

OBSKURA

أمان غير مرئي لبياناتك

دليل الاستخدام

الإصدار 0.3.0

MACOS · WINDOWS · LINUX

أكتوبر 2026

دليل الاستخدام

المحتويات

01	مرحبًا بك في Obskura	ما يفعله البرنامج، قواعد البيانات والخزائن	03
02	التثبيت والتشغيل الأول	macOS وWindows وLinux · مفتاح الوصول · الواجهة	04
03	كلمات المرور وملفات المفاتيح	بيانات الاعتماد، Argon2id، اختيار خوارزمية التشفير	05
04	قواعد بيانات كلمات المرور	الإنشاء، فتح القفل، تنظيم العناصر	07
05	إدارة العناصر	المولّد، الحقول، المرفقات، السجل	08
06	أدوات قاعدة البيانات	البحث، النسخ الآمن، قائمة قاعدة البيانات	09
07	خزائن الملفات	إنشاء خزنة وتشفير الملفات	10
08	العمل مع الملفات	الفتح والتعديل والتصدير	11
09	الخوادم البعيدة	SFTP وWebDAV وSMB وFTP/FTPS	12
10	عدة أجهزة في الوقت الفعلي	مزامنة فورية، إشعارات	14
11	مفتاح الوصول والأجهزة	الملفات المرافقة، معرّفات كل جهاز ومساراته	15
12	النسخ الاحتياطي التلقائي	وجهة ثانية، نسخ مؤرخة، لكل جهاز	17
13	الاستيراد والتصدير	المديرون على الإنترنت، CSV من KeePass وغيره	18
14	اللغات	لغة تلقائية، ملفات XML، ترجمات جديدة	20
15	القفل والإعدادات	القفل التلقائي، الحافظة، المظهر، اسم الجهاز	23
16	الاختصارات والتشفير	اختصارات لوحة المفاتيح والتفاصيل التقنية	24
17	الممارسات الجيدة وحل المشكلات	النسخ الاحتياطي، الأسئلة الشائعة	25

اصطلاحات

تظهر أسماء الأزرار والقوائم **بخط عريض**. وتُكتب اختصارات المفاتيح هكذا: `Ctrl/⌘` + `L`، حيث يخص `Ctrl` نظامي Windows وLinux ويخص `⌘` نظام macOS. وتظهر أسماء الملفات وامتداداتها `بخط ثابت العرض`. تعرض لقطات الشاشة الواجهة بلغة هذا الدليل.

مقدمة

01 مرحبًا بك في OBSKURA

يحمي Obskura كلمات المرور والملفات بتشفير بمستوى عسكري. لا حسابات ولا خدمات خارجية: تبقى بياناتك حيث تقرر أنت، على حاسوبك أو على خادمك.

كل قاعدة بيانات وكل خزنة مجرد ملف أو مجلد عادي. يمكنك حفظها على قرص الحاسوب أو على ذاكرة USB أو في مجلد متزامن مثل Dropbox أو OneDrive أو iCloud Drive، أو مباشرة على خادمك الخاص SFTP أو WebDAV أو SMB أو FTP، ويمكنك امتلاك ما تشاء منها: واحدة شخصية وأخرى للعمل وثالثة مشتركة مع العائلة. ويمكن لعدة حواسيب استخدامها معًا ورؤية تعديلات بعضها فورًا، حتى لو وصلت إليها عبر مسارات مختلفة.

قاعدة بيانات كلمات المرور

ملف `.obk` واحد على نهج KeePass. يضم عناصر فيها اسم المستخدم وكلمة المرور والعنوان والملاحظات والحقول المخصصة والمرفقات وسجل التعديلات، مرتبة في مجموعات.

خزنة الملفات

مجلد على نهج Cryptomator. تسحب إليه المستندات والصور والأرشيفات: يُشفَّر كل ملف على حدة، بما في ذلك الأسماء وبنية المجلدات.

كيف تعمل الحماية

عند إنشاء قاعدة بيانات أو خزنة تختار **كلمة مرور رئيسية** أو **ملف مفتاح** أو كليهما. ومن هذه البيانات يشتق Obskura مفتاح التشفير بخوارزمية Argon2id، المصممة خصيصًا لجعل محاولات تخمين كلمة المرور بطيئة جدًا. ثم تُشفَّر البيانات بـ AES-256، المعيار المعتمد للمعلومات المصنفة **سري للغاية (TOP SECRET)**.

لا تُحفظ بيانات الاعتماد في أي مكان. ومن دونها يتعذر على أي شخص قراءة المحتوى، بمن في ذلك المطورون.

مهم

لا توجد أي طريقة لاستعادة كلمة مرور منسية أو ملف مفتاح مفقود. اختر كلمة مرور تتذكرها، واحتفظ بنسخة من ملف المفتاح في مكان آمن ومنفصل.

باختصار

AES-256-GCM · XChaCha20-Poly1305 · Serpent · Twofish · Camellia · تشفير متتالٍ · Argon2id حتى 2 GiB · HKDF-SHA256

AES-SIV لأسماء الملفات · مسح الذاكرة عند الإغلاق · بلا حساب · FTPS · SMB · WebDAV · SFTP · في الوقت الفعلي · نسخ احتياطي تلقائي

مسارات لكل جهاز · 8 لغات · macOS · Windows · Linux

البداية

02 التثبيت والتشغيل الأول

macOS

افتح ملف `.dmg` واسحب Obskura إلى **التطبيقات**. إذا منع macOS التطبيق عند التشغيل الأول، فانتقل إلى **إعدادات النظام ← الخصوصية والأمن** واختر **الفتح على أي حال**.

Windows

شغّل برنامج التثبيت `.exe` الذي يستخدم لغة Windows تلقائيًا، أو شغّل النسخة المحمولة دون تثبيت. إذا ظهر تحذير SmartScreen فانقر **مزيد من المعلومات ← التشغيل على أي حال**.

Linux

استخدم حزمة `.deb` (Debian وUbuntu) أو `.rpm` (Fedora وopenSUSE) أو ملف `.AppImage` الذي لا يحتاج إلى تثبيت: اجعله قابلًا للتنفيذ ثم شغّله.

التشغيل الأول: اللغة ومفتاح الوصول

يُفتح Obskura بلغة النظام (الإيطالية أو الإنجليزية أو الألمانية أو الإسبانية أو الروسية أو الصينية أو اليابانية أو العربية؛ وبالإنجليزية لغيرها). وعند التشغيل الأول يطلب منك إنشاء **مفتاح الوصول إلى Obskura**، أو إدخال المفتاح الذي أنشأته على حاسوب آخر إن كنت تستخدم Obskura هناك. يشرح الفصل 11 الغرض منه.

الشاشة الرئيسية



الشكل 1 شاشة الترحيب مع الشريط الجانبي.

يضم **الشريط الجانبي** قسمي **قواعد كلمات المرور** و**خزائن الملفات**. وبجانب كل عنوان زران: المجلد **لفتح** عنصر موجود، و**+** لإنشاء عنصر جديد.

- يبقى كل عنصر فُتح مؤخرًا في القائمة باسمه فقط: لا تظهر المسارات أبدًا. ويدل القفل على الحالة: **مغلق** إذا كان مقفلًا، و**مفتوح** إذا كان غير مقفل.
- عند تمرير المؤشر فوق عنصر تظهر **×** لإزالته من العناصر الأخيرة (لا يُحذف الملف) أو قفل لإقفاله فورًا.
- في الأسفل: **قفل الكل** وترس **الإعدادات**.

حماية البيانات

03 كلمات المرور وملفات المفاتيح

تُفتح قواعد البيانات والخزائن بـ**كلمة مرور رئيسية** أو **ملف مفتاح** أو بهما معًا. والجمع بينهما أقوى حماية: يلزم شيء تعرفه وشيء تملكه.

