Kripta

User manual

Guided encryption of USB sticks and partitions, with password recovery through your company Help Desk.



Version 1.2 · Windows · macOS · Linux

November 2026

Contents

1 What Kripta is — what it does, what you need

2 First start — company configuration and components

3 The main window — indicators, alerts, menu bar icon

4 Encrypting a drive — the 4-step wizard

5 Splitting a disk into partitions — encrypted area and free area

6 Using an encrypted drive — unlock, open, lock

7 Changing the password

8 I forgot the password — recovery with the Help Desk

9 Settings — language, configuration, updates

10 Using the drive on other computers

11 Messages and troubleshooting

12 Frequently asked questions

A Appendix for IT — packages, signed configuration, languages

Conventions

Text shown on screen (buttons, titles, items) is written like this: **Encrypt a drive**. Screenshots come from the macOS version: on Windows and Linux the window is identical, only device names differ (for example `E:` or `/dev/sdb1` instead of `/dev/disk4s1`).

1 What Kripta is

Kripta protects the data on your **USB sticks** and on **partitions** of external disks with AES-256 encryption. After encryption, the content of the drive can only be read by someone who knows the password: if you lose the stick, nobody else can open it.

Guided encryption
Four steps: choose the drive, choose the password, confirm, wait.

Automatic unlock
When you connect an encrypted drive, Kripta asks for the password right away and opens it.

Works everywhere
The same stick opens on Windows, macOS and Linux (standard VeraCrypt format).

Self-service setup
Kripta installs and updates VeraCrypt by itself; the company configuration is imported from a file.

Nine languages
Italian, English, French, Spanish, German, Russian, Arabic, Chinese and Japanese, plus any you add.

Recovery with the Help Desk
If you forget the password, the Help Desk can help you set a new one without losing data.

What you need

- **Kripta** installed on the computer. At first start Kripta installs **VeraCrypt**, the encryption engine (on macOS also **FUSE-T**), if it is missing: chapter 2.
- The **signed configuration file** (`.kripta-config`) received from the Help Desk, unless IT has already configured the computer.
- A **connection to the company network** (or VPN) when you encrypt a new drive: the recovery key is sent to the Help Desk immediately. Unlocking an already encrypted drive does not need the network.
- The computer's **administrator credentials**, when the system asks for them (see box).

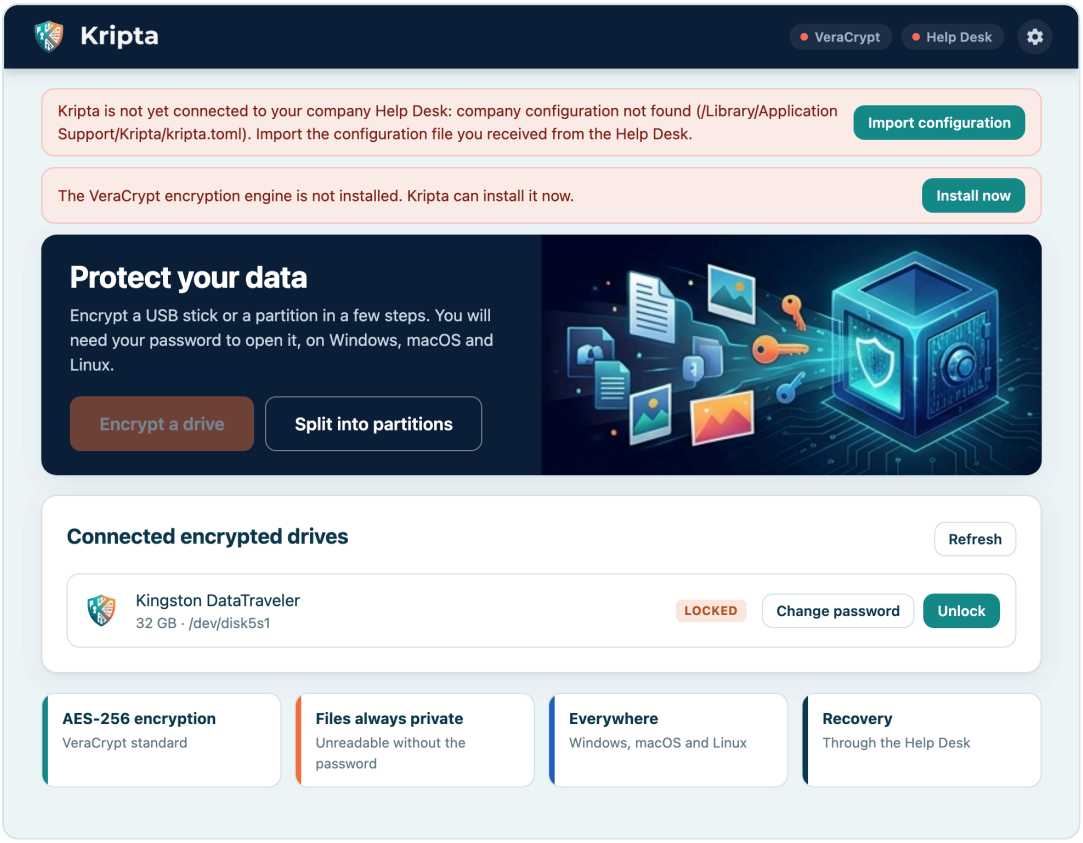
> **Authorization requests**
> To read and write directly on the drive, install components and save the configuration, Kripta needs administrator rights. On **Windows** the User Account Control window appears at start. On **macOS** and **Linux** the message “Kripta needs administrator authorization to complete the operation” appears. If IT has installed the Kripta system service, these requests do not appear.

