3.0

MACOS · WINDOWS · LINUX

OCTOBER 2026

USER MANUAL

CONTENTS

01	Welcome to Obskura	What it does, databases and vaults	03
02	Installation and first launch	macOS, Windows, Linux · the access key · the interface	04
03	Passwords and key files	Credentials, Argon2id, choosing the cipher	05
04	Password databases	Create, unlock, organise entries	07
05	Managing entries	Generator, fields, attachments, history	08
06	Database tools	Search, safe copy, the database menu	09
07	File vaults	Create a vault and encrypt files	10
08	Working with files	Open, edit, export	11
09	Remote servers	SFTP, WebDAV, SMB, FTP/FTPS	12
10	Multiple devices in real time	Real-time sync, notifications	14
11	Access key and devices	Companion files, IDs and paths of each device	15
12	Automatic backup	Second destination, dated copies, per device	17
13	Import and export	Online managers, CSV from KeePass and others	18
14	Languages	Automatic language, XML files, new translations	20
15	Locking and settings	Automatic lock, clipboard, theme, device name	23
16	Shortcuts and cryptography	Keyboard shortcuts and technical details	24
17	Good practice and troubleshooting	Backups, frequently asked questions	25

CONVENTIONS

Button and menu names are in **bold**. Key combinations are written like this: `Ctrl/⌘` + `L`, where `Ctrl` applies to Windows and Linux and `⌘` to macOS. File names and extensions are in `monospace`. The screenshots show the interface in the language of this manual.

INTRODUCTION

01 WELCOME TO OBSKURA

Obskura protects passwords and files with military-grade encryption. No account and no third-party service: your data stays where you decide, on your computer or on your own server.

Every database and every vault is an ordinary file or folder. You can keep them on your computer's disk, on a USB stick, in a synced folder such as Dropbox, OneDrive or iCloud Drive, or directly on your own SFTP, WebDAV, SMB or FTP server, and have as many as you like: a personal one, a work one, one shared with the family. Several computers can use them together and see each other's changes in real time, even when they reach them through different paths.

PASSWORD DATABASE

A single `.obk` file, modelled on KeePass. It contains entries with user name, password, address, notes, custom fields, attachments and change history, organised in groups.

FILE VAULT

A folder, modelled on Cryptomator. You drag documents, photos and archives into it: every file is encrypted individually, including names and folder structure.

HOW THE PROTECTION WORKS

When you create a database or a vault you choose a **master password**, a **key file** or both. From these credentials Obskura derives the encryption key with Argon2id, an algorithm designed precisely to make password guessing extremely slow. The data is then encrypted with AES-256, the standard approved for information classified **TOP SECRET**.

The credentials are never stored anywhere. Without them the contents are unreadable to anyone, developers included.

IMPORTANT

There is no way to recover a forgotten password or a lost key file. Choose a password you will remember, and keep a copy of the key file in a safe, separate place.

AT A GLANCE

AES-256-GCM · XChaCha20-Poly1305 · Serpent · Twofish · Camellia · Cipher cascades · Argon2id up to 2 GiB · HKDF-SHA256 · AES-SIV for file names · Memory wiped on close · No account · SFTP · WebDAV · SMB · FTPS · Real time · Automatic backup · Per-device paths · 8 languages · macOS · Windows · Linux

GETTING STARTED

02 INSTALLATION AND FIRST LAUNCH

macOS

Open the `.dmg` file and drag Obskura to **Applications**. On first launch, if macOS blocks the app, go to **System Settings → Privacy & Security** and choose **Open Anyway**.

Windows

Run the `.exe` installer, which automatically uses the Windows language, or start the portable version without installing anything. If the SmartScreen warning appears, click **More info → Run anyway**.

Linux

Use the `.deb` package (Debian, Ubuntu), the `.rpm` package (Fedora, openSUSE) or the `.AppImage`, which needs no installation: make it executable and run it.

FIRST LAUNCH: LANGUAGE AND ACCESS KEY

Obskura opens in the system language (Italian, English, German, Spanish, Russian, Chinese, Japanese or Arabic; for other languages it uses English). On first launch it asks you to create the **Obskura access key** or, if you already use Obskura on another computer, to enter the one you generated there. Chapter 11 explains what it is for.

THE START SCREEN

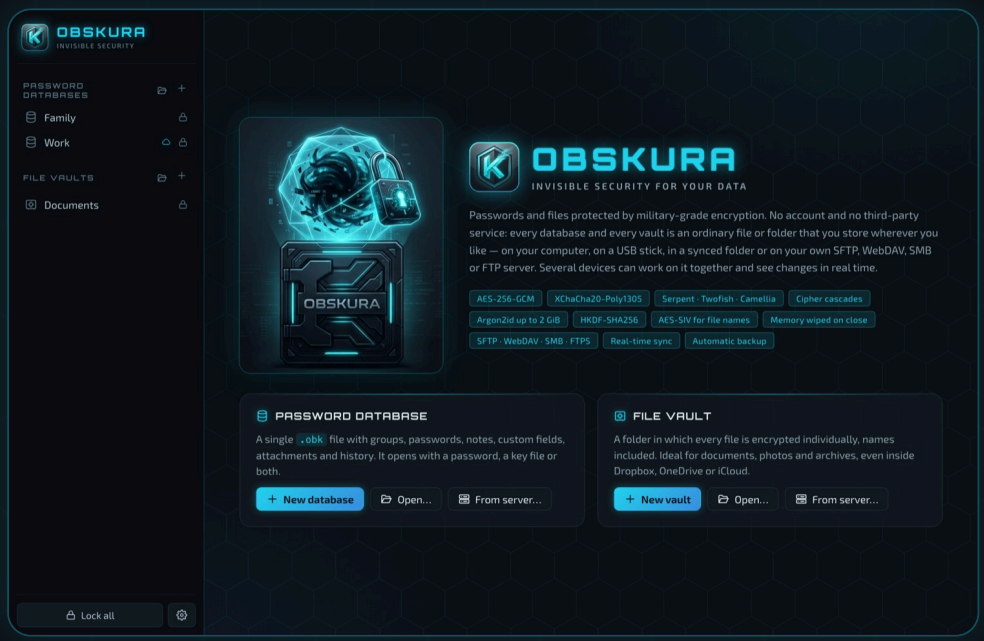


FIG. 1 The welcome screen, with the sidebar.

The **sidebar** contains the **Password databases** and **File vaults** sections. Next to each heading there are two buttons: the folder to **open** an existing item and **+** to create a new one.

- Every recently opened item stays in the list, with its name only: paths never appear. The padlock shows the state: **closed** when locked, **open** when unlocked.
- Hovering over an item shows a **×** to remove it from the recents (the file is not deleted) or a padlock to lock it right away.
- At the bottom: **Lock all** and the **Settings** gear.

