Kripta

Benutzerhandbuch

Geführte Verschlüsselung von USB-Sticks und Partitionen, mit Passwortwiederherstellung über den Help Desk Ihres Unternehmens.



Version 1.2 · Windows · macOS · Linux

November 2026

Inhalt

1 Was ist Kripta — wozu es dient, was Sie brauchen

2 Erster Start — Unternehmenskonfiguration und Komponenten

3 Das Hauptfenster — Anzeigen, Hinweise, Symbol

4 Ein Laufwerk verschlüsseln — der Assistent in 4 Schritten

5 Einen Datenträger partitionieren — verschlüsselter und freier Bereich

6 Ein verschlüsseltes Laufwerk verwenden — entsperren, öffnen, sperren

7 Passwort ändern

8 Passwort vergessen — Wiederherstellung mit dem Help Desk

9 Einstellungen — Sprache, Konfiguration, Aktualisierungen

10 Das Laufwerk an anderen Computern verwenden

11 Meldungen und Fehlerbehebung

12 Häufige Fragen

A Anhang für die IT — Pakete, signierte Konfiguration, Sprachen

Konventionen

Texte auf dem Bildschirm (Schaltflächen, Titel, Einträge) sind so geschrieben: **Laufwerk verschlüsseln**. Die Bildschirmfotos stammen aus der macOS-Version: Unter Windows und Linux ist das Fenster identisch, nur die Gerätenamen unterscheiden sich (zum Beispiel `E:` oder `/dev/sdb1` statt `/dev/disk4s1`).

1 Was ist Kripta

Kripta schützt die Daten Ihrer **USB-Sticks** und der **Partitionen** externer Festplatten mit AES-256-Verschlüsselung. Nach der Verschlüsselung kann nur lesen, wer das Passwort kennt: Verlieren Sie den Stick, kann ihn niemand sonst öffnen.

Geführte Verschlüsselung
Vier Schritte: Laufwerk wählen, Passwort wählen, bestätigen, warten.

Automatisches Entsperren
Wenn Sie ein verschlüsseltes Laufwerk anschließen, fragt Kripta sofort nach dem Passwort und öffnet es.

Funktioniert überall
Derselbe Stick öffnet sich unter Windows, macOS und Linux (Standardformat VeraCrypt).

Selbstständige Installation
Kripta installiert und aktualisiert VeraCrypt selbst; die Unternehmenskonfiguration wird aus einer Datei importiert.

Neun Sprachen
Italienisch, Englisch, Französisch, Spanisch, Deutsch, Russisch, Arabisch, Chinesisch und Japanisch – plus eigene.

Wiederherstellung mit dem Help Desk
Wenn Sie das Passwort vergessen, hilft der Help Desk beim Setzen eines neuen, ohne Datenverlust.

Was Sie brauchen

- **Kripta** auf dem Computer. Beim ersten Start installiert Kripta selbst **VeraCrypt**, die Verschlüsselungs-Engine (unter macOS auch **FUSE-T**), falls es fehlt: Kapitel 2.
- Die **signierte Konfigurationsdatei** (`.kripta-config`) vom Help Desk, sofern die IT den Computer nicht schon konfiguriert hat.
- Eine **Verbindung zum Unternehmensnetz** (oder VPN), wenn Sie ein neues Laufwerk verschlüsseln: Der Wiederherstellungsschlüssel wird sofort an den Help Desk gesendet. Zum Entsperren eines bereits verschlüsselten Laufwerks ist kein Netz nötig.
- Die **Administrator-Zugangsdaten** des Computers, wenn das System danach fragt (siehe Kasten).

> **Autorisierungsanfragen**
> Um direkt auf das Laufwerk zu lesen und zu schreiben, Komponenten zu installieren und die Konfiguration zu speichern, braucht Kripta Administratorrechte. Unter **Windows** erscheint beim Start die Benutzerkontensteuerung. Unter **macOS** und **Linux** erscheint die Meldung „Kripta benötigt die Autorisierung eines Administrators, um den Vorgang abzuschließen“. Hat die IT den Kripta-Systemdienst installiert, erscheinen diese Anfragen nicht.

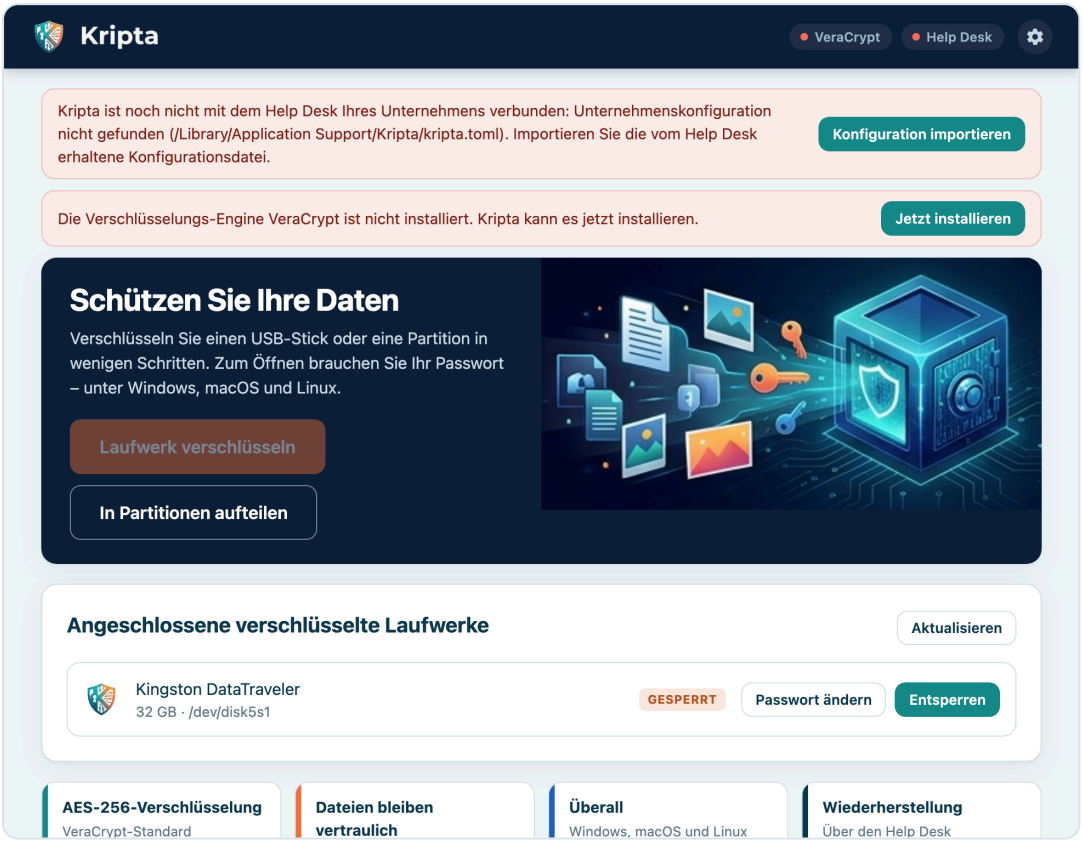
Die Wiederherstellung in Kürze

Bei der Verschlüsselung erzeugt Kripta einen 48-stelligen **Wiederherstellungsschlüssel**, schützt ihn und sendet ihn an das Archiv des Help Desk. Sie müssen ihn weder sehen noch aufbewahren. Nur Help-Desk-

Mitarbeiter können ihn nach Prüfung Ihrer Identität abrufen, und jeder Abruf wird protokolliert.

2 Erster Start

Beim ersten Start prüft Kripta zwei Dinge: ob es mit dem Help Desk Ihres Unternehmens verbunden ist und ob VeraCrypt auf dem Computer vorhanden ist. Fehlt etwas, erscheint oben im Fenster ein Hinweis mit einer Schaltfläche zur Behebung. Sie können alles selbst erledigen.

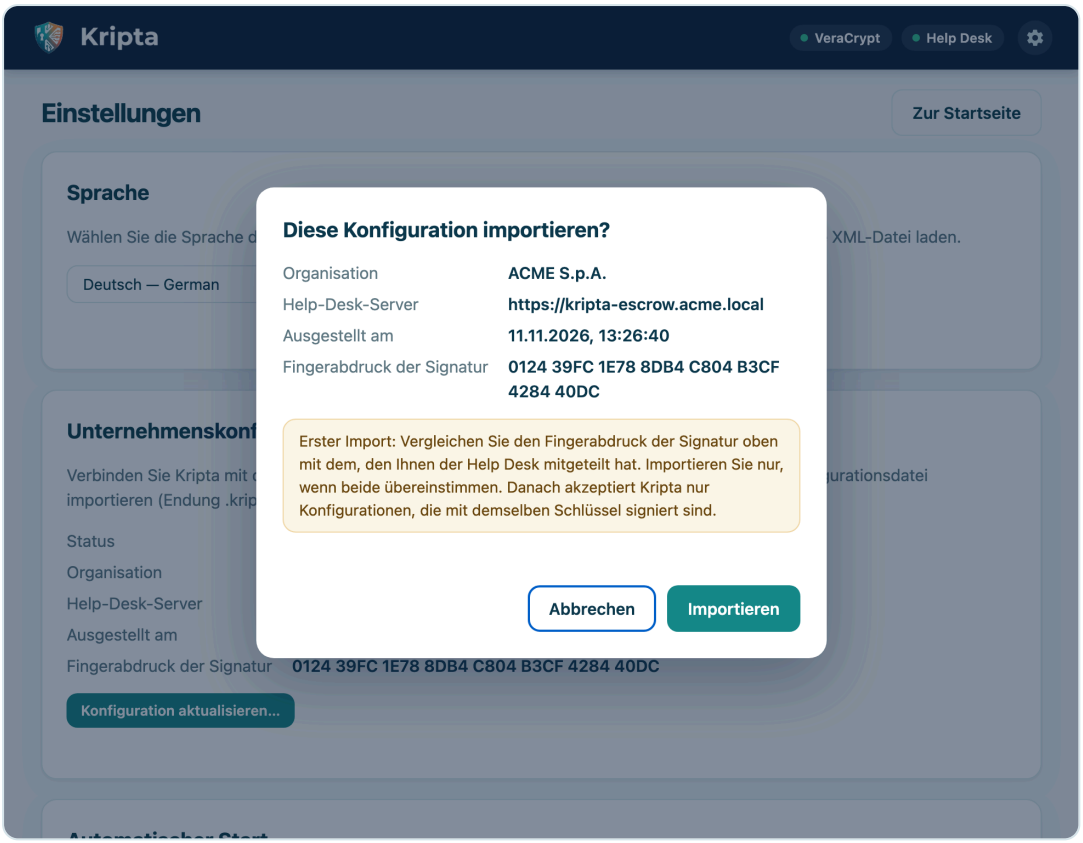


Erster Start: Konfiguration importieren und VeraCrypt installieren.

Die Unternehmenskonfiguration importieren

Die Konfiguration teilt Kripta mit, an welches Help-Desk-Archiv die Wiederherstellungsschlüssel gesendet werden. Der Help Desk gibt sie Ihnen als Datei mit der Endung `.kripta-config`, digital signiert: Niemand kann sie ändern, ohne dass Kripta es bemerkt.