How recovery works, in short

During encryption Kripta generates a 48-digit **recovery key**, protects it and sends it to the Help Desk archive. You never need to see or keep it. Only Help Desk operators can look it up, after verifying your identity, and every lookup is logged.

2 First start

At first start Kripta checks two things: whether it is connected to your company Help Desk and whether VeraCrypt is on the computer. If something is missing, an alert with a button to fix it appears at the top of the window. You can do everything yourself.

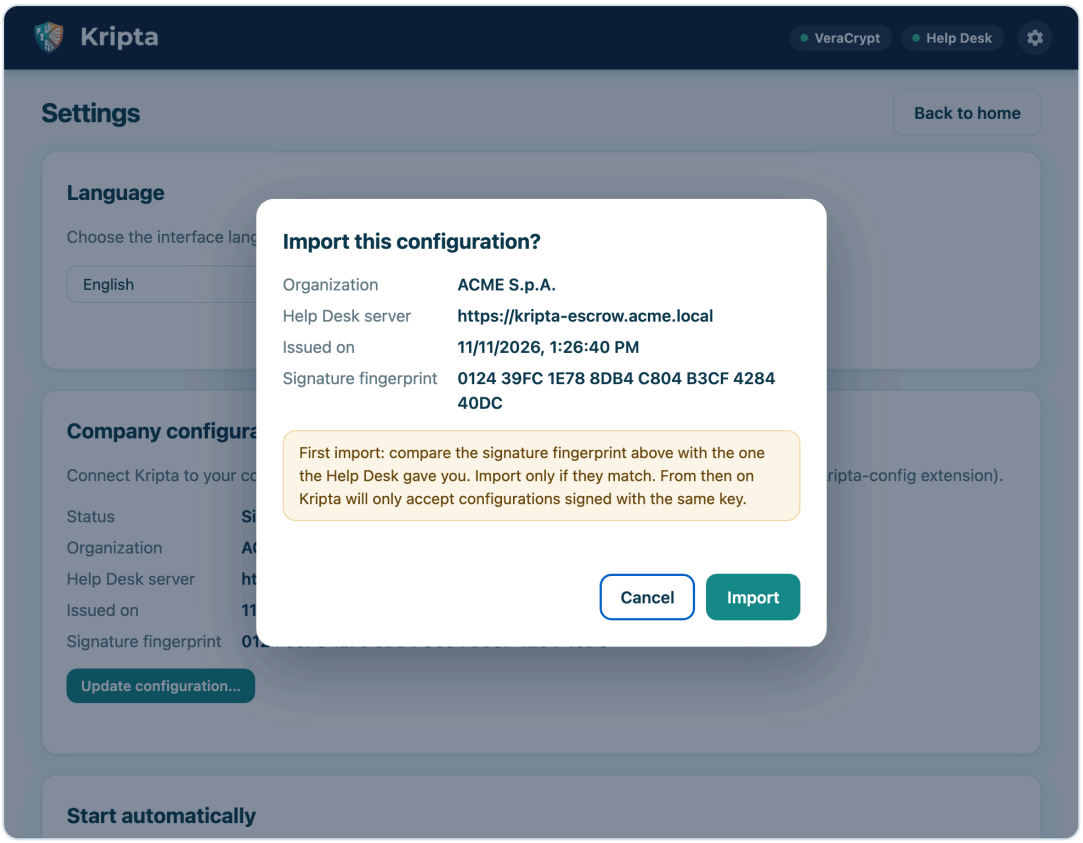


First start: configuration to import and VeraCrypt to install.

Importing the company configuration

The configuration tells Kripta which Help Desk archive to send recovery keys to. The Help Desk gives it to you as a file with the `.kripta-config` extension, digitally signed: nobody can change it without Kripta noticing.

1. Save the file you received on the computer (by e-mail, from the company portal or on a stick).
2. Press **Import configuration** in the alert, or open **Settings** (the gear at the top right) and press **Import signed configuration…**.
3. Choose the file. Kripta checks its signature and shows organization, Help Desk server, issue date and **signature fingerprint**.
4. On the first import **compare the fingerprint** with the one the Help Desk gave you (by phone, on the intranet…). If it matches, press **Import**.
5. Confirm the system authorization request. **Configuration imported** appears and the **Help Desk** indicator turns green.

