Kripta

دليل المستخدم

تشفير موجَّه لذاكرات USB والأقسام، مع استرداد كلمة المرور عبر مكتب الدعم في مؤسستك.



الإصدار 1.2 · Windows · macOS · Linux

نوفمبر 2026

المحتويات

1	ما هو Kripta	الغرض منه وما تحتاج إليه
2	التشغيل الأول	إعدادات المؤسسة والمكوّنات
3	النافذة الرئيسية	المؤشرات والتنبيهات والأيقونة
4	تشفير محرك أقراص	المعالج في 4 خطوات
5	تقسيم قرص إلى أقسام	منطقة مشفّرة ومنطقة حرّة
6	استخدام محرك مشفّر	فتح القفل والفتح والقفل
7	تغيير كلمة المرور	
8	نسيت كلمة المرور	الاسترداد عبر مكتب الدعم
9	الإعدادات	اللغة والإعدادات والتحديثات
10	استخدام المحرك على حواسيب أخرى	
11	الرسائل وحل المشكلات	
12	الأسئلة الشائعة	
A	ملحق لقسم تقنية المعلومات	الحزم والإعدادات الموقّعة واللغات

اصطلاحات

تُكتب النصوص التي تظهر على الشاشة (الأزرار والعناوين والعناصر) هكذا: **تشفير محرك أقراص** . الصور مأخوذة من إصدار macOS: على Windows وLinux تكون النافذة مطابقة، وتختلف أسماء الأجهزة فقط (مثل `E:` أو `/dev/sdb1` بدلاً من `/dev/disk4s1`).

1 ما هو Kripta

يحمي Kripta بيانات **ذاكرات USB** و**أقسام** الأقراص الخارجية بتشفير AES-256. بعد التشفير لا يستطيع قراءة محتوى المحرك إلا من يعرف كلمة المرور: إذا فقدت الذاكرة، فلن يتمكن أحد غيرك من فتحها.

تشفير موجَّه

أربع خطوات: اختر المحرك، اختر كلمة المرور، أكّد، انتظر.

فتح تلقائي

عند وصل محرك مشفّر يطلب Kripta كلمة المرور فورًا ويفتحه.

يعمل في كل مكان

تُفتح الذاكرة نفسها على Windows وmacOS وLinux (تنسيق VeraCrypt القياسي).

تثبيت ذاتي

يثبّت Kripta برنامج VeraCrypt ويحدّثه بنفسه، وتُستورد إعدادات المؤسسة من ملف.

تسع لغات

الإيطالية والإنجليزية والفرنسية والإسبانية والألمانية والروسية والعربية والصينية واليابانية، إضافة إلى ما تضيفه أنت.

الاسترداد عبر مكتب الدعم

إذا نسيت كلمة المرور، يساعدك مكتب الدعم على تعيين كلمة جديدة دون فقدان البيانات.

ما تحتاج إليه

- تثبيت **Kripta** على الحاسوب. عند التشغيل الأول يثبّت Kripta بنفسه **VeraCrypt**، محرك التشفير (وعلى macOS أيضًا **FUSE-T**)، إذا كان مفقودًا: الفصل 2.
- **ملف الإعدادات الموقّع** (`.kripta-config`) الذي يرسله مكتب الدعم، ما لم يكن قسم تقنية المعلومات قد أعدّ الحاسوب مسبقًا.
- **الاتصال بشبكة المؤسسة** (أو VPN) عند تشفير محرك جديد: يُرسل مفتاح الاسترداد فورًا إلى مكتب الدعم. لا حاجة إلى الشبكة لفتح محرك مشفّر مسبقًا.
- **بيانات اعتماد المسؤول** للحاسوب عندما يطلبها النظام (انظر الإطار).

طلبات التفويض

يحتاج Kripta إلى صلاحيات المسؤول للقراءة والكتابة مباشرة على المحرك وتثبيت المكوّنات وحفظ الإعدادات. على **Windows** تظهر نافذة التحكم في حساب المستخدم عند التشغيل. وعلى **macOS** و**Linux** تظهر الرسالة «يحتاج Kripta إلى تفويض المسؤول لإكمال العملية». إذا ثبّت قسم تقنية المعلومات خدمة نظام Kripta، فلن تظهر هذه الطلبات.

كيف يعمل الاسترداد باختصار

أثناء التشفير ينشئ Kripta **مفتاح استرداد** من 48 رقمًا، ويحميه ويرسله إلى أرشيف مكتب الدعم. لا تحتاج إلى رؤيته أو الاحتفاظ به. لا يمكن الاطلاع عليه إلا لموظفي مكتب الدعم بعد التحقق من هويتك، ويُسجَّل كل اطلاع.

2 التشغيل الأول

عند التشغيل الأول يتحقق Kripta من أمرين: هل هو مرتبط بمكتب الدعم في مؤسستك، وهل VeraCrypt مثبّت على الحاسوب. إذا كان شيء ما مفقودًا، يظهر في أعلى النافذة تنبيه مع زر لإصلاحه. يمكنك القيام بكل شيء بنفسك.

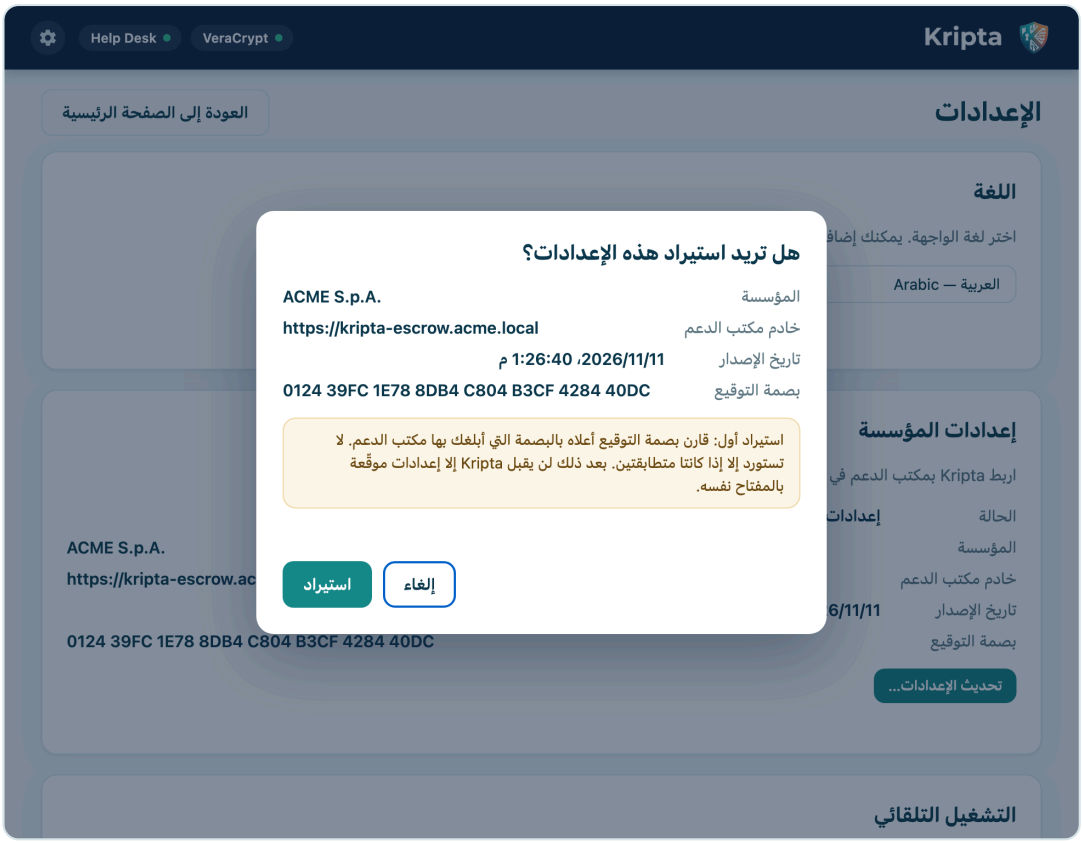


التشغيل الأول: إعدادات يجب استيرادها وVeraCrypt يجب تثبيته.

استيراد إعدادات المؤسسة

تخبر الإعدادات Kripta بالأرشيف الذي يرسل إليه مفاتيح الاسترداد. يزوّدك بها مكتب الدعم في ملف بامتداد `.kripta-config` موقّع رقميًا: لا يمكن لأحد تعديله دون أن يلاحظ Kripta ذلك.

1. احفظ الملف الذي استلمته على الحاسوب (بالبريد الإلكتروني أو من بوابة المؤسسة أو من ذاكرة USB).
2. اضغط **استيراد الإعدادات** في التنبيه، أو افتح **الإعدادات** (الترس في الأعلى) واضغط **استيراد إعدادات موقّعة...**.
3. اختر الملف. يتحقق Kripta من التوقيع ويعرض المؤسسة وخادم مكتب الدعم وتاريخ الإصدار و**بصمة التوقيع**.
4. عند الاستيراد الأول **قارن البصمة** بالبصمة التي أبلغك بها مكتب الدعم (بالهاتف أو عبر الشبكة الداخلية...). إذا تطابقت، اضغط **استيراد**.
5. أكّد طلب التفويض من النظام. تظهر رسالة **تم استيراد الإعدادات** ويتحول مؤشر **Help Desk** إلى الأخضر.

