Kripta

Manuel utilisateur

Chiffrement guidé des clés USB et des partitions, avec récupération du mot de passe via le Help Desk de l'entreprise.



Version 1.2 · Windows · macOS · Linux

Novembre 2026

Sommaire

1 Qu'est-ce que Kripta — à quoi il sert, ce qu'il vous faut

2 Premier démarrage — configuration de l'entreprise et composants

3 La fenêtre principale — indicateurs, alertes, icône

4 Chiffrer un lecteur — l'assistant en 4 étapes

5 Diviser un disque en partitions — zone chiffrée et zone libre

6 Utiliser un lecteur chiffré — déverrouiller, ouvrir, verrouiller

7 Changer le mot de passe

8 J'ai oublié le mot de passe — récupération avec le Help Desk

9 Paramètres — langue, configuration, mises à jour

10 Utiliser le lecteur sur d'autres ordinateurs

11 Messages et résolution des problèmes

12 Questions fréquentes

A Annexe pour l'informatique — paquets, configuration signée, langues

Conventions

Les textes affichés à l'écran (boutons, titres, éléments) sont écrits ainsi : **Chiffrer un lecteur**. Les captures proviennent de la version macOS : sous Windows et Linux la fenêtre est identique, seuls les noms des périphériques changent (par exemple `E:` ou `/dev/sdb1` au lieu de `/dev/disk4s1`).

1 Qu'est-ce que Kripta

Kripta protège les données de vos **clés USB** et des **partitions** de disques externes par un chiffrement AES-256. Après le chiffrement, le contenu du lecteur n'est lisible que par qui connaît le mot de passe : si vous perdez la clé, personne d'autre ne peut l'ouvrir.

Chiffrement guidé
Quatre étapes : choisir le lecteur, choisir le mot de passe, confirmer, patienter.

Déverrouillage automatique
Lorsque vous branchez un lecteur chiffré, Kripta demande aussitôt le mot de passe et l'ouvre.

Fonctionne partout
La même clé s'ouvre sous Windows, macOS et Linux (format standard VeraCrypt).

Installation autonome
Kripta installe et met à jour VeraCrypt tout seul ; la configuration de l'entreprise s'importe depuis un fichier.

Neuf langues
Italien, anglais, français, espagnol, allemand, russe, arabe, chinois et japonais, plus celles que vous ajoutez.

Récupération avec le Help Desk
Si vous oubliez le mot de passe, le Help Desk vous aide à en définir un nouveau sans perdre de données.

Ce qu'il vous faut

- **Kripta** installé sur l'ordinateur. Au premier démarrage, Kripta installe lui-même **VeraCrypt**, le moteur de chiffrement (sous macOS aussi **FUSE-T**), s'il manque : chapitre 2.
- Le **fichier de configuration signé** (`.kripta-config`) reçu du Help Desk, si l'informatique n'a pas déjà configuré l'ordinateur.
- Une **connexion au réseau de l'entreprise** (ou VPN) lorsque vous chiffrez un nouveau lecteur : la clé de récupération est envoyée immédiatement au Help Desk. Pour déverrouiller un lecteur déjà chiffré, le réseau n'est pas nécessaire.
- Les **identifiants administrateur** de l'ordinateur, lorsque le système les demande (voir encadré).

> **Demandes d'autorisation**
> Pour lire et écrire directement sur le lecteur, installer des composants et enregistrer la configuration, Kripta a besoin des droits d'administrateur. Sous **Windows**, la fenêtre du Contrôle de compte d'utilisateur apparaît au démarrage. Sous **macOS** et **Linux** apparaît le message « Kripta a besoin de l'autorisation d'un administrateur pour terminer l'opération ». Si l'informatique a installé le service système de Kripta, ces demandes n'apparaissent pas.

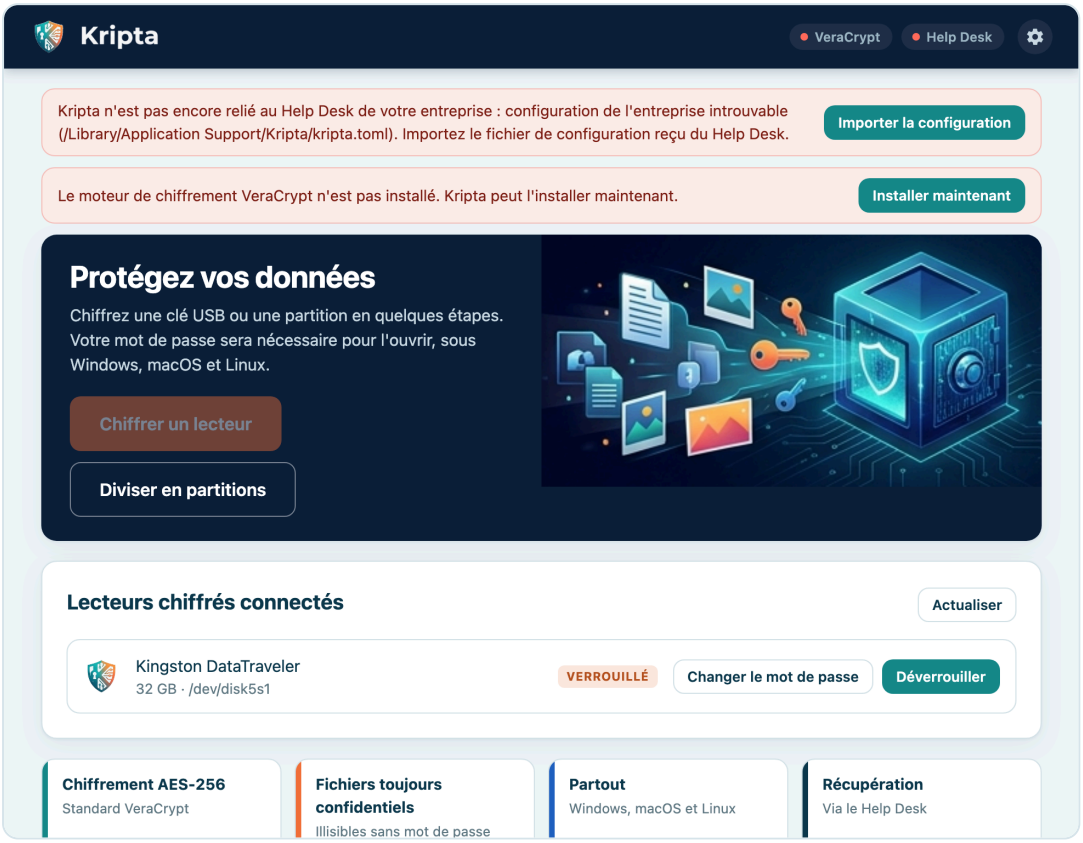
La récupération en bref

Pendant le chiffrement, Kripta génère une **clé de récupération** de 48 chiffres, la protège et l'envoie à l'archive du Help Desk. Vous n'avez ni à la voir ni à la conserver. Seuls les opérateurs du Help Desk

peuvent la consulter, après avoir vérifié votre identité, et chaque consultation est journalisée.

2 Premier démarrage

Au premier démarrage, Kripta vérifie deux choses : s'il est relié au Help Desk de votre entreprise et si VeraCrypt est présent sur l'ordinateur. S'il manque quelque chose, une alerte avec un bouton pour y remédier apparaît en haut de la fenêtre. Vous pouvez tout faire vous-même.

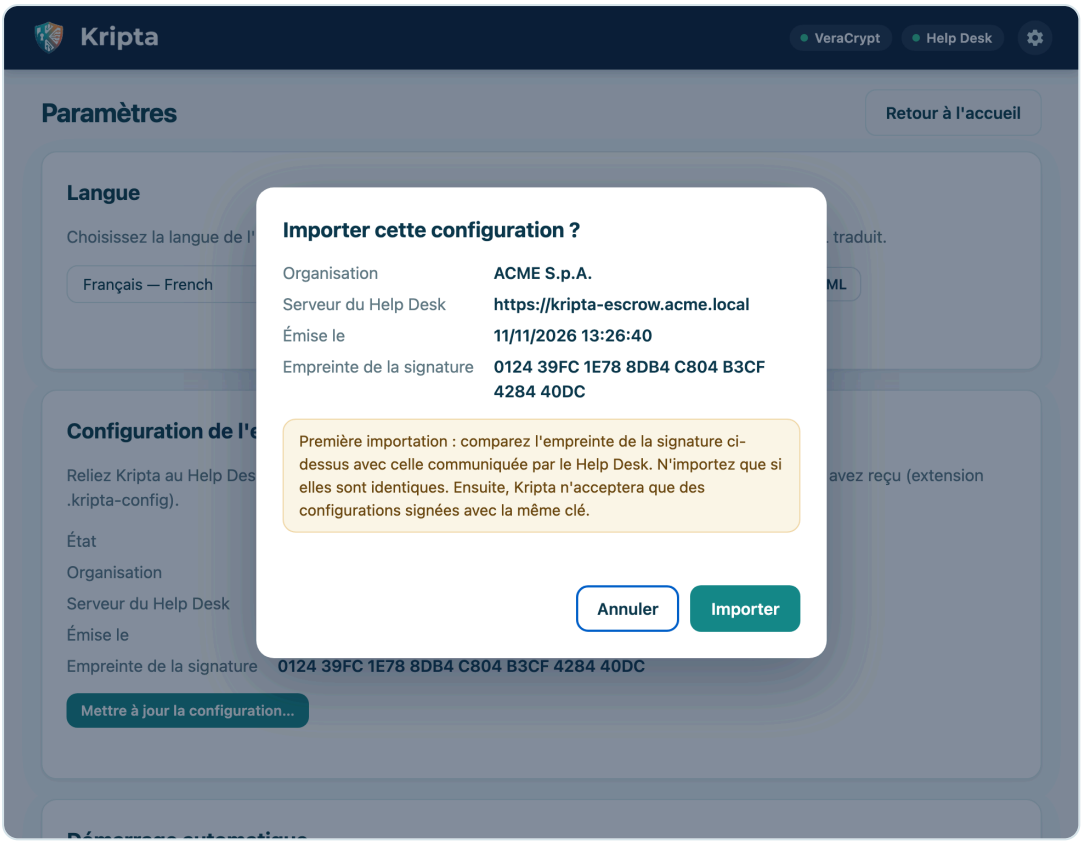


Premier démarrage : configuration à importer et VeraCrypt à installer.

Importer la configuration de l'entreprise

La configuration indique à Kripta à quelle archive du Help Desk envoyer les clés de récupération. Le Help Desk vous la fournit sous forme de fichier avec l'extension `.kripta-config`, signé numériquement : personne ne peut le modifier sans que Kripta s'en aperçoive.