PROTECTING YOUR DATA

03 PASSWORDS AND KEY FILES

Databases and vaults open with a **master password**, a **key file** or both together. Combining the two is the strongest protection: you need something you *know* and something you *have*.

MASTER PASSWORD

A long phrase is safer than a complex word: four or five random words are easy to remember and extremely hard to guess. The meter under the field estimates its strength in bits.

The dice button opens the **generator** if you prefer a random password.

KEY FILE

As in KeePass, **any file** can act as a key. You can choose **Use an existing file** or **Generate new**: Obskura creates a random key file in the location you specify.

Keep it, for example, on a USB stick, separate from the database. Obskura remembers where it is on each device and looks for it by itself every time it opens (chapter 11).

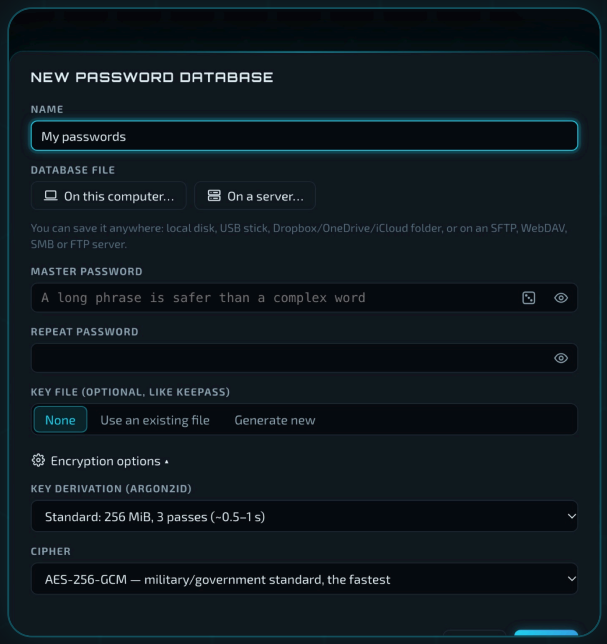


FIG. 2 Creating a database with the encryption options open.

ENCRYPTION OPTIONS

With **Encryption options** you choose how costly the key derivation should be and which cipher to use. The defaults, Standard and AES-256-GCM, are already safe for any use; all the alternatives are described on the next page.

> **NEVER MODIFY THE KEY FILE**
>
> If you use an arbitrary file (a photo, a document) as a key, even the smallest change makes it unusable. The files generated by Obskura use a recognised text format that stays valid even if line endings change. In any case keep a backup copy.

PROTECTING YOUR DATA

03 CHOOSING THE CIPHER

KEY DERIVATION (ARGON2ID)

Argon2id turns your credentials into the encryption key: the more memory and passes it uses, the more costly it is for an attacker to try millions of passwords.

LEVEL	PARAMETERS	OPENING TIME
Standard	256 MiB of memory, 3 passes	about 0.5–1 seconds
High	1 GiB, 4 passes	about 2–4 seconds
Extreme	2 GiB, 6 passes	about 5–12 seconds

EXTREME LEVEL

Every opening requires **2 GiB of free memory**. On a computer with little RAM the database or vault might not open: choose it only if you will use your files on suitable computers.

CIPHERS

All ciphers use 256-bit keys and are **authenticated**: any tampering with the data is detected.

CIPHER	CHARACTERISTICS
AES-256-GCM	**Default.** US standard approved for TOP SECRET information, the fastest thanks to hardware acceleration.
XChaCha20-Poly1305	Stream cipher, fast on any processor even without AES instructions.
Serpent-256-GCM	AES competition finalist, with the widest security margin (32 rounds). Slower.
Twofish-256-GCM	AES competition finalist, designed by Bruce Schneier and colleagues.
Camellia-256-GCM	International ISO/IEC standard, recommended in Europe (NESSIE) and Japan (CRYPTREC).
Cascade AES · Twofish · Serpent	**The strongest choice.** Three encryptions in sequence with independent keys: the data stays protected even if two of the three algorithms were ever broken.
Cascade AES · XChaCha20	Combines a block cipher and a stream cipher from completely different families.

VAULTS

In vaults the chosen cipher protects both the keys and the contents of each file. If you change it with **Change password / key file**, existing files stay encrypted with the previous one and files added from then on use the new one. The active cipher is shown at the bottom right of the vault.

PASSWORD MANAGER

04 PASSWORD DATABASES

CREATING A DATABASE

1. Click **New database** on the start screen, or **+** next to **Password databases**.
2. Type a **name** and choose where to save the `.obk` file: **On this computer…** or **On a server…**.
3. Set a password and/or key file (chapter 03).
4. Press **Create**. The database opens already unlocked.

OPENING AND UNLOCKING

1. Select the database in the sidebar, or use the folder icon to open an existing `.obk` file.
2. Enter the password. The key file and the backup copy are found automatically; if the key file cannot be found, choose it with **Choose…**.
3. Press **Unlock** or `Enter`.

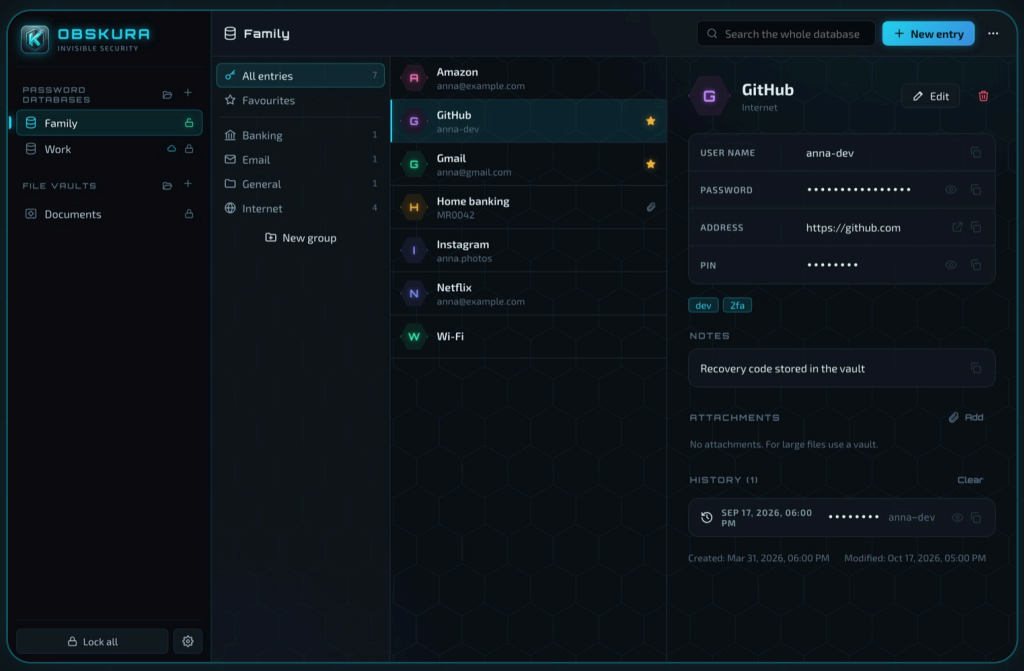


FIG. 3 An unlocked database: groups, list of entries and details of the selected entry.

