

OBSKURA

为你的数据提供无形的安全

使用手册

版本 0.3.0

MACOS · WINDOWS · LINUX

2026 年 10 月

使用手册

目录

01	欢迎使用 Obskura	功能简介、数据库与保险库	03
02	安装与首次启动	macOS、Windows、Linux · 访问密钥 · 界面	04
03	密码与密钥文件	凭据、Argon2id、选择加密算法	05
04	密码数据库	创建、解锁、整理条目	07
05	管理条目	生成器、字段、附件、历史记录	08
06	数据库工具	搜索、安全复制、数据库菜单	09
07	文件保险库	创建保险库并加密文件	10
08	处理文件	打开、修改、导出	11
09	远程服务器	SFTP、WebDAV、SMB、FTP/FTPS	12
10	多设备实时协作	实时同步、通知	14
11	访问密钥与设备	伴随文件、每台设备的标识和路径	15
12	自动备份	第二位置、带日期的副本、按设备设置	17
13	导入和导出	在线密码管理器、KeePass 等的 CSV	18
14	语言	自动语言、XML 文件、新的翻译	20
15	锁定与设置	自动锁定、剪贴板、主题、设备名称	23
16	快捷键与加密细节	键盘快捷键和技术细节	24
17	最佳实践与故障排除	备份、常见问题	25

约定

按钮和菜单名称以**粗体**表示。组合键写作：`Ctrl/⌘` + `L`，其中 `Ctrl` 适用于 Windows 和 Linux，`⌘` 适用于 macOS。文件名和扩展名使用`等宽字体`。截图显示的是本手册语言的界面。

简介

01 欢迎使用 OBSKURA

Obskura 以军用级加密保护密码和文件。无需账户，不依赖任何第三方服务：数据保存在你决定的地方——你的电脑或你的服务器。

每个数据库和每个保险库都只是普通的文件或文件夹。你可以把它们放在电脑硬盘、U 盘、Dropbox、OneDrive 或 iCloud Drive 等同步文件夹中，或直接放在你自己的 SFTP、WebDAV、SMB 或 FTP 服务器上，数量不限：个人的、工作的、和家人共享的。多台电脑可以同时使用，并实时看到彼此的修改，即使它们通过不同的路径访问。

密码数据库

仿照 KeePass 的单个 `.obk` 文件。包含按分组整理的条目，每个条目有用户名、密码、地址、备注、自定义字段、附件和修改历史。

文件保险库

仿照 Cryptomator 的文件夹。把文档、照片和归档拖进去：每个文件都单独加密，包括文件名和文件夹结构。

保护原理

创建数据库或保险库时，你需要选择**主密码**、**密钥文件**或两者。Obskura 用 Argon2id 从这些凭据派生出加密密钥——这种算法专门用来让猜测密码变得极其缓慢。随后数据用 AES-256 加密，这是获准用于**绝密**（TOP SECRET）级信息的标准。

凭据不会保存在任何地方。没有它们，任何人（包括开发者）都无法读取内容。

重要

忘记的密码或丢失的密钥文件无法以任何方式找回。请选择你能记住的密码，并把密钥文件的副本保存在安全且独立的地方。

概览

AES-256-GCM · XChaCha20-Poly1305 · Serpent · Twofish · Camellia · 级联加密 · Argon2id 最高 2 GiB · HKDF-SHA256 · 文件名使用 AES-SIV · 关闭时清除内存 · 无需账户 · SFTP · WebDAV · SMB · FTPS · 实时同步 · 自动备份 · 按设备记录路径 · 8 种语言 · macOS · Windows · Linux

入门

02 安装与首次启动

macOS

打开 `.dmg` 文件，把 Obskura 拖到**应用程序**。首次启动时如果 macOS 阻止了该应用，请前往**系统设置 → 隐私与安全性**并选择**仍要打开**。

Windows

运行 `.exe` 安装程序（会自动使用 Windows 的语言），或直接运行无需安装的便携版。如果出现 SmartScreen 警告，请点按**更多信息 → 仍要运行**。

Linux

使用 `.deb` 包（Debian、Ubuntu）、`.rpm` 包（Fedora、openSUSE），或无需安装的 `.AppImage`：给它添加可执行权限后运行。

首次启动：语言和访问密钥

Obskura 会以系统语言打开（意大利语、英语、德语、西班牙语、俄语、中文、日语或阿拉伯语；其他语言则使用英语）。首次启动时，它会要求你创建 **Obskura 访问密钥**；如果你已经在另一台电脑上使用 Obskura，则输入在那里生成的密钥。第 11 章会说明它的用途。