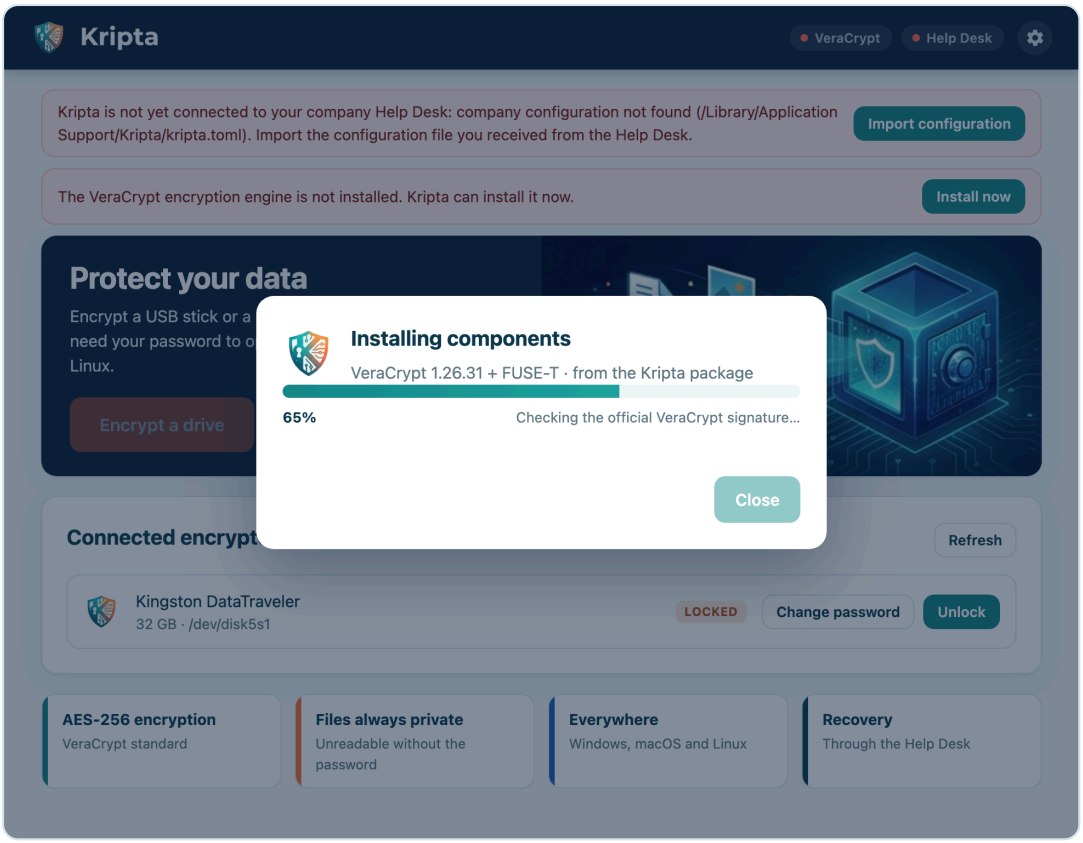


Confirming the import with the signature fingerprint.

> **If the fingerprint does not match, do not import**
>
> The file might not come from your company. Cancel and contact the Help Desk. After the first import Kripta only accepts updates signed with the same key: a forged file is rejected automatically.

Installing VeraCrypt

Kripta already contains the official VeraCrypt installer (and FUSE-T for macOS). Press **Install now** in the alert and confirm the authorization request: Kripta checks the official signature of the installers and installs them without further questions.