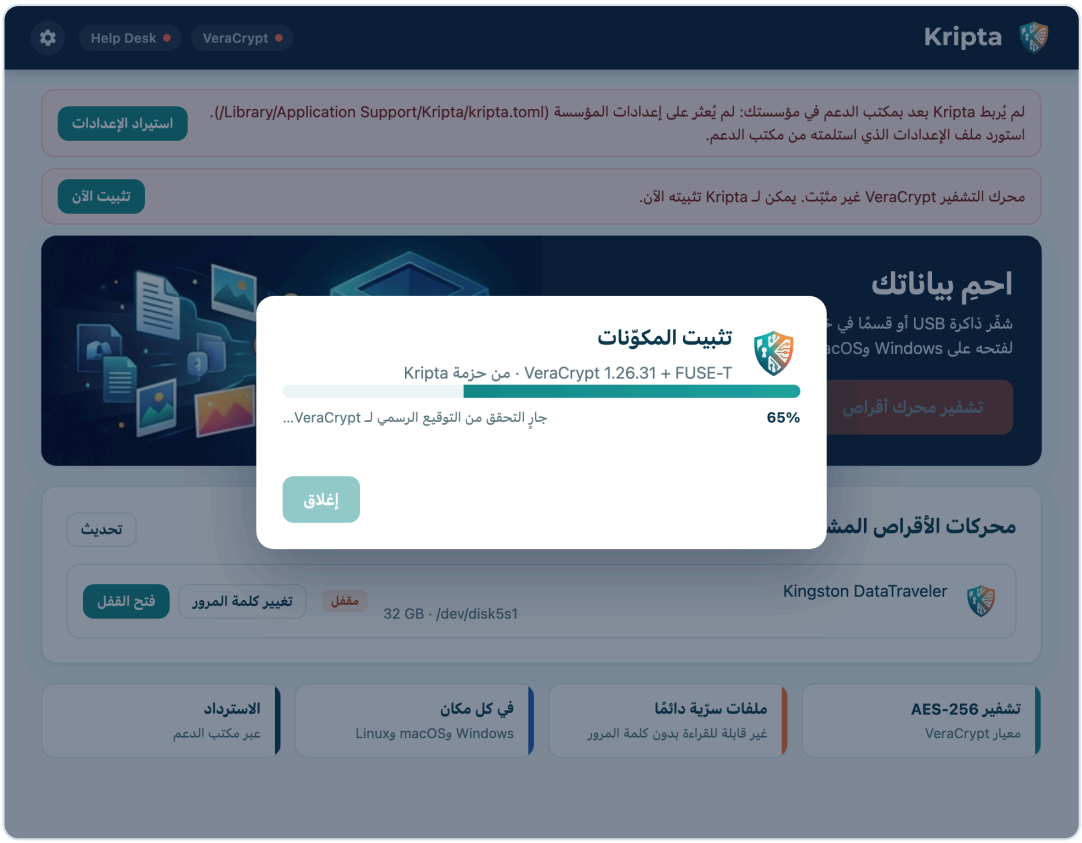


تأكيد الاستيراد مع بصمة التوقيع.

> **إذا لم تتطابق البصمة فلا تستورد**
>
> قد لا يكون الملف صادرًا عن مؤسستك. ألغِ العملية وتواصل مع مكتب الدعم. بعد الاستيراد الأول لا يقبل Kripta إلا التحديثات الموقّعة بالمفتاح نفسه: يُرفض أي ملف مزيّف تلقائيًا.

تثبيت VeraCrypt

يحتوي Kripta مسبقًا على المثبّت الرسمي لـ VeraCrypt (وFUSE-T لنظام macOS). اضغط **تثبيت الآن** في التنبيه وأكّد طلب التفويض: يتحقق Kripta من التوقيع الرسمي للمثبّتات ويثبّتها دون أسئلة أخرى.



تثبيت المكوّنات مع التحقق من التوقيع الرسمي.

في النهاية تظهر رسالة **اكتمل التثبيت**. قد يُطلب إعادة تشغيل الحاسوب على Windows.

تحديثات VeraCrypt

عند كل تشغيل (ثم مرة يوميًا) يتحقق Kripta من صدور إصدار أحدث من VeraCrypt. إذا وُجد، يظهر تنبيه أزرق مع زر **تحديث**. يُنزَّل الإصدار الجديد من الموقع الرسمي ولا يُثبَّت إلا إذا كان توقيع مطوري VeraCrypt صالحًا.



يتوفر تحديث لـ VeraCrypt.

قبل التحديث

اقفل جميع المحركات المشفّرة المفتوحة: لا يحدّث Kripta برنامج VeraCrypt ما دام هناك محرك مفتوح. يمكنك إيقاف التحقق التلقائي من الإعدادات (الفصل 9).

3 النافذة الرئيسية

عند الفتح يعرض Kripta الشاشة الرئيسية. من هنا يمكنك تشفير محرك جديد وإدارة المحركات المشفّرة المتصلة بالحاسوب.



الشاشة الرئيسية مع محرك مشفّر متصل ومفتوح.

العنصر	وظيفته
VeraCrypt	نقطة **خضراء**: محرك التشفير مثبّت. **حمراء**: غير مثبّت (الفصل 2). عند تمرير المؤشر يظهر الإصدار.
Help Desk	أخضر: أرشيف المفاتيح متاح. أحمر: غير متاح (لا توجد شبكة، أو VPN مطفأ، أو الإعدادات مفقودة).
الترس	يفتح **الإعدادات**: اللغة وإعدادات المؤسسة والمكوّنات (الفصل 9).
تشفير محرك أقراص	يبدأ المعالج (الفصل 4). يكون معطّلاً إذا لم يُعدّ Kripta أو كان VeraCrypt مفقودًا.
التقسيم إلى أقسام	يقسم ذاكرة USB أو قرصًا خارجيًا إلى عدة أقسام (الفصل 5).
محركات الأقراص المشفّرة المتصلة	محركات Kripta المتصلة مع الحالة **مقفل** أو **مفتوح** والأزرار الخاصة بها.

التنبيهات

قد تظهر في أعلى النافذة مربعات ملوّنة مع زر لحل المشكلة:



تعذّر الوصول إلى خادم مكتب الدعم ومفتاح استرداد بانتظار الإرسال.

- **تعذّر الوصول إلى خادم مكتب الدعم:** يمكنك متابعة فتح المحركات، لكن لا يمكنك تشفير محركات جديدة.
- **مفاتيح استرداد بانتظار الإرسال:** يعيد Kripta المحاولة بنفسه؛ اضغط **أعد المحاولة الآن** عند عودة الاتصال. **أبقِ Kripta مفتوحًا حتى يختفي التنبيه.**
- **لم يُربط Kripta بعد بمكتب الدعم / VeraCrypt غير مثبّت / يتوفر VeraCrypt...:** انظر الفصل 2.

أيقونة Kripta: شريط القوائم ومنطقة الإشعارات

يعمل Kripta في الخلفية ليلاحظ وصل محرك مشفّر، ويُتحكَّم فيه من أيقونة تحمل الشعار:

النظام	مكان الأيقونة	معلومات مفيدة
macOS	في **شريط القوائم** أعلى يمين الشاشة. لا **يظهر Kripta في Dock**.	في أجهزة MacBook ذات النتوء، تُخفى الأيقونات الزائدة عند امتلاء الشريط: أزل ما لا تستخدمه أو اسحبها مع الضغط على ⌘.
Windows	في **منطقة الإشعارات** أسفل يمين الشاشة بجوار الساعة.	إذا كانت ضمن الأيقونات المخفية، انقر السهم ^ واسحب الشعار إلى الشريط.
Linux	في **منطقة الإشعارات** في اللوحة.	على GNOME «الصرف» (Fedora وDebian) يلزم الامتداد **AppIndicator and KStatusNotifierItem Support**.

تحتوي قائمة الأيقونة على **فتح Kripta** و**تشفير محرك أقراص...** و**التقسيم إلى أقسام...** و**قفل جميع المحركات** و**الإعدادات...** و**إنهاء Kripta**. تتبع العناصر اللغة المختارة.

إغلاق النافذة لا يُنهي Kripta

يبقى Kripta نشطًا في شريط القوائم أو منطقة الإشعارات. لإعادة فتح النافذة استخدم **فتح Kripta** ، أو شغّل Kripta مرة أخرى: ستظهر النافذة العاملة.

التشغيل التلقائي

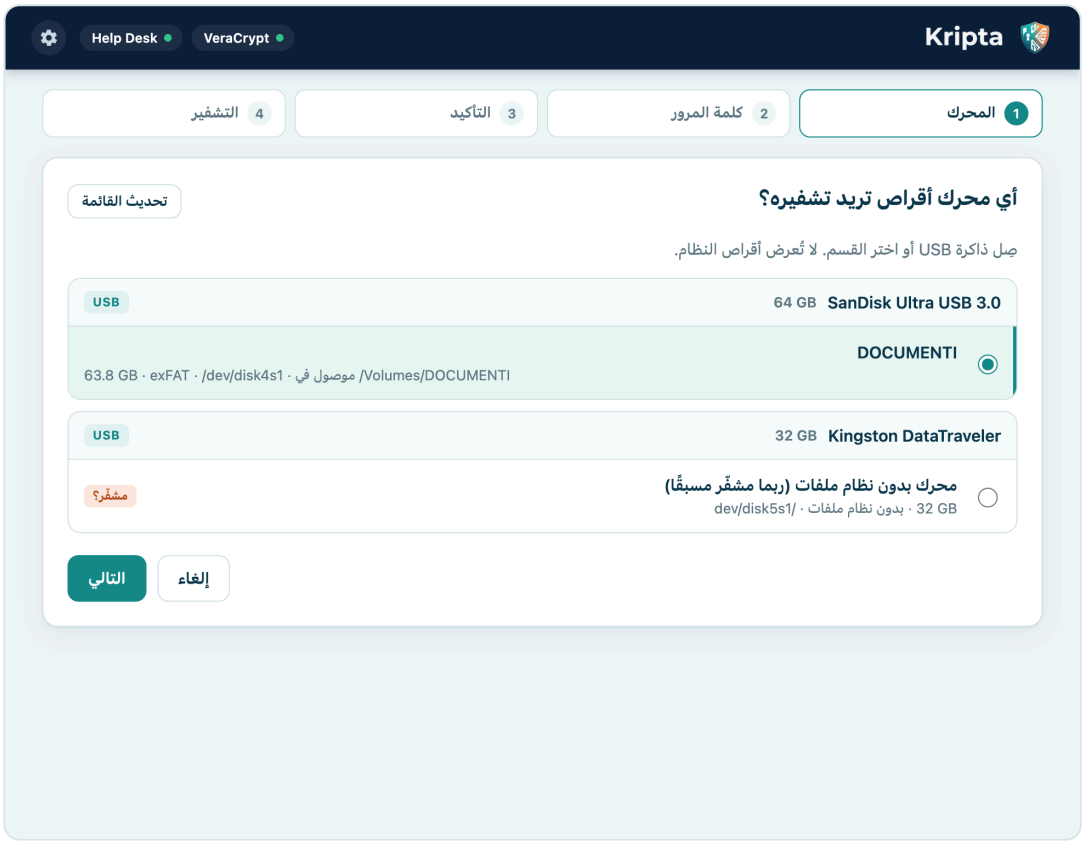
بعد التثبيت **يبدأ Kripta تلقائيًا عند كل تسجيل دخول** دون فتح النافذة، ويبقى في وضع الاستماع دائمًا: ما إن توصل وحدة تخزين مشفّرة حتى يطلب كلمة المرور. يمكنك إيقاف ذلك من **الإعدادات ‹ التشغيل التلقائي** (الفصل 9). يؤدي **الخروج من Kripta** إلى إغلاقه حتى تسجيل الدخول التالي.