主界面



图 1 欢迎界面和侧边栏。

侧边栏包含**密码数据库**和**文件保险库**两部分。每个标题旁有两个按钮：文件夹图标用于**打开**已有项目，**+** 用于新建。

- 最近打开的项目会保留在列表中，只显示名称，从不显示路径。锁图标表示状态：**闭合**表示已锁定，**打开**表示已解锁。
- 鼠标悬停在项目上时会出现 **×**，可将其从最近使用中移除（文件不会被删除），或出现锁图标以立即锁定。
- 底部：**全部锁定**和**设置**齿轮。

保护数据

03 密码与密钥文件

数据库和保险库可用**主密码**、**密钥文件**或两者一起打开。两者结合是最强的保护：既需要你*知道*的东西，也需要你*拥有*的东西。

主密码

长句子比复杂的单词更安全：四五个随机词容易记住，却极难被猜中。字段下方的指示器以比特估计其强度。

如果想要随机密码，骰子按钮会打开**生成器**。

密钥文件

与 KeePass 一样，**任何文件**都可以作为密钥。你可以选择**使用已有文件**或**生成新文件**：Obskura 会在你指定的位置创建一个随机密钥文件。

比如把它保存在 U 盘上，与数据库分开。Obskura 会记住它在每台设备上的位置，并在每次打开时自动查找（第 11 章）。



图 2　创建数据库，加密选项已展开。

加密选项

在**加密选项**中可以选择密钥派生的代价和使用的加密算法。默认值“标准”和 AES-256-GCM 已足以应对任何用途；所有可选项见下一页。

绝不要修改密钥文件

如果用任意文件（照片、文档）作为密钥，哪怕最微小的改动也会使其失效。Obskura 生成的文件采用可识别的文本格式，即使换行符改变也仍然有效。无论如何，请保留一份备份。

保护数据

03 选择加密算法

密钥派生（ARGON2ID）

Argon2id 把你的凭据转换为加密密钥：使用的内存和轮数越多，攻击者尝试数百万个密码的代价就越高。

级别	参数	打开时间
标准	256 MiB 内存，3 轮	约 0.5–1 秒
高	1 GiB，4 轮	约 2–4 秒
极高	2 GiB，6 轮	约 5–12 秒

极高级别

每次打开都需要 **2 GiB 可用内存**。在内存较小的电脑上，数据库或保险库可能无法打开：只有当你会在合适的电脑上使用文件时才选择它。

加密算法

所有算法都使用 256 位密钥并经过**认证**：任何对数据的篡改都会被发现。

加密算法	特点
AES-256-GCM	**默认。**获准用于绝密信息的美国标准，借助硬件加速速度最快。
XChaCha20-Poly1305	流密码，即使没有 AES 指令，在任何处理器上都很快。
Serpent-256-GCM	AES 竞赛决赛算法，安全余量最大（32 轮）。较慢。
Twofish-256-GCM	AES 竞赛决赛算法，由 Bruce Schneier 等人设计。
Camellia-256-GCM	国际 ISO/IEC 标准，获欧洲（NESSIE）和日本（CRYPTREC）推荐。
级联 AES · Twofish · Serpent	**最强的选择。**使用独立密钥依次进行三次加密：即使将来三种算法中有两种被攻破，数据仍然受到保护。
级联 AES · XChaCha20	结合一种分组密码和一种流密码，二者属于完全不同的算法家族。

保险库

在保险库中，所选算法同时保护密钥和每个文件的内容。如果通过**更改密码 / 密钥文件**更换算法，已有文件仍使用原算法加密，之后添加的文件使用新算法。当前算法显示在保险库右下角。

密码管理器

04 密码数据库

创建数据库

1. 在主界面点按**新建数据库**，或点按**密码数据库**旁的 +。
2. 输入**名称**并选择 `.obk` 文件的保存位置：**在这台电脑上…**或**在服务器上…**。
3. 设置密码和/或密钥文件（第 03 章）。
4. 按**创建**。数据库会以已解锁状态打开。

打开与解锁

1. 在侧边栏选择数据库，或用文件夹图标打开已有的 `.obk` 文件。
2. 输入密码。密钥文件和备份副本会自动查找；如果找不到密钥文件，请点按**选择…**手动选择。
3. 按**解锁**或 `Enter`。



图 3　已解锁的数据库：分组、条目列表和所选条目的详情。

三栏

- **分组**：**所有条目**、**收藏**以及你的文件夹。悬停在分组上会出现新建子分组、编辑或删除的命令；**新建分组**位于列表底部。
- **条目**：每个条目的标题和用户名。星标表示收藏，回形针表示有附件。**双击**可直接复制密码。
- **详情**：条目的所有字段，以及显示、复制或在浏览器中打开地址的按钮。