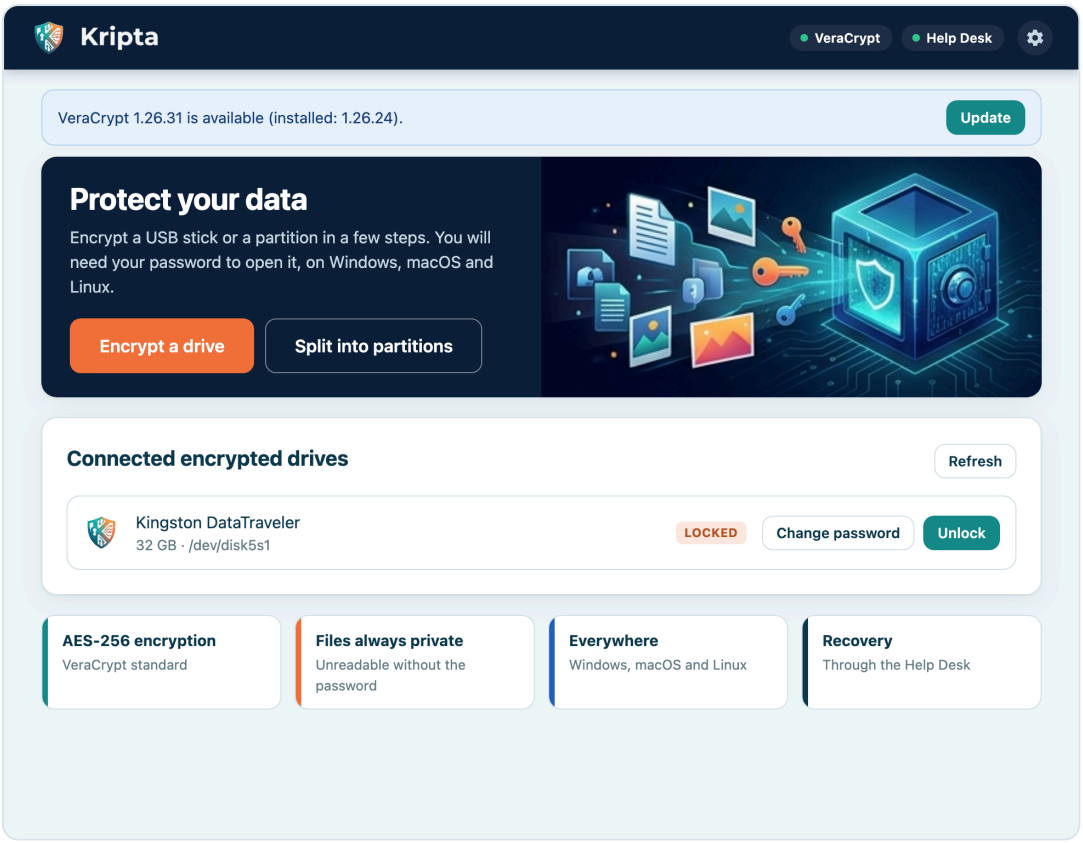


Installing components, with verification of the official signature.

When it finishes, **Installation completed** appears. On Windows a restart may be required.

VeraCrypt updates

At every start (and then once a day) Kripta checks whether a newer version of VeraCrypt has been released. If so, a blue alert appears with the **Update** button. The new version is downloaded from the official site and installed only if the VeraCrypt developers' signature is valid.



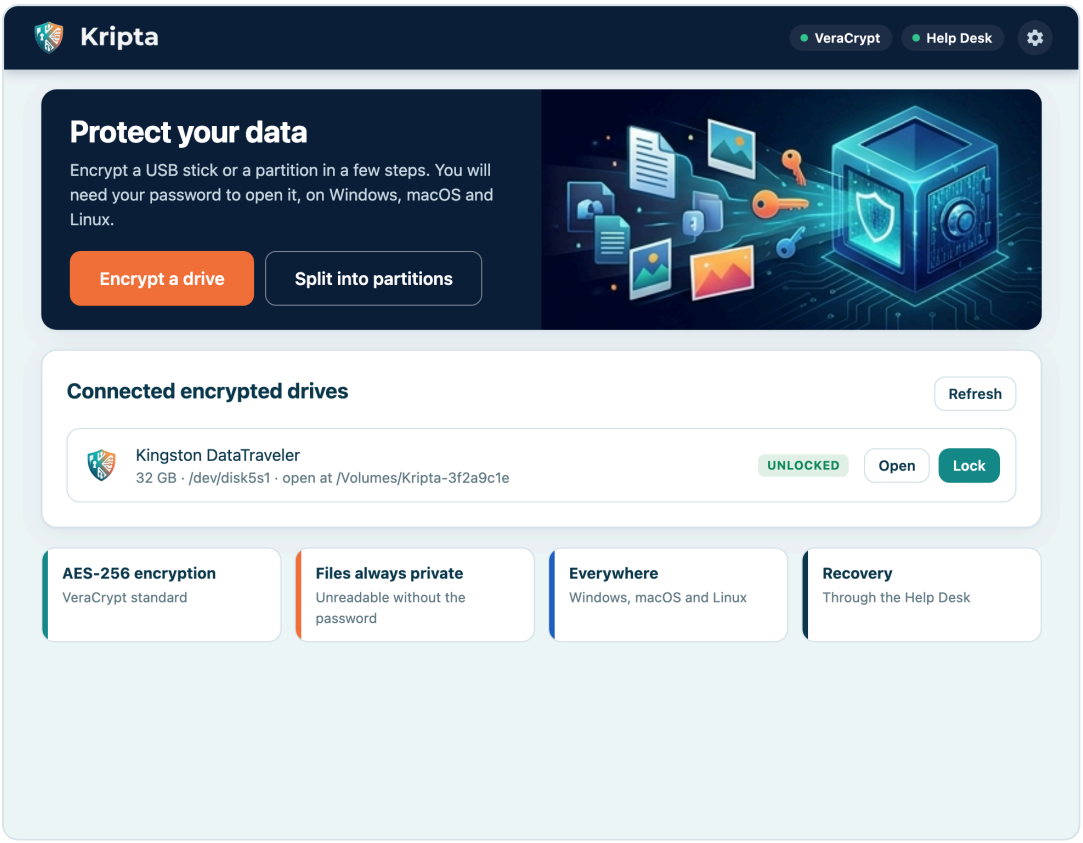
VeraCrypt update available.

Before updating

Lock all open encrypted drives: Kripta does not update VeraCrypt while a drive is unlocked. You can turn off the automatic check in Settings (chapter 9).

3 The main window

When it opens, Kripta shows the home screen. From here you can encrypt a new drive and manage the encrypted drives connected to the computer.