1. Speichern Sie die erhaltene Datei auf dem Computer (per E-Mail, aus dem Unternehmensportal oder von einem Stick).
2. Klicken Sie im Hinweis auf **Konfiguration importieren** oder öffnen Sie die **Einstellungen** (Zahnrad oben rechts) und klicken Sie auf **Signierte Konfiguration importieren…**.
3. Wählen Sie die Datei. Kripta prüft die Signatur und zeigt Organisation, Help-Desk-Server, Ausstellungsdatum und den **Fingerabdruck der Signatur**.
4. Beim ersten Import **vergleichen Sie den Fingerabdruck** mit dem vom Help Desk mitgeteilten (telefonisch, im Intranet…). Stimmt er überein, klicken Sie auf **Importieren**.
5. Bestätigen Sie die Autorisierungsanfrage des Systems. **Konfiguration importiert** erscheint und die Anzeige **Help Desk** wird grün.

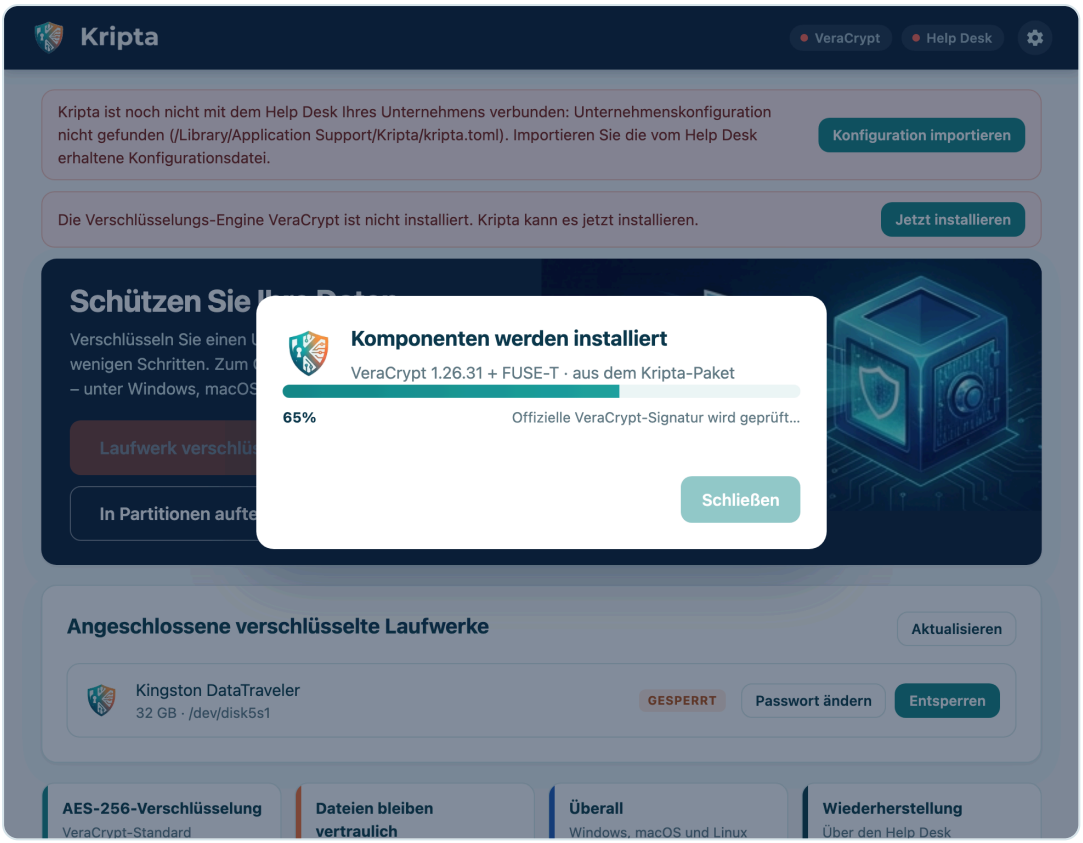


Bestätigung des Imports mit dem Fingerabdruck der Signatur.

> **Stimmt der Fingerabdruck nicht überein, nicht importieren**
> Die Datei stammt möglicherweise nicht von Ihrem Unternehmen. Brechen Sie ab und wenden Sie sich an den Help Desk. Nach dem ersten Import akzeptiert Kripta nur Aktualisierungen mit demselben Schlüssel: Eine gefälschte Datei wird automatisch abgelehnt.

VeraCrypt installieren

Kripta enthält bereits das offizielle Installationsprogramm von VeraCrypt (und FUSE-T für macOS). Klicken Sie im Hinweis auf **Jetzt installieren** und bestätigen Sie die Autorisierungsanfrage: Kripta prüft die offizielle Signatur der Installationsprogramme und installiert sie ohne weitere Fragen.

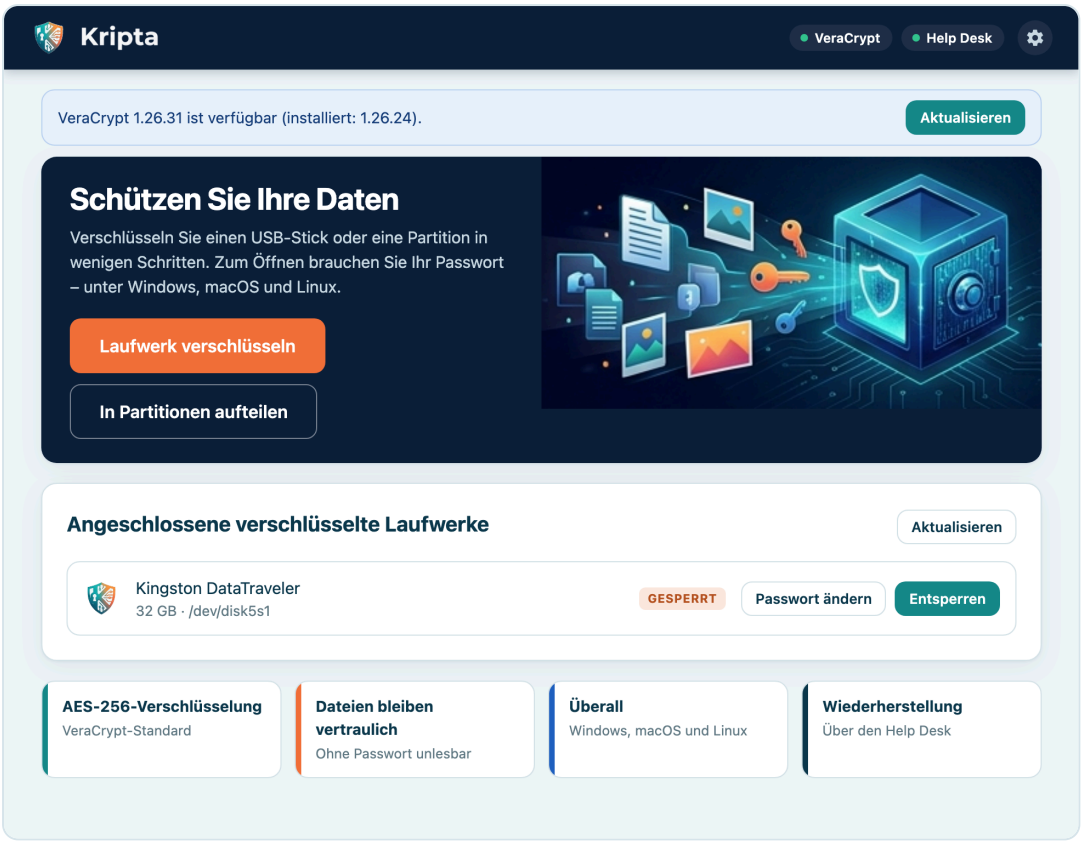


Installation der Komponenten mit Prüfung der offiziellen Signatur.

Am Ende erscheint **Installation abgeschlossen**. Unter Windows kann ein Neustart erforderlich sein.

VeraCrypt-Aktualisierungen

Bei jedem Start (und danach einmal täglich) prüft Kripta, ob eine neuere Version von VeraCrypt erschienen ist. Wenn ja, erscheint ein blauer Hinweis mit der Schaltfläche **Aktualisieren**. Die neue Version wird von der offiziellen Website geladen und nur installiert, wenn die Signatur der VeraCrypt-Entwickler gültig ist.



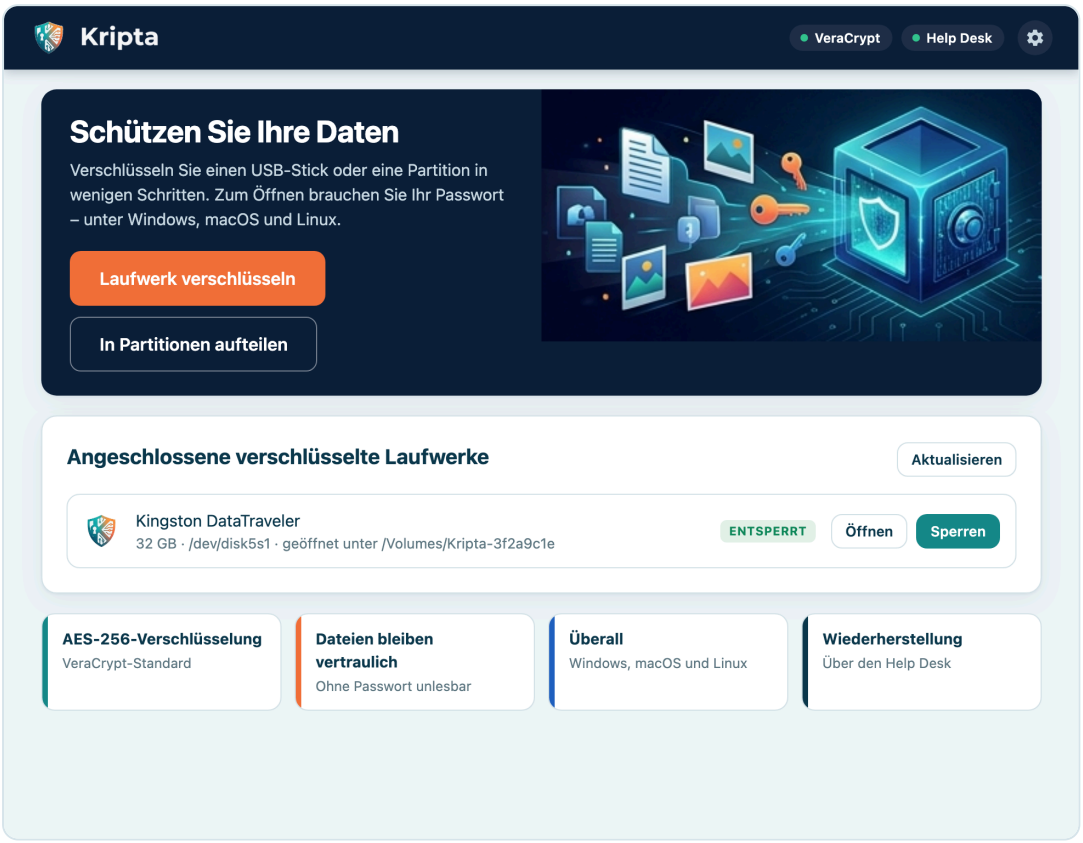
VeraCrypt-Aktualisierung verfügbar.

Vor dem Aktualisieren

Sperren Sie alle geöffneten verschlüsselten Laufwerke: Kripta aktualisiert VeraCrypt nicht, solange ein Laufwerk entsperrt ist. Die automatische Prüfung lässt sich in den Einstellungen abschalten (Kapitel 9).