كلمة المرور الرئيسية

العبارة الطويلة أكثر أمانًا من كلمة معقدة: أربع أو خمس كلمات عشوائية سهلة التذكر وصعبة التخمين للغاية. ويقدّر المؤشر أسفل الحقل قوتها بالبت.

يفتح زر النرد **المولّد** إذا كنت تفضّل كلمة مرور عشوائية.

ملف المفتاح

كما في KeePass، يمكن لـ**أي ملف** أن يكون مفتاحًا. يمكنك اختيار **استخدام ملف موجود** أو **إنشاء ملف جديد**: فينشئ Obskura ملف مفتاح عشوائيًا في الموضع الذي تحدده.

احتفظ به مثلًا على ذاكرة USB، منفصلًا عن قاعدة البيانات. يتذكر Obskura مكانه على كل جهاز ويبحث عنه بنفسه عند كل فتح (الفصل 11).



الشكل 2 إنشاء قاعدة بيانات مع فتح خيارات التشفير.

خيارات التشفير

تختار في **خيارات التشفير** مدى كلفة اشتقاق المفتاح والخوارزمية المستخدمة. الإعدادات الافتراضية، القياسي وAES-256-GCM، آمنة لأي استخدام؛ وتُشرح البدائل كلها في الصفحة التالية.

لا تعدّل ملف المفتاح أبدًا

إذا استخدمت ملفًا عاديًا (صورة أو مستندًا) مفتاحًا، فإن أقل تعديل يجعله غير صالح. أما الملفات التي ينشئها Obskura فبتنسيق نصي معروف يبقى صالحًا حتى لو تغيّرت نهايات الأسطر. وفي كل الأحوال احتفظ بنسخة احتياطية منه.

حماية البيانات

03 اختيار خوارزمية التشفير

اشتقاق المفتاح (ARGON2ID)

يحوّل Argon2id بيانات اعتمادك إلى مفتاح التشفير: كلما زادت الذاكرة والتمريرات زادت كلفة تجربة ملايين كلمات المرور على المهاجم.

المستوى	المعاملات	زمن الفتح
قياسي	ذاكرة 256 MiB، 3 تمريرات	نحو 0.5–1 ثانية
عالٍ	1 GiB، 4 تمريرات	نحو 2–4 ثوانٍ
أقصى	2 GiB، 6 تمريرات	نحو 5–12 ثانية

المستوى الأقصى

يتطلب كل فتح **2 GiB من الذاكرة الحرة**. وقد لا تُفتح قاعدة البيانات أو الخزنة على حاسوب ذي ذاكرة قليلة: اختره فقط إذا كنت ستستخدم ملفاتك على حواسيب مناسبة.

خوارزميات التشفير

تستخدم كل الخوارزميات مفاتيح بطول 256 بت وهي **موثَّقة**: يُكتشف أي عبث بالبيانات.

الخوارزمية	الخصائص
AES-256-GCM	**الافتراضية**. معيار أمريكي معتمد للمعلومات السرية للغاية، والأسرع بفضل التسريع في العتاد.
XChaCha20-Poly1305	تشفير تدفقي، سريع على أي معالج حتى دون تعليمات AES.
Serpent-256-GCM	من نهائيي مسابقة AES، وأوسعها هامش أمان (32 جولة). أبطأ.
Twofish-256-GCM	من نهائيي مسابقة AES، صممها Bruce Schneier وزملاؤه.
Camellia-256-GCM	معيار دولي ISO/IEC، موصى به في أوروبا (NESSIE) واليابان (CRYPTREC).
تتابع AES · Twofish · Serpent	**الخيار الأقوى**. ثلاث عمليات تشفير متتالية بمفاتيح مستقلة: تبقى البيانات محمية حتى لو اختُرقت اثنتان من الخوارزميات الثلاث يومًا ما.
تتابع AES · XChaCha20	يجمع بين خوارزمية كتلية وأخرى تدفقية من عائلتين مختلفتين تمامًا.

الخزائن

في الخزائن تحمي الخوارزمية المختارة المفاتيح ومحتوى كل ملف معًا. وإذا غيّرتها عبر **تغيير كلمة المرور / ملف المفتاح**، تبقى الملفات الموجودة مشفرة بالخوارزمية السابقة وتستخدم الملفات المضافة بعد ذلك الجديدة. وتظهر الخوارزمية الحالية أسفل الخزنة.

مدير كلمات المرور

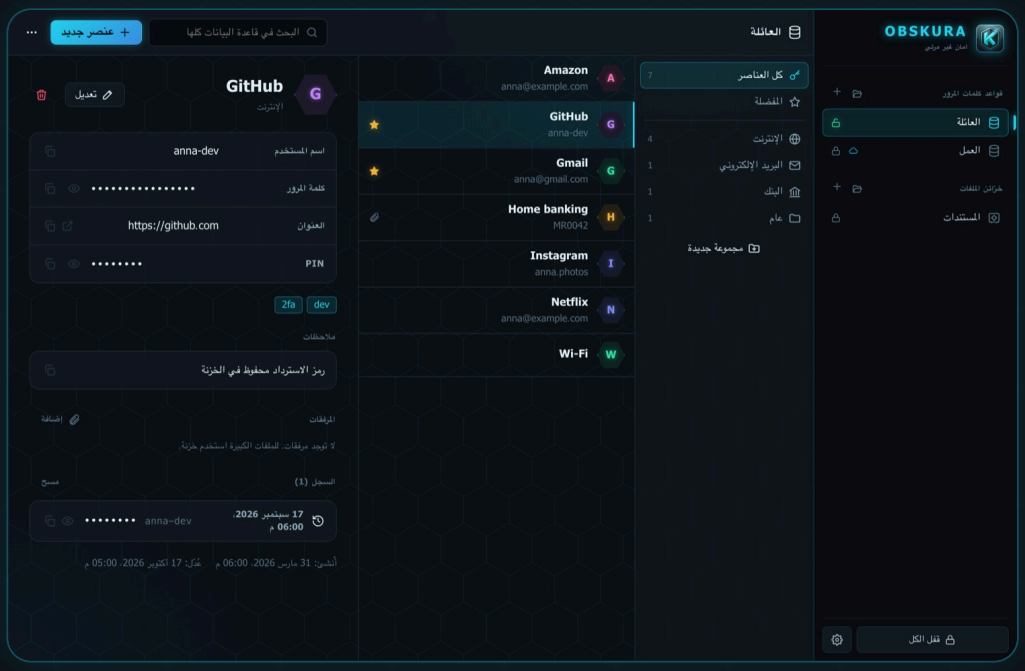
04 قواعد بيانات كلمات المرور

إنشاء قاعدة بيانات

1. انقر **قاعدة بيانات جديدة** في الشاشة الرئيسية، أو **+** بجانب **قواعد كلمات المرور**.
2. اكتب **اسمًا** واختر مكان حفظ ملف `.obk`: **على هذا الحاسوب**... أو **على خادم**....
3. عيّن كلمة مرور و/أو ملف مفتاح (الفصل 03).
4. اضغط **إنشاء**. تُفتح قاعدة البيانات وهي غير مقفلة.

الفتح وفك القفل

1. اختر قاعدة البيانات في الشريط الجانبي، أو استخدم أيقونة المجلد لفتح ملف `.obk` موجود.
2. أدخل كلمة المرور. يُبحث عن ملف المفتاح والنسخة الاحتياطية تلقائيًا؛ وإذا لم يُعثر على ملف المفتاح فاختره عبر **اختيار**....
3. اضغط **فتح القفل** أو `Enter`.



الشكل 3 قاعدة بيانات غير مقفلة: المجموعات وقائمة العناصر وتفاصيل العنصر المحدد.