密码数据库

05 管理条目

要添加条目，请按**新建条目**（或 `Ctrl/⌘` + `N`）；要修改，选中条目后按**编辑**。用底部按钮或 `Ctrl/⌘` + `S` 保存。每次修改都会立即写入数据库文件。



图 4　条目编辑器，生成器已打开。

条目的字段

标题和分组	条目名称及其所在文件夹。
用户名	账户、电子邮件或客户编号。
密码	带强度指示器和生成器。
地址	可在详情中用浏览器打开。
备注	自由文本，与其他内容一样加密。
标签	用逗号分隔的关键词。
过期时间	超过该日期应更换密码。

顶部的**星标**可将条目加入**收藏**。

密码生成器

点按密码字段中的骰子。选择**长度**（8 到 64 个字符）和字符类别（`a-z`、`A-Z`、`0-9`、`!@#$`）；**排除易混淆字符**会避开 l、1、O、0 这类容易混淆的字符。然后**重新生成**、**复制**或**使用此密码**。密码由系统的加密随机数生成器产生。

自定义字段

添加 PIN、恢复代码或安全问题等额外信息。勾选**受保护**后，它们会像密码一样隐藏显示。

附件与历史记录

每个附件最大 64 MB（更大的文件请使用保险库）。每次修改都会保留上一版本：**历史记录**保存最近 20 个版本，可复制旧密码。

密码数据库

06 数据库工具

搜索

顶部的**在整个数据库中搜索**字段（或 `Ctrl/⌘` + `F`）会在输入时筛选所有分组的条目。`Esc` 清空搜索。

安全复制

用户名、密码和受保护字段旁的复制按钮会把值放入剪贴板，Obskura 会在 20 秒后**自动清空**（可在设置中更改）。只有当剪贴板中仍是复制的值时才会清空：如果你在此期间复制了别的内容，则不会动它。

数据库菜单

右上角的 ⋯ 按钮包含：

菜单项	用途
数据库属性	更改数据库的名称和描述。
更改密码 / 密钥文件	设置新凭据。数据库会用新密钥重新加密。
保存备份副本…	将数据库的加密副本写到另一个位置。
自动备份…	配置副本的第二个保存位置（第 12 章）。
设备和路径…	查看哪些设备在使用数据库及其路径（第 11 章）。
导入 / 导出	从在线密码管理器或 CSV 导入，或导出为 CSV（第 13 章）。
锁定数据库	关闭数据库并从内存中清除其数据。

保存与同步

每次修改都会立即以**原子方式**保存：新文件单独写入，只有完整写完后才替换旧文件，因此断电也不会损坏它。如果此期间另一台电脑修改了数据库，Obskura 会在保存前**合并**两个版本：不会丢失任何内容（第 10 章）。唯一需要你决定的情况是另一台设备更改了**密码或密钥文件**：Obskura 会建议锁定数据库，再用新凭据重新打开。

> **提示**
> 要在多台电脑上使用同一个数据库，请把它放在你的服务器上（第 09 章）或同步文件夹中：它可以在各处同时保持打开。

加密文件

07 文件保险库

保险库是一个以加密形式存放文件的文件夹。从外部看，它只是一堆文件名无法读取的文件：既看不出内容，也看不出组织结构。

创建保险库

1. 点按**新建保险库**，或点按**文件保险库**旁的 +。
2. 选择名称和创建它的文件夹，可以在 Dropbox、OneDrive、iCloud Drive 内，也可以在服务器上。
3. 设置密码和/或密钥文件，然后按**创建**。

添加文件

- 把文件和文件夹从访达 / 资源管理器**拖**到窗口中：它们会被加密到当前查看的文件夹。
- 也可以使用**添加文件**或**添加文件夹**。
- 原文件不会被改动：加密后可自行删除。



图 5 已解锁的保险库。

命令栏

↑ 返回上级文件夹 · **新建文件夹**创建子文件夹 · **打开**、**导出**、**重命名**、**移动**和**删除**作用于所选项目。用 `Ctrl/⌘` + 点按或 `Shift` + 点按可多选。底部状态栏显示项目数量和操作进度。