3 Das Hauptfenster

Beim Öffnen zeigt Kripta die Startseite. Hier verschlüsseln Sie ein neues Laufwerk und verwalten die angeschlossenen verschlüsselten Laufwerke.

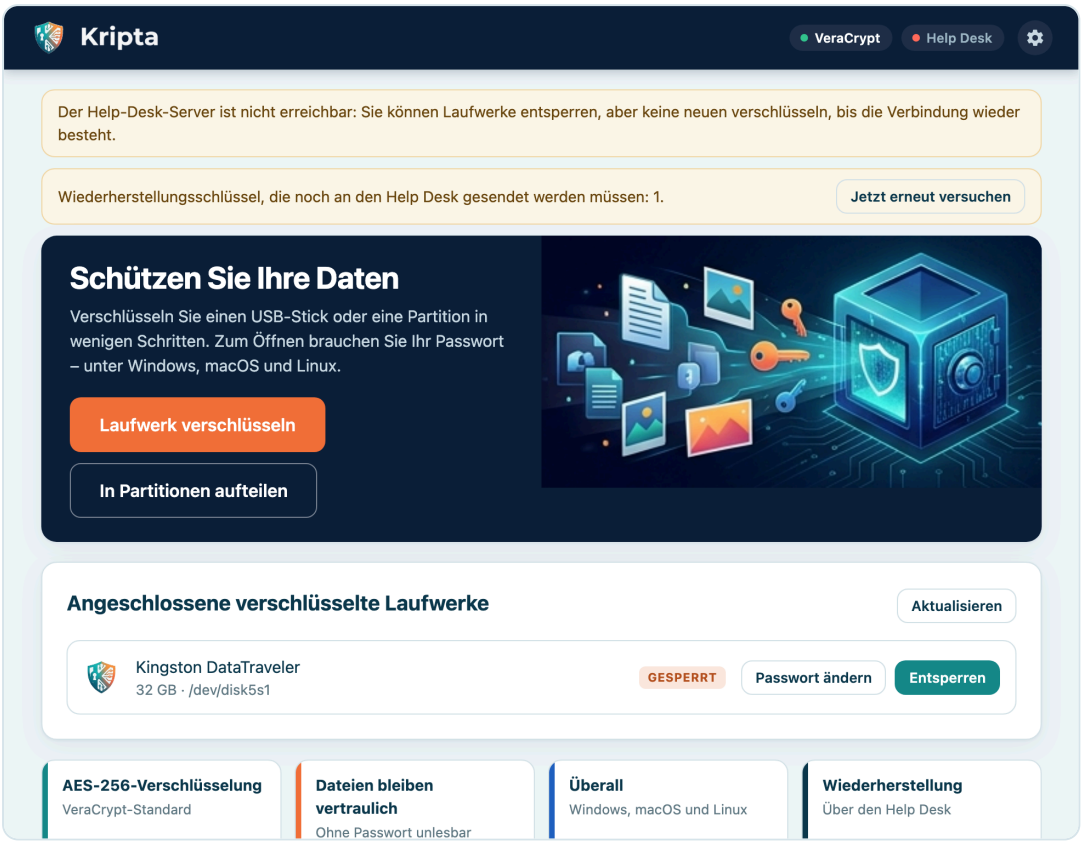


Startseite mit einem angeschlossenen, entsperrten verschlüsselten Laufwerk.

Element	Wozu es dient
VeraCrypt	**Grüner** Punkt: Die Verschlüsselungs-Engine ist installiert. **Rot**: nicht installiert (Kapitel 2). Beim Darüberfahren sehen Sie die Version.
Help Desk	Grün: Das Schlüsselarchiv ist erreichbar. Rot: nicht erreichbar (kein Netz, VPN aus, Konfiguration fehlt).
Zahnrad	Öffnet die **Einstellungen**: Sprache, Unternehmenskonfiguration, Komponenten (Kapitel 9).
Laufwerk verschlüsseln	Startet den Assistenten (Kapitel 4). Deaktiviert, wenn Kripta nicht konfiguriert ist oder VeraCrypt fehlt.
In Partitionen aufteilen	Teilt einen USB-Stick oder eine externe Festplatte in mehrere Partitionen (Kapitel 5).
Angeschlossene verschlüsselte Laufwerke	Die angeschlossenen Kripta-Laufwerke mit Status **Gesperrt** oder **Entsperrt** und den zugehörigen Schaltflächen.

Hinweise

Oben im Fenster können farbige Kästen mit einer Schaltfläche zur Behebung erscheinen:



Help-Desk-Server nicht erreichbar und ein Wiederherstellungsschlüssel wartet auf Versand.

- **Help-Desk-Server nicht erreichbar:** Sie können weiterhin Laufwerke entsperren, aber keine neuen verschlüsseln.
- **Wiederherstellungsschlüssel warten auf Versand:** Kripta versucht es selbst erneut; klicken Sie auf `Jetzt erneut versuchen`, sobald Sie wieder online sind. **Lassen Sie Kripta geöffnet, bis der Hinweis verschwindet.**
- **Kripta ist noch nicht mit dem Help Desk verbunden / VeraCrypt ist nicht installiert / VeraCrypt … ist verfügbar:** siehe Kapitel 2.

Das Kripta-Symbol: Menüleiste und Infobereich

Kripta arbeitet im Hintergrund, um das Anschließen verschlüsselter Laufwerke zu erkennen, und wird über ein Symbol mit dem Emblem gesteuert:

System	Wo das Symbol ist	Gut zu wissen
macOS	In der **Menüleiste** oben rechts. Kripta **erscheint nicht im Dock**.	Bei MacBooks mit Notch werden überzählige Symbole bei voller Leiste ausgeblendet: Entfernen Sie unbenutzte oder verschieben Sie sie mit gedrückter ⌘-Taste.

System	Wo das Symbol ist	Gut zu wissen
Windows	Im **Infobereich** unten rechts neben der Uhr.	Ist es bei den ausgeblendeten Symbolen, klicken Sie auf den Pfeil **^** und ziehen Sie das Emblem auf die Leiste.
Linux	Im **Infobereich** der Leiste.	Unter „reinem“ GNOME (Fedora, Debian) wird die Erweiterung **AppIndicator and KStatusNotifierItem Support** benötigt.

Das Symbolmenü enthält **Kripta öffnen**, **Laufwerk verschlüsseln…**, **In Partitionen aufteilen…**, **Alle Laufwerke sperren**, **Einstellungen…** und **Kripta beenden**. Die Einträge folgen der gewählten Sprache.

> **Das Schließen des Fensters beendet Kripta nicht**
> Kripta bleibt in der Menüleiste bzw. im Infobereich aktiv. Zum erneuten Öffnen verwenden Sie **Kripta öffnen** oder starten Sie Kripta erneut: Das bereits laufende Fenster wird angezeigt.

Automatischer Start

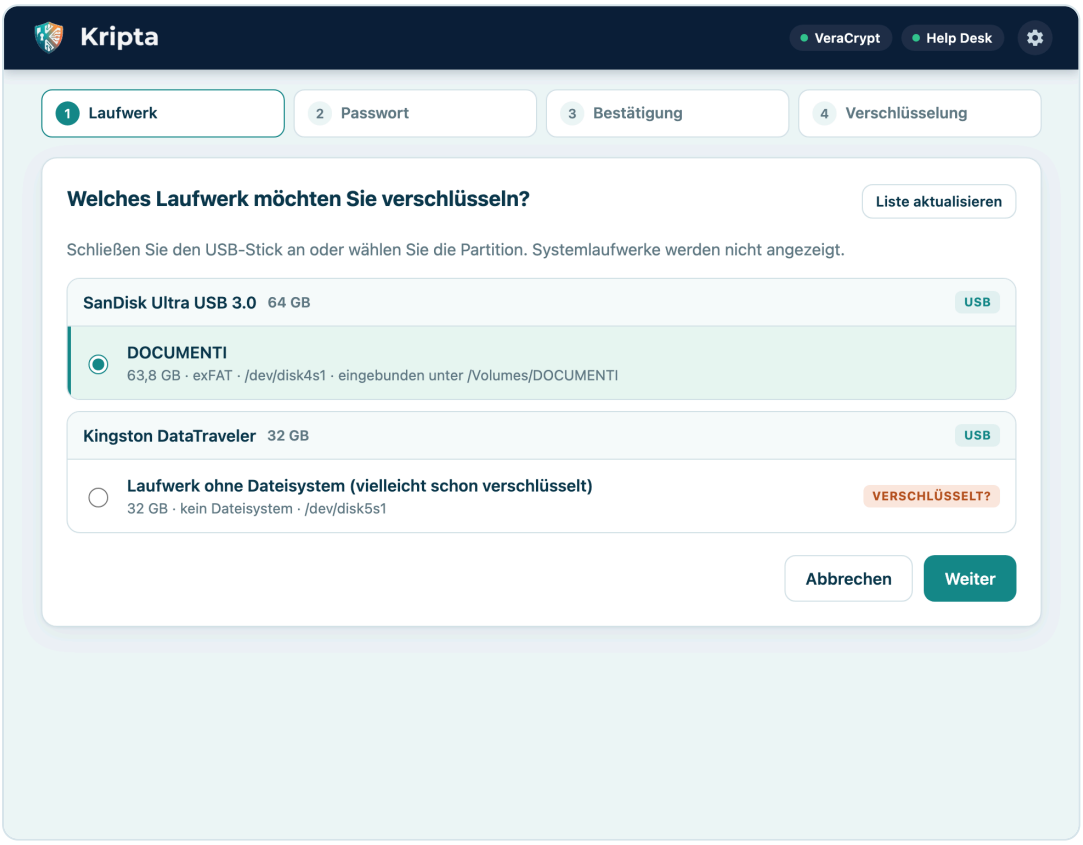
Nach der Installation **startet Kripta bei jeder Anmeldung von selbst**, ohne das Fenster zu öffnen, und bleibt ständig aktiv: Sobald Sie ein verschlüsseltes Laufwerk anschließen, fragt es nach dem Passwort. Sie können dies unter **Einstellungen › Automatischer Start** abschalten (Kapitel 9). **Kripta beenden** schließt es bis zur nächsten Anmeldung.

4 Ein Laufwerk verschlüsseln

Die Verschlüsselung löscht den gesamten Inhalt des Laufwerks.
Kopieren Sie vorher die Dateien, die Sie behalten möchten, an einen anderen Ort. Danach können Sie sie wieder auf das geschützte Laufwerk kopieren.

Schließen Sie den Stick an, prüfen Sie, dass die Anzeige **Help Desk** grün ist, und klicken Sie auf **Laufwerk verschlüsseln**.