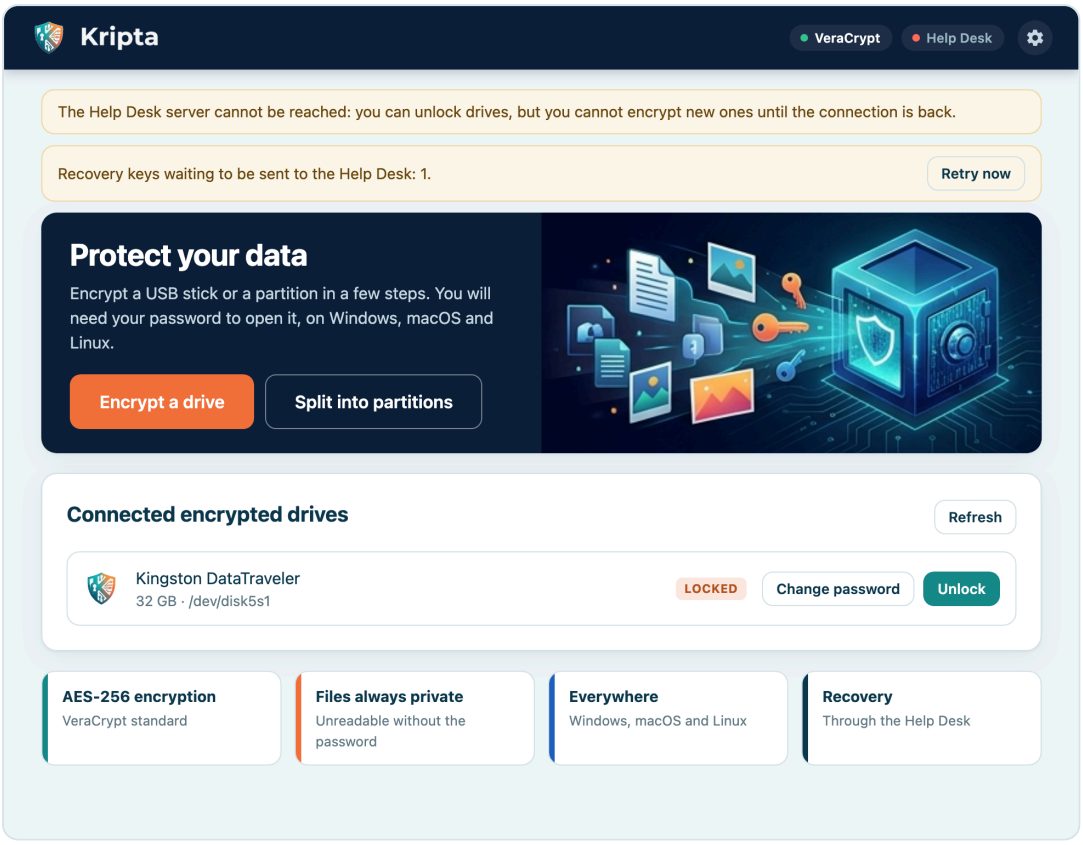


Home screen with an encrypted drive connected and unlocked.

Element	What it is for
VeraCrypt	**Green** dot: the encryption engine is installed. **Red**: it is not (chapter 2). Hover to see the version.
Help Desk	Green: the key archive can be reached. Red: it cannot (no network, VPN off, configuration missing).
Gear	Opens **Settings**: language, company configuration, components (chapter 9).
Encrypt a drive	Starts the wizard (chapter 4). Disabled if Kripta is not configured or VeraCrypt is missing.
Split into partitions	Splits a USB stick or an external disk into several partitions (chapter 5).
Connected encrypted drives	The Kripta drives connected, with status **Locked** or **Unlocked** and their buttons.

Alerts

Coloured boxes with a button to solve the problem may appear at the top of the window:



Help Desk server unreachable and one recovery key waiting to be sent.

- **Help Desk server unreachable:** you can still unlock drives, but not encrypt new ones.
- **Recovery keys waiting to be sent:** Kripta retries by itself; press **Retry now** when you are back online. **Keep Kripta running until the alert disappears.**
- **Kripta is not yet connected to the Help Desk / VeraCrypt is not installed / VeraCrypt … is available:** see chapter 2.

The Kripta icon: menu bar and notification area

Kripta works in the background to notice when you connect an encrypted drive, and is controlled from an icon with the emblem:

System	Where the icon is	Good to know
macOS	In the **menu bar** at the top right. Kripta **does not appear in the Dock**.	On MacBooks with a notch, extra icons are hidden when the bar is full: remove the ones you do not use or drag them while holding ⌘.
Windows	In the **notification area** at the bottom right, near the clock.	If it is among the hidden icons, click the ^ arrow and drag the emblem onto the bar.

System	Where the icon is	Good to know
Linux	In the panel's **notification area**.	On “plain” GNOME (Fedora, Debian) the **AppIndicator and KStatusNotifierItem Support** extension is needed.

The icon menu contains **Open Kripta**, **Encrypt a drive…**, **Split into partitions…**, **Lock all drives**, **Settings…** and **Quit Kripta**. The items follow the chosen language.

> **Closing the window does not quit Kripta**
>
> Kripta stays active in the menu bar or notification area. To reopen the window use **Open Kripta**, or start Kripta again: the window already running will be shown.