文件保险库

08 处理文件

打开并修改文件

双击文件（或选中后按**打开**）。Obskura 会把它解密到受保护的临时文件夹，并用系统默认应用打开。

1. 在其他应用中照常修改并保存文件。
2. Obskura 中会出现一条横幅，显示已打开和已修改的文件。
3. 按**将修改保存到保险库**，重新加密新版本。

> **临时的未加密副本**
>
> 文件打开期间，其解密副本存在于磁盘上。锁定保险库时，Obskura 会先保存剩余的修改，然后**删除临时副本**。请在锁定前关闭其他应用中的文件。

导出

导出会把所选项目（包括文件夹）解密到你选择的文件夹。导出的文件是**未加密**的：只在需要在保险库之外使用时才这样做。

整理

用**重命名**或 `F2` 重命名；用**移动**并选择目标文件夹来移动。**删除**（或 `Delete`）总会要求确认。**筛选**字段只显示名称包含所输入文字的项目。

与云端同步

保险库中的每个文件都单独加密：修改一份文档时，同步服务只会上传这个文件。因此保险库很适合放在 Dropbox、OneDrive、Google Drive 或 iCloud Drive 中。

保险库在磁盘上的样子

项目	内容
`vault.obkv`	保险库的密钥，用你的凭据加密。
`vault.obkv.bak`	完全相同的安全副本，以防第一个文件损坏。
`vault.obkx`	伴随文件，用访问密钥加密：密钥文件、备份以及每台设备的路径（第 11 章）。
`d/`	所有加密的文件和文件夹并列存放：看不出真实的结构。

要打开已有的保险库，请使用**文件保险库**旁的文件夹图标并选择它的主文件夹。不要手动修改或移动其中的文件。

保存位置

09 远程服务器

数据库和保险库不一定要放在电脑上：Obskura 可以直接在你的服务器上打开和保存它们，中间不需要同步软件。数据在传输时和保存在服务器上时都**已经加密**：服务器管理员或入侵者只能看到无法读取的文件。

协议	使用场景	说明
SFTP	NAS（Synology、QNAP、TrueNAS）、Linux 服务器、VPS	推荐。密码或 SSH 密钥。
WebDAV	Nextcloud、ownCloud、Synology、QNAP、Box、Koofr	基于 HTTPS。Nextcloud 的路径为 `/remote.php/dav/files/<用户>`。
SMB	Windows 共享文件夹、NAS、Samba	SMB 2 和 3；需填写共享名称。
FTPS	带 TLS 的主机和 FTP 服务器	使用 `AUTH TLS` 加密的 FTP。
FTP	传统 FTP 服务器	服务器凭据以明文传输：最好使用 FTPS 或 SFTP。

配置连接

1. 打开**设置 → 服务器连接**并按**新建连接**。
2. 选择协议，并输入地址、端口（若不是标准端口）、用户和密码。
3. 按**测试连接**，然后按**保存**。

服务器密码保存在**系统钥匙串**中（macOS 钥匙串、Windows 凭据管理器、Linux 的 Secret Service），绝不会写入设置文件。它还会以加密形式复制到伴随文件中：你的其他电脑会自动重建连接。



图 6 新建 SFTP 连接。

服务器密钥（SFTP）

首次连接时，Obskura 会显示服务器密钥的**指纹**并请你接受，就像 `ssh` 一样。如果之后指纹发生变化，连接会被拒绝，直到你再次确认：这可能是有人冒充你的服务器。如果服务器没有任何变化，请不要接受。

在服务器上打开和保存

- **打开：**密码数据库或文件保险库旁的文件夹图标提供**从这台电脑…**和**从服务器…**。主界面的**从服务器…**按钮作用相同。
- **创建：**在**新建数据库**或**新建保险库**窗口中选择**在服务器上…**而不是**在这台电脑上…**。
- 服务器上的项目在最近使用中带有**云**图标；打开后，顶部栏会显示 服务器 标签。



图 7　服务器浏览器：选择连接和文件夹。

在浏览器左上角选择连接，然后在文件夹间移动。对于数据库，点按 `.obk` 文件；对于保险库，进入它的文件夹（包含 `vault.obkv` 的那个）并按**打开此保险库**。“文件夹+”图标用于在服务器上新建文件夹。

性能

数据库很小，即使远程也能瞬间打开。保险库每次只在你打开或导出时传输一个文件：文件很大时，连接速度很重要。

协作

10 多设备实时协作

同一个数据库或保险库可以在多台电脑上同时打开：在一台上做的修改会在几秒内出现在其他电脑上。



图 8 一条通知：另一台设备添加并修改了条目。

工作原理

- 在本地磁盘或同步文件夹中，Obskura 每 **2 秒**检查一次文件；在服务器上每 **5 秒**检查一次。检查只读取文件的前 88 个字节。
- 发现新版本后，它会逐条与你的版本**合并**，显示通知列出新增、修改或删除的条目，并立即更新列表。
- 如果两人修改了**同一个条目**，最新的修改生效；另一个修改不会丢失，而是进入该条目的**历史记录**。
- 删除会同步给所有人，除非此期间有人修改了该条目：此时修改优先，条目保留。
- 在保险库中，当有人在你正在查看的文件夹中添加、重命名或删除文件时，列表会自动更新。