4 تشفير محرك أقراص

يمحو التشفير كل محتوى المحرك.
قبل البدء انسخ الملفات التي تريد الاحتفاظ بها إلى مكان آخر. بعد التشفير يمكنك نسخها مرة أخرى إلى المحرك المحمي.

صِل الذاكرة، وتأكد من أن مؤشر **Help Desk** أخضر، واضغط **تشفير محرك أقراص** .

الخطوة 1 — المحرك

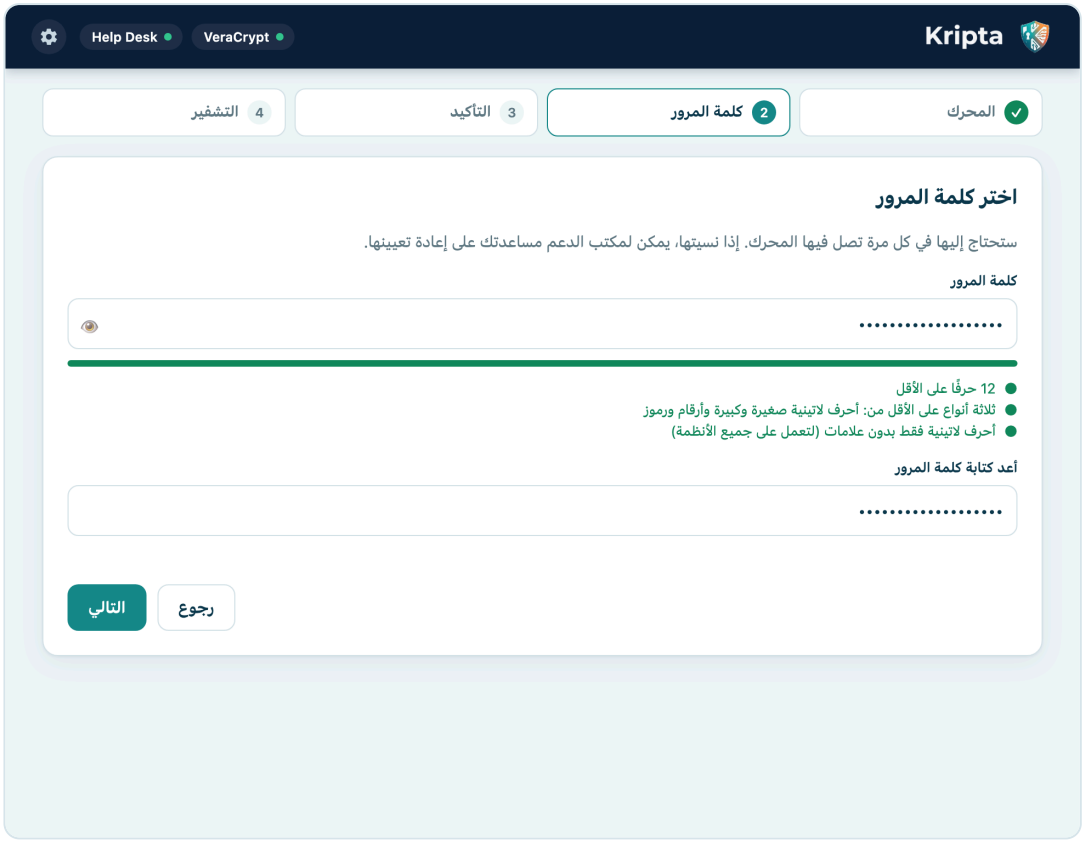


اختيار المحرك المراد تشفيره.

1. يعرض Kripta الأجهزة المتصلة، والأجهزة القابلة للإزالة أولاً. **لا تُعرض أقراص النظام أبدًا.**
2. تحقق بعناية من **السعة والاسم** للتأكد من اختيار المحرك الصحيح.
3. إذا لم تظهر الذاكرة، أعد وصلها واضغط **تحديث القائمة** .
4. اختر المحرك واضغط **التالي** .

علامة «مشفّر؟»
تشير إلى محرك بدون نظام ملفات معروف: على الأرجح هو مشفّر مسبقًا. إذا شفّرته مجددًا فسيضيع محتواه الحالي.

الخطوة 2 — كلمة المرور

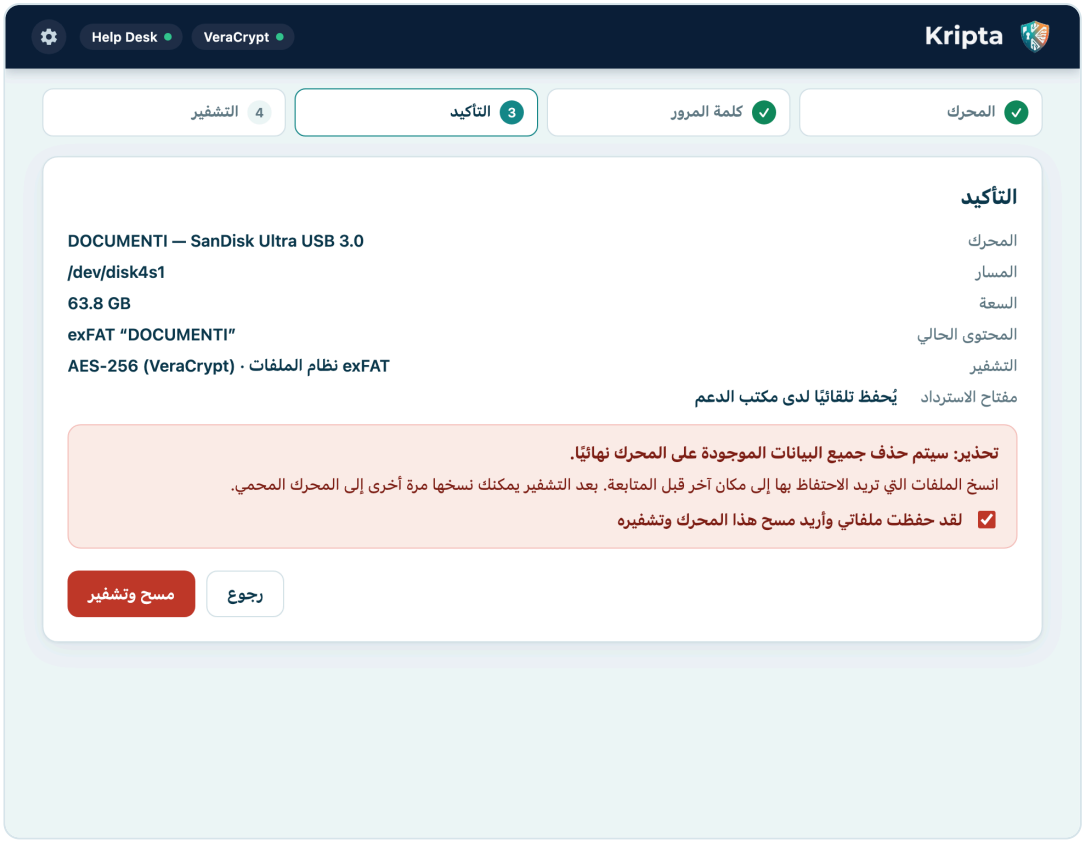


تتحول القواعد إلى الأخضر عند استيفائها.

يجب أن تتكون كلمة المرور من **12 حرفًا على الأقل**، و**ثلاثة أنواع على الأقل** من الأحرف اللاتينية الصغيرة والكبيرة والأرقام والرموز، و**أحرف لاتينية فقط دون علامات**: قد تُكتب الأحرف العربية أو المشكّلة بشكل مختلف على أنظمة أخرى. يبيّن الشريط الملوّن قوة كلمة المرور، ويعرضها الزر 👁. أعد كتابتها في الحقل الثاني واضغط **التالي**.

> **نصيحة**
>
> عبارة من عدة كلمات تربطها رموز وأرقام (مثل `Qitar-Buhaira-Akhdar-47`) آمنة وسهلة التذكر. لا تستخدم كلمة مرور حسابك في المؤسسة.