1. Enregistrez sur l'ordinateur le fichier reçu (par e-mail, depuis le portail de l'entreprise ou sur une clé).
2. Appuyez sur **Importer la configuration** dans l'alerte, ou ouvrez les **Paramètres** (l'engrenage en haut à droite) et appuyez sur **Importer une configuration signée…**.
3. Choisissez le fichier. Kripta vérifie sa signature et affiche l'organisation, le serveur du Help Desk, la date d'émission et l'**empreinte de la signature**.
4. Lors de la première importation, **comparez l'empreinte** avec celle communiquée par le Help Desk (par téléphone, sur l'intranet…). Si elle correspond, appuyez sur **Importer**.
5. Confirmez la demande d'autorisation du système. **Configuration importée** apparaît et l'indicateur **Help Desk** devient vert.

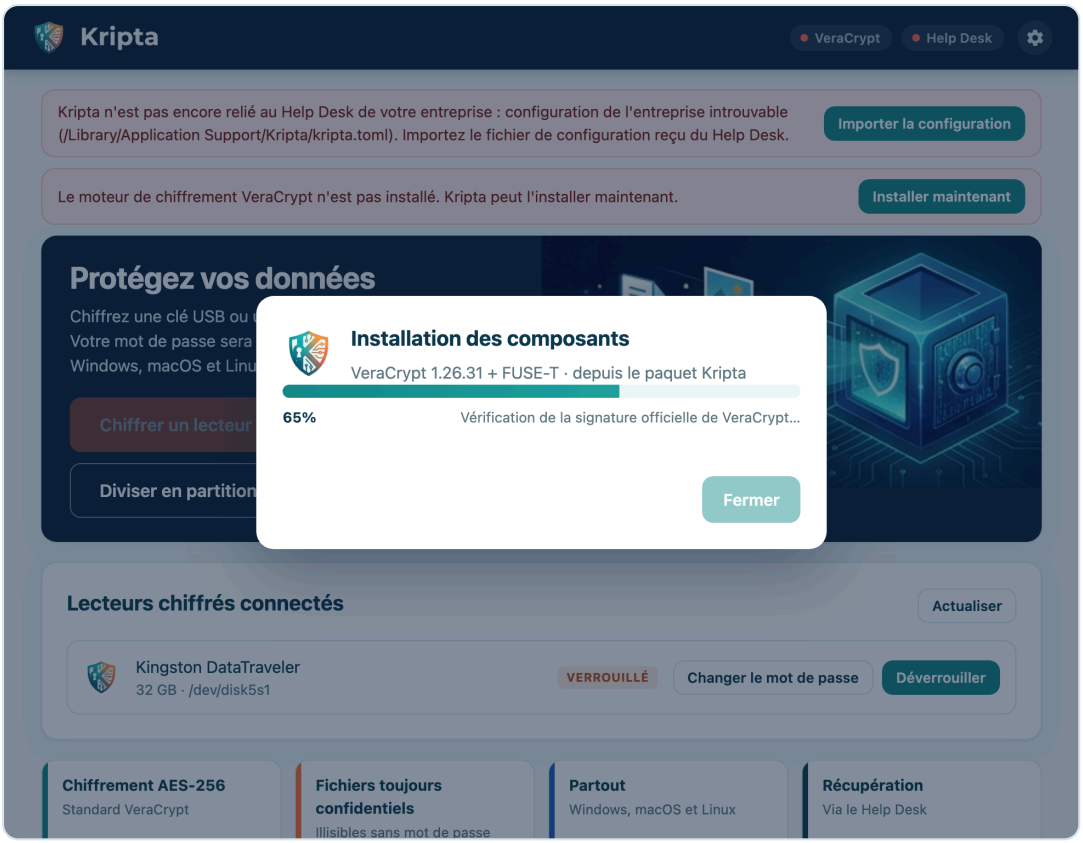


Confirmation de l'importation avec l'empreinte de la signature.

> **Si l'empreinte ne correspond pas, n'importez pas**
>
> Le fichier pourrait ne pas provenir de votre entreprise. Annulez et contactez le Help Desk. Après la première importation, Kripta n'accepte que les mises à jour signées avec la même clé : un faux fichier est refusé automatiquement.

Installer VeraCrypt

Kripta contient déjà le programme d'installation officiel de VeraCrypt (et de FUSE-T pour macOS). Appuyez sur **Installer maintenant** dans l'alerte et confirmez la demande d'autorisation : Kripta vérifie la signature officielle des programmes d'installation et les installe sans autre question.

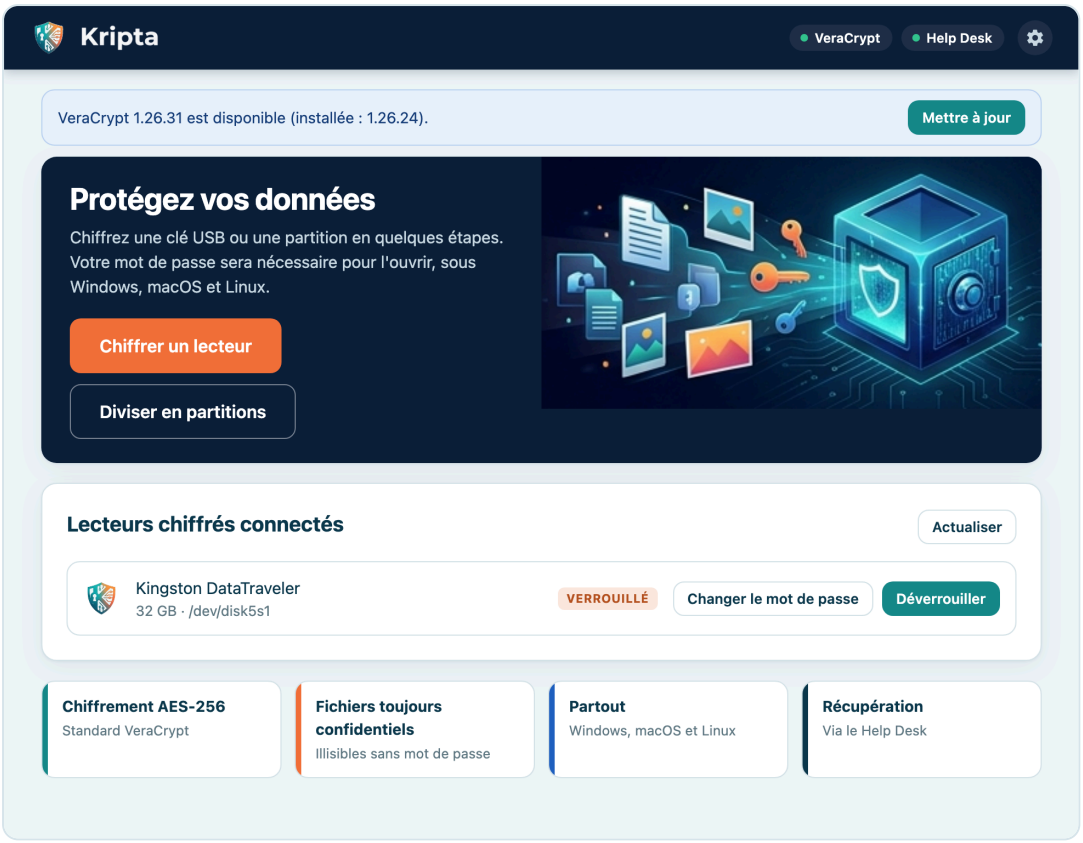


Installation des composants avec vérification de la signature officielle.

À la fin apparaît **Installation terminée**. Sous Windows, un redémarrage peut être demandé.

Mises à jour de VeraCrypt

À chaque démarrage (puis une fois par jour), Kripta vérifie si une version plus récente de VeraCrypt est sortie. Si oui, une alerte bleue apparaît avec le bouton **Mettre à jour**. La nouvelle version est téléchargée depuis le site officiel et installée uniquement si la signature des développeurs de VeraCrypt est valide.



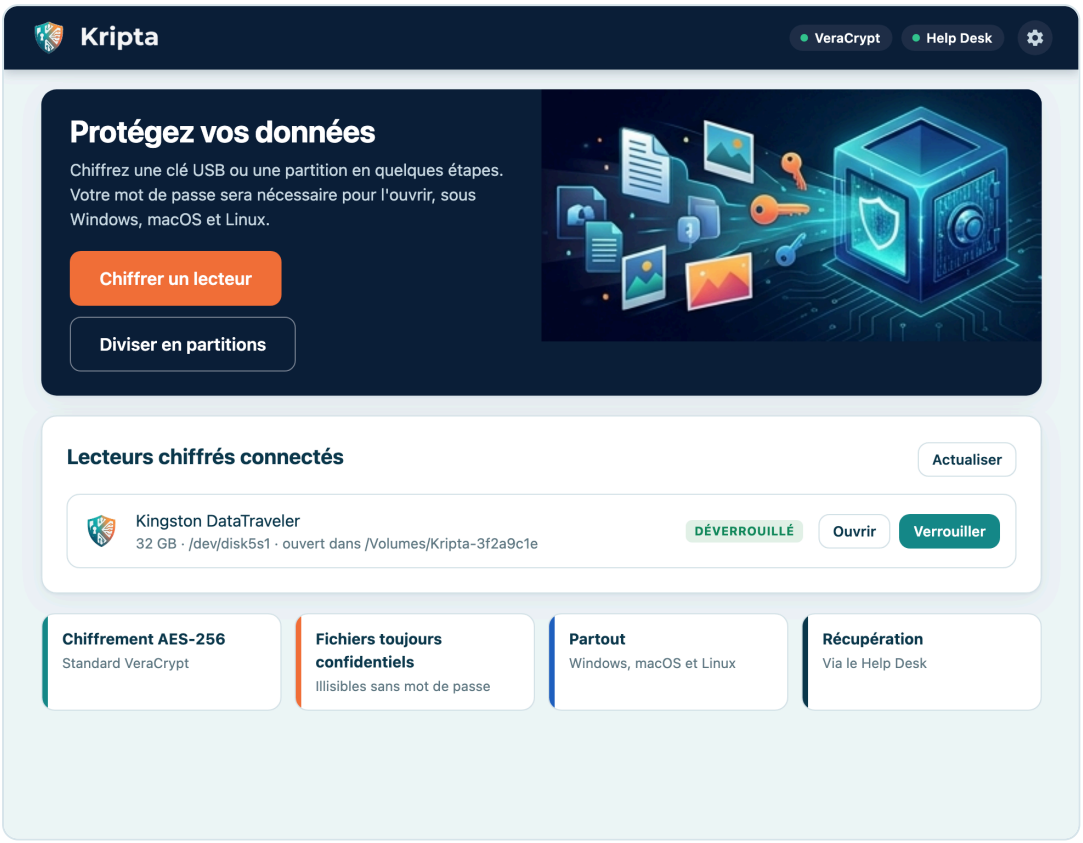
Mise à jour de VeraCrypt disponible.