THE THREE COLUMNS

- **Groups**: **All entries**, **Favourites** and your folders. Hovering over a group shows the commands to create a subgroup, edit or delete it; **New group** is at the end of the list.
- **Entries**: title and user name of each entry. The star marks favourites, the paperclip attachments. A **double click** copies the password directly.
- **Details**: all the entry's fields, with buttons to show, copy or open the address in the browser.

PASSWORD DATABASES

05 MANAGING ENTRIES

To add an entry press **New entry** (or `Ctrl/⌘` + `N`); to change one select it and press **Edit**. Save with the button at the bottom or with `Ctrl/⌘` + `S`. Every change is written to the database file immediately.



FIG. 4 The entry editor with the generator open.

FIELDS OF AN ENTRY

Title and group	Name of the entry and the folder it is in.
User name	Account, email or customer number.
Password	With strength meter and generator.
Address	Opens in the browser from the details.
Notes	Free text, encrypted like everything else.
Tags	Keywords separated by commas.
Expiry	Date after which to change the password.

The **star** at the top adds the entry to the **Favourites**.

PASSWORD GENERATOR

Click the dice in the password field. Choose the **length** (8 to 64 characters) and the character families (`a–z`, `A–Z`, `0–9`, `!@#$`); **Exclude ambiguous** avoids look-alike characters such as l, 1, O and 0. Then **Regenerate**, **Copy** or **Use this password**. Passwords come from the system's cryptographic random generator.

CUSTOM FIELDS

Add extra information such as PINs, recovery codes or security questions. Tick **Protected** to show them hidden, like a password.

ATTACHMENTS AND HISTORY

Attach files up to **64 MB** each (for larger files use a vault). Every change keeps the previous version: the **History** keeps the last **20** and lets you copy an old password.

PASSWORD DATABASES

06 DATABASE TOOLS

SEARCHING

The **Search the whole database** field at the top (or `Ctrl/⌘` + `F`) filters the entries of all groups as you type. `Esc` clears the search.

COPYING SAFELY

The copy buttons next to user name, password and protected fields put the value on the clipboard, which Obskura **clears automatically** after 20 seconds (adjustable in the settings). The clipboard is cleared only if it still contains the copied value: if you have copied something else in the meantime, it is left alone.

THE DATABASE MENU

The ⋯ button at the top right contains:

ITEM	WHAT IT DOES
Database properties	Change the database's name and description.
Change password / key file	Set new credentials. The database is re-encrypted with new keys.
Save a backup copy…	Write an encrypted copy of the database to another location.
Automatic backup…	Configure the second destination for copies (chapter 12).
Devices and paths…	See which devices use the database and their paths (chapter 11).
Import / Export	From an online manager or from CSV, and to CSV (chapter 13).
Lock database	Close the database and wipe its data from memory.

SAVING AND SYNCING

Every change is saved immediately and **atomically**: the new file is written separately and replaces the old one only when complete, so a power cut cannot corrupt it. If another computer has changed the database in the meantime, Obskura **merges** the two versions before saving: nothing is lost (chapter 10). The only case that needs a decision is when the **password or key file** has been changed on another device: Obskura offers to lock the database so you can reopen it with the new credentials.

> **TIP**
>
> To use the same database on several computers put it on your own server (chapter 09) or in a synced folder: you can keep it open everywhere at the same time.

ENCRYPTED FILES

07 FILE VAULTS

A vault is a folder that contains your files in encrypted form. From the outside it is just a set of files with unreadable names: you can tell neither what they contain nor how they are organised.

CREATING A VAULT

1. Click **New vault**, or **+** next to **File vaults**.
2. Choose a name and the folder to create it in, even inside Dropbox, OneDrive or iCloud Drive, or on a server.
3. Set a password and/or key file and press **Create**.

ADDING FILES

- **Drag** files and folders from Finder / Explorer into the window: they are encrypted into the folder you are viewing.
- Or use **Add files** or **Add folder**.
- The originals are not touched: once encrypted you can delete them yourself.

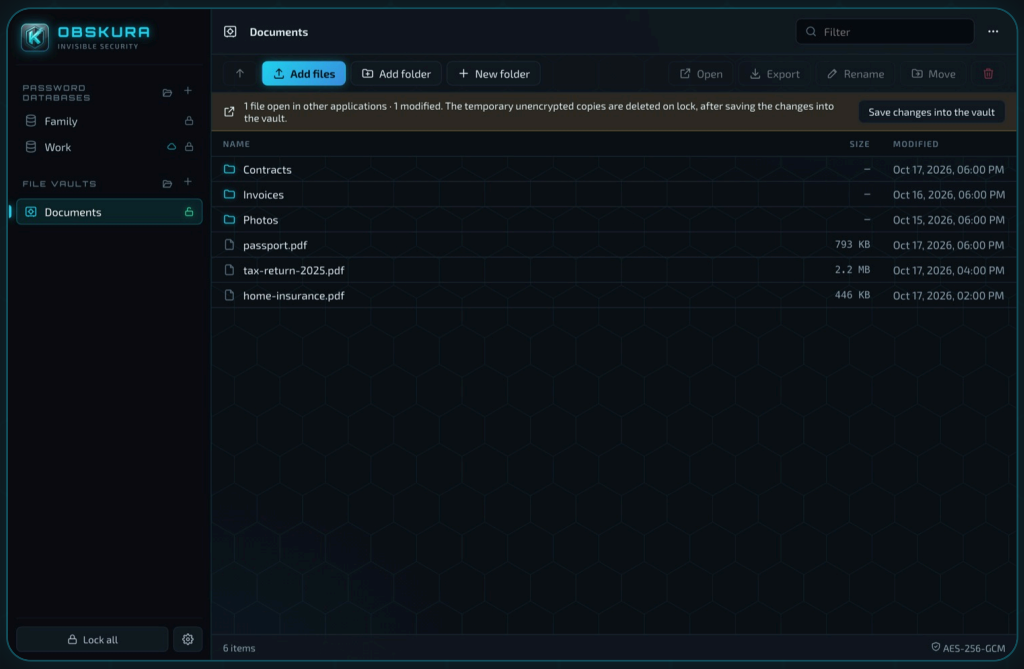


FIG. 5 An unlocked vault.