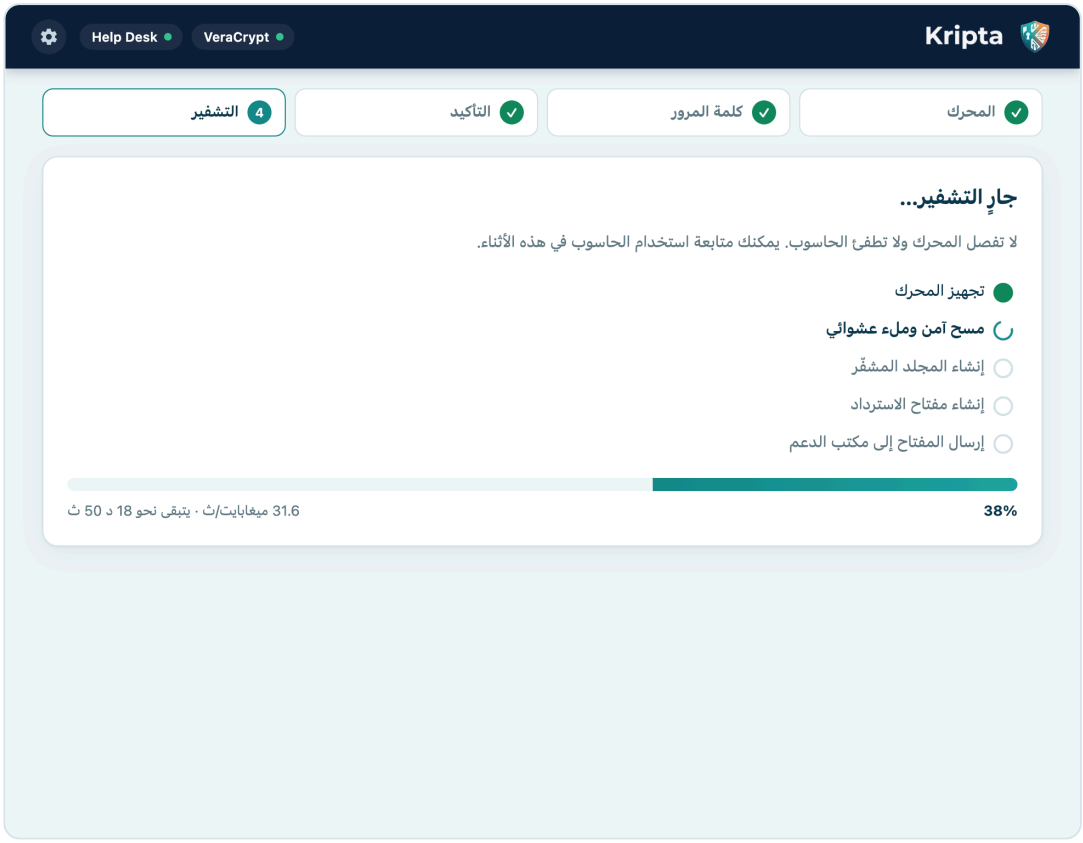
الخطوة 3 — التأكيد



الملخص وتأكيد المسح.

راجع الملخص، وحدّد **لقد حفظت ملفاتي وأريد مسح هذا المحرك وتشفيره** ثم اضغط **مسح وتشفير**. قد يطلب النظام تفويض المسؤول.

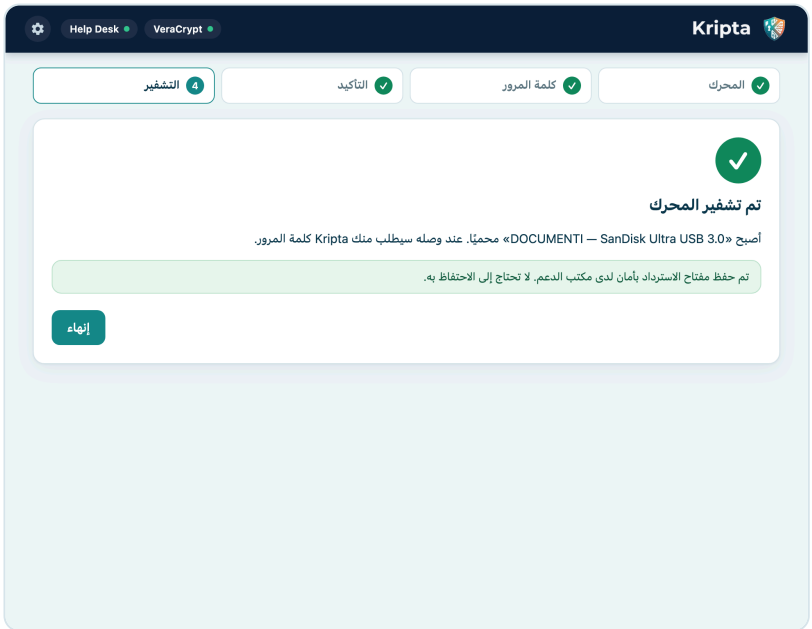
الخطوة 4 — التشفير



التقدّم مع السرعة والوقت المتبقي.

يجهّز Kripta المحرك، ويعيد كتابته بالكامل ببيانات عشوائية (أطول مرحلة)، وينشئ المجلد المشفّر بنظام exFAT، ويولّد مفتاح الاسترداد ويرسله إلى مكتب الدعم.

> **أثناء التشفير**
> لا تفصل المحرك ولا تطفئ الحاسوب ولا تضعه في وضع السكون. تستغرق ذاكرة سعتها 64 غيغابايت من 15 دقيقة إلى ساعة تقريبًا.



اكتمل التشفير.

إذا ظهرت رسالة **لم يُرسل مفتاح الاسترداد بعد**، فالمحرك مشفّر وقابل للاستخدام: أبقِ Kripta مفتوحًا ومتصلاً، وسيرسل المفتاح في أقرب وقت. إذا فشل التشفير، توضح الرسالة السبب (الفصل 11).

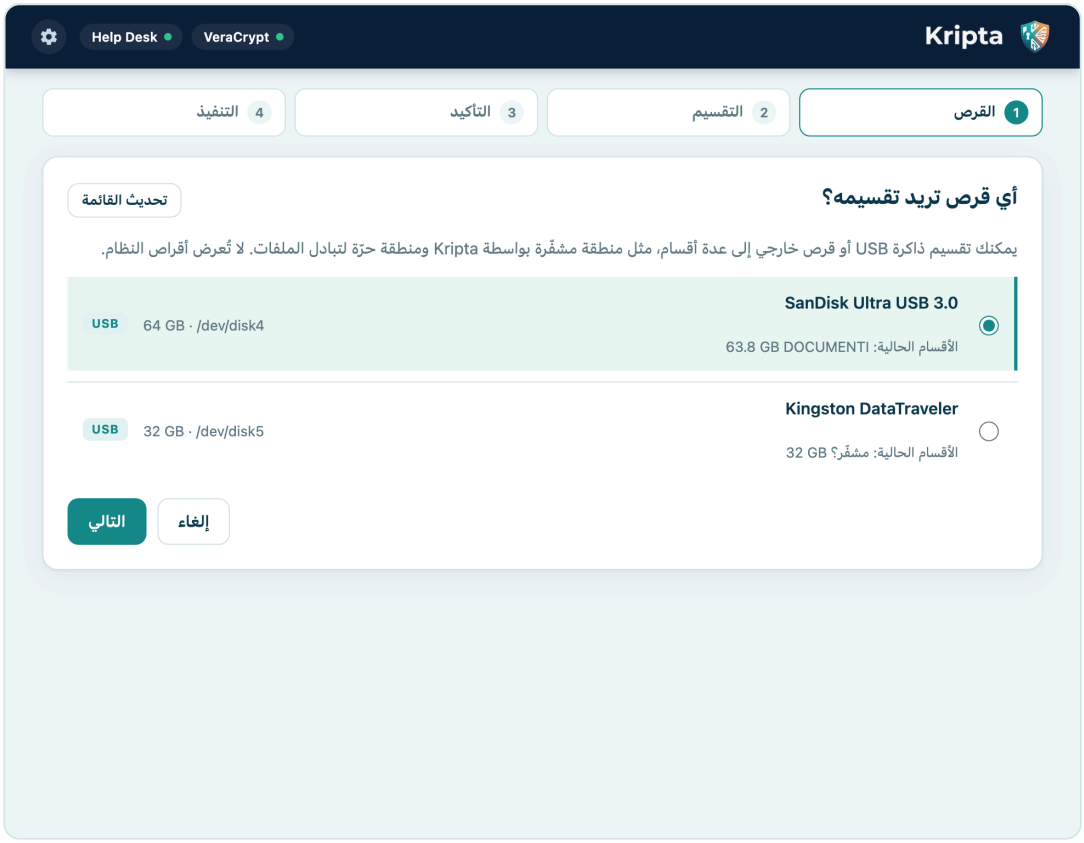
5 تقسيم قرص إلى أقسام

باستخدام **التقسيم إلى أقسام** تقسم ذاكرة USB أو قرصًا خارجيًا إلى عدة أجزاء مستقلة، لكل منها اسمه ونظام ملفاته. الاستخدام المعتاد: **منطقة مشفّرة** للبيانات السرّية و**منطقة حرّة** لتبادل الملفات مع حواسيب لا يوجد عليها Kripta.