Avant de mettre à jour

Verrouillez tous les lecteurs chiffrés ouverts : Kripta ne met pas VeraCrypt à jour tant qu'un lecteur est déverrouillé. Vous pouvez désactiver la vérification automatique dans les Paramètres (chapitre 9).

3 La fenêtre principale

À l'ouverture, Kripta affiche l'écran d'accueil. Vous pouvez y chiffrer un nouveau lecteur et gérer les lecteurs chiffrés connectés à l'ordinateur.

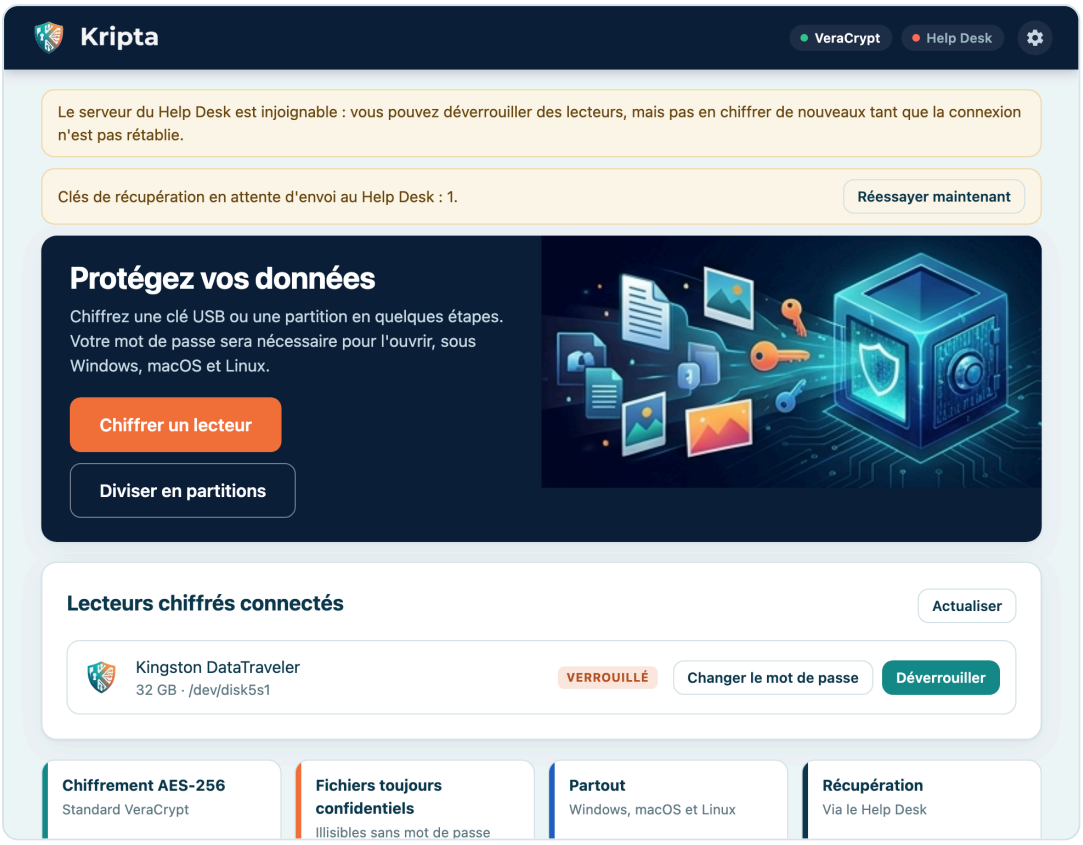


Écran d'accueil avec un lecteur chiffré connecté et déverrouillé.

Élément	À quoi il sert
VeraCrypt	Point **vert** : le moteur de chiffrement est installé. **Rouge** : il ne l'est pas (chapitre 2). Au survol, la version s'affiche.
Help Desk	Vert : l'archive des clés est joignable. Rouge : elle ne l'est pas (pas de réseau, VPN éteint, configuration manquante).
Engrenage	Ouvre les **Paramètres** : langue, configuration de l'entreprise, composants (chapitre 9).
Chiffrer un lecteur	Lance l'assistant (chapitre 4). Désactivé si Kripta n'est pas configuré ou si VeraCrypt manque.
Diviser en partitions	Divise une clé USB ou un disque externe en plusieurs partitions (chapitre 5).
Lecteurs chiffrés connectés	Les lecteurs Kripta connectés, avec l'état **Verrouillé** ou **Déverrouillé** et leurs boutons.

Alertes

Des encadrés colorés avec un bouton pour résoudre le problème peuvent apparaître en haut de la fenêtre :



Serveur du Help Desk injoignable et une clé de récupération en attente d'envoi.

- **Serveur du Help Desk injoignable :** vous pouvez toujours déverrouiller les lecteurs, mais pas en chiffrer de nouveaux.
- **Clés de récupération en attente d'envoi :** Kripta réessaie tout seul ; appuyez sur `Réessayer maintenant` une fois de retour en ligne. **Laissez Kripta ouvert jusqu'à la disparition de l'alerte.**
- **Kripta n'est pas encore relié au Help Desk / VeraCrypt n'est pas installé / VeraCrypt … est disponible :** voir chapitre 2.

L'icône de Kripta : barre des menus et zone de notification

Kripta fonctionne en arrière-plan pour détecter le branchement d'un lecteur chiffré ; il se pilote depuis une icône avec l'emblème :

Système	Emplacement de l'icône	À savoir
macOS	Dans la **barre des menus** en haut à droite. Kripta **n'apparaît pas dans le Dock**.	Sur les MacBook à encoche, les icônes en trop sont masquées si la barre est pleine : retirez celles que vous n'utilisez pas ou déplacez-les en maintenant ⌘.
Windows	Dans la **zone de notification** en bas à droite, près de l'horloge.	Si elle est parmi les icônes masquées, cliquez sur la flèche ^ et faites glisser l'emblème sur la barre.

Système	Emplacement de l'icône	À savoir
Linux	Dans la **zone de notification** du panneau.	Sous GNOME « pur » (Fedora, Debian), l'extension **AppIndicator and KStatusNotifierItem Support** est nécessaire.

Le menu de l'icône contient **Ouvrir Kripta**, **Chiffrer un lecteur…**, **Diviser en partitions…**, **Verrouiller tous les lecteurs**, **Paramètres…** et **Quitter Kripta**. Les éléments suivent la langue choisie.

> **Fermer la fenêtre ne quitte pas Kripta**
> Kripta reste actif dans la barre des menus ou la zone de notification. Pour rouvrir la fenêtre, utilisez **Ouvrir Kripta** ou relancez Kripta : la fenêtre déjà active s'affiche.

Démarrage automatique

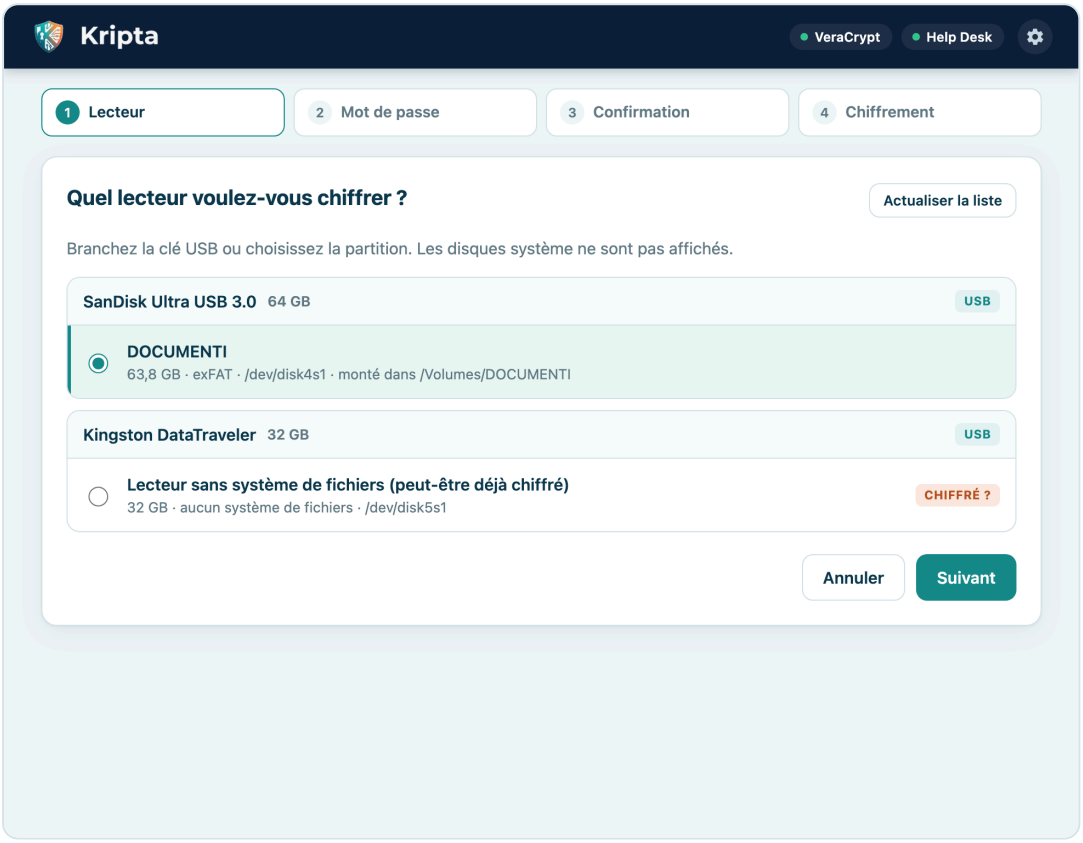
Après l'installation, Kripta **démarre tout seul à chaque ouverture de session**, sans ouvrir la fenêtre, et reste toujours à l'écoute : dès que vous branchez un lecteur chiffré, il vous demande le mot de passe. Vous pouvez le désactiver dans **Réglages › Démarrage automatique** (chapitre 9). **Quitter Kripta** le ferme jusqu'à la prochaine ouverture de session.

4 Chiffrer un lecteur

> **Le chiffrement efface tout le contenu du lecteur.**
> Avant de commencer, copiez ailleurs les fichiers à conserver. Après le chiffrement, vous pourrez les recopier sur le lecteur protégé.