الأعمدة الثلاثة

- **المجموعات**: **كل العناصر** و**المفضلة** ومجلداتك. عند تمرير المؤشر فوق مجموعة تظهر أوامر إنشاء مجموعة فرعية وتعديلها وحذفها؛ و**مجموعة جديدة** في آخر القائمة.
- **العناصر**: عنوان كل عنصر واسم مستخدمه. تدل النجمة على المفضلة، ومشبك الورق على المرفقات. و**النقر المزدوج** ينسخ كلمة المرور مباشرة.
- **التفاصيل**: كل حقول العنصر مع أزرار الإظهار والنسخ وفتح العنوان في المتصفح.

قواعد بيانات كلمات المرور

05 إدارة العناصر

لإضافة عنصر اضغط **عنصر جديد** (أو `Ctrl/⌘` + `N`)؛ ولتغييره حدّده واضغط **تعديل**. احفظ بالزر في الأسفل أو بـ `Ctrl/⌘` + `S`. يُكتب كل تعديل فورًا في ملف قاعدة البيانات.

حقول العنصر

العنوان والمجموعة	اسم العنصر والمجلد الذي يوجد فيه.
اسم المستخدم	الحساب أو البريد الإلكتروني أو رقم العميل.
كلمة المرور	مع مؤشر القوة والمولّد.
العنوان	يُفتح في المتصفح من التفاصيل.
الملاحظات	نص حر، مشفر مثل كل شيء آخر.
الوسوم	كلمات مفتاحية مفصولة بفواصل.
تاريخ الانتهاء	التاريخ الذي ينبغي تغيير كلمة المرور بعده.

تضيف **النجمة** في الأعلى العنصر إلى **المفضلة**.



الشكل 4 محرر العنصر مع فتح المولّد.

مولّد كلمات المرور

انقر النرد في حقل كلمة المرور. اختر **الطول** (من 8 إلى 64 حرفًا) وأنواع الأحرف (`a-z` و`A-Z` و`0-9` و`!@#$`)؛ ويتجنب **استبعاد المتشابهة** الأحرف التي يُخلط بينها مثل l و1 وO و0. ثم **توليد من جديد** أو **نسخ** أو **استخدام كلمة المرور هذه**. تُولَّد كلمات المرور بمولّد الأرقام العشوائية التشفيري في النظام.

الحقول المخصصة

أضف معلومات إضافية مثل رمز PIN أو رموز الاسترداد أو أسئلة الأمان. فعّل **محمي** لإظهارها مخفية مثل كلمة المرور.

المرفقات والسجل

أرفق ملفات حتى **64 MB** لكل منها (للملفات الأكبر استخدم خزنة). يحتفظ كل تعديل بالإصدار السابق: يحفظ **السجل** آخر **20** إصدارًا ويتيح نسخ كلمة مرور قديمة.

قواعد بيانات كلمات المرور

06 أدوات قاعدة البيانات

البحث

يصفّي حقل **البحث في قاعدة البيانات كلها** في الأعلى (أو `Ctrl/⌘` + `F`) عناصر كل المجموعات أثناء الكتابة. ويمسح `Esc` البحث.

النسخ الآمن

تضع أزرار النسخ بجانب اسم المستخدم وكلمة المرور والحقول المحمية القيمة في الحافظة، التي **يمسحها** Obskura **تلقائيًا** بعد 20 ثانية (قابلة للتغيير في الإعدادات). ولا تُمسح الحافظة إلا إذا كانت لا تزال تحتوي على القيمة المنسوخة؛ إذا نسخت شيئًا آخر في الأثناء فلن يُمس.

قائمة قاعدة البيانات

يحتوي الزر ⋯ أعلى الشاشة على:

البند	الغرض
خصائص قاعدة البيانات	تغيير اسم قاعدة البيانات ووصفها.
تغيير كلمة المرور / ملف المفتاح	تعيين بيانات اعتماد جديدة. يُعاد تشفير قاعدة البيانات بمفاتيح جديدة.
حفظ نسخة احتياطية...	كتابة نسخة مشفرة من قاعدة البيانات في موضع آخر.
النسخ الاحتياطي التلقائي...	ضبط الوجهة الثانية للنسخ (الفصل 12).
الأجهزة والمسارات...	معرفة الأجهزة التي تستخدم قاعدة البيانات ومساراتها (الفصل 11).
الاستيراد / التصدير	من مدير على الإنترنت أو من CSV، وإلى CSV (الفصل 13).
قفل قاعدة البيانات	إغلاق قاعدة البيانات ومسح بياناتها من الذاكرة.

الحفظ والمزامنة

يُحفظ كل تعديل فورًا وبطريقة **ذرّية**: يُكتب الملف الجديد منفصلًا ولا يحل محل القديم إلا بعد اكتماله، فلا يمكن لانقطاع الكهرباء أن يتلفه. وإذا عدّل حاسوب آخر قاعدة البيانات في الأثناء، **يدمج** Obskura الإصدارين قبل الحفظ: لا يضيع شيء (الفصل 10). والحالة الوحيدة التي تتطلب قرارًا هي تغيير **كلمة المرور أو ملف المفتاح** على جهاز آخر: يقترح Obskura قفل قاعدة البيانات لإعادة فتحها ببيانات الاعتماد الجديدة.

> **نصيحة**
> لاستخدام قاعدة البيانات نفسها على عدة حواسيب ضعها على خادمك (الفصل 09) أو في مجلد متزامن: يمكن أن تبقى مفتوحة في كل مكان في الوقت نفسه.

ملفات مشفرة

07 خزائن الملفات

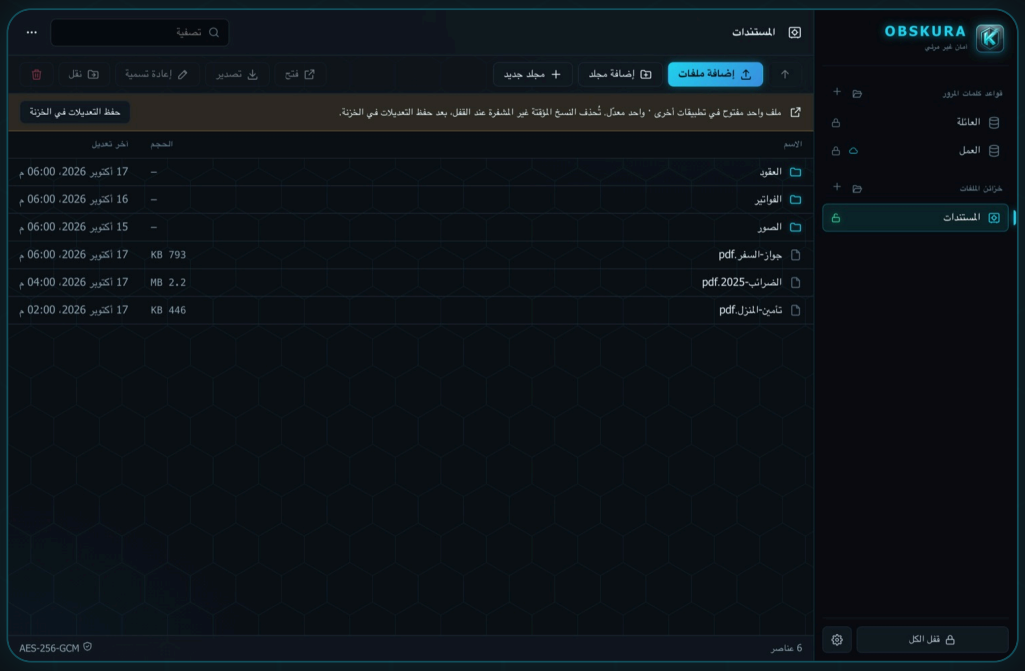
الخزنة مجلد يحتوي على ملفاتك بصورة مشفرة. ومن الخارج لا تبدو إلا مجموعة ملفات بأسماء غير مقروءة: لا يُعرف ما تحتويه ولا كيف نُظّمت.