Automatic start

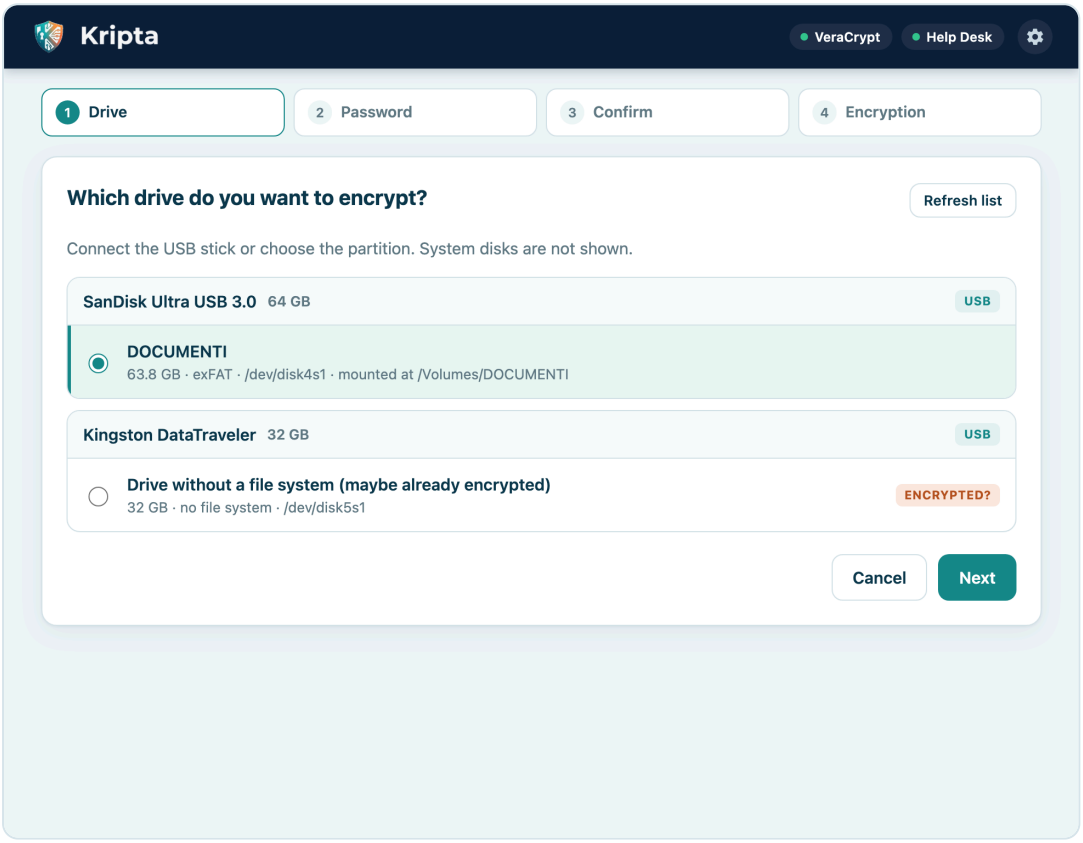
After installation Kripta **starts by itself every time you sign in**, without opening the window, and keeps listening: as soon as you connect an encrypted drive it asks for the password. You can turn this off in **Settings › Start automatically** (chapter 9). **Quit Kripta** closes it until your next sign-in.

4 Encrypting a drive

> **Encryption erases the whole content of the drive.**
> Before starting, copy the files you want to keep somewhere else. After encryption you can copy them back onto the protected drive.

Connect the stick, check that the **Help Desk** indicator is green and press **Encrypt a drive**.