Branchez la clé, vérifiez que l'indicateur **Help Desk** est vert et appuyez sur **Chiffrer un lecteur**.

Étape 1 — Lecteur

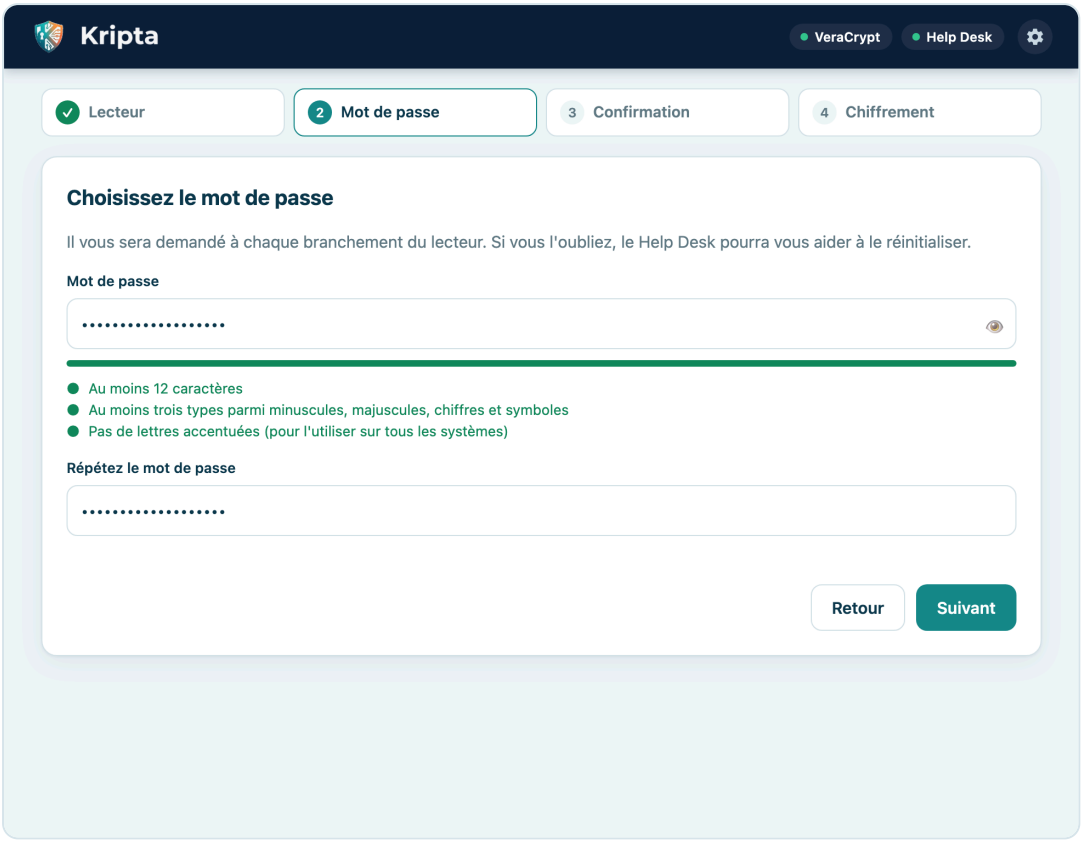


Choix du lecteur à chiffrer.

1. Kripta liste les périphériques connectés, les amovibles en premier. Les **disques système ne sont jamais affichés**.
2. Vérifiez attentivement la **capacité et le nom** pour être sûr de choisir le bon lecteur.
3. Si la clé n'apparaît pas, rebranchez-la et appuyez sur **Actualiser la liste**.
4. Sélectionnez le lecteur et appuyez sur **Suivant**.

> **Étiquette « Chiffré ? »**
> Elle signale un lecteur sans système de fichiers reconnaissable : il est probablement déjà chiffré. Si vous le chiffrez à nouveau, son contenu actuel sera perdu.

Étape 2 — Mot de passe

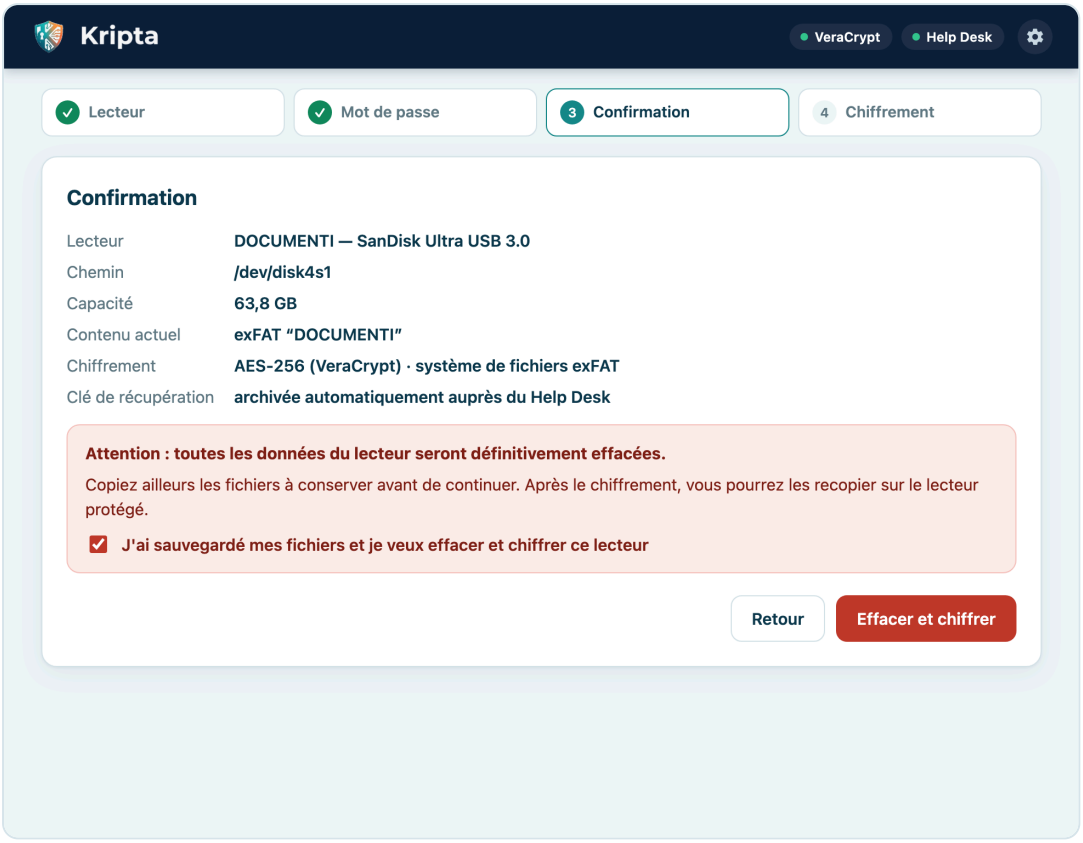


Les règles deviennent vertes au fur et à mesure qu'elles sont respectées.

Le mot de passe doit comporter **au moins 12 caractères**, **au moins trois types** parmi minuscules, majuscules, chiffres et symboles, et **aucune lettre accentuée** (à, è, ü…), que d'autres systèmes pourraient saisir différemment. La barre colorée indique la robustesse ; le bouton 👁 affiche le mot de passe. Répétez-le dans le second champ et appuyez sur **Suivant**.

> **Conseil**
> Une phrase de plusieurs mots reliés par des symboles et des chiffres (par exemple `Train-Lac-Vert-47`) est sûre et facile à retenir. N'utilisez pas le mot de passe de votre compte professionnel.

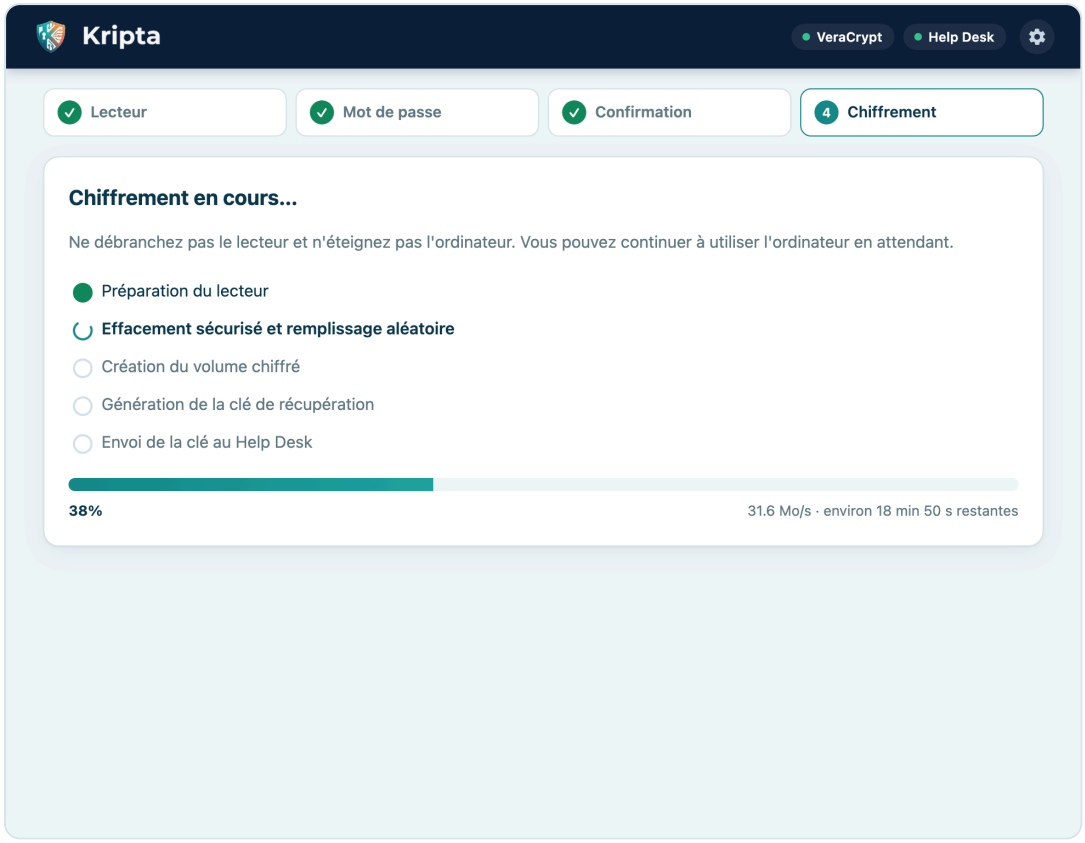
Étape 3 — Confirmation



Récapitulatif et confirmation de l'effacement.

Vérifiez le récapitulatif, cochez **J'ai sauvegardé mes fichiers et je veux effacer et chiffrer ce lecteur** et appuyez sur **Effacer et chiffrer**. Le système peut demander l'autorisation d'un administrateur.