Schritt 1 — Laufwerk

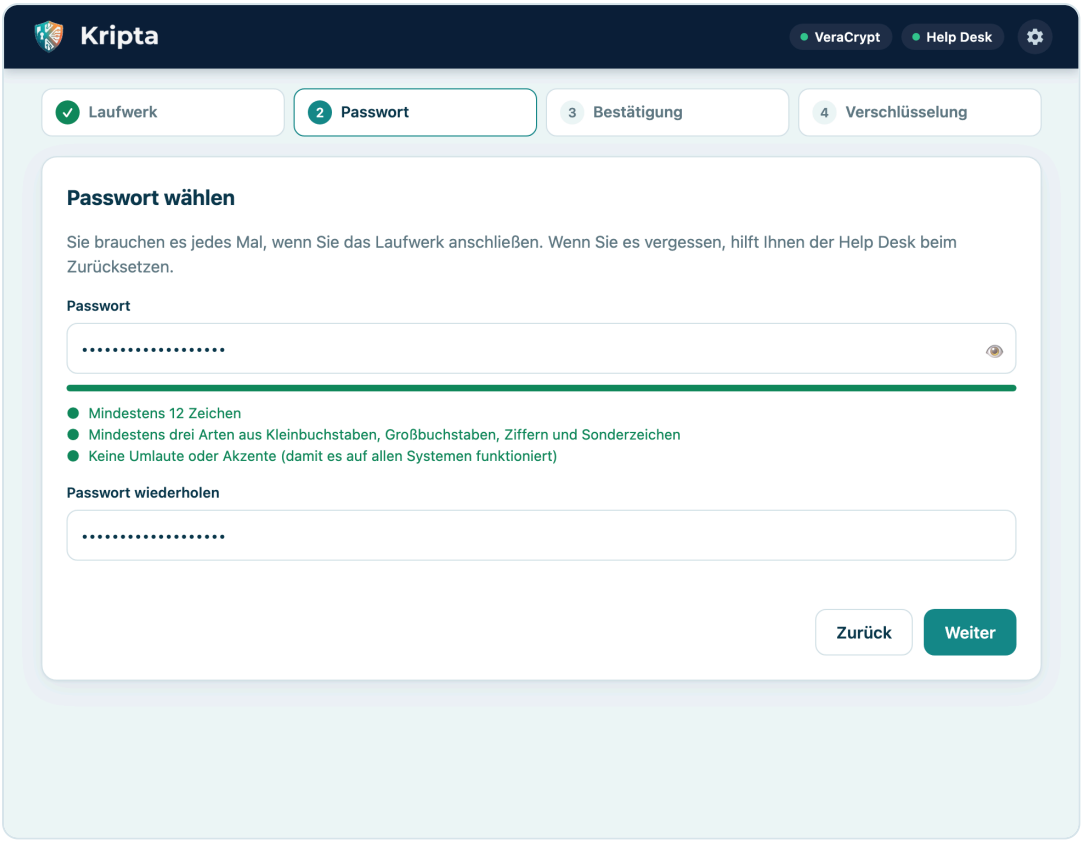


Auswahl des zu verschlüsselnden Laufwerks.

1. Kripta listet die angeschlossenen Geräte auf, Wechseldatenträger zuerst. **Systemlaufwerke werden nie angezeigt**.
2. Prüfen Sie **Kapazität und Namen** sorgfältig, um sicher das richtige Laufwerk zu wählen.
3. Erscheint der Stick nicht, schließen Sie ihn erneut an und klicken Sie auf **Liste aktualisieren**.
4. Wählen Sie das Laufwerk und klicken Sie auf **Weiter**.

Kennzeichnung „Verschlüsselt?“
Sie markiert ein Laufwerk ohne erkennbares Dateisystem: Es ist wahrscheinlich schon verschlüsselt. Verschlüsseln Sie es erneut, geht der aktuelle Inhalt verloren.

Schritt 2 — Passwort

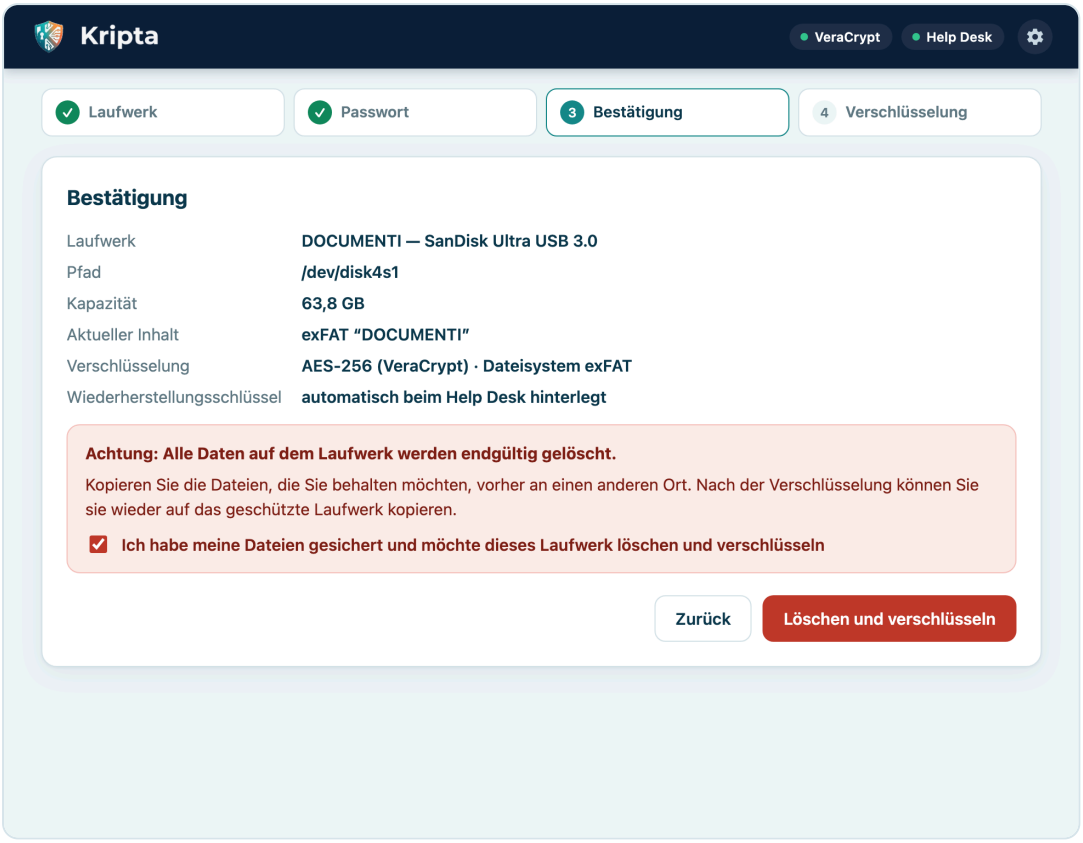


Die Regeln werden grün, sobald sie erfüllt sind.

Das Passwort muss **mindestens 12 Zeichen**, **mindestens drei Arten** aus Klein-, Großbuchstaben, Ziffern und Symbolen und **keine Umlaute oder Akzente** (ä, é, ß…) enthalten, die andere Systeme anders eingeben könnten. Der farbige Balken zeigt die Stärke; die Schaltfläche 👁 zeigt das Passwort an. Wiederholen Sie es im zweiten Feld und klicken Sie auf **Weiter**.

> **Tipp**
> Ein Satz aus mehreren Wörtern mit Symbolen und Ziffern (zum Beispiel `Zug-See-Gruen-47`) ist sicher und leicht zu merken. Verwenden Sie nicht das Passwort Ihres Firmenkontos.

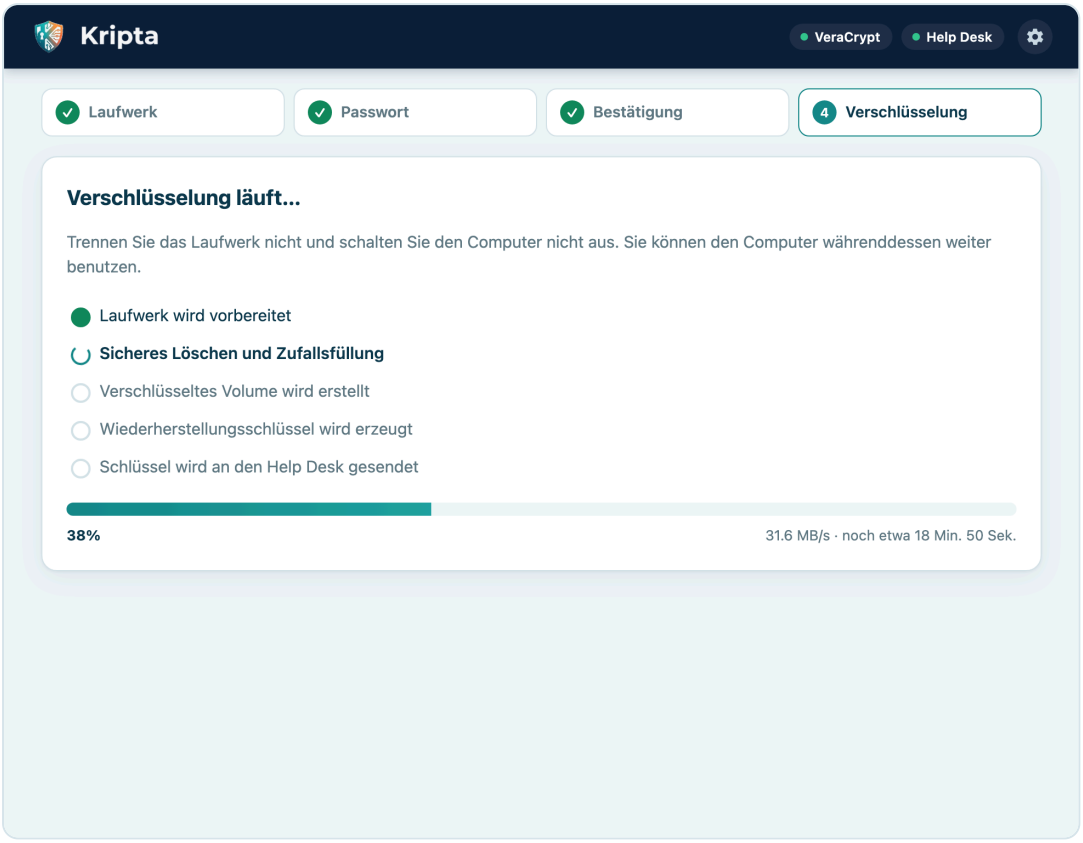
Schritt 3 — Bestätigung



Zusammenfassung und Bestätigung des Löschens.

Prüfen Sie die Zusammenfassung, aktivieren Sie **Ich habe meine Dateien gesichert und möchte dieses Laufwerk löschen und verschlüsseln** und klicken Sie auf **Löschen und verschlüsseln**. Das System kann nach Administratorrechten fragen.

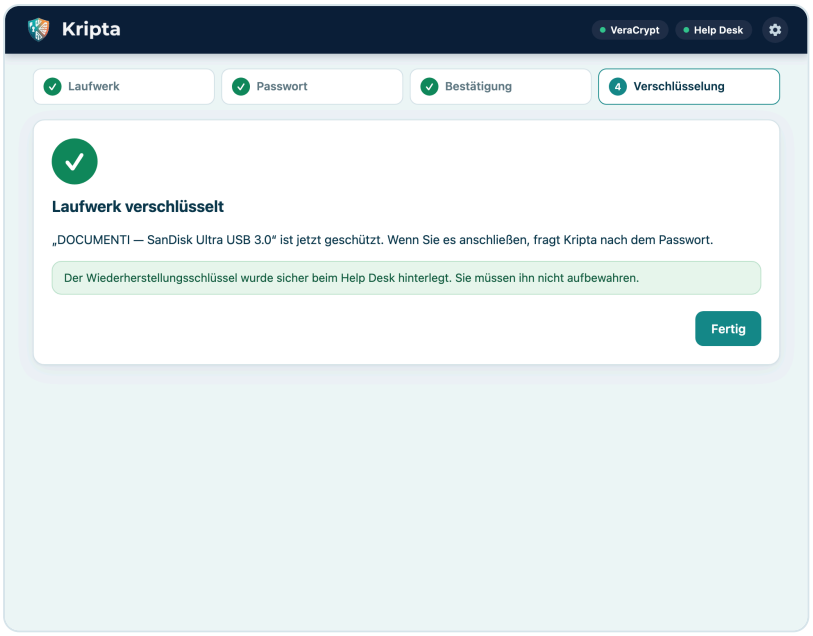
Schritt 4 — Verschlüsselung



Fortschritt mit Geschwindigkeit und Restzeit.