التقسيم يمحو القرص بالكامل

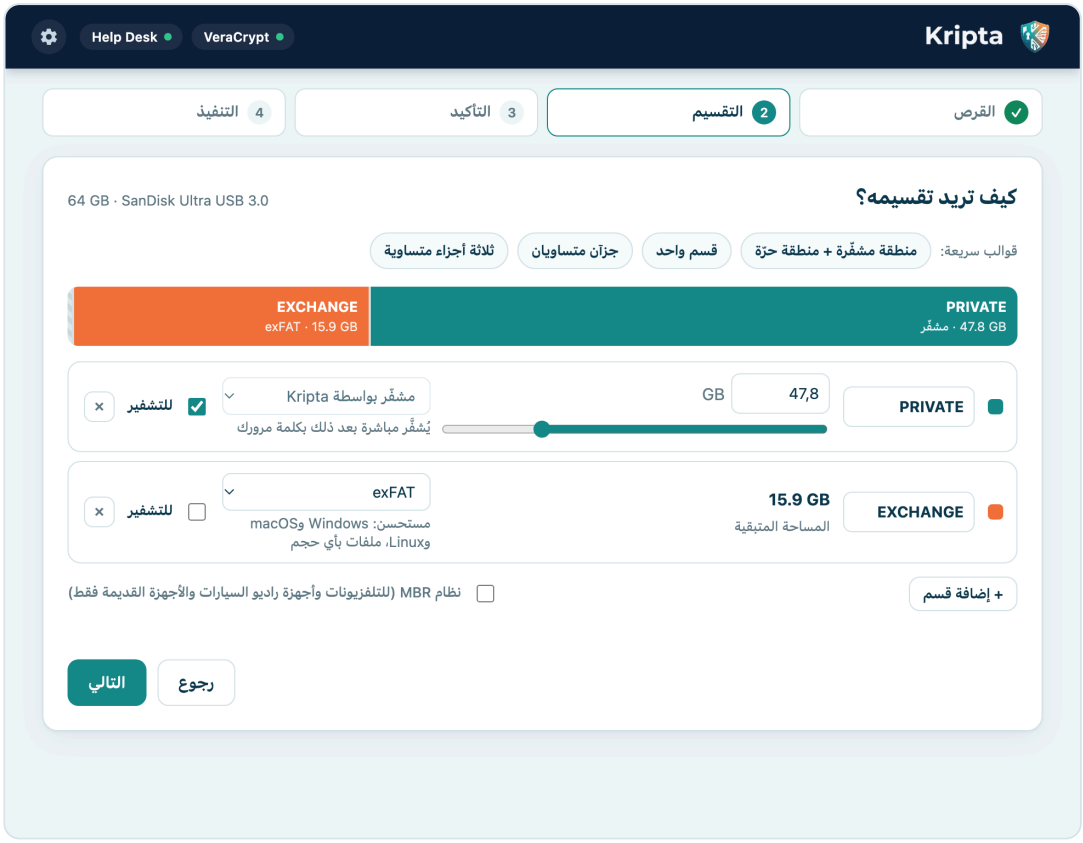
، بما في ذلك الأقسام الموجودة والمحركات المشفّرة مسبقًا. احفظ الملفات التي تريدها في مكان آخر.

الخطوة 1 — القرص



اختيار القرص مع أقسامه الحالية.

الخطوة 2 — التقسيم



يبيّن الشريط الملوّن التقسيم بالنسبة والتناسب.

القالب	النتيجة
منطقة مشفّرة + منطقة حرّة	ثلاثة أرباع القرص للتشفير والباقي حرّ بنظام exFAT. هذا هو القالب المقترح في البداية.
قسم واحد	القرص كله في قسم واحد.
جزآن / ثلاثة أجزاء متساوية	يُقسم القرص إلى أجزاء متساوية الحجم.

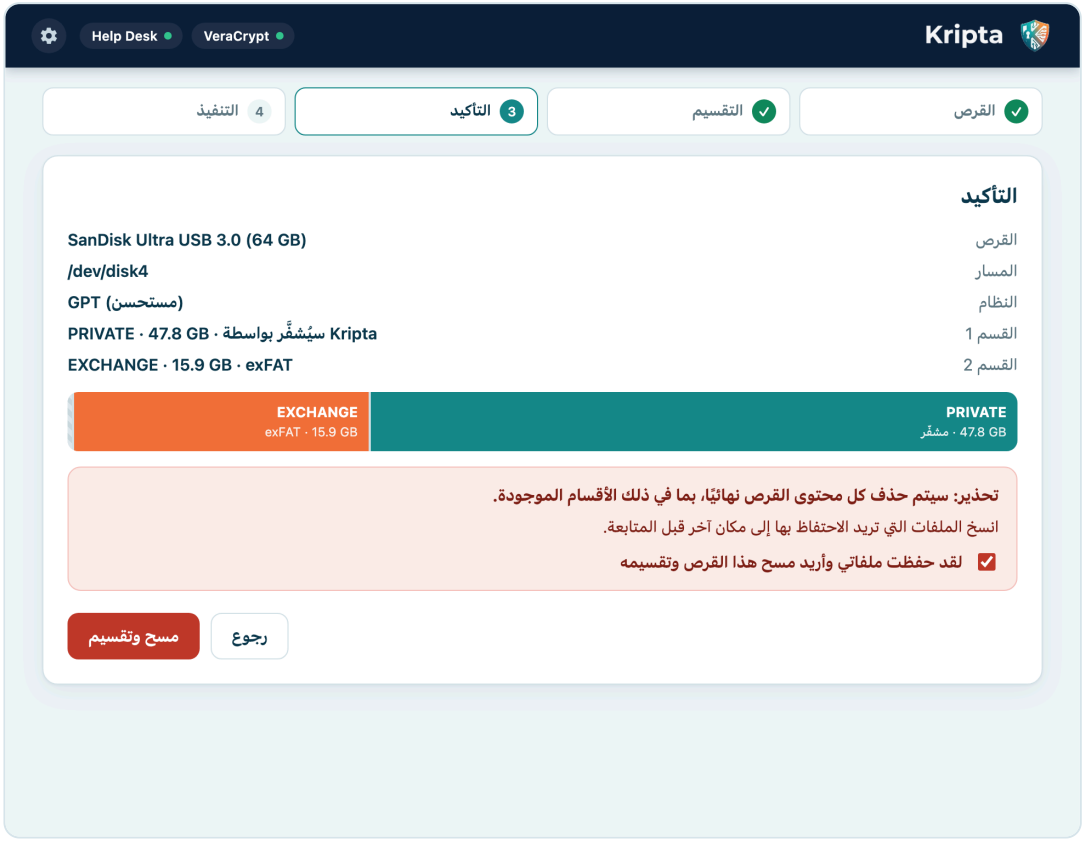
لكل قسم تحدد **الاسم** (حتى 11 حرفًا: أحرف لاتينية وأرقام و `_` و `-`)، و**الحجم** (يأخذ القسم الأخير المساحة المتبقية)، و**نظام الملفات**، وخيار **للتشفير**. يضيف **+ إضافة قسم** قسمًا آخر (حتى 8).

نظام الملفات	يُفتح على	ملاحظات
exFAT (مستحسن)	Windows وmacOS وLinux	لا حد عمليًا لحجم الملفات.
FAT32	معظم الأجهزة تقريبًا	ملفات حتى 4 غيغابايت؛ وعلى Windows أقسام حتى 32 غيغابايت.
NTFS	Windows؛ وقراءة فقط على macOS	يتطلب `ntfs-3g` على Linux.
APFS وMac OS **Extended**	Mac فقط	متاحان فقط من جهاز Mac.
ext4	Linux فقط	متاح فقط من Linux.

نظام MBR

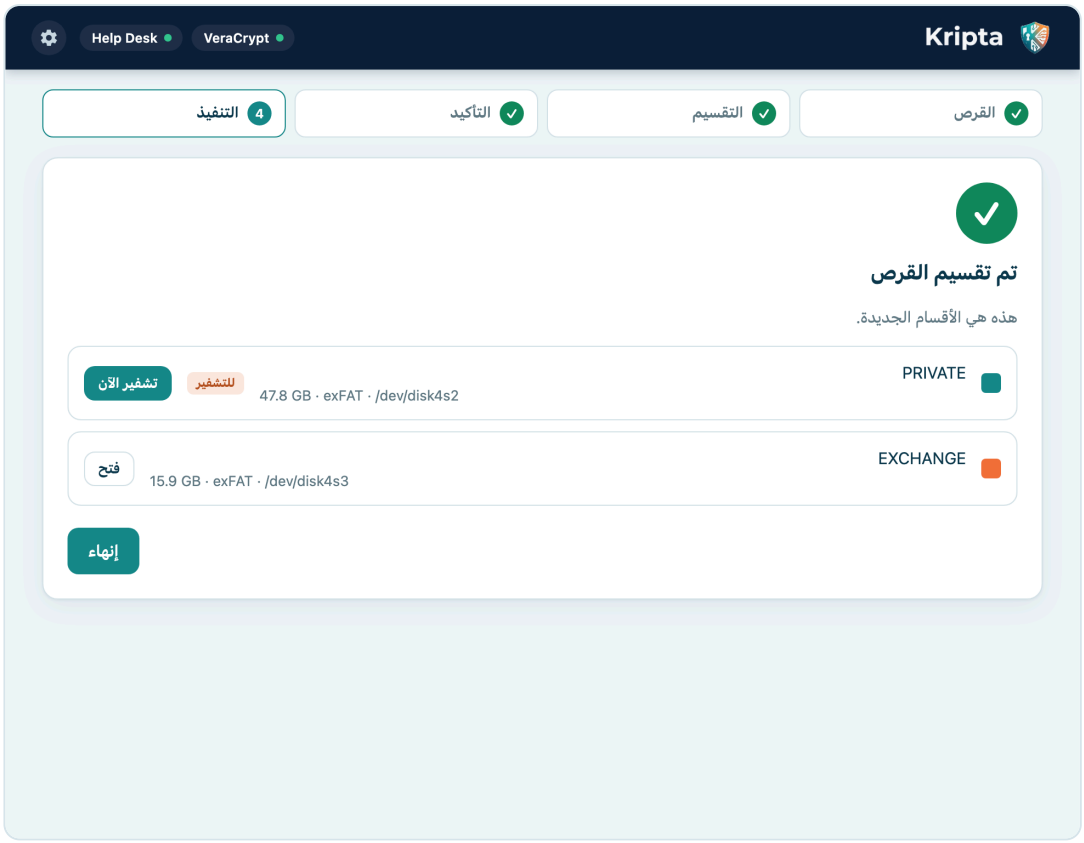
فعّله فقط إذا كان يجب أن تعمل الذاكرة مع التلفزيونات أو أجهزة راديو السيارات أو الحواسيب القديمة جدًا: 4 أقسام و2 تيرابايت كحد أقصى.