THE COMMAND BAR

↑ goes to the parent folder · **New folder** creates a subfolder · **Open**, **Export**, **Rename**, **Move** and **Delete** act on the selected items. Select several items with `Ctrl/⌘` + click or `Shift` + click. At the bottom, the status bar shows the number of items and the progress of operations.

FILE VAULTS

08 WORKING WITH FILES

OPENING AND EDITING A FILE

Double-click a file (or select it and press **Open**). Obskura decrypts it into a protected temporary folder and opens it with the system's default application.

1. Edit and save the file normally in the other application.
2. A banner appears in Obskura showing the open and the modified files.
3. Press **Save changes into the vault** to re-encrypt the new version.

> **TEMPORARY UNENCRYPTED COPIES**
>
> While a file is open, its decrypted copy exists on disk. When you lock the vault Obskura first saves any remaining changes and then **deletes the temporary copies**. Close the file in the other application before locking.

EXPORTING

Export decrypts the selected items, folders included, into a folder of your choice. The exported files are **unencrypted**: use this only when you need them outside the vault.

ORGANISING

Rename with **Rename** or `F2`; move with **Move** by choosing the destination folder. **Delete** (or `Del`) always asks for confirmation. The **Filter** field shows only the items whose name contains the text entered.

SYNCING WITH THE CLOUD

Every file in the vault is encrypted separately: if you change a document, the sync service uploads only that file. That is why vaults work well inside Dropbox, OneDrive, Google Drive or iCloud Drive.

WHAT A VAULT LOOKS LIKE ON DISK

ITEM	CONTENTS
`vault.obkv`	The vault keys, encrypted with your credentials.
`vault.obkv.bak`	Identical safety copy, in case the first file gets damaged.
`vault.obkx`	The companion file, encrypted with the access key: key file, backup and the paths of each device (chapter 11).
`d/`	All the encrypted files and folders, side by side: the real structure is not visible.

To open an existing vault use the folder icon next to **File vaults** and choose its main folder. Do not modify or move the files inside it by hand.

WHERE TO SAVE

09 REMOTE SERVERS

Databases and vaults do not have to live on your computer: Obskura opens and saves them directly on your own server, with no sync software in between. The data travels and stays on the server **already encrypted**: the server administrator, or anyone who breaks into it, sees only unreadable files.

PROTOCOL	WHERE IT IS USED	NOTES
SFTP	NAS (Synology, QNAP, TrueNAS), Linux servers, VPS	Recommended. Password or SSH key.
WebDAV	Nextcloud, ownCloud, Synology, QNAP, Box, Koofr	Over HTTPS. For Nextcloud the path is `/remote.php/dav/files/<user>`.
SMB	Windows shared folders, NAS, Samba	SMB 2 and 3; enter the share name.
FTPS	Hosting and FTP servers with TLS	FTP encrypted with `AUTH TLS`.
FTP	Traditional FTP servers	Server credentials travel in clear text: prefer FTPS or SFTP.

SETTING UP A CONNECTION

1. Open **Settings → Server connections** and press **New connection**.
2. Choose the protocol and enter address, port (if different from the standard one), user and password.
3. Press **Test connection**, then **Save**.

The server password goes into the **system keychain** (macOS Keychain, Windows Credential Manager, Secret Service on Linux), never into the settings file. It is also copied, encrypted, into the companion file: your other computers recreate the connection by themselves.

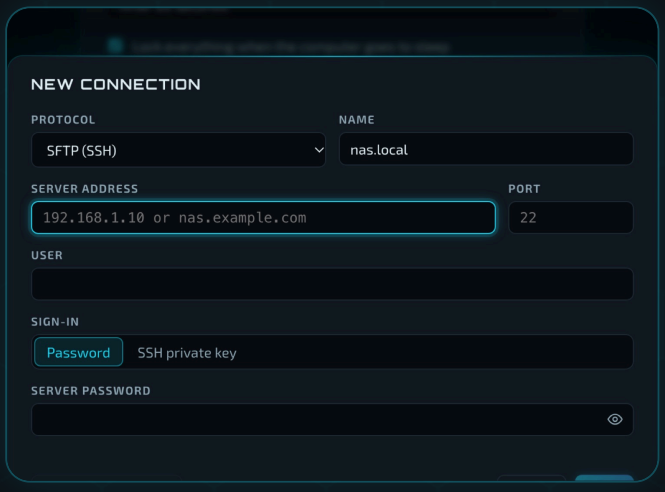


FIG. 6 A new SFTP connection.

SERVER KEY (SFTP)

On the first connection Obskura shows the **fingerprint** of the server key and asks you to accept it, as `ssh` does. If the fingerprint changes later, the connection is refused until you confirm it again: it could be someone impersonating your server. If nothing has changed on the server, do not accept.

OPENING AND SAVING ON A SERVER

- **Open:** the folder icon next to **Password databases** or **File vaults** offers **From this computer…** and **From a server…**. The same on the start screen with **From server…**.
- **Create:** in the **New database** or **New vault** window choose **On a server…** instead of **On this computer…**.
- Items on a server appear among the recents with the **cloud** icon; once open they show the `SERVER` label in the top bar.

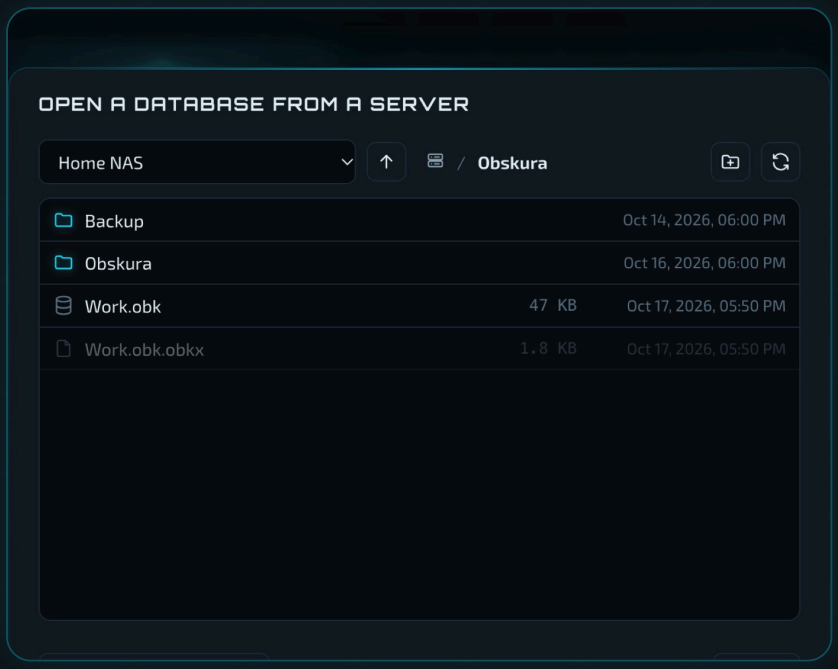


FIG. 7 The server browser: choose the connection and the folder.