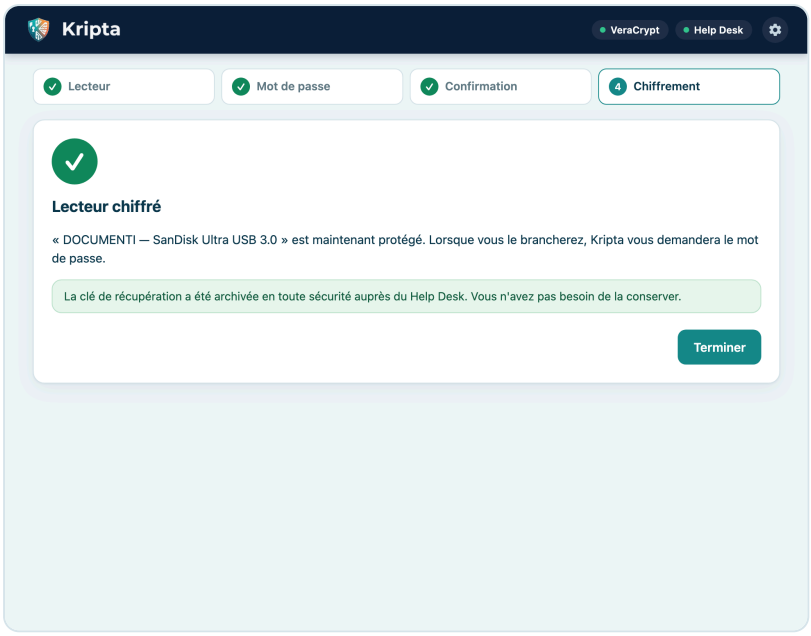
Étape 4 — Chiffrement



Progression avec vitesse et temps restant.

Kripta prépare le lecteur, le réécrit entièrement avec des données aléatoires (la phase la plus longue), crée le volume chiffré exFAT, génère la clé de récupération et l'envoie au Help Desk.

> **Pendant le chiffrement**
> Ne débranchez pas le lecteur et n'éteignez pas ni ne mettez en veille l'ordinateur. Une clé de 64 Go demande environ 15 minutes à une heure.



Chiffrement terminé.

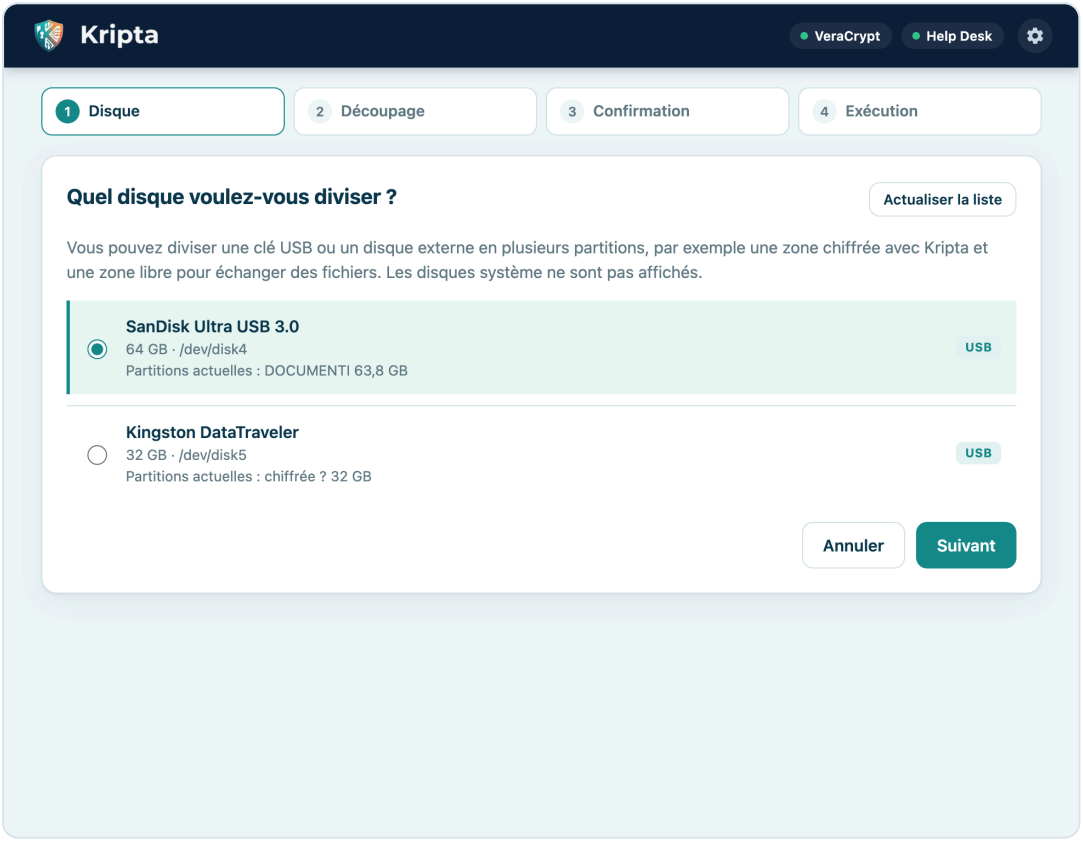
Si **la clé de récupération n'a pas encore été envoyée** apparaît, le lecteur est quand même chiffré et utilisable : laissez Kripta ouvert et connecté, il enverra la clé dès que possible. Si le chiffrement échoue, le message en explique la raison (chapitre 11).

5 Diviser un disque en partitions

Avec **Diviser en partitions**, vous divisez une clé USB ou un disque externe en plusieurs parties indépendantes, chacune avec son nom et son système de fichiers. L'usage typique : une **zone chiffrée** pour les données confidentielles et une **zone libre** pour échanger des fichiers avec des ordinateurs sans Kripta.

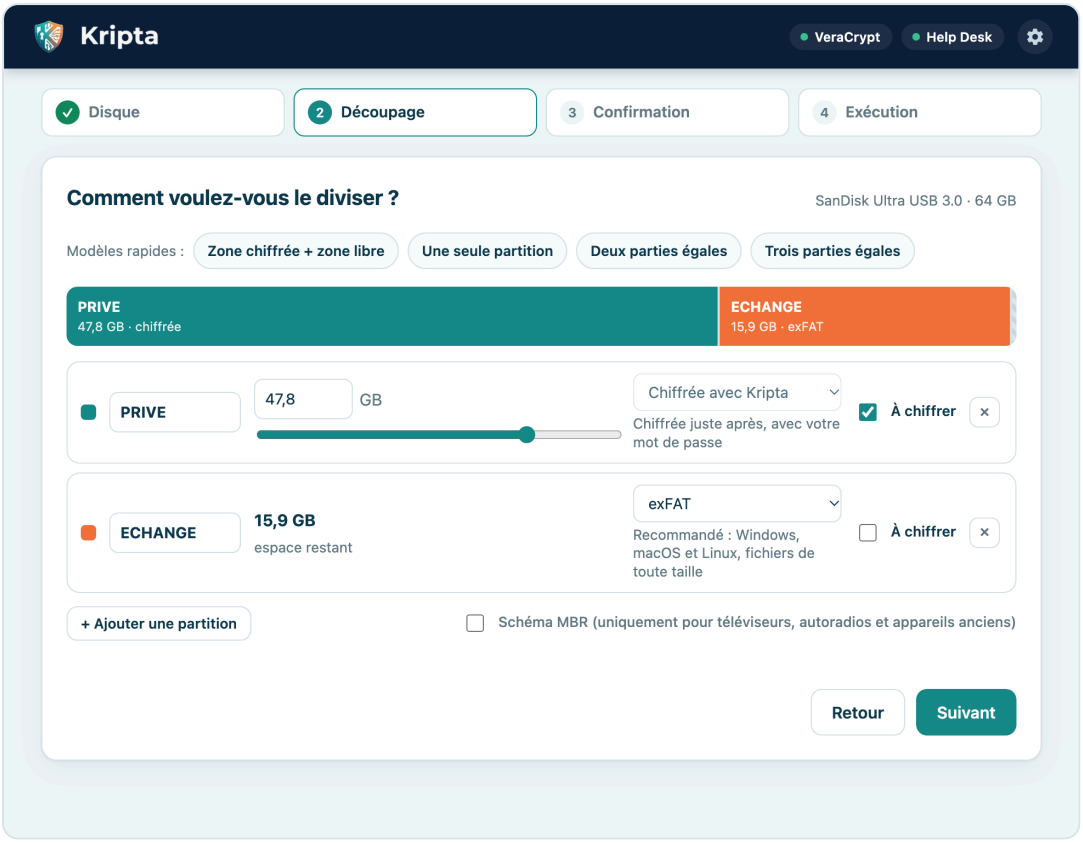
> **La division efface tout le disque**
> , y compris les partitions existantes et les lecteurs déjà chiffrés. Sauvegardez ailleurs les fichiers à conserver.

Étape 1 — Disque



Choix du disque, avec ses partitions actuelles.

Étape 2 — Découpage



La barre colorée montre le découpage en proportion.