Kripta bereitet das Laufwerk vor, überschreibt es vollständig mit Zufallsdaten (die längste Phase), erstellt das verschlüsselte exFAT-Volume, erzeugt den Wiederherstellungsschlüssel und sendet ihn an den Help Desk.

> **Während der Verschlüsselung**
> Trennen Sie das Laufwerk nicht und schalten Sie den Computer nicht aus oder in den Ruhezustand. Ein 64-GB-Stick braucht etwa 15 Minuten bis eine Stunde.



Verschlüsselung abgeschlossen.

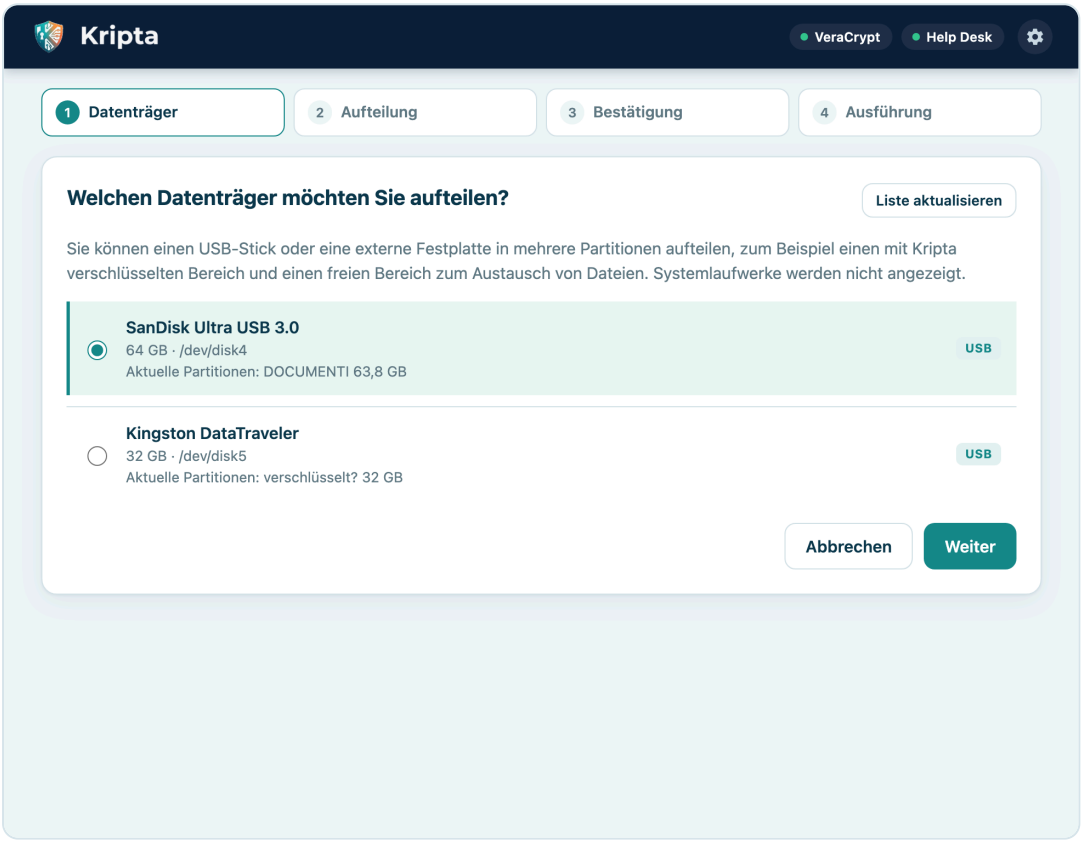
Erscheint **Der Wiederherstellungsschlüssel wurde noch nicht gesendet**, ist das Laufwerk trotzdem verschlüsselt und nutzbar: Lassen Sie Kripta geöffnet und verbunden, es sendet den Schlüssel so bald wie möglich. Schlägt die Verschlüsselung fehl, erklärt die Meldung den Grund (Kapitel 11).

5 Einen Datenträger partitionieren

Mit **In Partitionen aufteilen** teilen Sie einen USB-Stick oder eine externe Festplatte in mehrere unabhängige Teile, jeweils mit eigenem Namen und Dateisystem. Typisch ist ein **verschlüsselter Bereich** für vertrauliche Daten und ein **freier Bereich** zum Austausch mit Computern ohne Kripta.

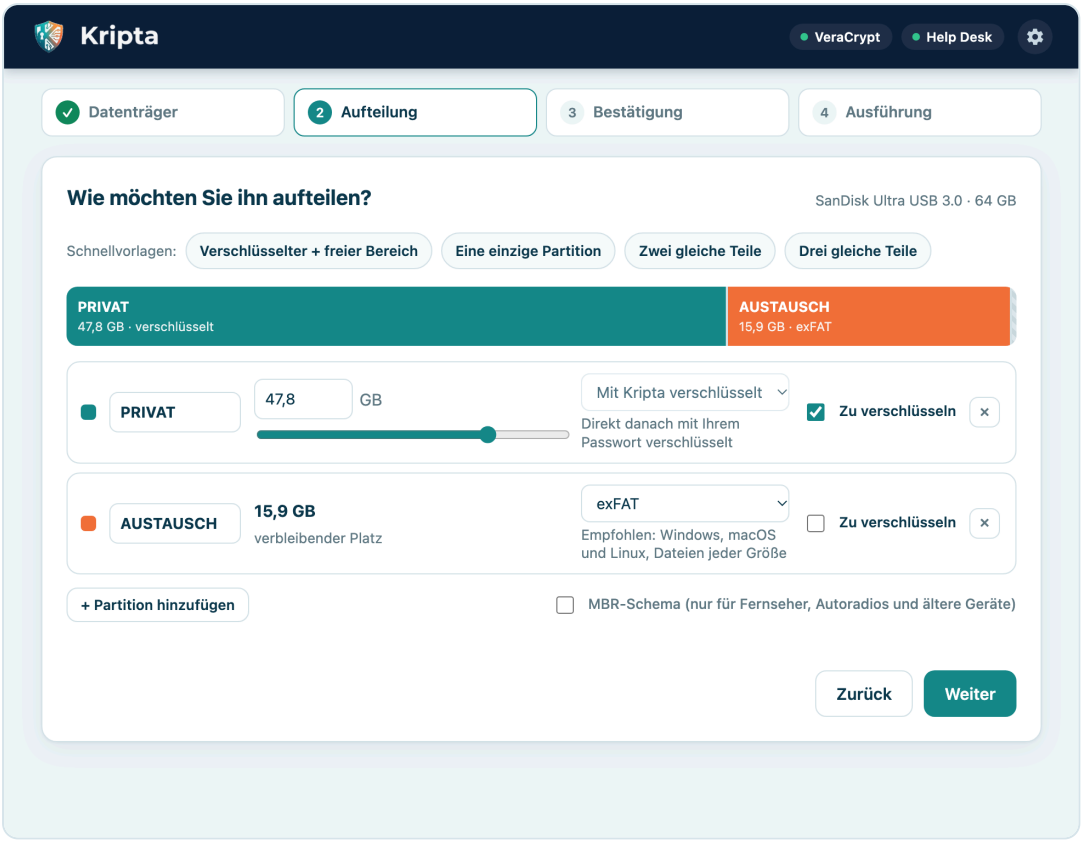
> **Das Aufteilen löscht den gesamten Datenträger**
> , einschließlich vorhandener Partitionen und bereits verschlüsselter Laufwerke. Sichern Sie zu behaltende Dateien woanders.

Schritt 1 — Datenträger



Auswahl des Datenträgers mit seinen aktuellen Partitionen.

Schritt 2 — Aufteilung



Der farbige Balken zeigt die Aufteilung maßstabsgetreu.

Vorlage	Ergebnis
Verschlüsselter + freier Bereich	Drei Viertel des Datenträgers zum Verschlüsseln, der Rest frei in exFAT. Diese Vorlage wird anfangs vorgeschlagen.
Eine einzige Partition	Der ganze Datenträger in einer Partition.
Zwei / Drei gleiche Teile	Der Datenträger in gleich große Teile aufgeteilt.

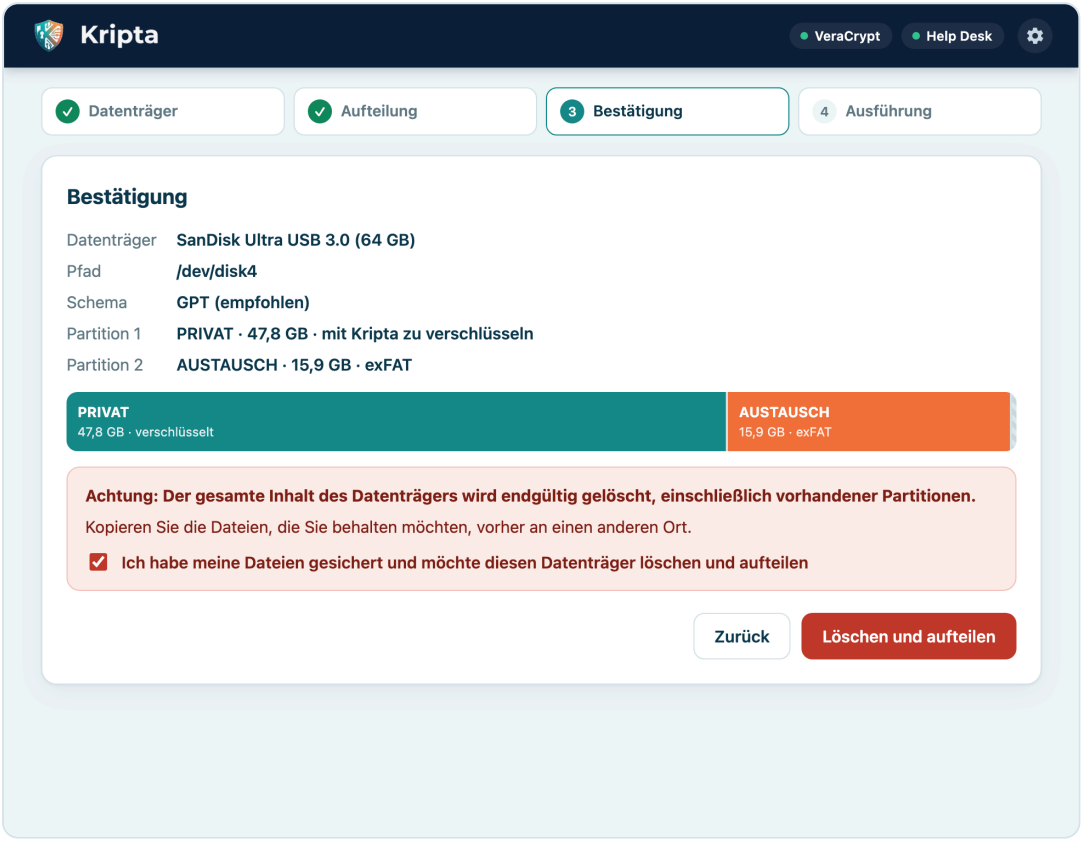
Für jede Partition legen Sie **Name** (bis 11 Zeichen: Buchstaben, Ziffern, `_` und `-`), **Größe** (die letzte erhält den restlichen Platz), **Dateisystem** und **Zu verschlüsseln** fest. **+ Partition hinzufügen** fügt eine weitere hinzu (bis 8).