الخطوة 3 — التأكيد والخطوة 4 — التنفيذ



الملخص قبل المسح.

حدّد مربع التأكيد واضغط **مسح وتقسيم** . يستغرق ذلك عادة أقل من دقيقة.



تم إنشاء الأقسام: للمنطقة المراد تشفيرها زر «تشفير الآن».

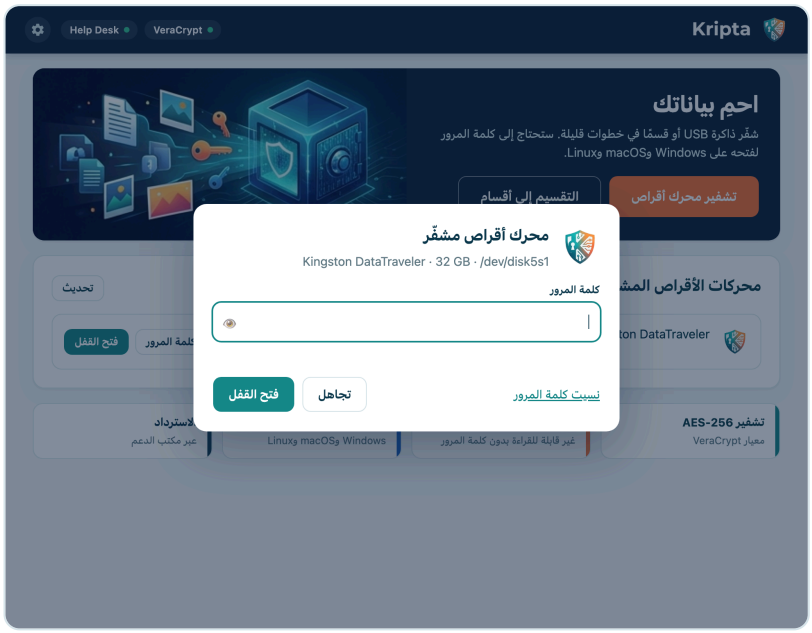
بجوار الأقسام المراد تشفيرها اضغط **تشفير الآن**: يبدأ التشفير (الفصل 4) والقسم محدد مسبقًا.

> **لا تكون المنطقة «للتشفير» محمية قبل تشفيرها**
> لا تنسخ إليها ملفات سرّية قبل اكتمال التشفير.

6 استخدام محرك مشفر

فتح القفل

عند وصل محرك مشفّر أثناء تشغيل Kripta، يظهر طلب كلمة المرور تلقائيًا.



طلب كلمة المرور عند الوصل.

1. اكتب كلمة المرور واضغط **فتح القفل** (أو Enter).
2. يُفتح المحرك كقرص عادي في مستكشف الملفات أو Finder أو مدير ملفات Linux.
3. باستخدام **تجاهل** يمكنك فتحه لاحقًا من النافذة الرئيسية.

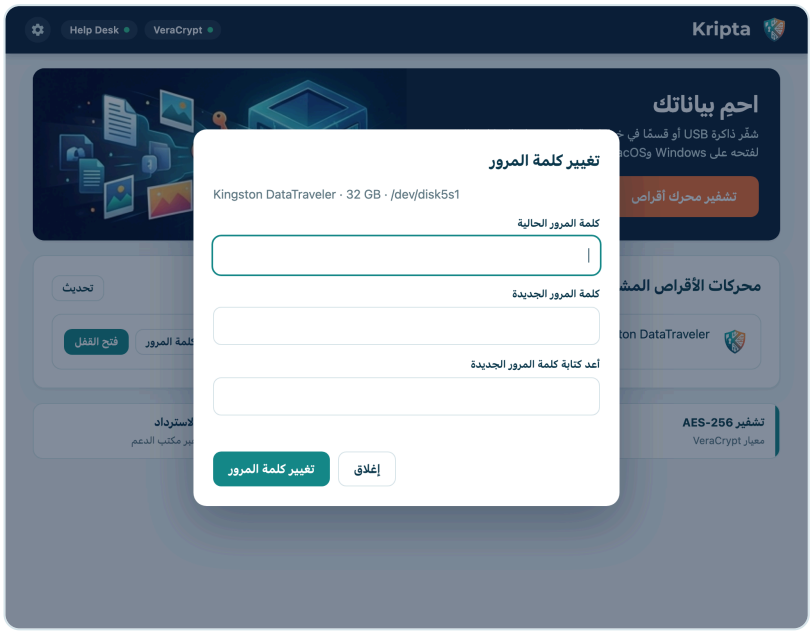
العمل مع الملفات والقفل

عندما يكون المحرك مفتوحًا تستخدم الملفات بشكل طبيعي: كل ما تكتبه يُشفَّر بشفافية. عند الانتهاء أغلق الملفات المفتوحة، واضغط **قفل**، ثم افصل المحرك.

> **لا تفصل محركًا مفتوحًا دون قفله**
> قد تفقد الملفات التي كنت تنسخها.

7 تغيير كلمة المرور

يمكنك تغيير كلمة المرور متى شئت إذا كنت تعرف الحالية. لا تتأثر البيانات الموجودة على المحرك.



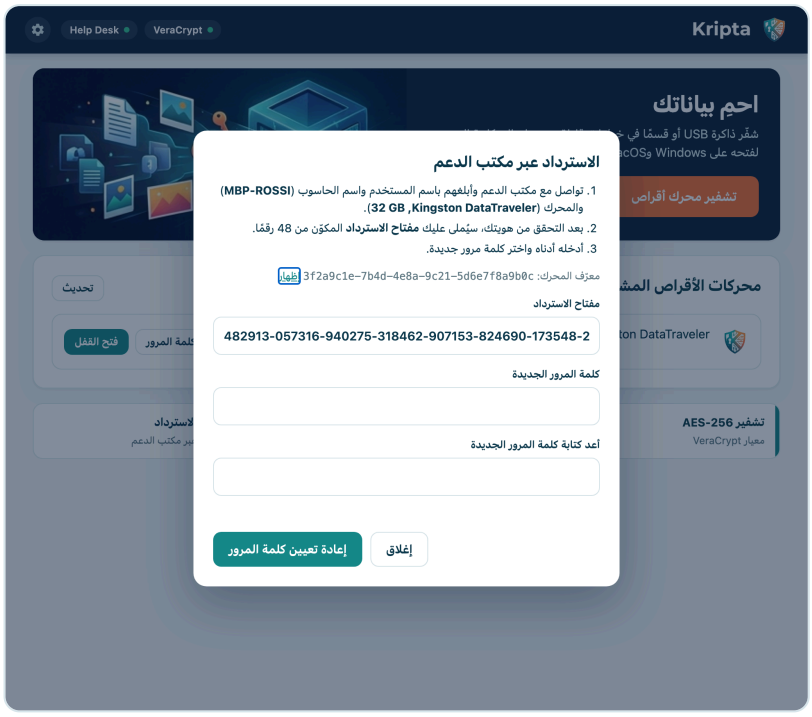
نافذة تغيير كلمة المرور.

1. إذا كان المحرك مفتوحًا، اضغط أولاً **قفل**.
2. اضغط **تغيير كلمة المرور** بجوار المحرك.
3. أدخل كلمة المرور الحالية ثم الجديدة مرتين (القواعد نفسها في الفصل 4)، ثم أكّد.

> **وماذا عن مفتاح الاسترداد؟**
> يبقى صالحًا: يمكن لمكتب الدعم مساعدتك حتى بعد تغيير كلمة المرور.

8 نسيت كلمة المرور

يمكن لمكتب الدعم تزويدك بمفتاح استرداد المحرك: به تعيّن كلمة مرور جديدة وتستعيد جميع ملفاتك.



الاسترداد عبر مكتب الدعم.

1. في طلب كلمة المرور اختر **نسيت كلمة المرور**.
2. تعرض النافذة اسم الحاسوب واسم المحرك؛ ويُظهر **إظهار** أيضًا معرّف المحرك.
3. **تواصل مع مكتب الدعم** وأبلغه بهذه البيانات. بعد التحقق من هويتك سيُملى عليك **المفتاح المكوّن من 48 رقمًا**.
4. اكتبه في حقل **مفتاح الاسترداد**، واختر كلمة مرور جديدة، واضغط **إعادة تعيين كلمة المرور**.