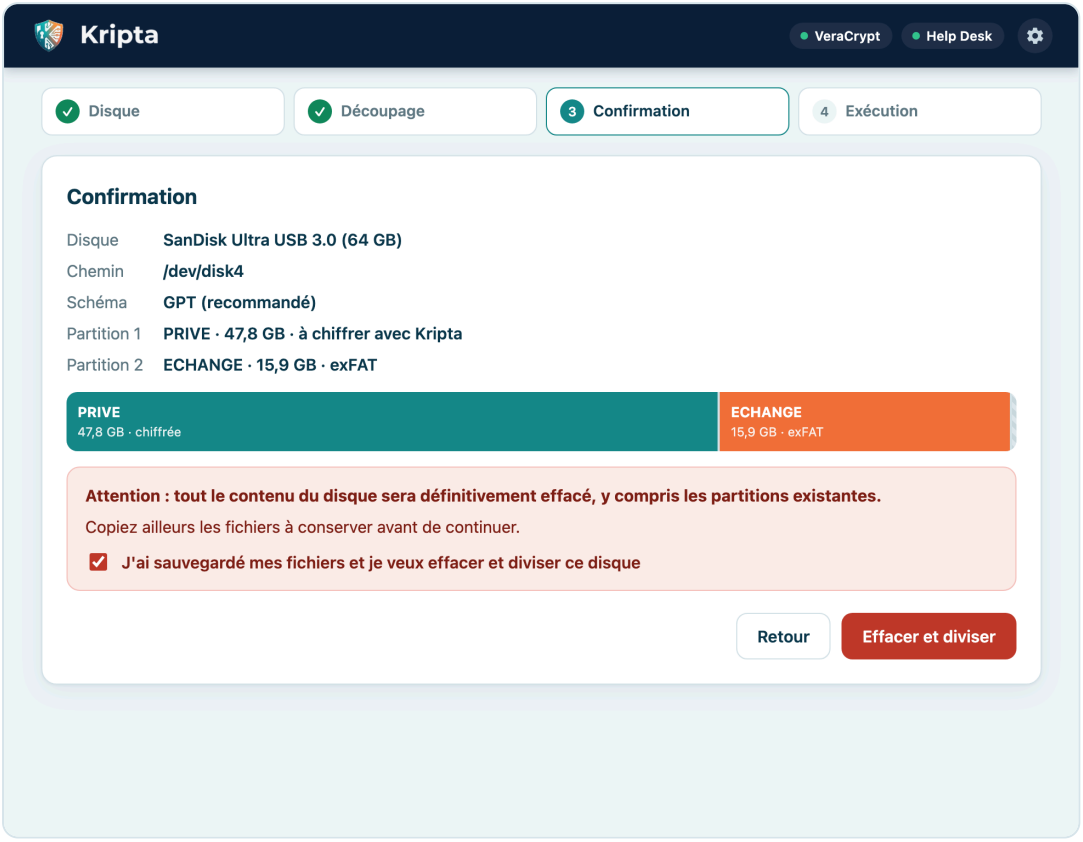
Modèle	Résultat
Zone chiffrée + zone libre	Trois quarts du disque à chiffrer et le reste libre en exFAT. C'est le modèle proposé au départ.
Une seule partition	Tout le disque en une seule partition.
Deux / Trois parties égales	Le disque divisé en parties de même taille.

Pour chaque partition, vous définissez le **nom** (jusqu'à 11 caractères : lettres, chiffres, `_` et `-`), la **taille** (la dernière occupe l'espace restant), le **système de fichiers** et **À chiffrer**. **+ Ajouter une partition** en ajoute une autre (jusqu'à 8).

Système de fichiers	S'ouvre sous	Remarques
exFAT (recommandé)	Windows, macOS, Linux	Pas de limite pratique sur la taille des fichiers.
FAT32	Presque tous les appareils	Fichiers jusqu'à 4 Go ; sous Windows, partition jusqu'à 32 Go.
NTFS	Windows ; macOS en lecture seule	Sous Linux, nécessite `ntfs-3g`.
APFS, **Mac OS étendu**	Mac uniquement	Disponibles uniquement depuis un Mac.
ext4	Linux uniquement	Disponible uniquement depuis Linux.

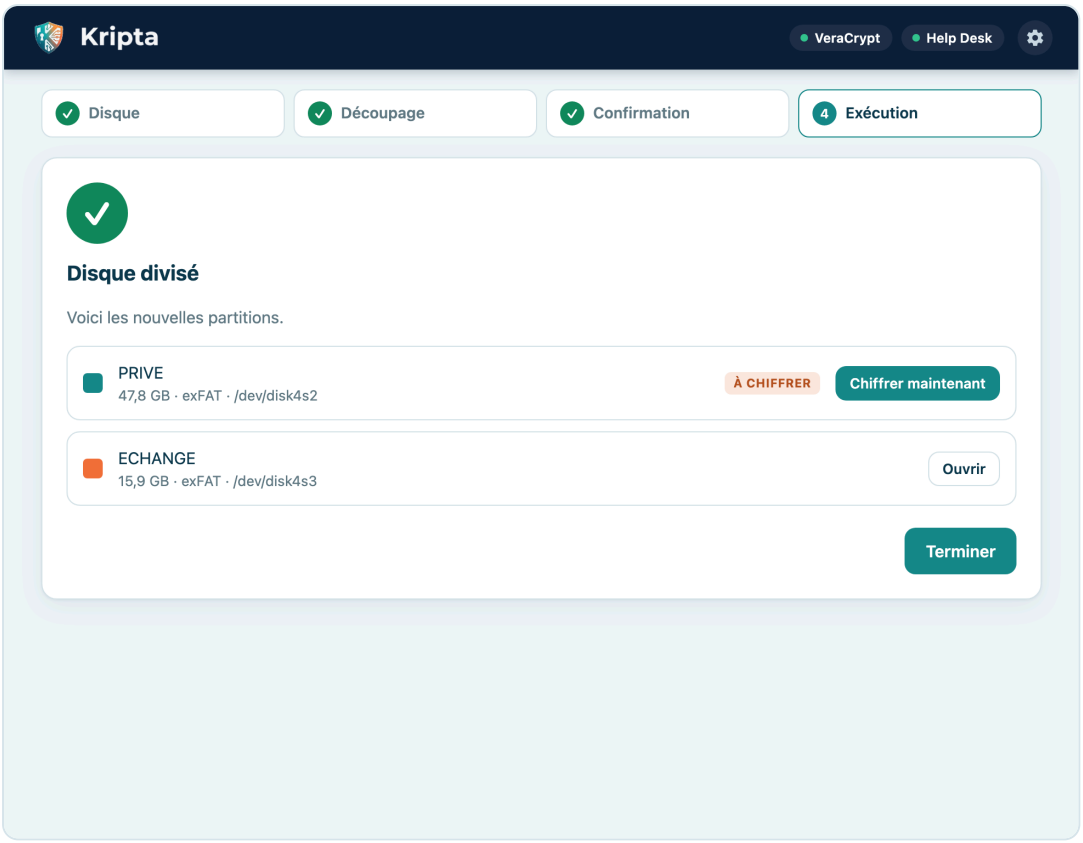
> **Schéma MBR**
> Activez-le uniquement si la clé doit fonctionner avec des téléviseurs, autoradios ou ordinateurs très anciens : 4 partitions et 2 To au maximum.

Étape 3 — Confirmation et étape 4 — Exécution



Récapitulatif avant l'effacement.

Cochez la case de confirmation et appuyez sur **Effacer et diviser**. En général, moins d'une minute suffit.



Partitions créées : la zone à chiffrer a le bouton « Chiffrer maintenant ».

À côté des partitions à chiffrer, appuyez sur **Chiffrer maintenant** : le chiffrement (chapitre 4) démarre avec la partition déjà sélectionnée.

> **Tant que vous ne la chiffrez pas, la zone « à chiffrer » n'est pas protégée**
> N'y copiez pas de fichiers confidentiels avant la fin du chiffrement.

6 Utiliser un lecteur chiffré

Déverrouiller

Lorsque vous branchez un lecteur chiffré alors que Kripta est en cours d'exécution, la demande de mot de passe apparaît automatiquement.



Demande de mot de passe au branchement.

1. Saisissez le mot de passe et appuyez sur **Déverrouiller** (ou Entrée).
2. Le lecteur s'ouvre comme un disque normal dans l'Explorateur de fichiers, le Finder ou le gestionnaire de fichiers Linux.
3. Avec **Ignorer**, vous le déverrouillerez plus tard depuis la fenêtre principale.

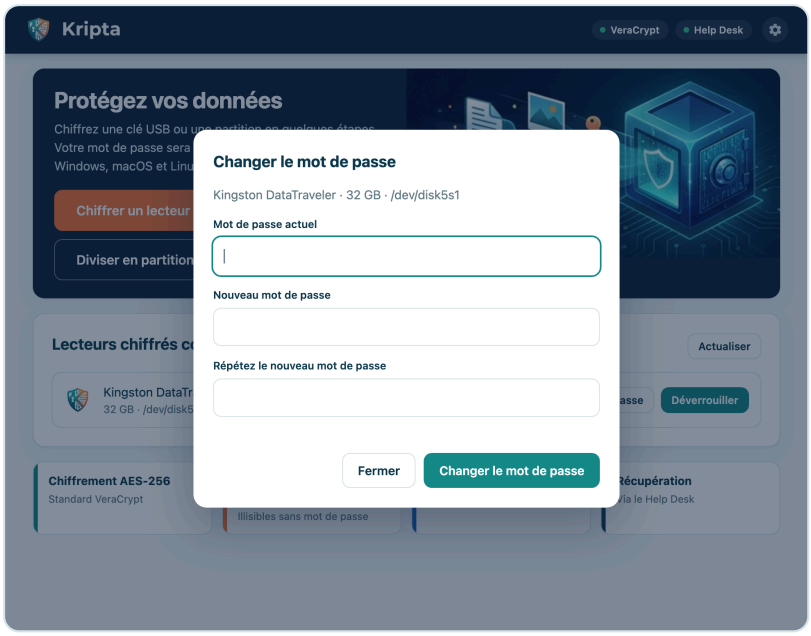
Travailler avec les fichiers et verrouiller

Lecteur déverrouillé, vous utilisez les fichiers normalement : tout ce que vous écrivez est chiffré de manière transparente. Une fois terminé, fermez les fichiers ouverts, appuyez sur **Verrouiller** et débranchez le lecteur.

> **Ne débranchez pas un lecteur déverrouillé sans le verrouiller**
> Vous pourriez perdre les fichiers en cours de copie.

7 Changer le mot de passe

Vous pouvez changer le mot de passe quand vous voulez, si vous connaissez l'actuel. Les données du lecteur ne sont pas modifiées.



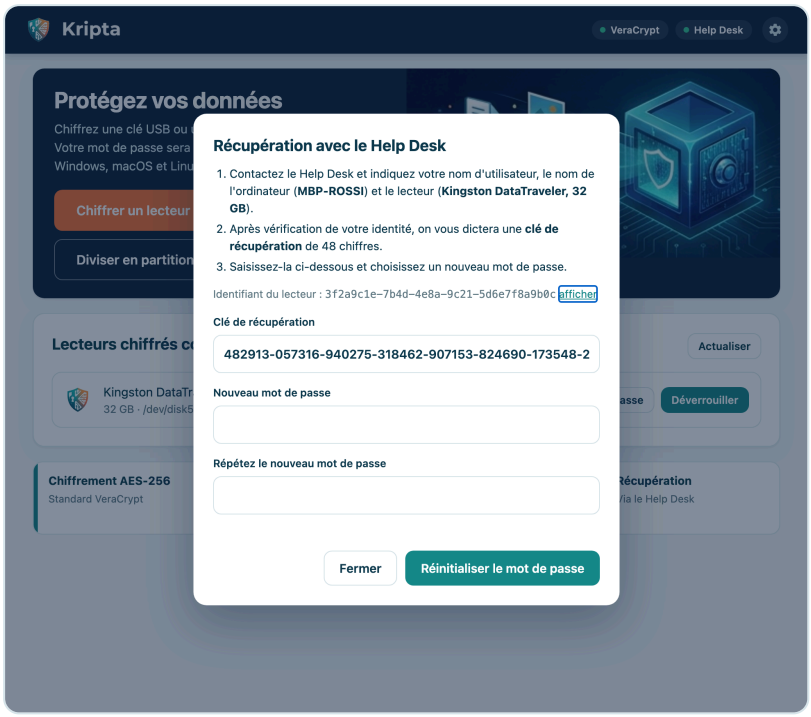
Fenêtre Changer le mot de passe.