电脑时钟

Obskura 根据电脑的时间判断哪个修改更新：请保持时钟同步（所有系统通常都默认开启自动设置时间）。

随处找回一切

11 访问密钥与设备

每个数据库和每个保险库旁边都有一个小的加密文件，记录密钥文件、备份和服务器的位置，以及你的每台设备访问它们的方式。它由 Obskura 访问密钥保护。

OBSKURA 访问密钥

这是首次启动时生成（或在另一台电脑上生成后输入）的 55 个字符的代码。它保存在系统钥匙串中；在**设置 → Obskura 访问密钥**中你可以：

- **显示**：查看并复制，以便在另一台电脑上输入。
- **更改密钥…**：生成新密钥。Obskura 会立即重新加密能访问到的伴随文件；其余的在下次打开时更新（旧密钥仍可用于读取）。
- **输入密钥…**：如果密钥在另一台电脑上被更改，可在此使用当前密钥。

伴随文件

它们用 AES-256-GCM 加密，没有访问密钥就无法读取：

文件	内容
`<名称>.obk.obkx`	位于每个数据库旁：密钥文件位置、备份配置、服务器连接和设备记录。
`vault.obkx`	位于每个保险库内：相同的信息。
`recenti.obkx`	位于应用数据文件夹中：最近使用列表。磁盘上不会留下明文路径。

从另一台电脑打开

在新电脑上输入访问密钥后，只需选择数据库：Obskura 会读取伴随文件，重建缺少的服务器连接，找到密钥文件（在该设备已知的位置、数据库旁、其他设备的路径或备份副本中），并在原件无法访问时提供备份副本。

> **重要**
>
> 访问密钥不能代替数据库密码：没有密码（和密钥文件），数据依然无法读取。但仍请妥善保管它：没有它，你就得手动选择密钥文件和备份。

设备和路径

每台使用 Obskura 的电脑都有一个首次启动时生成的**唯一标识**，以及一个**名称**（即电脑名称，可在**设置 → 这台设备的名称**中修改）。每次打开数据库或保险库时，它都会在加密的伴随文件中写入自己的记录：

数据	示例
标识和名称	`3f2a9c1e-…` ·“家里的 MacBook”
系统和版本	macOS · Obskura 0.3.0 · 上次访问
数据库路径	Mac 上为 `/Users/anna/Dropbox/accounts.obk`，PC 上为 `D:\Dropbox\accounts.obk`
密钥文件路径	`/Volumes/USB/key.obkey` 或 `E:\key.obkey`
自己的备份	该设备上的一个文件夹，或共用配置（第 12 章）

“设备和路径”窗口

在数据库或保险库的 ⋯ 菜单中选择**设备和路径…**：

- 可以看到所有已登记的设备，包括系统、版本、上次访问、是否使用密钥文件以及备份目标；
- 眼睛图标显示每台设备的路径；铅笔用于重命名这台设备；
- 垃圾桶用于**忘记**不再使用的设备：它的路径和备份会从文件中移除（如果它再次打开，会重新登记）。



图 9　使用某个数据库的设备。

为什么需要

同一个 Dropbox 中的数据库在 Mac、Windows 和 Linux 上路径各不相同，存放密钥文件的 U 盘也可能换了盘符或名称。借助按设备记录，每台设备都能找到自己的路径，而不会覆盖其他设备的路径。

数据安全

12 自动备份

每个数据库和每个保险库都可以有**第二个保存位置**，可以在这台电脑上（例如外置硬盘），也可以在任何已配置的服务器上。每次修改后，Obskura 都会在后台把新版本复制过去，不会拖慢你。

1. 在数据库或保险库的 ··· 菜单中选择**自动备份…**
2. 勾选**启用自动备份**并选择文件夹：**在这台电脑上…**或**在服务器上…**。
3. 如果目标是服务器，可以勾选**在所有设备上使用此配置**。
4. 对于数据库，选择要保留多少份**带日期的副本**。
5. 按**保存**。**立即运行**可强制完整复制一次。