إنشاء خزنة

1. انقر **خزنة جديدة**، أو **+** بجانب **خزائن الملفات**.
2. اختر اسمًا والمجلد الذي تُنشأ فيه، حتى داخل Dropbox أو OneDrive أو iCloud Drive، أو على خادم.
3. عيّن كلمة مرور و/أو ملف مفتاح واضغط **إنشاء**.

إضافة الملفات

- **اسحب** الملفات والمجلدات من Finder / المستكشف إلى النافذة: تُشفَّر في المجلد المعروض.
- أو استخدم **إضافة ملفات** أو **إضافة مجلد**.
- لا تُمس الملفات الأصلية: يمكنك حذفها بنفسك بعد تشفيرها.



الشكل 5 خزنة غير مقفلة.

شريط الأوامر

يعود ↑ إلى المجلد الأعلى · ينشئ **مجلد جديد** مجلدًا فرعيًا · وتعمل **فتح** و**تصدير** و**إعادة تسمية** و**نقل** و**حذف** على العناصر المحددة. تحدد عدة عناصر بـ `Ctrl/⌘` + نقر أو `Shift` + نقر. ويعرض شريط الحالة في الأسفل عدد العناصر وتقدم العمليات.

خزائن الملفات

08 العمل مع الملفات

فتح ملف وتعديله

انقر نقرًا مزدوجًا على ملف (أو حدّده واضغط **فتح**). يفك Obskura تشفيره في مجلد مؤقت محمي ويفتحه بالتطبيق الافتراضي في النظام.

1. عدّل الملف واحفظه كالمعتاد في التطبيق الآخر.
2. يظهر في Obskura شريط يبيّن الملفات المفتوحة والمعدّلة.
3. اضغط **حفظ التعديلات في الخزنة** لإعادة تشفير الإصدار الجديد.

> **نسخ مؤقتة غير مشفرة**
> ما دام الملف مفتوحًا فإن نسخته المفكوكة التشفير موجودة على القرص. وعند قفل الخزنة يحفظ Obskura أولًا التعديلات المتبقية ثم **يحذف النسخ المؤقتة**. أغلق الملف في التطبيق الآخر قبل القفل.

التصدير

يفك **تصدير** تشفير العناصر المحددة، بما فيها المجلدات، إلى مجلد تختاره. تكون الملفات المصدَّرة **غير مشفرة**: استخدم هذه الميزة فقط عندما تحتاج إليها خارج الخزنة.

التنظيم

أعد التسمية بـ **إعادة تسمية** أو `F2`؛ وانقل بـ **نقل** مع اختيار المجلد الوجهة. ويطلب **حذف** (أو `Delete`) التأكيد دائمًا. ويعرض حقل **تصفية** فقط العناصر التي يحتوي اسمها على النص المُدخل.

المزامنة مع السحابة

كل ملف في الخزنة مشفر على حدة: إذا غيّرت مستندًا رفعت خدمة المزامنة ذلك الملف وحده. لذلك تعمل الخزائن جيدًا داخل Dropbox وOneDrive وGoogle Drive وiCloud Drive.

شكل الخزنة على القرص

العنصر	المحتوى
`vault.obkv`	مفاتيح الخزنة، مشفرة ببيانات اعتمادك.
`vault.obkv.bak`	نسخة أمان مطابقة، تحسبًا لتلف الملف الأول.
`vault.obkx`	الملف المرافق، مشفر بمفتاح الوصول: ملف المفتاح والنسخ الاحتياطي ومسارات كل جهاز (الفصل 11).
`d/`	كل الملفات والمجلدات المشفرة متجاورة: لا تظهر البنية الحقيقية.

لفتح خزنة موجودة استخدم أيقونة المجلد بجانب **خزائن الملفات** واختر مجلدها الرئيسي. لا تعدّل الملفات التي بداخلها ولا تنقلها يدويًا.

أين تحفظ

09 الخوادم البعيدة

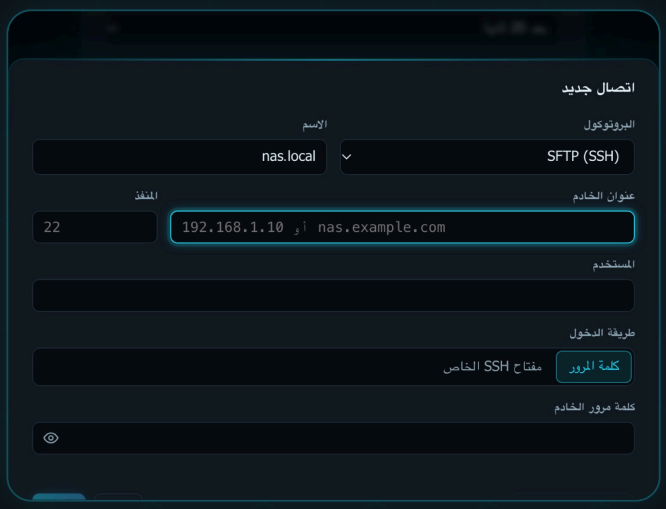
ليس من الضروري أن تكون قواعد البيانات والخزائن على الحاسوب: يفتحها Obskura ويحفظها مباشرة على خادمك، دون برامج مزامنة وسيطة. تنتقل البيانات وتبقى على الخادم **مشفرة مسبقًا**: لا يرى مسؤول الخادم أو من يخترقه إلا ملفات غير مقروءة.

البروتوكول	أين يُستخدم	ملاحظات
SFTP	NAS (Synology وQNAP وTrueNAS) وخوادم Linux وVPS	موصى به. كلمة مرور أو مفتاح SSH.
WebDAV	Nextcloud وownCloud وSynology وQNAP وBox وKoofr	عبر HTTPS. في Nextcloud يكون المسار `/remote.php/dav/files/<المستخدم>`.
SMB	مجلدات Windows المشتركة وNAS وSamba	SMB 2 وما فوق؛ حدّد اسم المجلد المشترك.
FTPS	الاستضافات وخوادم FTP مع TLS	FTP مشفر بـ `AUTH TLS`.
FTP	خوادم FTP التقليدية	تنتقل بيانات اعتماد الخادم دون تشفير: الأفضل FTPS أو SFTP.

ضبط اتصال

1. افتح **الإعدادات ← الاتصالات بالخوادم** واضغط **اتصال جديد**.
2. اختر البروتوكول وأدخل العنوان والمنفذ (إن كان غير القياسي) والمستخدم وكلمة المرور.
3. اضغط **اختبار الاتصال** ثم **حفظ**.

تُحفظ كلمة مرور الخادم في **سلسلة مفاتيح النظام** (سلسلة مفاتيح macOS، ومدير بيانات الاعتماد في Windows، وSecret Service في Linux)، ولا تُكتب أبدًا في ملف الإعدادات. كما تُنسخ مشفرة إلى الملف المرافق: فتعيد حواسيبك الأخرى إنشاء الاتصال بنفسها.



الشكل 6 اتصال SFTP جديد.

مفتاح الخادم (SFTP)

عند الاتصال الأول يعرض Obskura **بصمة** مفتاح الخادم ويطلب منك قبولها، كما يفعل `ssh`. وإذا تغيّرت البصمة لاحقًا يُرفض الاتصال حتى تؤكدها من جديد: فقد يكون أحدهم ينتحل صفة خادمك. وإن لم يتغير شيء على الخادم فلا تقبلها.

الفتح والحفظ على خادم

- **الفتح:** تقدم أيقونة المجلد بجانب **قواعد كلمات المرور** أو **خزائن الملفات** خياري **من هذا الحاسوب...** و**من خادم...**. والأمر نفسه في الشاشة الرئيسية بزر **من خادم...**.
- **الإنشاء:** في نافذة **قاعدة بيانات جديدة** أو **خزنة جديدة** اختر **على خادم...** بدلًا من **على هذا الحاسوب...**.
- تظهر العناصر الموجودة على خادم بين العناصر الأخيرة مع أيقونة **السحابة**؛ وبعد فتحها تُظهر وسم `خادم` في الشريط العلوي.