1. Si le lecteur est déverrouillé, appuyez d'abord sur **Verrouiller**.
2. Appuyez sur **Changer le mot de passe** à côté du lecteur.
3. Saisissez le mot de passe actuel puis deux fois le nouveau (mêmes règles qu'au chapitre 4), et confirmez.

> **Et la clé de récupération ?**
> Elle reste valide : le Help Desk pourra vous aider même après un changement de mot de passe.

8 J'ai oublié le mot de passe

Le Help Desk peut vous fournir la clé de récupération du lecteur : grâce à elle, vous définissez un nouveau mot de passe et retrouvez tous vos fichiers.



Récupération avec le Help Desk.

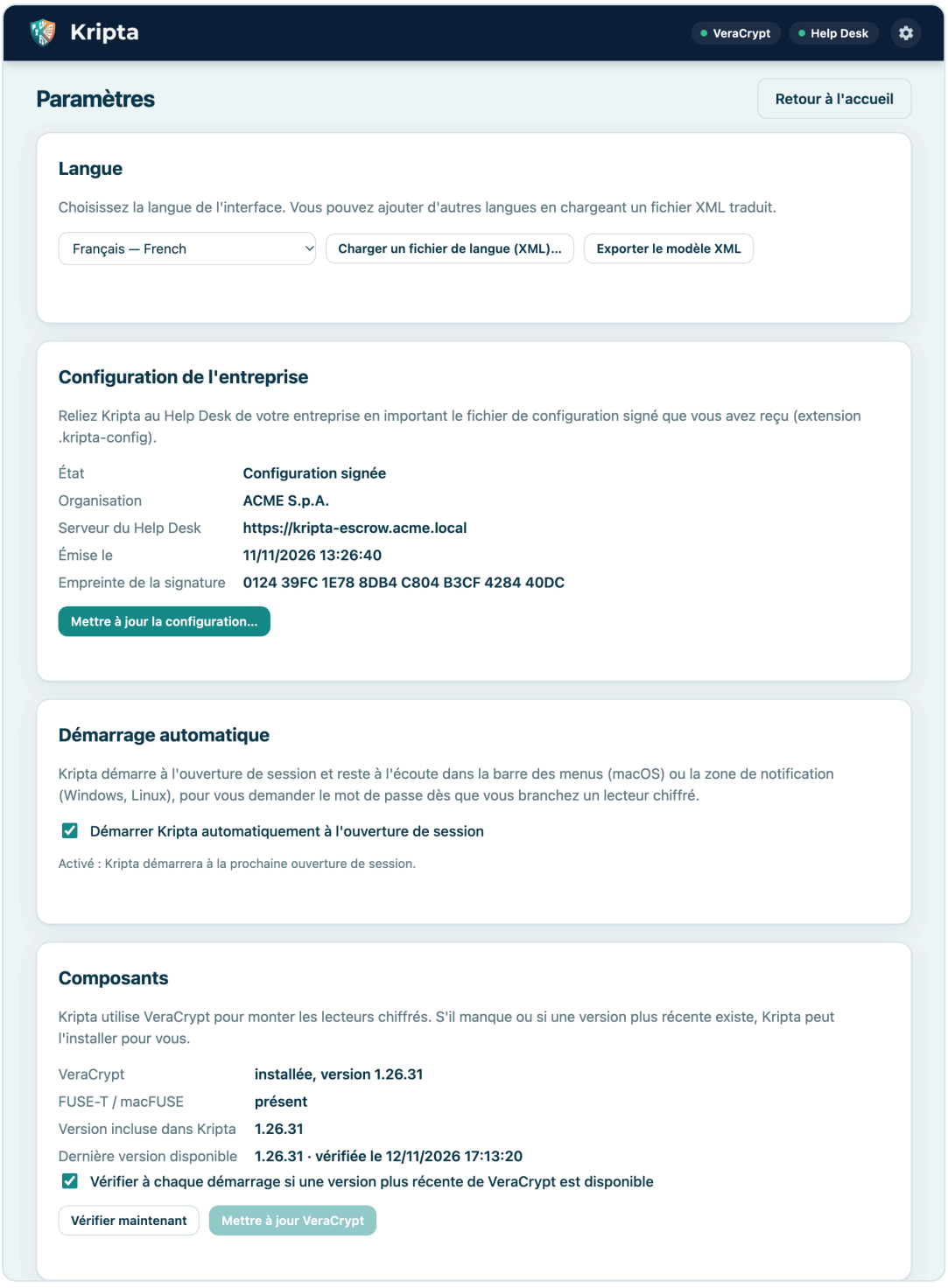
1. Dans la demande de mot de passe, choisissez **J'ai oublié le mot de passe**.
2. La fenêtre affiche le nom de l'ordinateur et du lecteur ; **afficher** montre aussi l'identifiant du lecteur.
3. **Contactez le Help Desk** et communiquez ces informations. Après vérification de votre identité, on vous dictera la **clé de 48 chiffres**.
4. Saisissez-la dans le champ **Clé de récupération**, choisissez un nouveau mot de passe et appuyez sur **Réinitialiser le mot de passe**.

> **Une clé, un seul usage**
> Après chaque récupération, Kripta génère une nouvelle clé et l'envoie au Help Desk.

> **Attention aux escroqueries**
> Le Help Desk ne vous demandera jamais votre mot de passe. C'est vous qui contactez le Help Desk, pas l'inverse.

9 Paramètres

Ils s'ouvrent avec l'engrenage en haut à droite ou avec **Paramètres…** dans le menu de l'icône.



Les Paramètres : langue, configuration de l'entreprise, composants, à propos.

Langue

Choisissez la langue dans la liste : l'interface, le menu de l'icône et les demandes d'autorisation changent immédiatement. Avec **Automatique**, Kripta utilise la langue du système. Langues incluses :

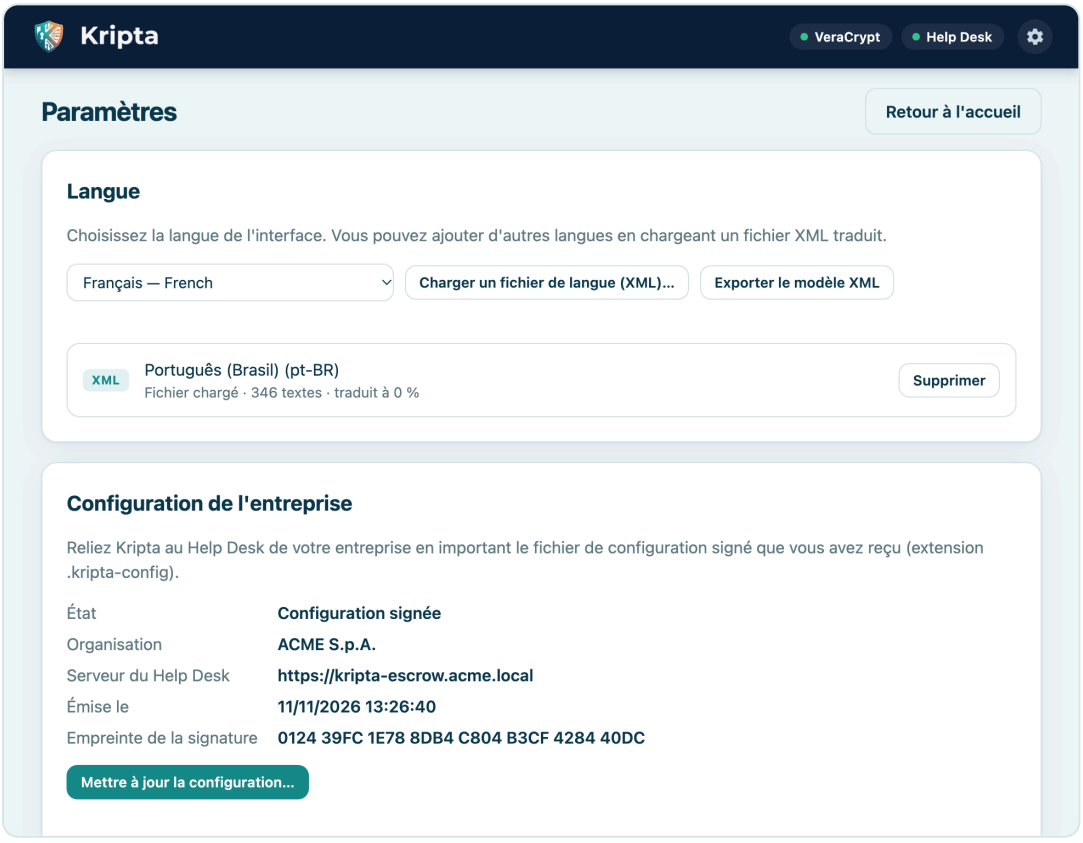
Italiano English Français Español Deutsch Русский العربية 中文 日本語

Ajouter une langue

Les traductions sont de simples fichiers **XML**, un par langue. Pour en ajouter une :

1. Appuyez sur **Exporter le modèle XML** : le fichier de la langue actuelle est enregistré dans le dossier Téléchargements.
2. Traduisez le texte de chaque élément `<string>` en laissant inchangés les attributs `id` et les marqueurs `{1}`, `{2}`.
3. En haut du fichier, définissez `code` (par exemple `pt` ou `pt-BR`), `name`, `english-name` et `dir` (`rtl` pour les langues écrites de droite à gauche).
4. Appuyez sur **Charger un fichier de langue (XML)…** et choisissez le fichier : la langue apparaît dans la liste avec le pourcentage de textes traduits. Les textes manquants s'affichent en anglais.

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



Une langue chargée depuis un fichier XML, avec le bouton Supprimer.

Charger un fichier avec le même code qu'une langue incluse la remplace (pratique pour corriger un terme) ; **Supprimer** rétablit l'original. Les fichiers des neuf langues incluses se trouvent à côté de ce manuel, dans le dossier `lang`.

Configuration de l'entreprise

Affiche l'organisation, le serveur du Help Desk, la date et l'empreinte de la configuration installée. **Mettre à jour la configuration…** importe un nouveau fichier reçu du Help Desk (chapitre 2).