Dateisystem	Lesbar unter	Hinweise
exFAT (empfohlen)	Windows, macOS, Linux	Keine praktische Grenze für die Dateigröße.
FAT32	Fast jedes Gerät	Dateien bis 4 GB; unter Windows Partitionen bis 32 GB.
NTFS	Windows; macOS nur lesend	Unter Linux ist `ntfs-3g` nötig.
APFS, **Mac OS Extended**	Nur Mac	Nur auf einem Mac verfügbar.

Dateisystem	Lesbar unter	Hinweise
ext4	Nur Linux	Nur unter Linux verfügbar.

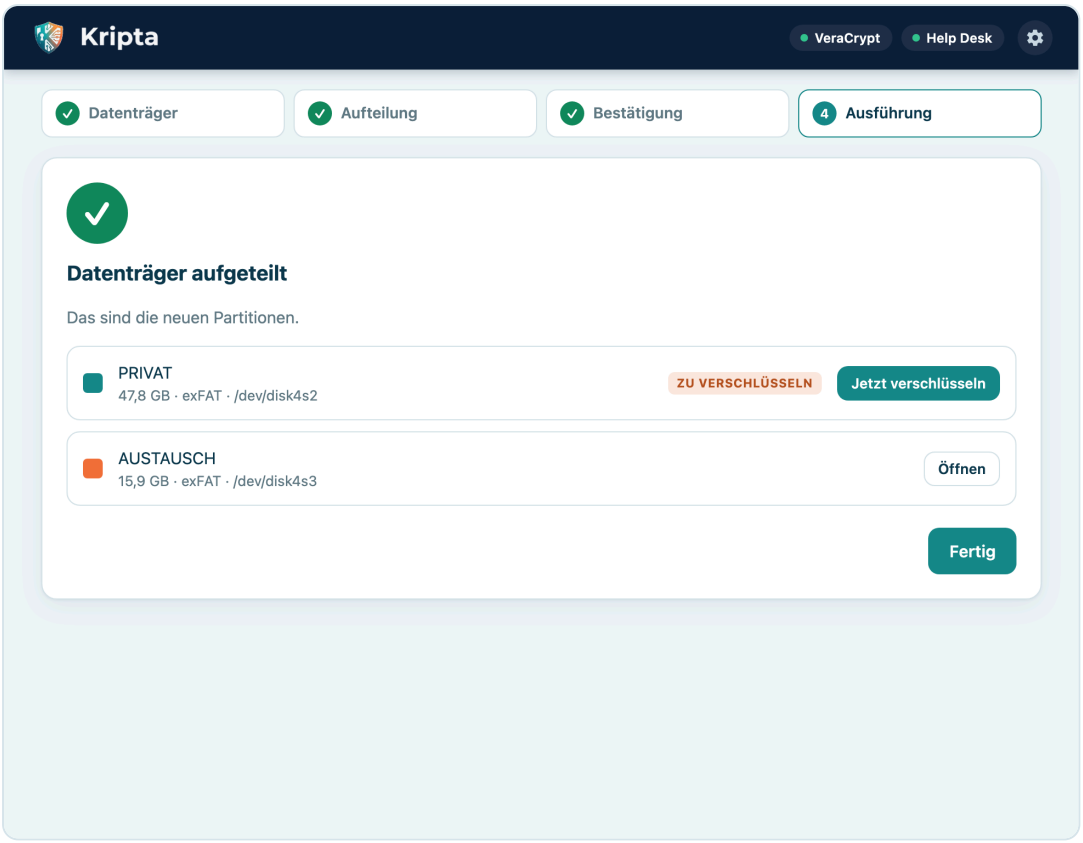
> **MBR-Schema**
> Nur aktivieren, wenn der Stick mit Fernsehern, Autoradios oder sehr alten Computern funktionieren muss: höchstens 4 Partitionen und 2 TB.

Schritt 3 — Bestätigung und Schritt 4 — Ausführung



Zusammenfassung vor dem Löschen.

Aktivieren Sie das Bestätigungskästchen und klicken Sie auf **Löschen und aufteilen**. Meist dauert es weniger als eine Minute.



Partitionen erstellt: Der zu verschlüsselnde Bereich hat die Schaltfläche „Jetzt verschlüsseln“.

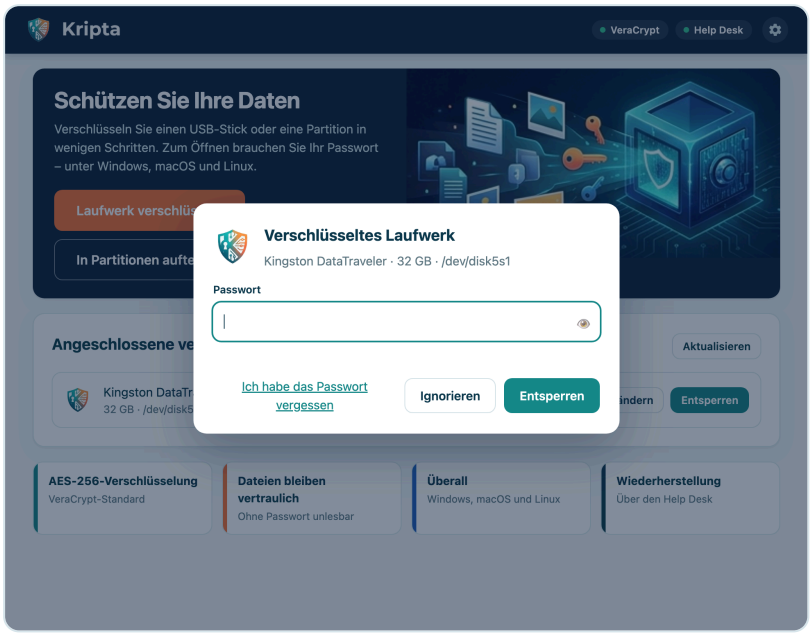
Neben den zu verschlüsselnden Partitionen klicken Sie auf **Jetzt verschlüsseln**: Die Verschlüsselung (Kapitel 4) beginnt mit der bereits gewählten Partition.

> **Bis zur Verschlüsselung ist der Bereich „zu verschlüsseln“ ungeschützt**
> Kopieren Sie vorher keine vertraulichen Dateien darauf.

6 Ein verschlüsseltes Laufwerk verwenden

Entsperren

Wenn Sie ein verschlüsseltes Laufwerk anschließen, während Kripta läuft, erscheint automatisch die Passwortabfrage.



Passwortabfrage beim Anschließen.

1. Geben Sie das Passwort ein und klicken Sie auf **Entsperren** (oder Eingabe).
2. Das Laufwerk öffnet sich wie ein normaler Datenträger im Explorer, im Finder oder im Linux-Dateimanager.
3. Mit **Ignorieren** entsperren Sie es später im Hauptfenster.

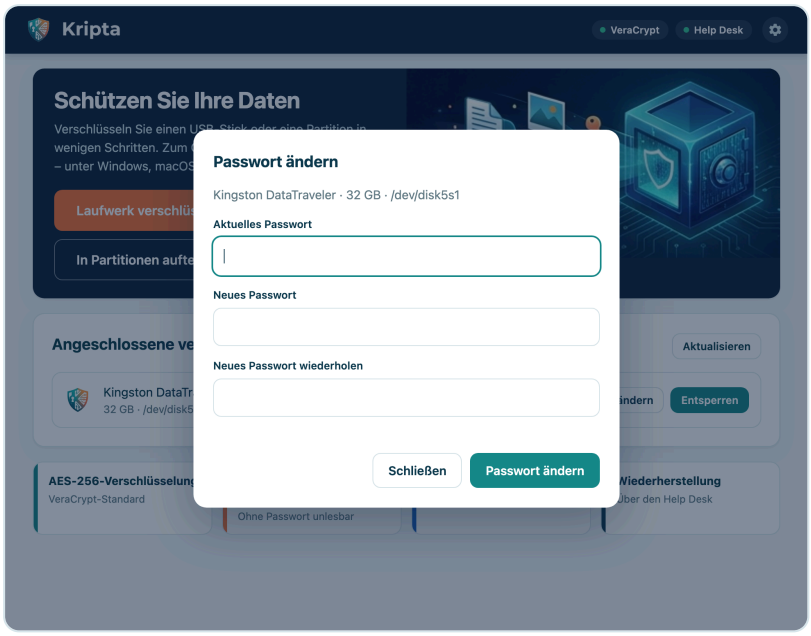
Mit Dateien arbeiten und sperren

Bei entsperrtem Laufwerk arbeiten Sie normal mit Dateien: Alles, was Sie schreiben, wird transparent verschlüsselt. Schließen Sie danach die geöffneten Dateien, klicken Sie auf **Sperren** und trennen Sie das Laufwerk.

> **Trennen Sie kein entsperrtes Laufwerk, ohne es zu sperren**
> Sie könnten gerade kopierte Dateien verlieren.

7 Passwort ändern

Sie können das Passwort jederzeit ändern, wenn Sie das aktuelle kennen. Die Daten auf dem Laufwerk bleiben unberührt.



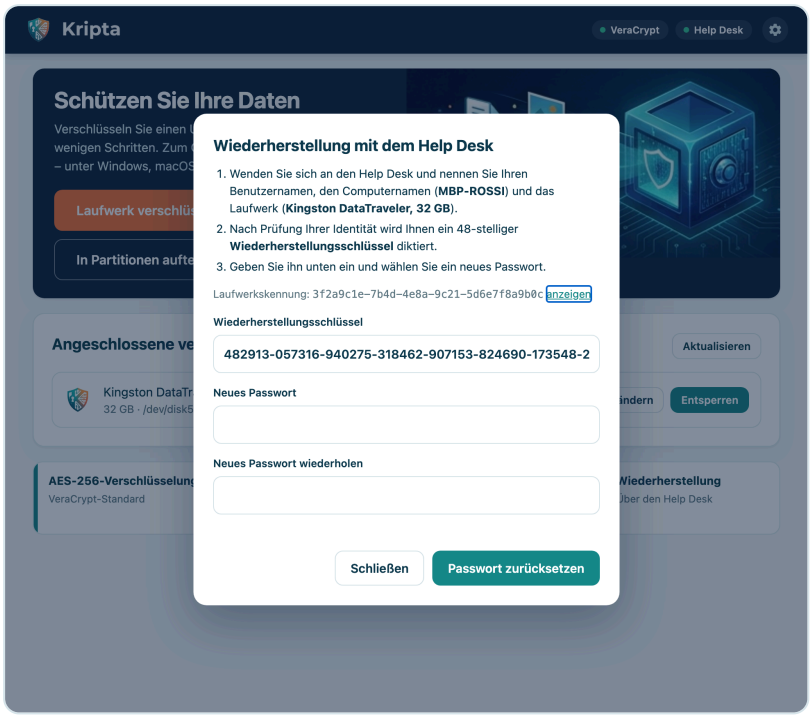
Fenster Passwort ändern.