الشكل 7 متصفح الخادم: اختر الاتصال والمجلد.

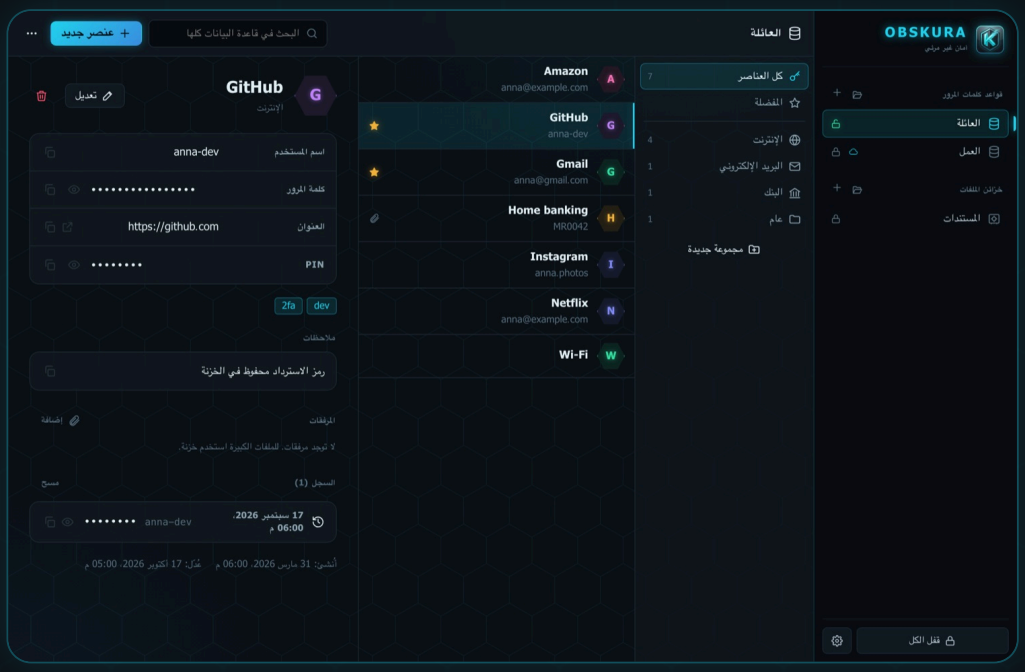
في المتصفح اختر الاتصال من الأعلى وتنقّل بين المجلدات. لقاعدة بيانات انقر ملف `.obk`؛ ولخزنة ادخل مجلدها (الذي يضم `vault.obkv`) واضغط **فتح هذه الخزنة**. وتنشئ أيقونة «مجلد+» مجلدًا جديدًا على الخادم.

> **الأداء**
>
> قواعد البيانات صغيرة وتُفتح في لحظة حتى عن بُعد. أما الخزائن فتنقل ملفًا واحدًا في كل مرة، عند فتحه أو تصديره: ومع الملفات الكبيرة جدًا تهم سرعة الاتصال.

العمل المشترك

10 عدة أجهزة في الوقت الفعلي

يمكن فتح قاعدة البيانات نفسها أو الخزنة نفسها على عدة حواسيب في آن واحد: تظهر التعديلات التي تُجرى على أحدها على البقية خلال ثوانٍ.



الشكل 8 إشعار: أضاف جهاز آخر عناصر وعدّلها.

كيف يعمل

- يفحص Obskura الملف كل **ثانيتين** على القرص المحلي أو في مجلد متزامن، وكل **5 ثوانٍ** على خادم. ولا يقرأ الفحص إلا أول 88 بايت من الملف.
- عندما يجد إصدارًا جديدًا **يدمجه** مع إصدارك عنصرًا بعنصر، ويعرض إشعارًا بالعناصر المضافة أو المعدّلة أو المحذوفة ويحدّث القائمة فورًا.
- إذا عدّل شخصان **العنصر نفسه** يفوز التعديل الأحدث؛ ولا يضيع الآخر: بل ينتقل إلى **سجل** العنصر.
- يصل الحذف إلى الجميع، ما لم يعدّل أحدهم ذلك العنصر في الأثناء: عندها تكون الأولوية للتعديل ويبقى العنصر.
- في الخزائن، عندما يضيف أحدهم ملفات أو يعيد تسميتها أو يحذفها في المجلد الذي تعرضه، تتحدث القائمة تلقائيًا.

ساعات الحواسيب

يعتمد Obskura على وقت الحواسيب لتحديد التعديل الأحدث: احرص على مزامنة الساعات (الضبط التلقائي للوقت مفعّل عادةً في كل الأنظمة).

اعثر على كل شيء في كل مكان

11 مفتاح الوصول والأجهزة

بجوار كل قاعدة بيانات وكل خزنة ملف صغير مشفر يتذكر أماكن ملف المفتاح والنسخ الاحتياطية والخوادم، وكيف يصل إليها كل جهاز من أجهزتك. ويحميه مفتاح الوصول إلى Obskura.

مفتاح الوصول إلى OBSKURA

رمز من 55 حرفًا يُنشأ عند التشغيل الأول (أو يُدخل إن كنت أنشأته على حاسوب آخر). يبقى في سلسلة مفاتيح النظام؛ ومن **الإعدادات** ← **مفتاح الوصول إلى Obskura** يمكنك:

- **إظهار**: رؤيته ونسخه لإدخاله على حاسوب آخر.
- **تغيير المفتاح...**: إنشاء مفتاح جديد. يعيد Obskura فورًا تشفير الملفات المرافقة التي يمكن الوصول إليها؛ وتُحدَّث البقية عند فتحها لاحقًا (تبقى المفاتيح السابقة صالحة لقراءتها).
- **إدخال المفتاح...**: استخدام المفتاح الحالي إذا غُيِّر على حاسوب آخر.

الملفات المرافقة

مشفرة بـ AES-256-GCM ولا يمكن قراءتها دون مفتاح الوصول:

الملف	يحتوي على
`<الاسم>.obk.obkx`	بجوار كل قاعدة بيانات: موضع ملف المفتاح، وإعدادات النسخ الاحتياطي، والاتصالات بالخوادم، وسجلات الأجهزة.
`vault.obkx`	داخل كل خزنة: المعلومات نفسها.
`recenti.obkx`	في مجلد بيانات التطبيق: قائمة العناصر الأخيرة. لا تبقى على القرص مسارات غير مشفرة.

الفتح من حاسوب آخر

بعد إدخال مفتاح الوصول على الحاسوب الجديد يكفي اختيار قاعدة البيانات: يقرأ Obskura الملف المرافق، ويعيد إنشاء الاتصالات بالخوادم الناقصة، ويعثر على ملف المفتاح (في الموضع المعروف لذلك الجهاز، أو بجوار قاعدة البيانات، أو في مسارات الأجهزة الأخرى، أو في النسخة الاحتياطية)، ويقترح النسخة الاحتياطية إذا تعذّر الوصول إلى الأصل.

> مهم
>
> لا يغني مفتاح الوصول عن كلمة مرور قاعدة البيانات: دون كلمة المرور (وملف المفتاح) تبقى البيانات غير مقروءة. ومع ذلك احفظه في مكان آمن: فدونه ستضطر إلى اختيار ملف المفتاح والنسخ الاحتياطية يدويًا.