Composants

Affiche la version de VeraCrypt installée, celle incluse dans Kripta et la dernière disponible. **Vérifier maintenant** vérifie aussitôt, **Installer** / **Mettre à jour VeraCrypt** lance l'installation. La case **Vérifier à chaque démarrage…** active ou désactive la vérification automatique.

Démarrage automatique

La case **Démarrer Kripta automatiquement à l'ouverture de session** est cochée par défaut. En dessous, Kripta indique si le démarrage automatique est enregistré dans le système. Si vous la décochez, Kripta ne détecte pas les lecteurs chiffrés tant que vous ne l'ouvrez pas.

10 Utiliser le lecteur sur d'autres ordinateurs

Les lecteurs chiffrés par Kripta utilisent le format standard **VeraCrypt** avec le système de fichiers **exFAT** : ils s'ouvrent sous Windows, macOS et Linux.

Ordinateur	Ce qui se passe quand vous branchez le lecteur
Avec Kripta configuré	La demande de mot de passe apparaît : tout est automatique.
Avec Kripta installé mais **sans configuration de l'entreprise** (par exemple à la maison)	La demande de mot de passe apparaît quand même et le lecteur se déverrouille. Si VeraCrypt manque, Kripta propose **Installer maintenant**. Sans configuration, impossible de chiffrer de nouveaux lecteurs ou de récupérer un mot de passe.
Avec VeraCrypt seul	Ouvrez VeraCrypt, choisissez un emplacement libre, **Sélectionner un périphérique**, choisissez la partition de la clé, puis **Monter** et saisissez le mot de passe.
Sans Kripta ni VeraCrypt	Aucune demande n'apparaît : les systèmes d'exploitation ne lancent pas de programmes depuis les clés USB. Le système peut proposer de **formater** le lecteur : **refusez toujours**. Installez Kripta (depuis le site de l'entreprise) et rebranchez le lecteur.

Droits d'administrateur
Ouvrir un lecteur chiffré sur n'importe quel ordinateur nécessite des droits d'administrateur, car VeraCrypt utilise un pilote système. Sur un ordinateur dont vous n'avez pas les identifiants, le lecteur ne peut pas être ouvert.

Zone libre pour l'échange
Si vous utilisez souvent des ordinateurs sans Kripta, divisez la clé avec le modèle **Zone chiffrée + zone libre** (chapitre 5) : vous pouvez aussi copier le programme d'installation de Kripta dans la zone libre.

11 Messages et résolution des problèmes

Message ou situation	Que faire
Kripta n'est pas encore relié au Help Desk de votre entreprise	Importez le fichier `.kripta-config` reçu du Help Desk (chapitre 2).
La signature du paquet n'est pas valide	Le fichier a été modifié ou endommagé : redemandez-le au Help Desk.
Le paquet est signé avec une clé différente / non approuvée	Le fichier ne provient pas de votre entreprise. Ne l'utilisez pas et contactez le Help Desk.
La configuration est gérée par l'informatique et ne peut pas être remplacée	L'ordinateur est configuré de manière centralisée : rien à importer.
Le moteur de chiffrement VeraCrypt n'est pas installé	Appuyez sur **Installer maintenant**. S'il n'y a pas de bouton, contactez le Help Desk.
La signature officielle de VeraCrypt n'est pas valide / le fichier ne correspond pas à la version signée	Le téléchargement a été altéré ou est incomplet : l'installation a été annulée. Réessayez plus tard.
Verrouillez tous les lecteurs chiffrés avant de mettre à jour VeraCrypt	Appuyez sur **Verrouiller** sur les lecteurs ouverts, puis recommencez la mise à jour.
Redémarrez l'ordinateur pour terminer la mise à jour (Windows)	Enregistrez votre travail et redémarrez.
Le serveur du Help Desk est injoignable. Le chiffrement n'a pas démarré.	Connectez-vous au réseau de l'entreprise ou au VPN et réessayez. Les données du lecteur n'ont pas été modifiées.
Clés de récupération en attente d'envoi	Connectez-vous au réseau et appuyez sur **Réessayer maintenant**. Laissez Kripta ouvert jusqu'à la disparition de l'alerte.
Aucun lecteur disponible	Rebranchez la clé (essayez un autre port USB) et appuyez sur **Actualiser la liste**.
Autorisation administrateur annulée / Délai dépassé	Recommencez l'opération et confirmez la demande du système.
Impossible de démonter / verrouiller le volume	Fermez les documents et fenêtres ouverts depuis le lecteur, puis réessayez.
Mot de passe incorrect	Vérifiez le verrouillage des majuscules et la disposition du clavier. Si vous l'avez oublié, voir le chapitre 8.
Clé de récupération incorrecte	Revérifiez les chiffres avec l'opérateur : il faut la clé **la plus récente**.

Message ou situation	Que faire
Le disque contient un lecteur Kripta déverrouillé	Verrouillez-le dans l'écran d'accueil, puis recommencez la division.
Le système n'a pas détecté les nouvelles partitions	Débranchez puis rebranchez le lecteur.
Le fichier de langue n'est pas un XML valide / élément non autorisé	Corrigez le fichier indiqué dans le message : seuls les éléments `<string>` avec du texte brut sont autorisés.
La fenêtre de déverrouillage n'apparaît pas au branchement	Vérifiez que Kripta est en cours d'exécution (icône dans la barre) et utilisez **Déverrouiller** depuis la fenêtre principale.

12 Questions fréquentes

Puis-je chiffrer une clé qui contient déjà des fichiers sans les perdre ?

Non. Le chiffrement efface le lecteur. Copiez les fichiers ailleurs, chiffrez le lecteur puis recopiez-les.

Puis-je chiffrer le disque interne de mon ordinateur ?

Non. Kripta est conçu pour les clés et disques externes ; les disques système ne sont pas affichés.

Le Help Desk peut-il lire mes fichiers ?

Le Help Desk ne conserve que la clé de récupération et ne peut la consulter qu'à votre demande, chaque accès étant journalisé.

Dois-je noter la clé de récupération ?

Non. Vous ne la voyez jamais et n'avez pas à la conserver : elle est archivée auprès du Help Desk.

Kripta installe-t-il des programmes sur mon ordinateur ?

Uniquement VeraCrypt (et FUSE-T sous macOS), après votre confirmation et seulement si la signature officielle des développeurs est valide.

Puis-je utiliser la clé sur un ordinateur personnel ?

Oui, en installant Kripta ou VeraCrypt (chapitre 10). Respectez toujours les règles de l'entreprise sur l'utilisation des données à l'extérieur.

La langue dont j'ai besoin n'existe pas. Que faire ?

Vous pouvez traduire le modèle XML et le charger depuis les Paramètres (chapitre 9), ou demander à l'informatique d'en distribuer un.

Pourquoi ne puis-je pas utiliser de lettres accentuées dans le mot de passe ?

Windows, macOS et Linux peuvent les coder différemment : le même mot de passe saisi sur un autre système pourrait ne pas être reconnu.

Combien d'espace le chiffrement occupe-t-il ?

Très peu : quelques centaines de kilo-octets pour les en-têtes du volume.

A Annexe pour l'informatique

Paquets

Système	Paquet	Remarques
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	Contient les MSI officiels de VeraCrypt (x64 et ARM64). L'application démarre avec les droits d'administrateur.
macOS 11+	`Kripta_1.2.0_universal.dmg`	Contient VeraCrypt (versions FUSE-T et macFUSE) et FUSE-T, qui ne nécessite aucune extension du noyau.
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	Contient VeraCrypt pour Ubuntu 22.04/24.04 et Debian 12/13 ; pour les autres versions, Kripta télécharge le paquet vérifié.
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	Contient VeraCrypt pour Fedora 44 ; installer aussi `exfatprogs`.
Autres distributions	`Kripta_1.2.0_amd64.AppImage`	Exécutable portable.

Configuration signée

Sur le serveur escrow, une seule fois, générer la clé de signature ; puis signer la configuration client (modèle dans `deploy/client/kripta.toml.example`) :

```
kripta-escrow keygen-sign           # clé privée (à conserver hors ligne) + publique + empreinte
kripta-escrow sign-config client.toml signature.key "ACME SA" acme.kripta-config
```

Distribuer `acme.kripta-config` aux utilisateurs et publier l'**empreinte** sur un canal fiable (intranet, téléphone du Help Desk). Kripta enregistre la configuration à l'emplacement système (`%ProgramData%\Kripta`, `/Library/Application Support/Kripta`, `/etc/kripta`) via le processus privilégié, avec la clé du signataire : les mises à jour suivantes doivent porter la même signature. Pour ne pas dépendre de la vérification de l'empreinte par l'utilisateur, compiler Kripta avec `KRIPTA_PROVISIONING_KEYS=<clé publique>` : seules ces clés seront acceptées. Une configuration copiée à la main par l'informatique (non signée) ne peut pas être remplacée par un paquet.

Installation et mise à jour de VeraCrypt

- Les programmes d'installation inclus sont préparés avec `scripts/fetch-veracrypt.py` lors de la compilation.
- Avant l'installation, le processus privilégié vérifie la signature OpenPGP de la liste SHA-256 officielle avec la clé IDRIX intégrée (empreinte `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`) ainsi que le hachage du fichier.

- Options dans `kripta.toml` : `veracrypt_update_check = false` désactive la vérification des mises à jour ; `veracrypt_release_api = "https://miroir.interne/…"` utilise un miroir interne au même format que l'API GitHub.

Langues

Les fichiers XML des langues se trouvent dans `app/ui/lang/` (inclus dans l'application) et dans `docs/manuale/lang/`. Les langues chargées par les utilisateurs sont enregistrées dans le dossier de données de l'utilisateur (`languages/`). Pour distribuer une nouvelle langue à tous, ajouter le fichier dans `app/ui/lang/` et son code dans la liste de `app/ui/i18n.js`.

Composants facultatifs

- **Démarrage à l'ouverture de session** dans la barre des menus / zone de notification (`kripta --background`) : **automatique**. Kripta l'enregistre à chaque démarrage (macOS : `~/Library/LaunchAgents/com.kripta.agent.plist`, relancé en cas d'arrêt anormal ; Windows : tâche planifiée « Kripta » à l'ouverture de session avec les privilèges les plus élevés, créée aussi par l'installeur et supprimée à la désinstallation ; Linux : `/etc/xdg/autostart/kripta.desktop` des paquets .deb/.rpm, `~/.config/autostart/kripta.desktop` pour l'AppImage). Désactivable dans les Réglages.
- **Assistant privilégié** en tant que service (aucune demande de mot de passe) : `deploy/macos/com.kripta.helper.plist`, `deploy/linux/kripta-helper.service`.