1. Ist das Laufwerk entsperrt, klicken Sie zuerst auf **Sperren**.
2. Klicken Sie neben dem Laufwerk auf **Passwort ändern**.
3. Geben Sie das aktuelle und zweimal das neue Passwort ein (gleiche Regeln wie in Kapitel 4) und bestätigen Sie.

> **Und der Wiederherstellungsschlüssel?**
> Er bleibt gültig: Der Help Desk kann Ihnen auch nach einer Passwortänderung helfen.

8 Passwort vergessen

Der Help Desk kann Ihnen den Wiederherstellungsschlüssel des Laufwerks geben: Damit setzen Sie ein neues Passwort und erhalten alle Dateien zurück.



Wiederherstellung mit dem Help Desk.

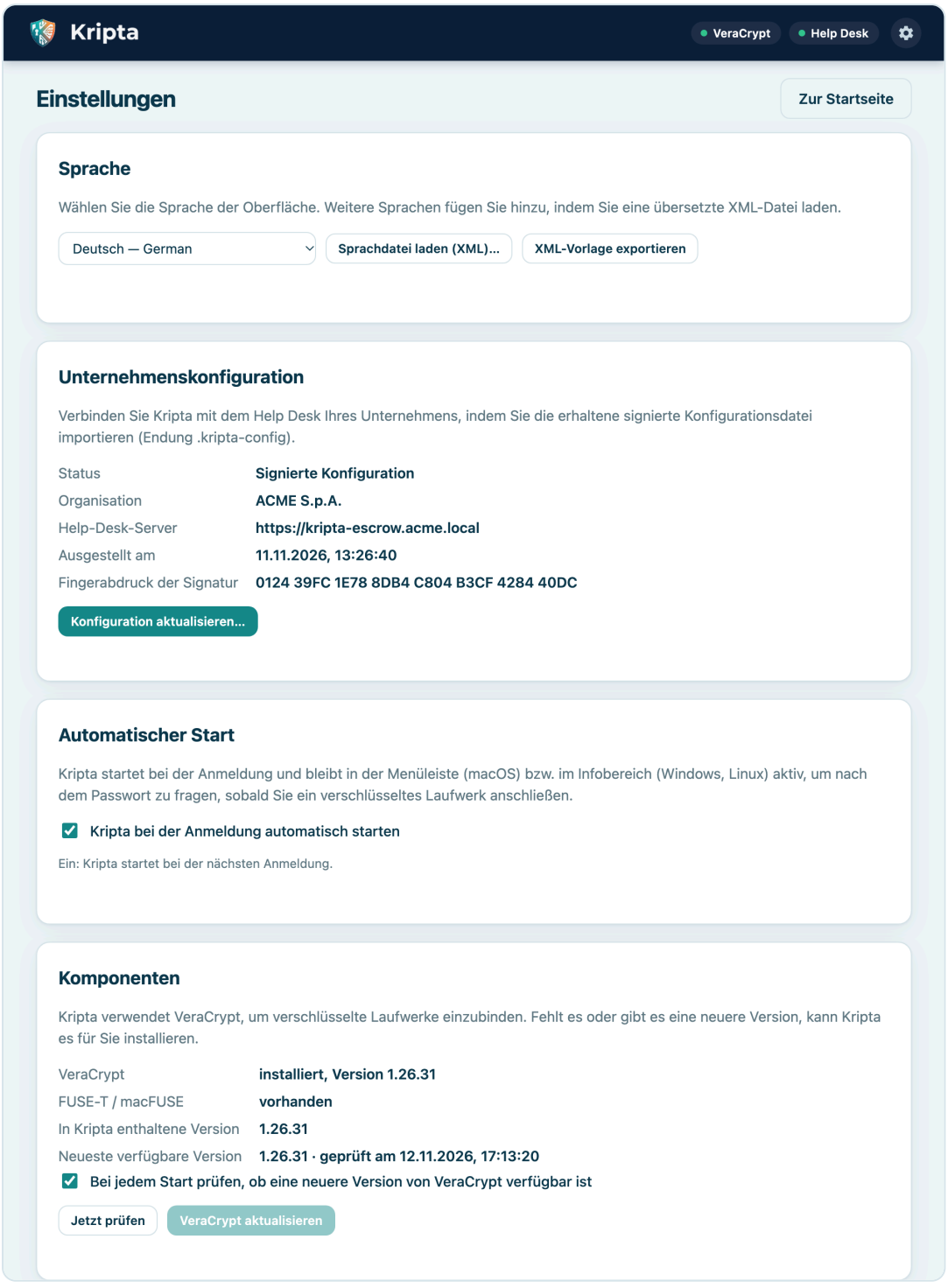
1. Wählen Sie in der Passwortabfrage **Ich habe das Passwort vergessen**.
2. Das Fenster zeigt Computer- und Laufwerksnamen; mit **anzeigen** erscheint auch die Laufwerkskennung.
3. **Wenden Sie sich an den Help Desk** und nennen Sie diese Angaben. Nach Prüfung Ihrer Identität wird Ihnen der **48-stellige Schlüssel** diktiert.
4. Geben Sie ihn im Feld **Wiederherstellungsschlüssel** ein, wählen Sie ein neues Passwort und klicken Sie auf **Passwort zurücksetzen**.

> **Ein Schlüssel, eine Verwendung**
> Nach jeder Wiederherstellung erzeugt Kripta einen neuen Schlüssel und sendet ihn an den Help Desk.

> **Vorsicht vor Betrug**
> Der Help Desk fragt Sie nie nach Ihrem Passwort. Sie kontaktieren den Help Desk, nicht umgekehrt.

9 Einstellungen

Sie öffnen sich über das Zahnrad oben rechts oder über **Einstellungen…** im Symbolmenü.



Die Einstellungen: Sprache, Unternehmenskonfiguration, Komponenten, Info.

Sprache

Wählen Sie die Sprache aus der Liste: Oberfläche, Symbolmenü und Autorisierungsanfragen wechseln sofort. Mit **Automatisch** verwendet Kripta die Systemsprache. Enthaltene Sprachen:

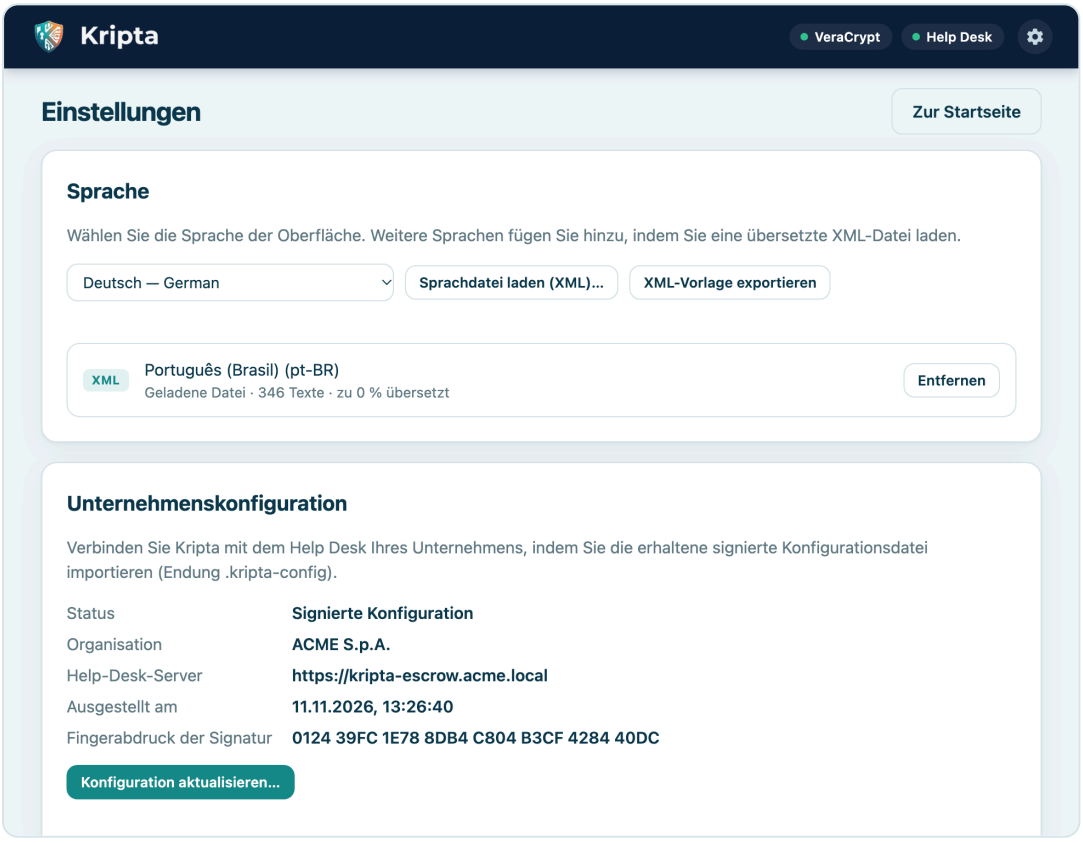
Italiano English Français Español Deutsch Русский العربية 中文 日本語

Eine Sprache hinzufügen

Übersetzungen sind einfache **XML**-Dateien, eine pro Sprache. So fügen Sie eine hinzu:

1. Klicken Sie auf **XML-Vorlage exportieren**: Die Datei der aktuellen Sprache wird im Ordner Downloads gespeichert.
2. Übersetzen Sie den Text jedes `<string>`-Elements; die Attribute `id` und die Platzhalter `{1}`, `{2}` bleiben unverändert.
3. Setzen Sie oben in der Datei `code` (zum Beispiel `pt` oder `pt-BR`), `name`, `english-name` und `dir` (`rtl` für Sprachen, die von rechts nach links geschrieben werden).
4. Klicken Sie auf **Sprachdatei laden (XML)…** und wählen Sie die Datei: Die Sprache erscheint in der Liste mit dem Anteil übersetzter Texte. Fehlende Texte werden auf Englisch angezeigt.

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



Eine aus einer XML-Datei geladene Sprache mit der Schaltfläche Entfernen.

Eine Datei mit demselben Code wie eine enthaltene Sprache ersetzt diese (nützlich, um einen Begriff zu korrigieren); **Entfernen** stellt das Original wieder her. Die Dateien der neun enthaltenen Sprachen liegen neben diesem Handbuch im Ordner `lang`.

Unternehmenskonfiguration

Zeigt Organisation, Help-Desk-Server, Datum und Fingerabdruck der installierten Konfiguration. **Konfiguration aktualisieren…** importiert eine neue Datei vom Help Desk (Kapitel 2).

Komponenten

Zeigt die installierte VeraCrypt-Version, die in Kripta enthaltene und die neueste verfügbare. **Jetzt prüfen** prüft sofort, **Installieren** / **VeraCrypt aktualisieren** startet die Installation. Das Kästchen **Bei jedem Start prüfen…** schaltet die automatische Prüfung ein oder aus.

Automatischer Start

Das Kästchen **Kripta bei der Anmeldung automatisch starten** ist standardmäßig aktiviert. Darunter wird angezeigt, ob der automatische Start im System registriert ist. Wenn Sie es deaktivieren, erkennt Kripta verschlüsselte Laufwerke erst, wenn Sie es öffnen.