الأجهزة والمسارات

لكل حاسوب يستخدم Obskura **معرّف فريد** يُنشأ عند التشغيل الأول، و**اسم** (اسم الحاسوب، ويمكن تغييره في **الإعدادات ← اسم هذا الجهاز**). وفي كل مرة يفتح فيها قاعدة بيانات أو خزنة يكتب سجله الخاص في الملف المرافق المشفر:

البيان	مثال
المعرّف والاسم	`3f2a9c1e-…` · «MacBook المنزل»
النظام والإصدار	macOS · Obskura 0.3.0 · آخر وصول
مسار قاعدة البيانات	`/Users/anna/Dropbox/accounts.obk` على Mac، و`D:\Dropbox\accounts.obk` على الحاسوب الشخصي
مسار ملف المفتاح	`/Volumes/USB/key.obkey` أو `E:\key.obkey`
النسخ الاحتياطي الخاص	مجلد على ذلك الجهاز، أو الإعداد المشترك (الفصل 12)

نافذة «الأجهزة والمسارات»

من القائمة ⋯ لقاعدة بيانات أو خزنة اختر **الأجهزة والمسارات…**:

- ترى كل الأجهزة المسجلة مع النظام والإصدار وآخر وصول واستخدام ملف المفتاح ووجهة النسخ الاحتياطي؛
- تُظهر أيقونة العين مسارات كل جهاز؛ ويعيد القلم تسمية هذا الجهاز؛
- تتيح سلة المهملات **نسيان** جهاز لم تعد تستخدمه: تُزال مساراته ونسخه الاحتياطي من الملف (وإذا فتحه مجددًا يُسجَّل من جديد).



الشكل 9 الأجهزة التي تستخدم قاعدة بيانات.

لماذا يهم ذلك

لقاعدة البيانات نفسها في Dropbox مسارات مختلفة على Mac وWindows وLinux، وقد يتغير حرف أو اسم ذاكرة USB التي تحمل ملف المفتاح. وبفضل السجلات الخاصة بكل جهاز يجد كل جهاز مساراته دون أن يكتب فوق مسارات غيره.

سلامة البيانات

12 النسخ الاحتياطي التلقائي

يمكن أن يكون لكل قاعدة بيانات وكل خزنة **وجهة ثانية**، على هذا الحاسوب (قرص خارجي مثلًا) أو على أي خادم مضبوط. وعند كل تعديل ينسخ Obskura الإصدار الجديد إليها في الخلفية دون أن يبطئك.

1. من القائمة ••• لقاعدة البيانات أو الخزنة اختر **النسخ الاحتياطي التلقائي...**
2. فعّل **النسخ الاحتياطي التلقائي مفعّل** واختر المجلد: **على هذا الحاسوب...** أو **على خادم...**.
3. إذا كانت الوجهة خادمًا يمكنك تفعيل **استخدام هذا الإعداد على كل الأجهزة**.
4. لقواعد البيانات اختر عدد **النسخ المؤرخة** التي تُحفظ.
5. اضغط **حفظ**. ويفرض **تشغيل الآن** نسخة كاملة.



الشكل 10 نسخ احتياطي إلى NAS، مشترك بين كل الأجهزة.

ماذا	كيف يُنسخ
قاعدة البيانات	ملف `.obk` في مجلد النسخ الاحتياطي، إضافة إلى النسخ المؤرخة `الاسم.YYYYMMDD-hhmmss.obk`؛ وتُحذف الأقدم بعد تجاوز الحد.
الخزنة	نسخة مطابقة من المجلد المشفر: عند كل تعديل لا يُعاد نسخ إلا الملفات المتأثرة. وتُفتح النسخة كخزنة عادية.
ملف المفتاح	اختياري: يُنسخ مرة واحدة عند حفظ الإعداد إلى المجلد الذي تحدده.

نسخة احتياطية لكل جهاز

- لكل جهاز **إعداده الخاص** المحفوظ مع معرّفه في الملف المرافق: المجلد المحلي (مثل القرص الخارجي لجهاز Mac) لا يسري إلا على ذلك الجهاز.
- يمكن لوجهة على خادم أن تصبح **مشتركة**: تستخدمها الأجهزة الأخرى، باستثناء التي لها إعداد خاص. وتبيّن النافذة من ضبطها.
- تبقى النسخ **مشفرة**: لا حاجة إلى الثقة بوجهة النسخ الاحتياطي.
- إذا فشل النسخ يظهر تنبيه؛ ويعيد Obskura المحاولة عند التعديل التالي.

ملف المفتاح والنسخ الاحتياطي

لا تضع ملف المفتاح في مجلد النسخة الاحتياطية نفسه: من يصل إلى ذلك المجلد سيملك قاعدة البيانات ونصف بيانات الاعتماد.

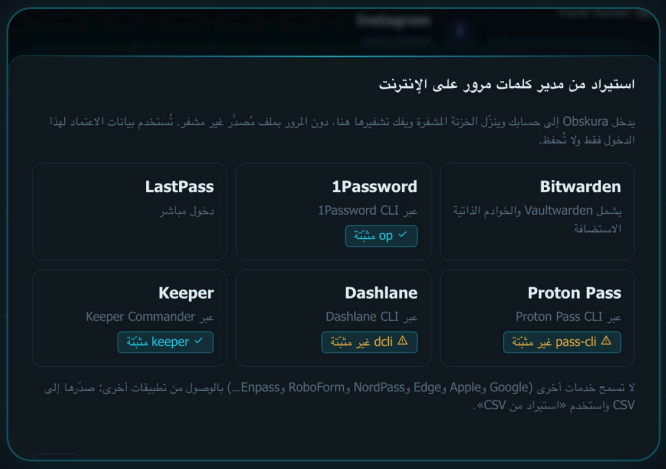
من البرامج الأخرى وإليها

13 الاستيراد والتصدير

الاستيراد من مدير على الإنترنت

يدخل Obskura مباشرة إلى خدمتك القديمة، وينزّل الخزنة المشفرة ويفك تشفيرها على حاسوبك، دون المرور بملف مُصدَّر غير مشفر. تُستخدم بيانات الاعتماد لهذا الدخول فقط ولا تُحفظ.

1. افتح قاعدة البيانات الوجهة واختر ⋯ ← **استيراد من مدير كلمات مرور على الإنترنت...**
2. اختر الخدمة وادخل؛ وإذا كنت تستخدم التحقق بخطوتين يطلب Obskura الرمز.
3. راجع المعاينة: عدد العناصر والمجلدات والأمثلة.
4. قرّر هل تُعاد المجلدات كمجموعات وهل تُتخطى العناصر الموجودة، ثم اضغط **استيراد**.



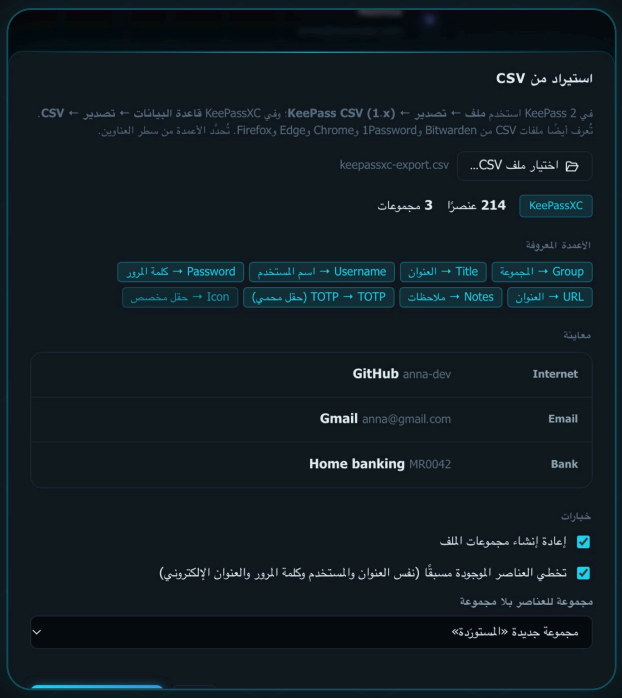
الشكل 11 اختيار الخدمة التي يُستورد منها.