In the browser choose the connection at the top left and move through the folders. For a database click the `.obk` file; for a vault enter its folder (the one with `vault.obkv`) and press **Open this vault**. The folder+ icon creates a new folder on the server.

PERFORMANCE

Databases are small and open in a moment even remotely. Vaults transfer one file at a time, when you open or export it: with very large files the connection speed matters.

COLLABORATION

10 MULTIPLE DEVICES IN REAL TIME

The same database or vault can be open on several computers at once: changes made on one appear on the others within seconds.

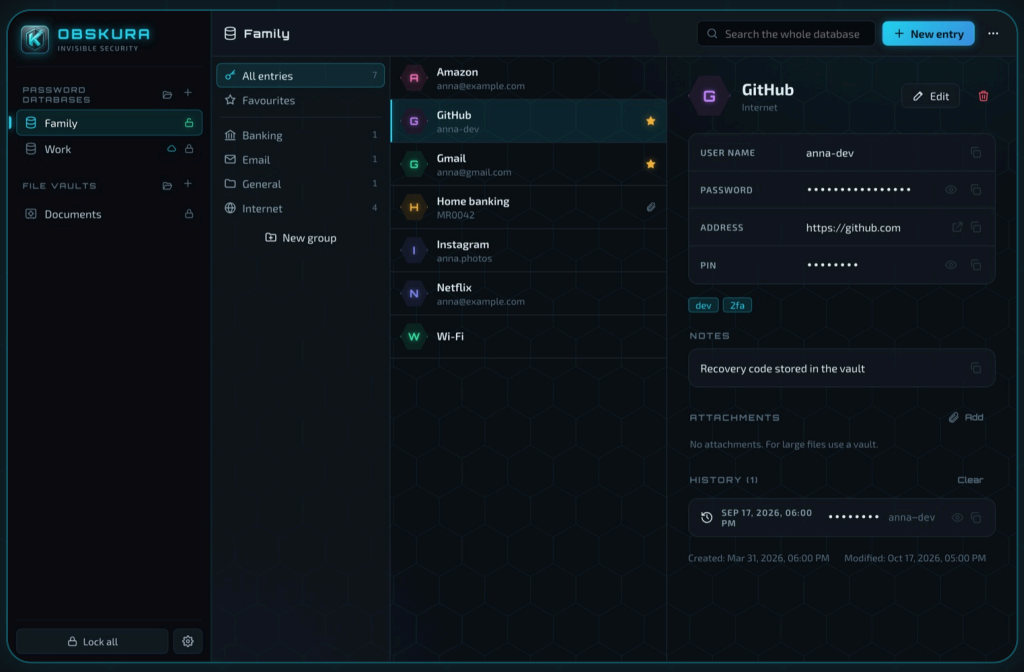


FIG. 8 A notification: another device has added and changed some entries.

HOW IT WORKS

- Obskura checks the file every **2 seconds** on a local disk or in a synced folder, every **5 seconds** on a server. The check reads only the first 88 bytes of the file.
- When it finds a new version it **merges** it with yours, entry by entry, shows a notification with the entries added, changed or deleted and updates the list immediately.
- If two people change the **same entry**, the most recent change wins; the other is not lost: it goes into the entry's **History**.
- A deletion reaches everyone, unless someone has changed that entry in the meantime: in that case the change takes precedence and the entry stays.
- In vaults, when someone adds, renames or deletes files in the folder you are viewing, the list updates by itself.

COMPUTER CLOCKS

To decide which change is more recent Obskura uses the computers' clocks: keep them synchronised (automatic time setting, usually on by default on all systems).

FIND EVERYTHING, EVERYWHERE

11 ACCESS KEY AND DEVICES

Every database and every vault has a small encrypted file next to it that remembers where the key file, backups and servers are, and how each of your devices reaches them. It is protected by the Obskura access key.

THE OBSKURA ACCESS KEY

It is a 55-character code generated on first launch (or entered, if you created it on another computer). It stays in the system keychain; from **Settings → Obskura access key** you can:

- **Show**: see and copy it, to enter it on another computer.
- **Change key…**: generate a new one. Obskura immediately re-encrypts the companion files it can reach; the others are updated the next time they are opened (previous keys remain valid for reading them).
- **Enter key…**: use the current key if it was changed on another computer.

COMPANION FILES

They are encrypted with AES-256-GCM and unreadable without the access key:

FILE	CONTAINS
`.obk.obkx`	Next to every database: location of the key file, backup configuration, server connections and the device records.
`vault.obkx`	Inside every vault: the same information.
`recenti.obkx`	In the app's data folder: the list of recents. No paths are left on disk in clear text.

OPENING FROM ANOTHER COMPUTER

Once the access key is entered on the new computer, just select the database: Obskura reads the companion file, recreates any missing server connections, finds the key file (at the location known for that device, next to the database, at the other devices' paths or in the backup copy) and offers the backup copy if the original cannot be reached.

> **IMPORTANT**
>
> The access key does not replace the database password: without the password (and key file) the data stays unreadable. Still, keep it in a safe place: without it you have to choose the key file and backups by hand.

DEVICES AND PATHS

Every computer that uses Obskura has a **unique identifier**, generated on first launch, and a **name** (the computer's, editable in **Settings → Name of this device**). Every time it opens a database or a vault, it writes its own record into the encrypted companion file:

DATA	EXAMPLE
Identifier and name	`3f2a9c1e-…` · "Home MacBook"
System and version	macOS · Obskura 0.3.0 · last access
Database path	`/Users/anna/Dropbox/accounts.obk` on the Mac, `D:\Dropbox\accounts.obk` on the PC
Key file path	`/Volumes/USB/key.obkey` or `E:\key.obkey`
Own backup	a folder of that device, or the shared configuration (chapter 12)

THE "DEVICES AND PATHS" WINDOW

From the ⋯ menu of a database or vault choose **Devices and paths…**:

- you see all registered devices, with system, version, last access, key file use and backup destination;
- the eye icon shows each device's paths; the pencil renames this device;
- the bin **forgets** a device you no longer use: its paths and its backup are removed from the file (if it opens it again, it registers again).