مفتاح واحد لاستخدام واحد

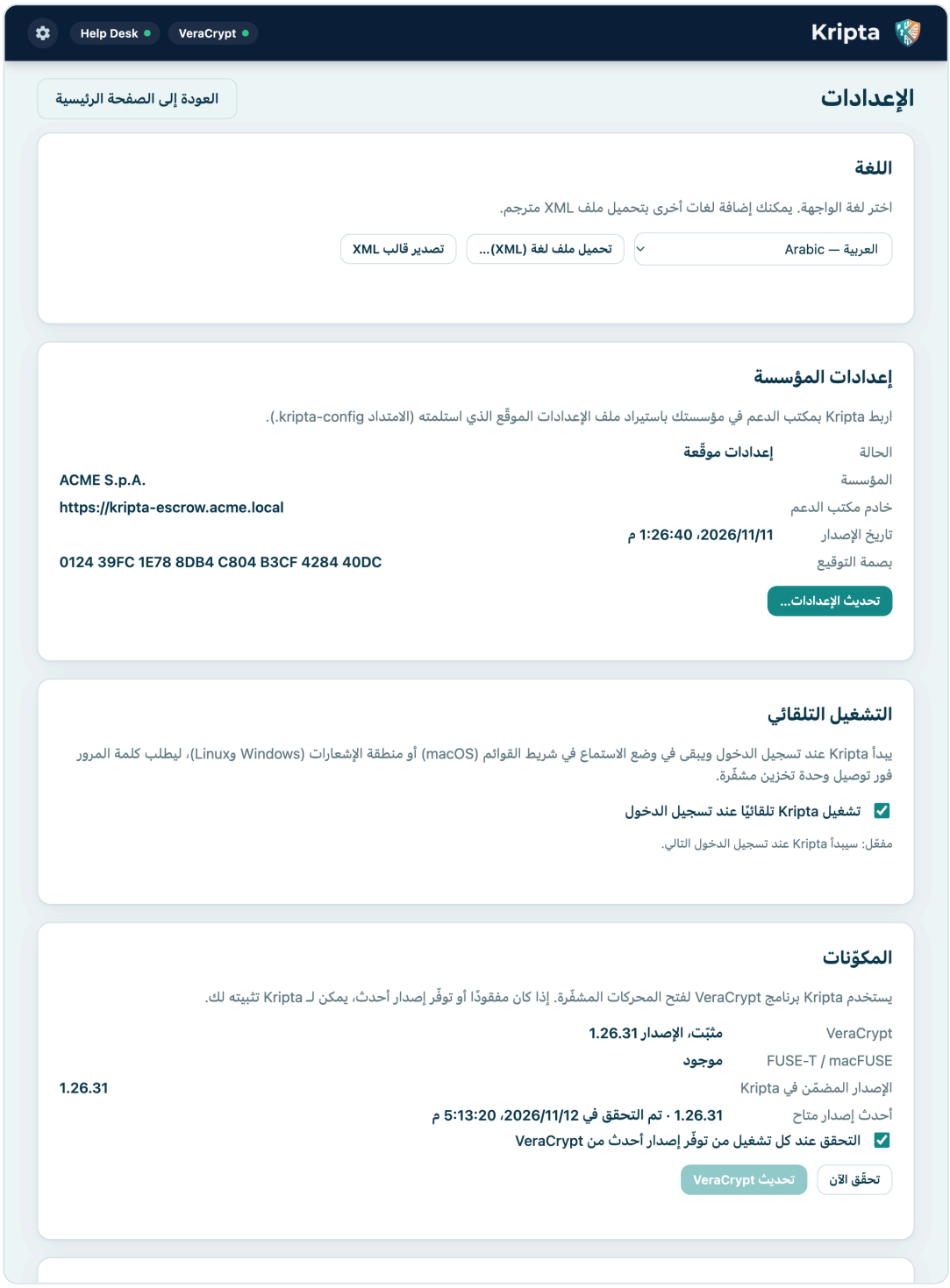
بعد كل عملية استرداد ينشئ Kripta مفتاحًا جديدًا ويرسله إلى مكتب الدعم.

احذر الاحتيال

لن يطلب منك مكتب الدعم كلمة مرورك أبدًا. أنت من يتواصل مع مكتب الدعم وليس العكس.

9 الإعدادات

تُفتح بالترس في الأعلى أو بالخيار **الإعدادات...** في قائمة الأيقونة.



الإعدادات: اللغة وإعدادات المؤسسة والمكوّنات والمعلومات.

اللغة

اختر اللغة من القائمة: تتغير الواجهة وقائمة الأيقونة وطلبات التفويض فورًا. مع **تلقائي** يستخدم Kripta لغة النظام. اللغات المضمّنة:

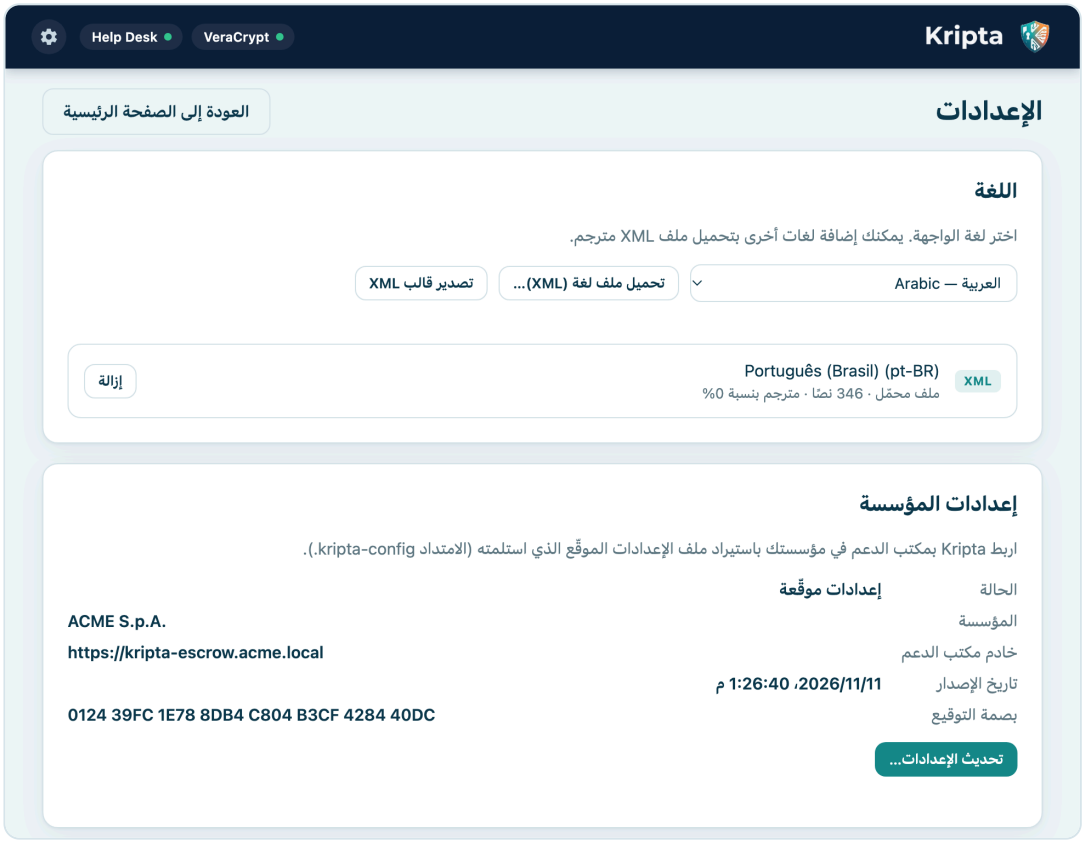
Italiano English Français Español Deutsch Русский العربية 中文 日本語

إضافة لغة

الترجمات ملفات **XML** بسيطة، ملف لكل لغة. لإضافة لغة:

1. اضغط **تصدير قالب XML**: يُحفظ ملف اللغة الحالية في مجلد التنزيلات.
2. ترجم نص كل عنصر `<string>` مع إبقاء السمات `id` والعناصر النائبة `{1}` و `{2}` دون تغيير.
3. في أعلى الملف عيّن `code` (مثل `pt` أو `pt-BR`) و `name` و `english-name` و `dir` (`rtl` للغات التي تُكتب من اليمين إلى اليسار).
4. اضغط **تحميل ملف لغة (XML)...** واختر الملف: تظهر اللغة في القائمة مع نسبة النصوص المترجمة. تُعرض النصوص الناقصة بالإنجليزية.

```
<kripta-language format="1" code="pt" name="Português" english-name="Portuguese" dir="ltr">
  <string id="home.title">Proteja os seus dados</string>
  …
</kripta-language>
```



لغة محمّلة من ملف XML مع زر الإزالة.

تحميل ملف بالرمز نفسه للغة مضمّنة يستبدلها (مفيد لتصحيح مصطلح)؛ ويعيد **إزالة** اللغة الأصلية. توجد ملفات اللغات التسع المضمّنة بجوار هذا الدليل في المجلد `lang`.

إعدادات المؤسسة

تعرض المؤسسة وخادم مكتب الدعم وتاريخ الإعدادات المثبّتة وبصمتها. يستورد **تحديث الإعدادات...** ملفًا جديدًا من مكتب الدعم (الفصل 2).

المكوّنات

تعرض إصدار VeraCrypt المثبّت والإصدار المضمّن في Kripta وأحدث إصدار متاح. يتحقق **تحقّق الآن** فورًا، ويبدأ **تثبيت / تحديث VeraCrypt** التثبيت. ويفعّل مربع **التحقق عند كل تشغيل...** التحقق التلقائي أو يوقفه.

التشغيل التلقائي

خانة **تشغيل Kripta تلقائيًا عند تسجيل الدخول** مفعّلة افتراضيًا. يظهر أسفلها ما إذا كان التشغيل التلقائي مسجّلًا في النظام. إذا ألغيت تفعيلها فلن يكتشف Kripta وحدات التخزين المشفّرة حتى تفتحه.

10 استخدام المحرك على حواسيب أخرى

تستخدم المحركات التي شفّرها Kripta تنسيق **VeraCrypt** القياسي مع نظام الملفات **exFAT**: تُفتح على Windows وmacOS وLinux.

الحاسوب	ما يحدث عند وصل المحرك
مع Kripta مُعدّ	يظهر طلب كلمة المرور: كل شيء تلقائي.
مع Kripta مثبّت لكن **دون إعدادات المؤسسة** (في المنزل مثلاً)	يظهر طلب كلمة المرور رغم ذلك ويُفتح المحرك. إذا كان VeraCrypt مفقودًا، يعرض Kripta `تثبيت الآن` . دون إعدادات لا يمكنك تشفير محركات جديدة ولا استرداد كلمات المرور.
مع VeraCrypt فقط	افتح VeraCrypt، واختر خانة فارغة، ثم **Select Device**، واختر قسم الذاكرة، ثم **Mount** وأدخل كلمة المرور.
دون Kripta ولا VeraCrypt	لا يظهر أي طلب: لا تشغّل أنظمة التشغيل البرامج من ذاكرات USB. قد يعرض النظام **تهيئة** المحرك: **ارفض دائمًا**. ثبّت Kripta (من موقع المؤسسة) وصِل المحرك مجددًا.