图 10　备份到 NAS，所有设备共用。

内容	复制方式
数据库	备份文件夹中的 `.obk` 文件，以及带日期的副本 `名称.YYYYMMDD-hhmmss.obk`；超出上限的最旧副本会被删除。
保险库	加密文件夹的镜像：每次修改只重新复制受影响的文件。该副本可像普通保险库一样打开。
密钥文件	可选：在保存设置时复制一次到你指定的文件夹。

每台设备各自备份

- 每台设备都有**自己的配置**，连同其标识保存在伴随文件中：本地文件夹（例如 Mac 的外置硬盘）只对该设备有效。
- 服务器上的目标可以成为**共用**配置：其他设备会使用它，有自己配置的设备除外。窗口会显示是谁设置的。
- 副本保持**加密**：无需信任备份目标。
- 如果备份失败会出现提示；Obskura 会在下次修改时重试。

密钥文件与备份

不要把密钥文件放在备份所在的文件夹：能访问该文件夹的人就同时拥有了数据库和一半的凭据。

与其他程序互通

13 导入和导出

从在线密码管理器导入

Obskura 会直接登录你原来的服务，下载加密的保险库并在你的电脑上解密，无需经过明文导出的文件。凭据仅用于这次登录，不会被保存。

1. 打开目标数据库并选择⋯ → **从在线密码管理器导入…**
2. 选择服务并登录；如果启用了两步验证，Obskura 会要求输入验证码。
3. 检查预览：条目数量、文件夹和示例。
4. 决定是否把文件夹重建为分组、是否跳过已存在的条目，然后按**导入**。

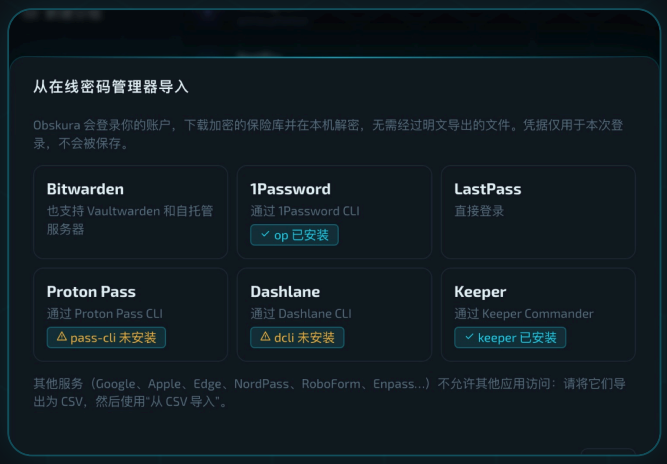


图 11 选择要导入的服务。

服务	访问方式
Bitwarden / Vaultwarden	直接登录，也支持 bitwarden.eu 和自托管服务器；也可以使用个人 API 密钥。
LastPass	直接登录，支持两步验证（验证码或在手机上确认）。
1Password	通过 1Password CLI（`op`），由 1Password 应用授权，或使用电子邮件、密码和 Secret Key。
Proton Pass	通过 Proton Pass CLI（`pass-cli`），在浏览器中登录。
Dashlane	通过 Dashlane CLI（`dcli`），需先在终端运行一次 `dcli sync`。
Keeper	通过 Keeper Commander（`keeper`）。

文件夹、自定义字段、TOTP 验证码、银行卡和备注都会保留。其他服务（Google、Apple、Edge、NordPass…）不允许其他应用访问：请将它们导出为 CSV。

从 CSV 导入（KEEPASS 等）

1. 在原程序中导出为 CSV：KeePass 2 使用**文件 → 导出 → KeePass CSV (1.x)**，KeePassXC 使用**数据库 → 导出 → CSV 文件**，Bitwarden、1Password、Chrome、Edge 和 Firefox 在各自的设置中导出。
2. 在 Obskura 中打开数据库，选择⋯ → **从 CSV 导入（KeePass...）**...
3. 选择文件：Obskura 会识别格式和列并显示预览。
4. 决定是否重建文件中的分组、是否跳过已存在的条目，然后按**导入**。



图 12　KeePassXC 导出文件的预览。

分组、标签、TOTP 验证码（保存为受保护字段）、创建日期和过期时间都会保留；无法识别的列会成为自定义字段。重复导入同一文件不会产生重复条目。

导出为 CSV

⋯ → **导出为 CSV...**会生成一个包含 KeePassXC 各列以及标签、过期时间、收藏和自定义字段的文件：可重新导入 Obskura、KeePassXC 和大多数密码管理器。

> **CSV 未加密**
>
> 该文件以明文包含所有密码。只用它转移数据，之后立即删除。导入完成后，也请删除从旧程序导出的 CSV。备份请使用保持加密的自动备份。