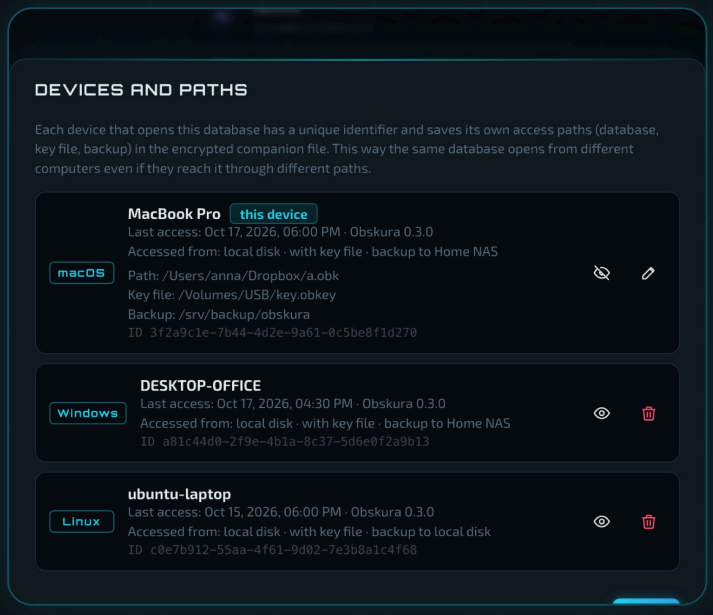


FIG. 9 The devices that use a database.

WHY IT MATTERS

The same database in Dropbox has different paths on Mac, Windows and Linux, and the USB stick with the key file changes drive letter or name. Thanks to the per-device records each one finds its own paths, without overwriting those of the others.

DATA SAFETY

12 AUTOMATIC BACKUP

Every database and every vault can have a **second destination**, on this computer (for example an external disk) or on any configured server. On every change Obskura copies the new version there in the background, without slowing you down.

1. From the ⋯ menu of the database or vault choose **Automatic backup…**
2. Turn on **Automatic backup on** and choose the folder: **On this computer…** or **On a server…**.
3. If the destination is a server, you can tick **Use this configuration on all devices**.
4. For databases choose how many **dated copies** to keep.
5. Press **Save**. **Run now** forces a full copy.

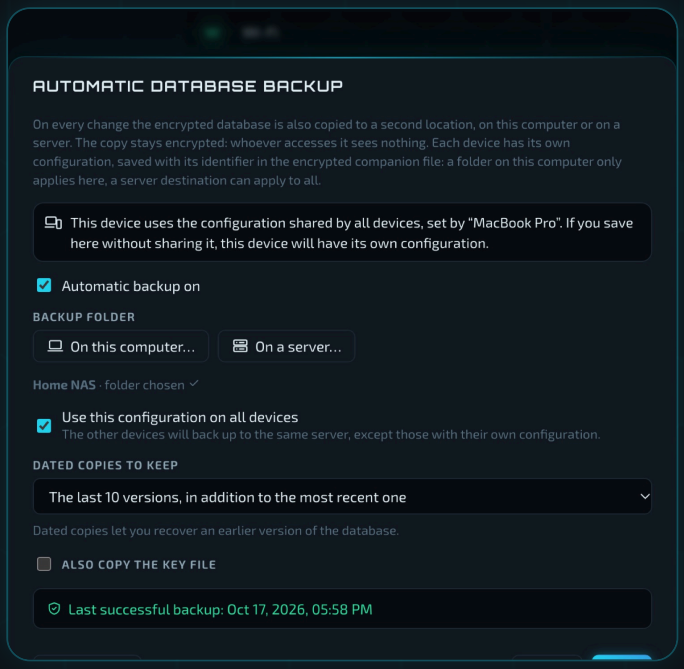


FIG. 10 Backup to a NAS, shared by all devices.

WHAT	HOW IT IS COPIED
Database	The `.obk` file in the backup folder, plus the dated copies `name.YYYYMMDD-hhmmss.obk`; the oldest beyond the limit are deleted.
Vault	A replica of the encrypted folder: on every change only the touched files are copied again. The copy opens like a normal vault.
Key file	Optional: copied once, when you save the setting, into the folder you specify.

A BACKUP FOR EVERY DEVICE

- Each device has its **own configuration**, saved with its identifier in the companion file: a local folder (for example the Mac's external disk) applies only to that device.
- A server destination can become **shared**: the other devices use it, except those that have their own configuration. The window shows who set it.
- The copies stay **encrypted**: the backup destination does not need to be trusted.
- If a backup fails a warning appears; Obskura tries again at the next change.

KEY FILE AND BACKUP

Do not put the key file in the same folder as the backup: anyone accessing that folder would have both the database and half of the credentials.

FROM AND TO OTHER PROGRAMS

13 IMPORT AND EXPORT

IMPORTING FROM AN ONLINE MANAGER

Obskura signs in directly to your old service, downloads the encrypted vault and decrypts it on your computer, without going through a file exported in clear text. The credentials are used only for that sign-in and are not saved.

1. Open the destination database and choose ⋯ → **Import from an online manager…**
2. Choose the service and sign in; if you use two-step verification Obskura asks for the code.
3. Check the preview: number of entries, folders, examples.
4. Decide whether to recreate the folders as groups and whether to skip entries already present, then press **Import**.

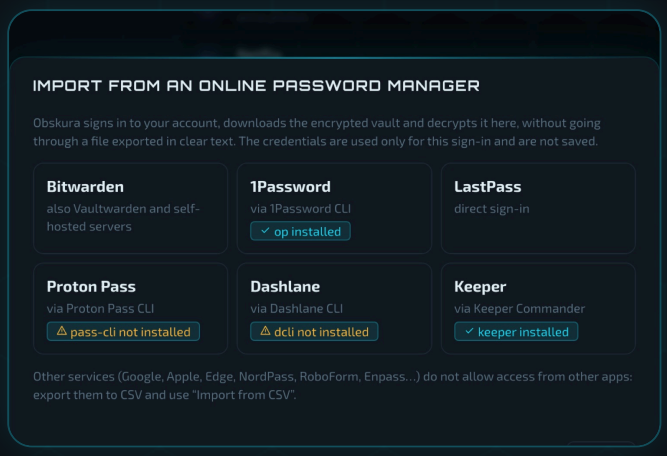


FIG. 11 Choosing the service to import from.

SERVICE	ACCESS
Bitwarden / Vaultwarden	Direct, including bitwarden.eu and self-hosted servers; alternatively with the personal API key.
LastPass	Direct, with two-step verification (code or confirmation on the phone).
1Password	Through 1Password CLI (`op`), authorised by the 1Password app or with email, password and Secret Key.
Proton Pass	Through Proton Pass CLI (`pass-cli`), with sign-in from the browser.
Dashlane	Through Dashlane CLI (`dcli`), after a first `dcli sync` in the terminal.
Keeper	Through Keeper Commander (`keeper`).

Folders, custom fields, TOTP codes, cards and notes are preserved. Other services (Google, Apple, Edge, NordPass…) do not allow access from other apps: export them to CSV.

IMPORTING FROM CSV (KEEPASS AND OTHERS)

1. In the source program export to CSV: KeePass 2 **File → Export → KeePass CSV (1.x)**, KeePassXC **Database → Export → CSV File**, Bitwarden, 1Password, Chrome, Edge and Firefox from their settings.
2. In Obskura open the database and choose ⋯ **→ Import from CSV (KeePass, …)…**
3. Choose the file: Obskura recognises the format and the columns and shows a preview.
4. Decide whether to recreate the file's groups and whether to skip entries already present, then press **Import**.