Step 1 — Drive

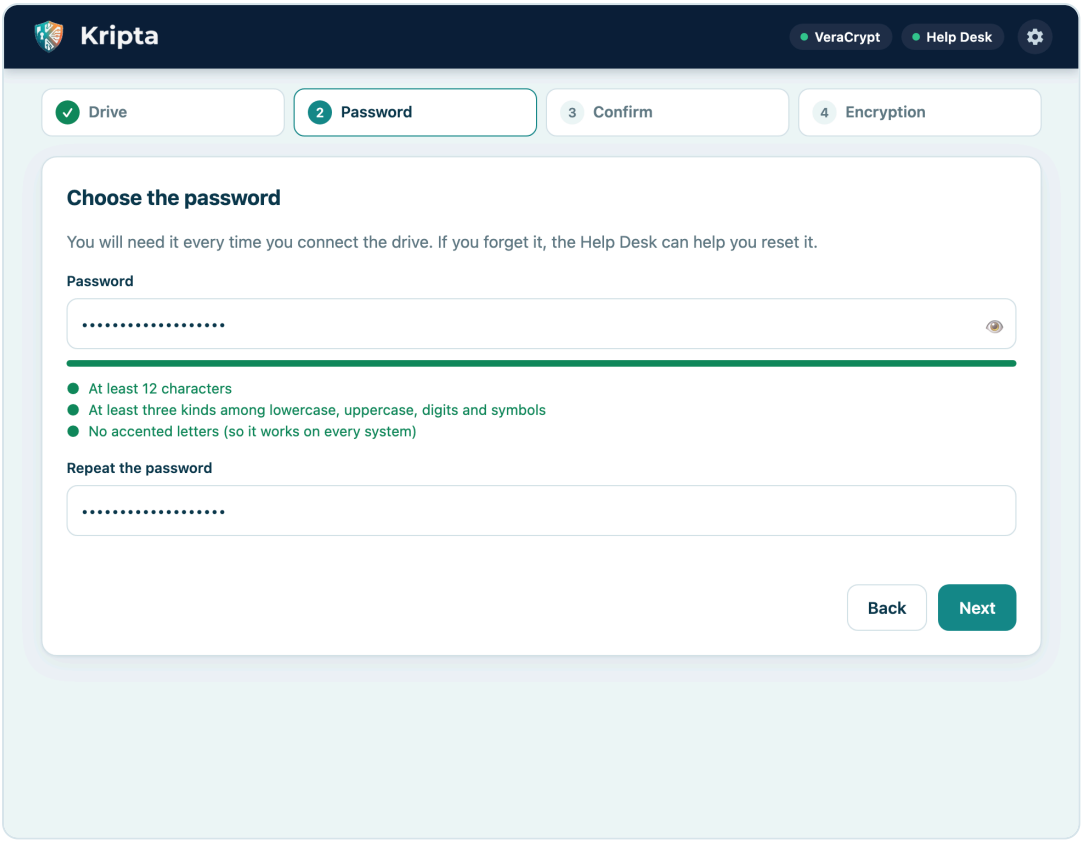


Choosing the drive to encrypt.

1. Kripta lists the connected devices, removable ones first. **System disks are never shown**.
2. Check **capacity and name** carefully to be sure you choose the right drive.
3. If the stick does not appear, reconnect it and press **Refresh list**.
4. Select the drive and press **Next**.

> **“Encrypted?” label**
> It marks a drive without a recognizable file system: it is probably already encrypted. If you encrypt it again, its current content will be lost.

Step 2 — Password

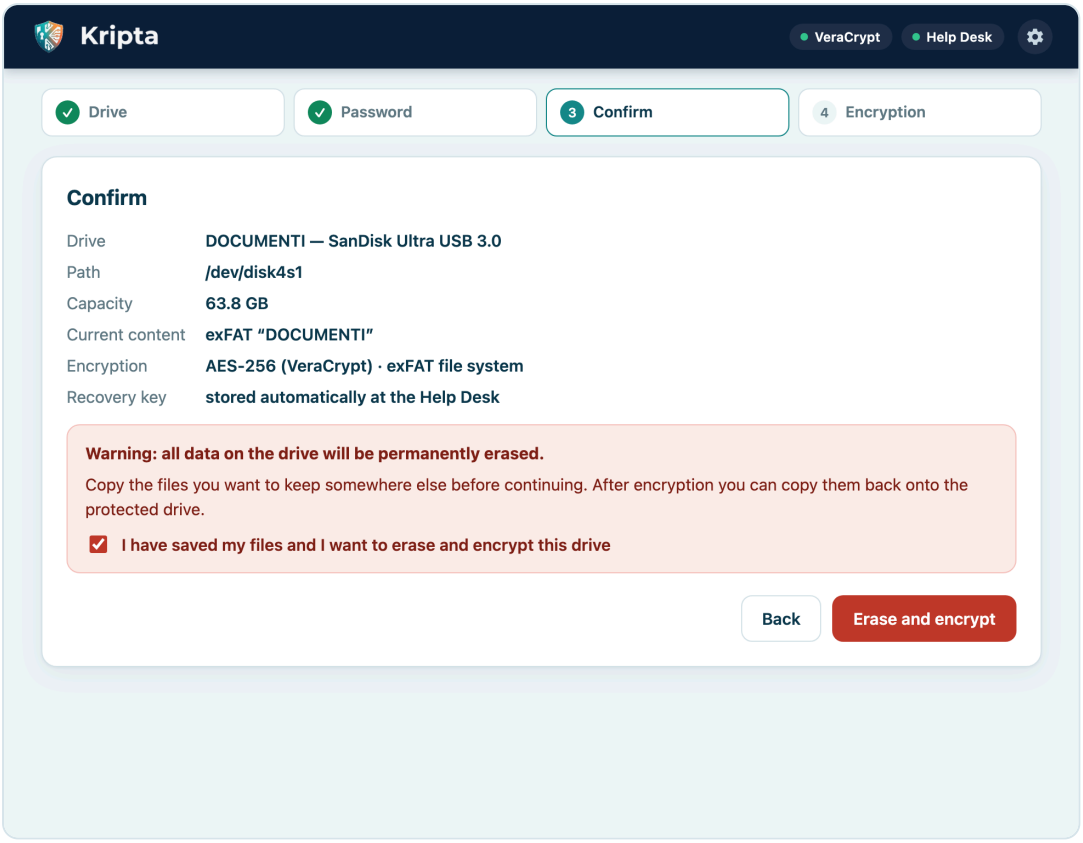


The rules turn green as they are met.

The password must have **at least 12 characters**, **at least three kinds** among lowercase, uppercase, digits and symbols, and **no accented letters** (à, è, ü…), which other systems might type differently. The coloured bar shows the strength; the 👁 button shows the password. Repeat it in the second field and press **Next**.

> **Tip**
> A phrase of several words joined by symbols and digits (for example `Train-Lake-Green-47`) is secure and easy to remember. Do not use your company account password.