个性化

14 语言

Obskura 支持八种语言，还可以添加更多：应用的所有文本都保存在 XML 文件中，每种语言一个。

选择语言

启动时，Obskura 使用系统语言；如果不在内置语言之列，则使用英语。在**设置 → 语言**中，可以保留**自动**或选择一种语言：更改立即生效，包括错误消息。阿拉伯语从右向左阅读，界面也会相应地镜像。

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



图 13　设置中的“语言”部分。

添加语言

1. 在**设置 → 语言**中按**导出 XML 模板...**：你会得到当前语言的完整文件（也可以从网站下载包含所有语言 XML 文件的 zip）。
2. 在文件头中修改 `code`（语言代码，例如 `fr` 或 `pt-BR`）、`name`，从右向左书写的语言还要设置 `dir="rtl"`。
3. 用任何文本编辑器翻译每个 `<string>` 元素的文本，并以 UTF-8 保存。
4. 按**导入语言文件（XML）...**：该语言会立即出现在列表中，并在使用该语言的系统上自动启用。

文件格式

语言文件是一个 XML，包含一个 `<language>` 元素，每条文本对应一个 `<string>`：

```
<?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>
```

- `key` 属性不要翻译也不要修改；
- 花括号中的占位符，例如 `{count}` 或 `{name}`，必须保持原样：应用会用数字和名称替换它们；
- 文本中的 `<b>` 和 `<code>` 标签必须保留；
- 以 `.one`、`.two`、`.few`、`.many` 和 `.other` 结尾的键是复数形式：使用你的语言所需的形式，`.other` 必须提供；
- 缺少的文本会以英语显示，所以部分翻译也能直接使用。

修正内置语言

与内置语言 `code` 相同（例如 `zh`）的 XML 文件不会替换该语言，只会修正其中包含的条目。它在设置中会标注为**修正**，点按 × 即可移除并恢复原始文本。