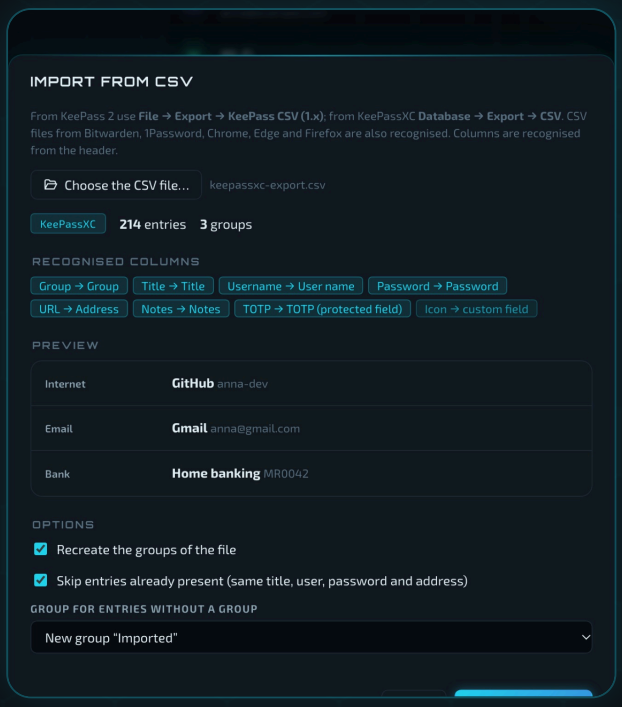


FIG. 12 Preview of a KeePassXC export.

Groups, tags, TOTP codes (saved as a protected field), creation dates and expiry dates are preserved; unrecognised columns become custom fields. Re-importing the same file creates no duplicates.

EXPORTING TO CSV

⋯ **→ Export to CSV…** creates a file with the KeePassXC columns, plus tags, expiry, favourites and custom fields: it can be re-imported into Obskura, KeePassXC and most password managers.

> **CSV IS NOT ENCRYPTED**
>
> The file contains all the passwords in clear text. Use it only to move data, then delete it. After importing, also delete the CSV exported from the old program. For backups use the automatic backup, which stays encrypted.

CUSTOMISING

14 LANGUAGES

Obskura speaks eight languages and more can be added: all of the app's texts are in XML files, one per language.

CHOOSING THE LANGUAGE

At start-up Obskura uses the system language; if it is not one of those included it uses English. In **Settings → Language** you can leave **Automatic** or choose one: the change is immediate, error messages included. Arabic reads from right to left and the interface is mirrored accordingly.

Italiano	it
English	en
Deutsch	de
Español	es
Русский	ru
中文（简体）	zh
日本語	ja
العربية	ar

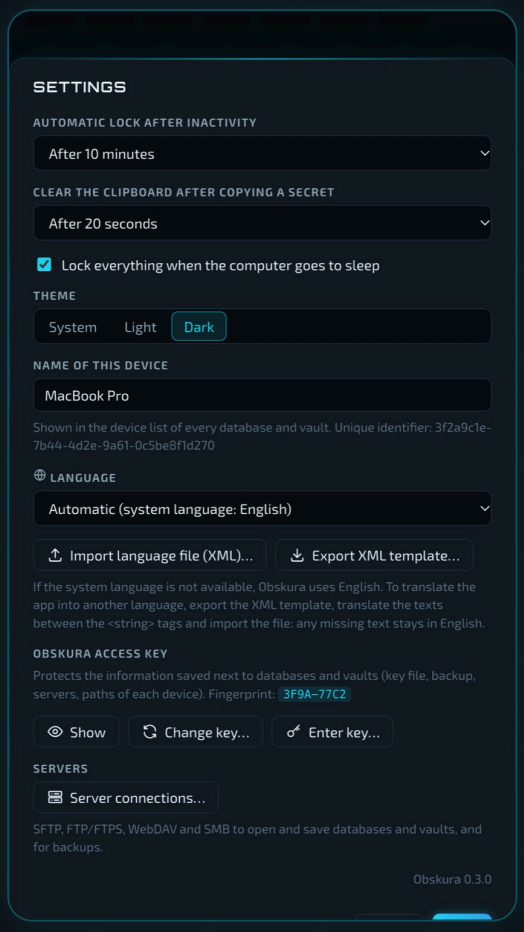


FIG. 13 The Language section in the settings.

ADDING A LANGUAGE

1. In **Settings → Language** press **Export XML template...**: you get the complete file of the current language (or download the zip with the XML files of all languages from the website).
2. In the header change `code` (the language code, for example `fr` or `pt-BR`), `name` and, for right-to-left languages, `dir="rtl"`.
3. Translate the text of each `<string>` element with any text editor, saving in UTF-8.
4. Press **Import language file (XML)...**: the language appears in the list immediately and is used automatically on systems in that language.

THE FILE FORMAT

A language file is an XML file with a `<language>` element and one `<string>` per text:

```
<?xml version="1.0" encoding="UTF-8"?>
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.cancel">Annuler</string>
  <string key="db.syncFailed">Échec de la synchronisation : {message}</string>
  <string key="vault.itemsN.one">{count} élément</string>
  <string key="vault.itemsN.other">{count} éléments</string>
</language>
```

- the `key` attribute must not be translated or changed;
- placeholders in braces, such as `{count}` or `{name}`, must be left as they are: the app replaces them with numbers and names;
- the `<b>` and `<code>` tags in the text must be kept;
- keys ending in `.one`, `.two`, `.few`, `.many` and `.other` are plural forms: use those of your language, `.other` is mandatory;
- a missing text is shown in English, so a partial translation already works.

CORRECTING AN INCLUDED LANGUAGE

An XML file with the same `code` as an included language (for example `en`) does not replace it: it only corrects the entries it contains. In the settings it appears marked **corrections** and is removed with the ×, returning to the original texts.

> **TIP**
>
> Imported files stay in the app's data folder and apply only to that computer: import them on the others too.

TRANSLATING WITH THE EMPTY XML TEMPLATE

For a new language you can start from the empty template `obskura-translation-template.xml`, which you download from the website (`obskura.bytenooks.com`, Download section). It has one line for each text of the app: write the text between `<string …>` and `</string>`; the `en` attribute holds the English reference text and can stay where it is (the app ignores it).

```
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.lock" en="Lock">Verrouiller</string>
  <string key="common.settings" en="Settings">Paramètres</string>
  <string key="common.cancel" en="Cancel">Annuler</string>
</language>
```

1. Download the template and save it with the code of your language, for example `fr.xml`.
2. In the first `<language>` line fill in `code`, `name`, `english-name` and, if needed, `dir="rtl"`.
3. Write the translations with a text editor that saves in UTF-8, following the rules above.
4. **Delete the lines you do not translate**: a text left empty would appear blank in the app, while a missing line is shown in English.
5. Import the file in **Settings → Language** and check the texts in the app.