الخدمة	طريقة الوصول
Bitwarden / Vaultwarden	مباشر، يشمل bitwarden.eu والخوادم الذاتية الاستضافة؛ أو بمفتاح API الشخصي.
LastPass	مباشر، مع التحقق بخطوتين (رمز أو تأكيد على الهاتف).
1Password	عبر 1Password CLI (`op`)، بتفويض من تطبيق 1Password أو بالبريد الإلكتروني وكلمة المرور وSecret Key.
Proton Pass	عبر Proton Pass CLI (`pass-cli`)، مع الدخول من المتصفح.
Dashlane	عبر Dashlane CLI (`dcli`)، بعد تنفيذ `dcli sync` أول مرة في الطرفية.
Keeper	عبر Keeper Commander (`keeper`).

تُحفظ المجلدات والحقول المخصصة ورموز TOTP والبطاقات والملاحظات. ولا تسمح خدمات أخرى (Google وApple وEdge وNordPass...) بالوصول من تطبيقات أخرى: صدّرها إلى CSV.

الاستيراد من CSV (KEEPASS وغيره)

1. صدّر إلى CSV في البرنامج الأصلي: في KeePass 2 **ملف ← تصدير ← KeePass CSV (1.x)**، وفي KeePassXC **قاعدة البيانات ← تصدير ← ملف CSV**، وفي Bitwarden و1Password و Chrome و Edge و Firefox من إعداداتها.
2. في Obskura افتح قاعدة البيانات واختر ⋯ ← **استيراد من CSV (KeePass…)...**
3. اختر الملف: يتعرف Obskura على التنسيق والأعمدة ويعرض معاينة.
4. قرّر هل تُعاد مجموعات الملف وهل تُتخطى العناصر الموجودة، ثم اضغط **استيراد**.



الشكل 12 معاينة تصدير من KeePassXC.

تُحفظ المجموعات والوسوم ورموز TOTP (كحقل محمي) وتواريخ الإنشاء والانتهاء؛ وتصبح الأعمدة غير المعروفة حقولًا مخصصة. ولا ينتج عن إعادة استيراد الملف نفسه عناصر مكررة.

التصدير إلى CSV

ينشئ ⋯ ← **تصدير إلى CSV...** ملفًا بأعمدة KeePassXC إضافة إلى الوسوم وتاريخ الانتهاء والمفضلة والحقول المخصصة: يمكن إعادة استيراده في Obskura و KeePassXC ومعظم مديري كلمات المرور.

> **ملف CSV غير مشفر**
>
> يحتوي الملف على كل كلمات المرور دون تشفير. استخدمه فقط لنقل البيانات ثم احذفه. وبعد الاستيراد احذف أيضًا ملف CSV المصدَّر من البرنامج القديم. وللنسخ الاحتياطي استخدم النسخ التلقائي الذي يبقى مشفرًا.

التخصيص

14 اللغات

يتحدث Obskura ثماني لغات ويمكن إضافة غيرها: كل نصوص التطبيق في ملفات XML، ملف لكل لغة.

اختيار اللغة

عند البدء يستخدم Obskura لغة النظام؛ وإذا لم تكن من اللغات المضمّنة يستخدم الإنجليزية. وفي **الإعدادات ← اللغة** يمكنك ترك **تلقائية** أو اختيار لغة؛ يسري التغيير فورًا، بما في ذلك رسائل الخطأ. وتُقرأ العربية من اليمين إلى اليسار فتنعكس الواجهة تبعًا لذلك.

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



الشكل 13 قسم اللغة في الإعدادات.

إضافة لغة

1. في **الإعدادات ← اللغة** اضغط **تصدير قالب XML...**: تحصل على الملف الكامل للغة الحالية (أو نزّل من الموقع ملف zip بملفات XML لكل اللغات).
2. غيّر في الترويسة `code` (رمز اللغة، مثل `fr` أو `pt-BR`) و`name`، وللغات التي تُكتب من اليمين إلى اليسار `dir="rtl"`.
3. ترجم نص كل عنصر `<string>` بأي محرر نصوص واحفظ بترميز UTF-8.
4. اضغط **استيراد ملف لغة (XML)...**: تظهر اللغة فورًا في القائمة وتُستخدم تلقائيًا على الأنظمة بتلك اللغة.

تنسيق الملف

ملف اللغة ملف XML فيه عنصر `<language>` وعنصر `<string>` لكل نص:

```
<?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>
```

- لا تُترجم السمة `key` ولا تُغيَّر؛
- تبقى العناصر النائبة بين الأقواس المعقوفة، مثل `{count}` أو `{name}`، كما هي: يستبدلها التطبيق بأرقام وأسماء؛
- يجب الإبقاء على الوسمين `<b>` و`<code>` في النص؛
- المفاتيح المنتهية بـ `.one` و`.two` و`.few` و`.many` و`.other` هي صيغ الجمع: استخدم صيغ لغتك، و`.other` إلزامية؛
- يظهر النص الناقص بالإنجليزية، لذا تعمل الترجمة الجزئية من الآن.

تصحيح لغة مضمّنة

ملف XML له `code` لغة مضمّنة (مثل `ar`) لا يستبدلها: بل يصحح فقط العناصر التي يحتويها. ويظهر في الإعدادات مع الإشارة **تصحيحات** ويُزال بعلامة × فتعود النصوص الأصلية.

> **نصيحة**
>
> تبقى الملفات المستوردة في مجلد بيانات التطبيق ولا تسري إلا على ذلك الحاسوب: استوردها على الحواسيب الأخرى أيضًا.