提示

导入的文件保存在应用的数据文件夹中，只对这台电脑有效：请在其他电脑上也导入。

使用空白 XML 模板翻译

添加新语言时，可以从空白模板 `obskura-translation-template.xml` 开始，它可在网站（`obskura.bytenooks.com`，“下载”部分）下载。模板中应用的每条文本占一行：译文写在 `<string …>` 与 `</string>` 之间；属性 `en` 是英文参考文本，可以保留不动（应用会忽略它）。

```
<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. 下载模板，并以你的语言代码命名保存，例如 `fr.xml`。
2. 在第一行 `<language>` 中填写 `code`、`name`、`english-name`，必要时填写 `dir="rtl"`。
3. 用能保存为 UTF-8 的文本编辑器填写译文，并遵守上面的规则。
4. **删除未翻译的行**：留空的文本在应用中会显示为空白，而缺少的行会以英文显示。
5. 在**设置 → 语言**中导入文件，并在应用中检查文本。

分享你的翻译

通过网站的联系页面发送给开发者：选择“翻译”主题并附上 XML 文件（最大 3 MB；完整的语言文件约 100–150 KB）。收到的翻译可能会收录到以后的版本中。

安全

15 锁定与设置

锁定数据库或保险库时，Obskura 会关闭会话并**从内存中清除**密钥和解密后的数据。重新打开需要再次输入凭据。

锁定方式

- 侧边栏底部的**全部锁定**，或 `Ctrl/⌘` + `L`。
- 侧边栏中已解锁项目旁的锁图标，或 ⋯ 菜单中的**锁定**。
- **自动**锁定：一段时间无操作后，或电脑进入睡眠时。

设置

设置项	作用	默认值
无操作时自动锁定	在 1–60 分钟未使用鼠标或键盘后全部锁定，或从不。	10 分钟
清空剪贴板	复制机密信息 10–120 秒后清空剪贴板，或从不。	20 秒
睡眠时锁定	电脑进入睡眠时全部锁定。	开启
主题	跟随系统、浅色或深色。	深色
这台设备的名称	显示在每个数据库和保险库的设备列表中；下方显示唯一标识。	电脑名称
语言	自动或某种可用语言；导入和导出 XML 文件（第 14 章）。	自动
Obskura 访问密钥	显示、更改或输入密钥（第 11 章）。	—
服务器	SFTP、FTP/FTPS、WebDAV 和 SMB 连接（第 09 章）。	—

设置中不包含任何机密：服务器密码保存在系统钥匙串中，最近使用列表用访问密钥加密。

参考

16 快捷键与加密细节

键盘快捷键

按键	位置	操作
`Ctrl/⌘` + `L`	任何位置	全部锁定
`Esc`	对话框	关闭窗口
`Ctrl/⌘` + `F`	数据库	搜索
`Ctrl/⌘` + `N`	数据库	新建条目
`Ctrl/⌘` + `S`	条目编辑器	保存条目
双击	条目列表	复制密码
`Ctrl/⌘` + `A`	保险库	全选
`Enter`	保险库	打开文件或文件夹
`F2`	保险库	重命名
`Del` · `⌘` + `⌫`	保险库	删除所选项目
`⌫`	保险库	返回上级文件夹

加密细节

组成部分	算法
密钥派生	Argon2id：256 MiB / 3 轮、1 GiB / 4 轮或 2 GiB / 6 轮，256 位随机盐。
复合密钥	对密码（NFC 规范化）和密钥文件做 SHA-256，与 KeePass KDBX4 相同。
加密	AES-256、XChaCha20、Serpent、Twofish、Camellia 或级联，始终经过认证（GCM 或 Poly1305）；级联中每层使用通过 HKDF 派生的独立密钥。
子密钥	HKDF-SHA256，每次保存使用新的种子。
完整性	文件头经过认证：任何篡改都会导致无法打开。
保险库中的文件名	AES-SIV，与所在文件夹绑定。
文件内容	64 KiB 分块，每个文件随机密钥，防止重排和截断。
伴随文件	AES-256-GCM，密钥通过 HKDF 从 Obskura 访问密钥（256 位随机数）派生。
内存	密钥和明文数据只存在于原生进程中，关闭时会被清除。

支持

17 最佳实践与故障排除

最佳实践

- **开启自动备份**，或定期把 `.obk` 文件和保险库文件夹复制到外置硬盘。它们已经加密，所以无论备份放在哪里都是安全的。
- **把密钥文件与数据库分开保存**，并至少保留一份备用副本。
- **保存好 Obskura 访问密钥**，写在纸上或存放在电脑以外的地方。
- **为每个服务使用不同的密码**，用生成器生成：你只需记住一个。
- **离开时锁定**：`Ctrl/⌘` + `L` 最快。
- 在**设备和路径**窗口中**忘记**不再使用的设备。

常见问题

我忘了主密码，能找回吗？

不能。正是这一点让 Obskura 安全：没有正确的凭据，任何人（包括开发者）都无法打开数据库或保险库。

提示“密码或密钥文件错误”，但我确定它们是对的。

检查你选择的密钥文件是否与创建时使用的相同，且没有被修改。如果同时使用了密码*和*密钥文件，两者都需要。也请检查大写锁定键。

打开需要几秒钟，正常吗？

正常：这是 Argon2id 的运行时间，目的就是减慢猜测密码的速度。“高”级别需要几秒钟和 1 GiB 可用内存，“极高”级别最多需要 12 秒和 2 GiB。

在另一台电脑上找不到密钥文件。

连接存放它的设备：Obskura 会在这台电脑上次使用的路径、数据库旁、其他设备的路径以及备份副本中查找。如果仍找不到，请用**选择…**手动选择：下次会为这台设备记住该路径。

出现“受另一个访问密钥保护”。

访问密钥在另一台电脑上被更改了。点按**输入当前密钥**并使用新密钥；你也可以直接用密码解锁并手动选择密钥文件。

出现了“凭据已在其他地方更改”。

有人在另一台设备上更改了数据库的密码或密钥文件。选择**锁定**，然后用新凭据重新打开；**覆盖**会撤销在其他地方所做的更改。

无法连接到服务器。

用**测试连接**检查地址、端口和凭据。WebDAV 请检查基础路径（Nextcloud 为 `/remote.php/dav/files/<用户>`）；SMB 请检查共享名称。使用自签名证书时，只在可信网络中开启**接受自签名证书**。

对保险库中文件的修改似乎没有保存。

确认已在其他应用中保存文件，然后按**将修改保存到保险库**。如果在文件仍打开时锁定保险库，Obskura 也会尝试在删除临时副本前保存它。

应用打开时不是我的语言。

Obskura 会跟随系统语言；如果你的语言不在内置之列，就使用英语。在**设置 → 语言**中选择语言，或导入 XML 文件（第 14 章）。

MACOS 或 WINDOWS 提示应用未经验证。

本应用没有使用商业证书签名。请按照第 02 章的说明进行首次打开。



OBSKURA

为你的数据提供无形的安全

密码管理器与加密文件保险库 · 在你的电脑或你的服务器上

macOS · Windows · Linux · 版本 0.3.0

https://obskura.bytenooks.com