10 Das Laufwerk an anderen Computern verwenden

Von Kripta verschlüsselte Laufwerke verwenden das Standardformat von **VeraCrypt** mit dem Dateisystem **exFAT**: Sie öffnen sich unter Windows, macOS und Linux.

Computer	Was beim Anschließen passiert
Mit konfiguriertem Kripta	Die Passwortabfrage erscheint: alles automatisch.
Mit installiertem Kripta, aber **ohne Unternehmenskonfiguration** (z. B. zu Hause)	Die Passwortabfrage erscheint trotzdem und das Laufwerk wird entsperrt. Fehlt VeraCrypt, bietet Kripta **Jetzt installieren** an. Ohne Konfiguration können Sie keine neuen Laufwerke verschlüsseln und keine Passwörter wiederherstellen.
Nur mit VeraCrypt	Öffnen Sie VeraCrypt, wählen Sie einen freien Slot, **Datenträger auswählen**, die Partition des Sticks, dann **Einbinden** und geben Sie das Passwort ein.
Ohne Kripta und VeraCrypt	Es erscheint keine Abfrage: Betriebssysteme starten keine Programme von USB-Sticks. Das System schlägt eventuell vor, das Laufwerk zu **formatieren**: **immer ablehnen**. Installieren Sie Kripta (von der Unternehmenswebsite) und schließen Sie das Laufwerk erneut an.

Administratorrechte

Zum Öffnen eines verschlüsselten Laufwerks sind auf jedem Computer Administratorrechte nötig, da VeraCrypt einen Systemtreiber verwendet. Auf einem Computer ohne Ihre Zugangsdaten lässt sich das Laufwerk nicht öffnen.

Freier Bereich zum Austausch

Nutzen Sie oft Computer ohne Kripta, teilen Sie den Stick mit der Vorlage **Verschlüsselter + freier Bereich** auf (Kapitel 5): In den freien Bereich können Sie auch das Kripta-Installationsprogramm kopieren.

11 Meldungen und Fehlerbehebung

Meldung oder Situation	Was tun
Kripta ist noch nicht mit dem Help Desk Ihres Unternehmens verbunden	Importieren Sie die vom Help Desk erhaltene Datei `.kripta-config` (Kapitel 2).
Die Signatur des Pakets ist ungültig	Die Datei wurde verändert oder ist beschädigt: Fordern Sie sie beim Help Desk erneut an.
Das Paket ist mit einem anderen / nicht genehmigten Schlüssel signiert	Die Datei stammt nicht von Ihrem Unternehmen. Nicht verwenden und den Help Desk kontaktieren.
Die Konfiguration wird von der IT verwaltet und kann nicht ersetzt werden	Der Computer ist zentral konfiguriert: Nichts zu importieren.
Die Verschlüsselungs-Engine VeraCrypt ist nicht installiert	Klicken Sie auf **Jetzt installieren**. Fehlt die Schaltfläche, wenden Sie sich an den Help Desk.
Die offizielle VeraCrypt-Signatur ist ungültig / die Datei entspricht nicht der signierten Version	Der Download wurde verändert oder ist unvollständig: Die Installation wurde abgebrochen. Später erneut versuchen.
Sperren Sie alle verschlüsselten Laufwerke, bevor Sie VeraCrypt aktualisieren	Klicken Sie bei den geöffneten Laufwerken auf **Sperren** und wiederholen Sie die Aktualisierung.
Starten Sie den Computer neu, um die Aktualisierung abzuschließen (Windows)	Speichern Sie Ihre Arbeit und starten Sie neu.
Der Help-Desk-Server ist nicht erreichbar. Die Verschlüsselung wurde nicht gestartet.	Verbinden Sie sich mit dem Unternehmensnetz oder VPN und versuchen Sie es erneut. Die Daten auf dem Laufwerk wurden nicht verändert.
Wiederherstellungsschlüssel warten auf Versand	Verbinden Sie sich mit dem Netz und klicken Sie auf **Jetzt erneut versuchen**. Lassen Sie Kripta geöffnet, bis der Hinweis verschwindet.
Kein Laufwerk verfügbar	Schließen Sie den Stick erneut an (anderen USB-Anschluss versuchen) und klicken Sie auf **Liste aktualisieren**.
Administrator-Autorisierung abgebrochen / Zeitüberschreitung	Wiederholen Sie den Vorgang und bestätigen Sie die Anfrage des Systems.
Volume kann nicht ausgehängt / gesperrt werden	Schließen Sie die vom Laufwerk geöffneten Dokumente und Fenster und versuchen Sie es erneut.
Falsches Passwort	Prüfen Sie die Feststelltaste und das Tastaturlayout. Haben Sie es vergessen, siehe Kapitel 8.
Falscher Wiederherstellungsschlüssel	Prüfen Sie die Ziffern mit dem Mitarbeiter erneut: Es wird der **neueste** Schlüssel benötigt.

Meldung oder Situation	Was tun
Auf dem Datenträger befindet sich ein entsperrtes Kripta-Laufwerk	Sperren Sie es auf der Startseite und wiederholen Sie die Aufteilung.
Das System hat die neuen Partitionen nicht erkannt	Trennen Sie das Laufwerk und schließen Sie es wieder an.
Die Sprachdatei ist kein gültiges XML / Element nicht erlaubt	Korrigieren Sie die genannte Datei: Erlaubt sind nur `<string>`-Elemente mit reinem Text.
Das Entsperrfenster erscheint beim Anschließen nicht	Prüfen Sie, ob Kripta läuft (Symbol in der Leiste), und verwenden Sie **Entsperren** im Hauptfenster.

12 Häufige Fragen

Kann ich einen Stick mit vorhandenen Dateien verschlüsseln, ohne sie zu verlieren?

Nein. Die Verschlüsselung löscht das Laufwerk. Kopieren Sie die Dateien woandershin, verschlüsseln Sie das Laufwerk und kopieren Sie sie zurück.

Kann ich die interne Festplatte meines Computers verschlüsseln?

Nein. Kripta ist für Sticks und externe Festplatten gedacht; Systemlaufwerke werden nicht angezeigt.

Kann der Help Desk meine Dateien lesen?

Der Help Desk bewahrt nur den Wiederherstellungsschlüssel auf und kann ihn nur auf Ihre Anfrage abrufen; jeder Zugriff wird protokolliert.

Muss ich mir den Wiederherstellungsschlüssel notieren?

Nein. Sie sehen ihn nie und müssen ihn nicht aufbewahren: Er ist beim Help Desk hinterlegt.

Installiert Kripta Programme auf meinem Computer?

Nur VeraCrypt (und FUSE-T unter macOS), nach Ihrer Bestätigung und nur bei gültiger offizieller Signatur der Entwickler.

Kann ich den Stick an einem privaten Computer verwenden?

Ja, durch Installation von Kripta oder VeraCrypt (Kapitel 10). Beachten Sie stets die Unternehmensregeln zur Nutzung von Daten außer Haus.

Meine Sprache fehlt. Was kann ich tun?

Sie können die XML-Vorlage übersetzen und in den Einstellungen laden (Kapitel 9) oder die IT bitten, eine zu verteilen.

Warum darf das Passwort keine Umlaute enthalten?

Windows, macOS und Linux können sie unterschiedlich kodieren: Dasselbe Passwort auf einem anderen System wird eventuell nicht erkannt.

Wie viel Platz kostet die Verschlüsselung?

Sehr wenig: einige hundert Kilobyte für die Volume-Header.

A Anhang für die IT

Pakete

System	Paket	Hinweise
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	Enthält die offiziellen VeraCrypt-MSI (x64 und ARM64). Die App startet mit Administratorrechten.
macOS 11+	`Kripta_1.2.0_universal.dmg`	Enthält VeraCrypt (FUSE-T- und macFUSE-Variante) und FUSE-T, das keine Kernel-Erweiterung benötigt.
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	Enthält VeraCrypt für Ubuntu 22.04/24.04 und Debian 12/13; für andere Versionen lädt Kripta das geprüfte Paket herunter.
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	Enthält VeraCrypt für Fedora 44; zusätzlich `exfatprogs` installieren.
Andere Distributionen	`Kripta_1.2.0_amd64.AppImage`	Portable Programmdatei.

Signierte Konfiguration

Auf dem Escrow-Server einmalig den Signaturschlüssel erzeugen; dann die Client-Konfiguration signieren (Vorlage in `deploy/client/kripta.toml.example`):

```
kripta-escrow keygen-sign            # privater Schlüssel (offline aufbewahren) + öffentlicher
+ Fingerabdruck
kripta-escrow sign-config client.toml signatur.key "ACME GmbH" acme.kripta-config
```

`acme.kripta-config` an die Benutzer verteilen und den **Fingerabdruck** über einen vertrauenswürdigen Kanal veröffentlichen (Intranet, Help-Desk-Telefon). Kripta speichert die Konfiguration über den privilegierten Prozess am Systemort (`%ProgramData%\Kripta`, `/Library/Application Support/Kripta`, `/etc/kripta`), zusammen mit dem Schlüssel des Unterzeichners: Spätere Aktualisierungen müssen dieselbe Signatur tragen. Um nicht auf die Prüfung des Fingerabdrucks durch Benutzer angewiesen zu sein, Kripta mit `KRIPTA_PROVISIONING_KEYS=<öffentlicher Schlüssel>` bauen: Dann werden nur diese Schlüssel akzeptiert. Eine von der IT manuell kopierte (unsignierte) Konfiguration kann nicht durch ein Paket ersetzt werden.

Installation und Aktualisierung von VeraCrypt

- Die enthaltenen Installationsprogramme werden beim Build mit `scripts/fetch-veracrypt.py` bereitgestellt.
- Vor der Installation prüft der privilegierte Prozess die OpenPGP-Signatur der offiziellen SHA-256-Liste mit dem eingebetteten IDRIX-Schlüssel (Fingerabdruck `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`) und den Hash der Datei.

- Optionen in `kripta.toml`: `veracrypt_update_check = false` schaltet die Aktualisierungsprüfung ab; `veracrypt_release_api = "https://spiegel.intern/…"` verwendet einen internen Spiegel im Format der GitHub-API.

Sprachen

Die XML-Sprachdateien liegen in `app/ui/lang/` (in der App enthalten) und in `docs/manuale/lang/`. Von Benutzern geladene Sprachen werden im Datenordner des Benutzers gespeichert (`languages/`). Um eine neue Sprache allen bereitzustellen, die Datei in `app/ui/lang/` ablegen und den Code in die Liste in `app/ui/i18n.js` eintragen.

Optionale Komponenten

- **Start bei der Anmeldung** in Menüleiste / Infobereich (`kripta --background`): **automatisch**. Kripta registriert ihn bei jedem Start (macOS: `~/Library/LaunchAgents/com.kripta.agent.plist`, Neustart bei abnormalem Ende; Windows: geplante Aufgabe „Kripta“ bei Anmeldung mit höchsten Rechten, auch vom Installer angelegt und bei der Deinstallation entfernt; Linux: `/etc/xdg/autostart/kripta.desktop` aus den .deb/.rpm-Paketen, `~/.config/autostart/kripta.desktop` für das AppImage). Abschaltbar in den Einstellungen.
- **Privilegierter Helfer** als Dienst (keine Passwortabfragen): `deploy/macos/com.kripta.helper.plist`, `deploy/linux/kripta-helper.service`.