الترجمة باستخدام قالب XML الفارغ

لإضافة لغة جديدة يمكنك البدء من القالب الفارغ `obskura-translation-template.xml`، الذي يُنزَّل من الموقع (`obskura.bytenooks.com`، قسم التنزيل). يحتوي على سطر لكل نص في التطبيق: يُكتب النص بين `<string …>` و`</string>`، أما السمة `en` فتحمل النص الإنجليزي المرجعي ويمكن أن تبقى مكانها (يتجاهلها التطبيق).

```
<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. نزّل القالب واحفظه باسم رمز لغتك، مثل `fr.xml`.
2. في السطر الأول `<language>` املأ `code` و`name` و`english-name`، وعند الحاجة `dir="rtl"`.
3. اكتب الترجمات بمحرّر نصوص يحفظ بترميز UTF-8، مع الالتزام بالقواعد أعلاه.
4. **احذف الأسطر التي لا تترجمها**: النص الفارغ سيظهر فارغًا في التطبيق، أما السطر المحذوف فيُعرض بالإنجليزية.
5. استورد الملف من **الإعدادات ← اللغة** وتحقّق من النصوص في التطبيق.

شارك ترجمتك

أرسلها إلى المطوّر من صفحة الاتصال في الموقع: اختر موضوع «الترجمة» وأرفق ملف XML (حتى 3 ميغابايت؛ يبلغ حجم ملف اللغة الكامل نحو 100–150 كيلوبايت). قد تُضمَّن الترجمات المستلمة في الإصدارات القادمة.

الأمان

15 القفل والإعدادات

عند قفل قاعدة بيانات أو خزنة، يغلق Obskura الجلسة و**يمسح من الذاكرة** المفاتيح والبيانات المفكوكة التشفير. ولإعادة فتحها تلزم بيانات الاعتماد مرة أخرى.

طرق القفل

- **قفل الكل** أسفل الشريط الجانبي، أو `Ctrl/⌘` + `L`.
- القفل بجانب عنصر غير مقفل في الشريط الجانبي، أو بند **قفل** في القائمة ⋯.
- **تلقائيًا**، بعد فترة من عدم النشاط أو عند دخول الحاسوب في وضع السكون.

الإعدادات

الإعداد	الأثر	الافتراضي
القفل التلقائي عند عدم النشاط	يقفل الكل بعد 1–60 دقيقة دون استخدام الفأرة أو لوحة المفاتيح، أو أبدًا.	10 دقائق
مسح الحافظة	يمسح الحافظة بعد 10–120 ثانية من نسخ سرّ، أو أبدًا.	20 ثانية
القفل عند السكون	يقفل الكل عند دخول الحاسوب في وضع السكون.	مفعّل
المظهر	النظام أو فاتح أو داكن.	داكن
اسم هذا الجهاز	يظهر في قائمة أجهزة كل قاعدة بيانات وخزنة؛ وتحته المعرّف الفريد.	اسم الحاسوب
اللغة	تلقائية أو إحدى اللغات المتاحة؛ استيراد ملفات XML وتصديرها (الفصل 14).	تلقائية
مفتاح الوصول إلى Obskura	إظهار المفتاح أو تغييره أو إدخاله (الفصل 11).	—
الخوادم	اتصالات SFTP وFTP/FTPS وWebDAV وSMB (الفصل 09).	—

لا تحتوي الإعدادات على أي أسرار: كلمات مرور الخوادم في سلسلة مفاتيح النظام، وقائمة العناصر الأخيرة مشفرة بمفتاح الوصول.

مرجع

16 الاختصارات والتشفير

اختصارات لوحة المفاتيح

المفاتيح	أين	الإجراء
Ctrl/⌘ + L	في أي مكان	قفل الكل
Esc	مربعات الحوار	يغلق النافذة
Ctrl/⌘ + F	قاعدة البيانات	بحث
Ctrl/⌘ + N	قاعدة البيانات	عنصر جديد
Ctrl/⌘ + S	محرر العنصر	حفظ العنصر
نقر مزدوج	قائمة العناصر	نسخ كلمة المرور
Ctrl/⌘ + A	الخزنة	تحديد الكل
Enter	الخزنة	يفتح الملف أو المجلد
F2	الخزنة	إعادة تسمية
Del · ⌘ + ⌫	الخزنة	حذف العناصر المحددة
⌫	الخزنة	العودة إلى المجلد الأعلى

تفاصيل التشفير

المكوّن	الخوارزمية
اشتقاق المفتاح	Argon2id: 256 MiB / 3 تمريرات، أو 1 GiB / 4 تمريرات، أو 2 GiB / 6 تمريرات، مع ملح عشوائي بطول 256 بت.
المفتاح المركّب	SHA-256 لكلمة المرور (بتطبيع NFC) وملف المفتاح، كما في KeePass KDBX4.
التشفير	AES-256 أو XChaCha20 أو Serpent أو Twofish أو Camellia أو سلاسل منها، موثّقة دائمًا (GCM أو Poly1305)؛ وفي السلاسل لكل طبقة مفتاح خاص مشتق عبر HKDF.
المفاتيح الفرعية	HKDF-SHA256 مع بذرة جديدة عند كل حفظ.
السلامة	ترويسة موثّقة: أي تعديل يمنع الفتح.
الأسماء في الخزائن	AES-SIV، مرتبطة بالمجلد الذي يحتويها.
محتوى الملفات	كتل بحجم 64 KiB، ومفتاح عشوائي لكل ملف، وحماية من إعادة الترتيب والاقتطاع.
الملفات المرافقة	AES-256-GCM بمفتاح مشتق عبر HKDF من مفتاح الوصول إلى Obskura (256 بت عشوائية).
الذاكرة	تبقى المفاتيح والبيانات غير المشفرة داخل العملية الأصلية وتُمسح عند الإغلاق.

الدعم

17 الممارسات الجيدة وحل المشكلات

الممارسات الجيدة

- **فعّل النسخ الاحتياطي التلقائي** أو انسخ ملفات `.obk` ومجلدات الخزائن بانتظام إلى قرص خارجي. فهي مشفرة مسبقًا، والنسخة آمنة أينما احتفظت بها.
- **احتفظ بملف المفتاح منفصلاً** عن قاعدة البيانات، ومعه نسخة احتياطية واحدة على الأقل.
- **احفظ مفتاح الوصول إلى Obskura** على ورقة أو في مكان غير الحاسوب.
- **استخدم كلمة مرور مختلفة لكل خدمة**، يولّدها المولّد: لن تحتاج إلى تذكّر سوى واحدة.
- **اقفل عندما تبتعد**: `Ctrl/⌘` + `L` أسرع طريقة.
- **انسَ الأجهزة** التي لم تعد تستخدمها، من نافذة **الأجهزة والمسارات**.

الأسئلة الشائعة

نسيت كلمة المرور الرئيسية. هل يمكنني استعادتها؟

لا. هذا بالضبط ما يجعل Obskura آمنًا: لا يمكن لأحد، ولا حتى المطورين، فتح قاعدة بيانات أو خزنة دون بيانات الاعتماد الصحيحة.

تظهر رسالة «كلمة المرور أو ملف المفتاح خاطئ» مع أنني متأكد من صحتهما.

تحقق من أنك اخترت ملف المفتاح نفسه المستخدم عند الإنشاء ومن أنه لم يُعدَّل. وإذا استخدمت كلمة مرور وملف مفتاح فكلاهما مطلوب. وتحقق أيضًا من مفتاح الأحرف الكبيرة.

يستغرق الفتح بضع ثوانٍ. هل هذا طبيعي؟

نعم: إنه زمن عمل Argon2id، المقصود لإبطاء من يحاول تخمين كلمة المرور. يحتاج المستوى العالي إلى بضع ثوانٍ و1 GiB من الذاكرة الحرة، والأقصى إلى ما يصل إلى 12 ثانية و2 GiB.

لا يُعثر على ملف المفتاح على حاسوب آخر.

صِل الوسيط الذي يحتويه: يبحث Obskura عنه في المسار الذي استخدمه ذلك الحاسوب آخر مرة، وبجوار قاعدة البيانات، وفي مسارات الأجهزة الأخرى، وفي النسخة الاحتياطية. وإن لم يجده فاختره عبر **اختيار...**: وفي المرة التالية سيُتذكَّر المسار لذلك الجهاز.

تظهر رسالة «محمية بمفتاح وصول مختلف».

غيّر مفتاح الوصول على حاسوب آخر. انقر **أدخل المفتاح الحالي** واستخدم الجديد؛ ويمكنك على أي حال فتح القفل بكلمة المرور واختيار ملف المفتاح يدويًا.

ظهرت رسالة «تغيرت بيانات الاعتماد في مكان آخر».

غيّر أحدهم كلمة مرور قاعدة البيانات أو ملف مفتاحها على جهاز آخر. اختر **قفل** وأعد فتحها ببيانات الاعتماد الجديدة؛ أما **الكتابة فوقها** فتلغي التغيير الذي أُجري في المكان الآخر.

لا أستطيع الاتصال بالخادم.

تحقق من العنوان والمنفذ وبيانات الاعتماد عبر **اختبار الاتصال**. في WebDAV تحقق من المسار الأساسي (في Nextcloud `/remote.php/dav/files/<المستخدم>`)، وفي SMB من اسم المجلد المشترك. ومع شهادة موقّعة ذاتيًا لا تفعّل **قبول الشهادات الموقّعة ذاتيًا** إلا في شبكة موثوقة.

لا يبدو أن تعديلات ملف في الخزنة قد حُفظت.

تأكد من حفظ الملف في التطبيق الآخر، ثم اضغط **حفظ التعديلات في الخزنة**. وإذا قفلت الخزنة والملف لا يزال مفتوحًا، يحاول Obskura حفظه على أي حال قبل حذف النسخة المؤقتة.

يُفتح التطبيق بلغة ليست لغتي.

يتبع Obskura لغة النظام؛ وإذا لم تكن لغتك مضمّنة فإنه يستخدم الإنجليزية. اختر اللغة في **الإعدادات ← اللغة** أو استورد ملف XML (الفصل 14).

يقول MACOS أو WINDOWS إن التطبيق غير موثّق.

التطبيق غير موقّع بشهادة تجارية. اتبع تعليمات الفصل 02 لفتحه أول مرة.



OBSKURA

أمان غير مرئي لبياناتك

مدير كلمات المرور وخزائن الملفات المشفرة · على حاسوبك أو خادمك

الإصدار **0.3.0** · macOS · Windows · Linux

https://obskura.bytenooks.com