صلاحيات المسؤول

يتطلب فتح محرك مشفّر على أي حاسوب صلاحيات المسؤول، لأن VeraCrypt يستخدم برنامج تشغيل للنظام. على حاسوب لا تملك بيانات اعتماده لا يمكن فتح المحرك.

منطقة حرّة للتبادل

إذا كنت تستخدم كثيرًا حواسيب دون Kripta، قسّم الذاكرة بالقالب `منطقة مشفّرة + منطقة حرّة` (الفصل 5): يمكنك نسخ مثبّت Kripta أيضًا إلى المنطقة الحرّة.

11 الرسائل وحل المشكلات

الرسالة أو الحالة	ما يجب فعله
لم يُربط Kripta بعد بمكتب الدعم في مؤسستك	استورد ملف `.kripta-config` الذي استلمته من مكتب الدعم (الفصل 2).
توقيع الحزمة غير صالح	تم تعديل الملف أو أنه تالف: اطلبه مجددًا من مكتب الدعم.
الحزمة موقّعة بمفتاح مختلف / غير معتمد	الملف ليس من مؤسستك. لا تستخدمه وتواصل مع مكتب الدعم.
يدير قسم تقنية المعلومات الإعدادات ولا يمكن استبدالها	الحاسوب مُعدّ مركزيًا: لا حاجة إلى استيراد أي شيء.
محرك التشفير VeraCrypt غير مثبّت	اضغط **تثبيت الآن** . إذا لم يظهر الزر، تواصل مع مكتب الدعم.
التوقيع الرسمي لـ VeraCrypt غير صالح / الملف لا يطابق الإصدار الموقّع	تم العبث بالتنزيل أو أنه غير مكتمل: أُلغي التثبيت. أعد المحاولة لاحقًا.
اقفل جميع المحركات المشفّرة قبل تحديث VeraCrypt	اضغط **قفل** على المحركات المفتوحة، ثم كرّر التحديث.
أعد تشغيل الحاسوب لإكمال التحديث (Windows)	احفظ عملك وأعد التشغيل.
تعذّر الوصول إلى خادم مكتب الدعم. لم يبدأ التشفير.	اتصل بشبكة المؤسسة أو VPN وأعد المحاولة. لم تتأثر البيانات على المحرك.
مفاتيح استرداد بانتظار الإرسال	اتصل بالشبكة واضغط **أعد المحاولة الآن** . أبقِ Kripta مفتوحًا حتى يختفي التنبيه.
لا يوجد محرك أقراص متاح	أعد وصل الذاكرة (جرّب منفذ USB آخر) واضغط **تحديث القائمة** .
تم إلغاء تفويض المسؤول / انتهت المهلة	كرّر العملية وأكّد طلب النظام.
تعذّر فصل المجلد / قفله	أغلق المستندات والنوافذ المفتوحة من المحرك، ثم أعد المحاولة.
كلمة المرور غير صحيحة	تحقق من مفتاح Caps Lock ومن تخطيط لوحة المفاتيح. إذا نسيتها، انظر الفصل 8.
مفتاح الاسترداد غير صحيح	راجع الأرقام مع الموظف: يلزم **أحدث** مفتاح.
يحتوي القرص على محرك Kripta مفتوح	اقفله من الشاشة الرئيسية، ثم كرّر التقسيم.
لم يكتشف النظام الأقسام الجديدة	افصل المحرك ثم صِله مجددًا .
ملف اللغة ليس XML صالحًا / عنصر غير مسموح	صحّح الملف المذكور في الرسالة: يُسمح فقط بعناصر `<string>` ذات نص عادي.
لا تظهر نافذة فتح القفل عند الوصل	تحقق من أن Kripta يعمل (الأيقونة في الشريط) واستخدم **فتح القفل** من النافذة الرئيسية.

12 الأسئلة الشائعة

هل يمكنني تشفير ذاكرة تحتوي على ملفات دون فقدانها؟

لا. يمحو التشفير المحرك. انسخ الملفات إلى مكان آخر، وشفّر المحرك، ثم أعد نسخها.

هل يمكنني تشفير القرص الداخلي لحاسوبي؟

لا. صُمّم Kripta للذاكرات والأقراص الخارجية، ولا تُعرض أقراص النظام.

هل يستطيع مكتب الدعم قراءة ملفاتي؟

يحتفظ مكتب الدعم بمفتاح الاسترداد فقط، ولا يمكنه الاطلاع عليه إلا بطلب منك، مع تسجيل كل اطلاع.

هل يجب أن أدوّن مفتاح الاسترداد؟

لا. لا تراه أبدًا ولا تحتاج إلى الاحتفاظ به: إنه محفوظ لدى مكتب الدعم.

هل يثبّت Kripta برامج على حاسوبي؟

فقط VeraCrypt (وFUSE-T على macOS)، بعد تأكيدك وفقط إذا كان التوقيع الرسمي للمطورين صالحًا.

هل يمكنني استخدام الذاكرة على حاسوب منزلي؟

نعم، بتثبيت Kripta أو VeraCrypt (الفصل 10). التزم دائمًا بقواعد المؤسسة بشأن استخدام البيانات خارج مقر العمل.

اللغة التي أحتاج إليها غير موجودة. ماذا أفعل؟

يمكنك ترجمة قالب XML وتحميله من الإعدادات (الفصل 9)، أو طلب توزيع ترجمة من قسم تقنية المعلومات.

لماذا لا يمكنني استخدام الأحرف العربية أو المشكّلة في كلمة المرور؟

قد ترمّزها أنظمة Windows وmacOS وLinux بطرق مختلفة: قد لا تُقبل كلمة المرور نفسها عند كتابتها على نظام آخر.

كم من المساحة يستهلك التشفير؟

القليل جدًا: بضع مئات من الكيلوبايتات لترويسات المجلد.

A ملحق لقسم تقنية المعلومات

الحزم

النظام	الحزمة	ملاحظات
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	تحتوي على ملفات MSI الرسمية لـ VeraCrypt (x64 وARM64). يبدأ التطبيق بصلاحيات المسؤول.
macOS 11+	`Kripta_1.2.0_universal.dmg`	تحتوي على VeraCrypt (إصدارا FUSE-T وmacFUSE) وFUSE-T الذي لا يحتاج إلى امتدادات للنواة.
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	تحتوي على VeraCrypt لـ Ubuntu 22.04/24.04 وDebian 12/13؛ للإصدارات الأخرى ينزّل Kripta الحزمة الموثّقة.
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	تحتوي على VeraCrypt لـ Fedora 44؛ ثبّت أيضًا `exfatprogs`.
توزيعات أخرى	`Kripta_1.2.0_amd64.AppImage`	ملف تنفيذي محمول.

الإعدادات الموقّعة

على خادم escrow أنشئ مفتاح التوقيع مرة واحدة، ثم وقّع إعدادات العميل (القالب في `deploy/client/kripta.toml.example`):

```
kripta-escrow keygen-sign           # private key (keep offline) + public key + fingerprint
kripta-escrow sign-config client.toml signing.key "ACME" acme.kripta-config
```

وزّع `acme.kripta-config` على المستخدمين وانشر **البصمة** عبر قناة موثوقة (الشبكة الداخلية، هاتف مكتب الدعم). يحفظ Kripta الإعدادات في موقع النظام (`%ProgramData%\Kripta` و`/Library/Application Support/Kripta` و`/etc/kripta`) عبر العملية ذات الصلاحيات، مع مفتاح الموقّع: يجب أن تحمل التحديثات اللاحقة التوقيع نفسه. لتجنّب الاعتماد على تحقق المستخدم من البصمة، ابنِ Kripta مع `KRIPTA_PROVISIONING_KEYS=<public key>`: لن تُقبل إلا تلك المفاتيح. لا يمكن استبدال إعدادات نسخها قسم تقنية المعلومات يدويًا (دون توقيع) بحزمة.

تثبيت VeraCrypt وتحديثه

- تُجهَّز المثبّتات المضمّنة عند البناء باستخدام `scripts/fetch-veracrypt.py`.
- قبل التثبيت تتحقق العملية ذات الصلاحيات من توقيع OpenPGP لقائمة SHA-256 الرسمية بمفتاح IDRIX المضمّن (البصمة `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`) ومن تجزئة الملف.
- خيارات في `kripta.toml`: يوقف `veracrypt_update_check = false` التحقق من التحديثات؛ ويستخدم `veracrypt_release_api = "https://mirror.internal/…"` مرآة داخلية بتنسيق واجهة GitHub نفسه.

اللغات

توجد ملفات XML للغات في `app/ui/lang/` (مضمّنة في التطبيق) وفي `docs/manuale/lang/`. تُحفظ اللغات التي يحمّلها المستخدمون في مجلد بيانات المستخدم (`languages/`). لتوزيع لغة جديدة على الجميع، أضف الملف إلى `app/ui/lang/` ورمزها إلى القائمة في `app/ui/i18n.js`.

مكوّنات اختيارية

- **التشغيل عند تسجيل الدخول** في شريط القوائم / منطقة الإشعارات (`kripta --background`): **تلقائي**. يسجّله Kripta عند كل تشغيل (macOS: `~/Library/LaunchAgents/com.kripta.agent.plist` مع إعادة التشغيل عند التوقف غير الطبيعي؛ Windows: مهمة مجدولة «Kripta» عند تسجيل الدخول بأعلى الصلاحيات، ينشئها المثبّت أيضًا وتُحذف عند إلغاء التثبيت؛ Linux: `/etc/xdg/autostart/kripta.desktop` من حزم .deb/.rpm و`~/.config/autostart/kripta.desktop` لـ AppImage). يمكن إيقافه من الإعدادات.
- **المساعد ذو الصلاحيات** كخدمة (دون طلبات كلمة مرور): `deploy/macos/com.kripta.helper.plist` و`deploy/linux/kripta-helper.service`.