SHARE YOUR TRANSLATION

Send it to the developer from the Contact page of the website: choose the “Translation” topic and attach the XML file (up to 3 MB; a complete language file is about 100–150 KB). Translations received may be included in future versions.

SECURITY

15 LOCKING AND SETTINGS

When you lock a database or a vault, Obskura closes the session and **wipes from memory** the keys and decrypted data. Reopening them requires the credentials again.

WAYS TO LOCK

- **Lock all** at the bottom of the sidebar, or `Ctrl/⌘` + `L`.
- The padlock next to an unlocked item in the sidebar, or the **Lock** item in the ⋯ menu.
- **Automatically**, after a period of inactivity or when the computer goes to sleep.

SETTINGS

SETTING	EFFECT	DEFAULT
Automatic lock after inactivity	Locks everything after 1–60 minutes without mouse or keyboard use, or never.	10 minutes
Clear the clipboard	Clears the clipboard 10–120 seconds after a secret is copied, or never.	20 seconds
Lock on sleep	Locks everything when the computer goes to sleep.	On
Theme	System, Light or Dark.	Dark
Name of this device	Shown in the device list of every database and vault; the unique identifier is shown below it.	Computer name
Language	Automatic or one of the available languages; import and export of XML files (chapter 14).	Automatic
Obskura access key	Show, change or enter the key (chapter 11).	—
Servers	The SFTP, FTP/FTPS, WebDAV and SMB connections (chapter 09).	—

The settings contain no secrets: server passwords are in the system keychain and the list of recents is encrypted with the access key.

REFERENCE

16 SHORTCUTS AND CRYPTOGRAPHY

KEYBOARD SHORTCUTS

KEYS	WHERE	ACTION
`Ctrl/⌘` + `L`	Anywhere	Lock all
`Esc`	Dialogs	Closes the window
`Ctrl/⌘` + `F`	Database	Search
`Ctrl/⌘` + `N`	Database	New entry
`Ctrl/⌘` + `S`	Entry editor	Save the entry
Double click	Entry list	Copy the password
`Ctrl/⌘` + `A`	Vault	Select all
`Enter`	Vault	Opens the file or folder
`F2`	Vault	Rename
`Del` · `⌘` + `⌫`	Vault	Delete the selected items
`⌫`	Vault	Go to the parent folder

CRYPTOGRAPHIC DETAILS

COMPONENT	ALGORITHM
Key derivation	Argon2id: 256 MiB / 3 passes, 1 GiB / 4 passes or 2 GiB / 6 passes, random 256-bit salt.
Composite key	SHA-256 of password (NFC-normalised) and key file, as in KeePass KDBX4.
Encryption	AES-256, XChaCha20, Serpent, Twofish, Camellia or cascades, always authenticated (GCM or Poly1305); in cascades each layer has its own key derived via HKDF.
Subkeys	HKDF-SHA256 with a new seed on every save.
Integrity	Authenticated header: any tampering prevents opening.
Names in vaults	AES-SIV, bound to the folder that contains them.
File contents	64 KiB blocks, random key per file, protection against reordering and truncation.
Companion files	AES-256-GCM with a key derived via HKDF from the Obskura access key (256 random bits).
Memory	Keys and plain-text data stay in the native process and are wiped on close.

SUPPORT

17 GOOD PRACTICE AND TROUBLESHOOTING

GOOD PRACTICE

- **Turn on automatic backup** or regularly copy the `.obk` files and vault folders to an external disk. They are already encrypted, so the backup is safe wherever you keep it.
- **Keep the key file separate** from the database and have at least one spare copy.
- **Keep the Obskura access key** on paper or somewhere other than the computer.
- **Use a different password for every service**, made with the generator: you will only have to remember one.
- **Lock when you step away**: `Ctrl/⌘` + `L` is the quickest gesture.
- **Forget the devices** you no longer use, from the **Devices and paths** window.

FREQUENTLY ASKED QUESTIONS

I FORGOT THE MASTER PASSWORD. CAN I RECOVER IT?

No. That is exactly what makes Obskura secure: nobody, not even the developers, can open a database or vault without the right credentials.

"WRONG PASSWORD OR KEY FILE", BUT I AM SURE THEY ARE RIGHT.

Check that you chose the same key file used at creation and that it has not been modified. If you used a password *and* a key file, both are needed. Also check Caps Lock.

OPENING TAKES A FEW SECONDS. IS THAT NORMAL?

Yes: it is the time Argon2id takes, intended to slow down anyone trying to guess the password. The High level needs a few seconds and 1 GiB of free memory, Extreme up to 12 seconds and 2 GiB.

ON ANOTHER COMPUTER THE KEY FILE IS NOT FOUND.

Connect the drive that holds it: Obskura looks for it at the path that computer used last time, next to the database, at the other devices' paths and in the backup copy. If it does not find it, choose it with **Choose…**: next time the path will be remembered for that device.

IT SAYS “PROTECTED WITH A DIFFERENT ACCESS KEY”.

The access key was changed on another computer. Click **Enter the current key** and use the new one; you can still unlock with the password and choose the key file by hand.

“CREDENTIALS CHANGED ELSEWHERE” APPEARED.

Someone changed the database's password or key file on another device. Choose **Lock** and reopen it with the new credentials; **Overwrite** would undo the change made elsewhere.

I CANNOT CONNECT TO THE SERVER.

Check address, port and credentials with **Test connection**. For WebDAV check the base path (for Nextcloud `/remote.php/dav/files/<user>`); for SMB the share name. With a self-signed certificate turn on **Accept self-signed certificates** only on a trusted network.

CHANGES TO A FILE IN THE VAULT DO NOT SEEM TO BE SAVED.

Make sure you saved the file in the other application, then press **Save changes into the vault**. If you lock the vault with the file still open, Obskura still tries to save it before deleting the temporary copy.

THE APP OPENS IN A LANGUAGE THAT IS NOT MINE.

Obskura follows the system language; if yours is not included it uses English. Choose the language in **Settings → Language** or import an XML file (chapter 14).

MACOS OR WINDOWS SAY THE APP IS NOT VERIFIED.

The app is not signed with a commercial certificate. Follow the instructions in chapter 02 to open it the first time.



OBSKURA

INVISIBLE SECURITY FOR YOUR DATA

Password manager and encrypted file vaults · on your computer or on your server

macOS · Windows · Linux · Version **0.3.0**

https://obskura.bytenooks.com