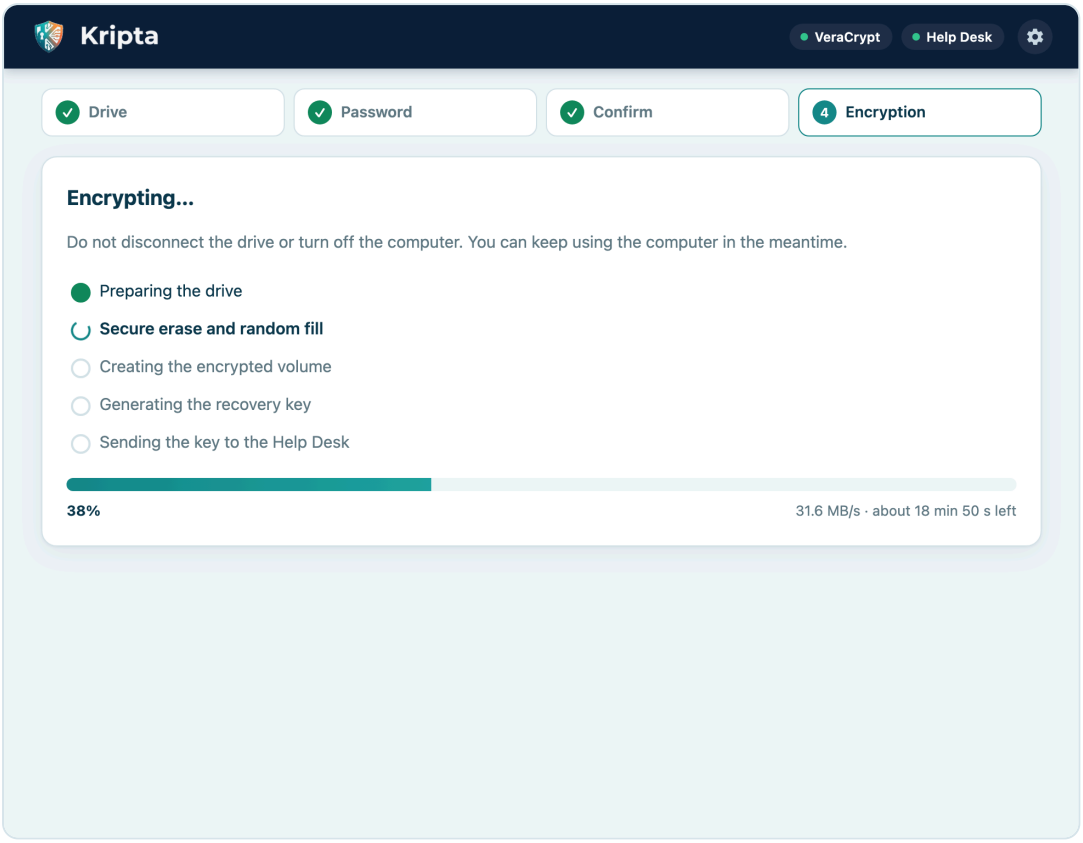
Step 3 — Confirm



Summary and confirmation of the erase.

Check the summary, tick **I have saved my files and I want to erase and encrypt this drive** and press **Erase and encrypt**. The system may ask for administrator authorization.

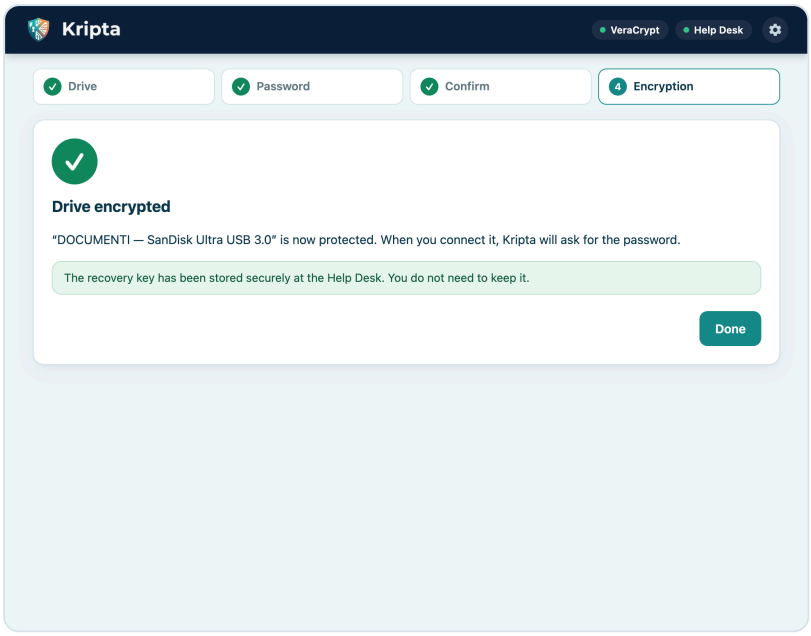
Step 4 — Encryption



Progress with speed and remaining time.

Kripta prepares the drive, overwrites it entirely with random data (the longest phase), creates the exFAT encrypted volume, generates the recovery key and sends it to the Help Desk.

> **During encryption**
> Do not disconnect the drive and do not turn off or put the computer to sleep. A 64 GB stick takes roughly 15 minutes to an hour.



Encryption completed.

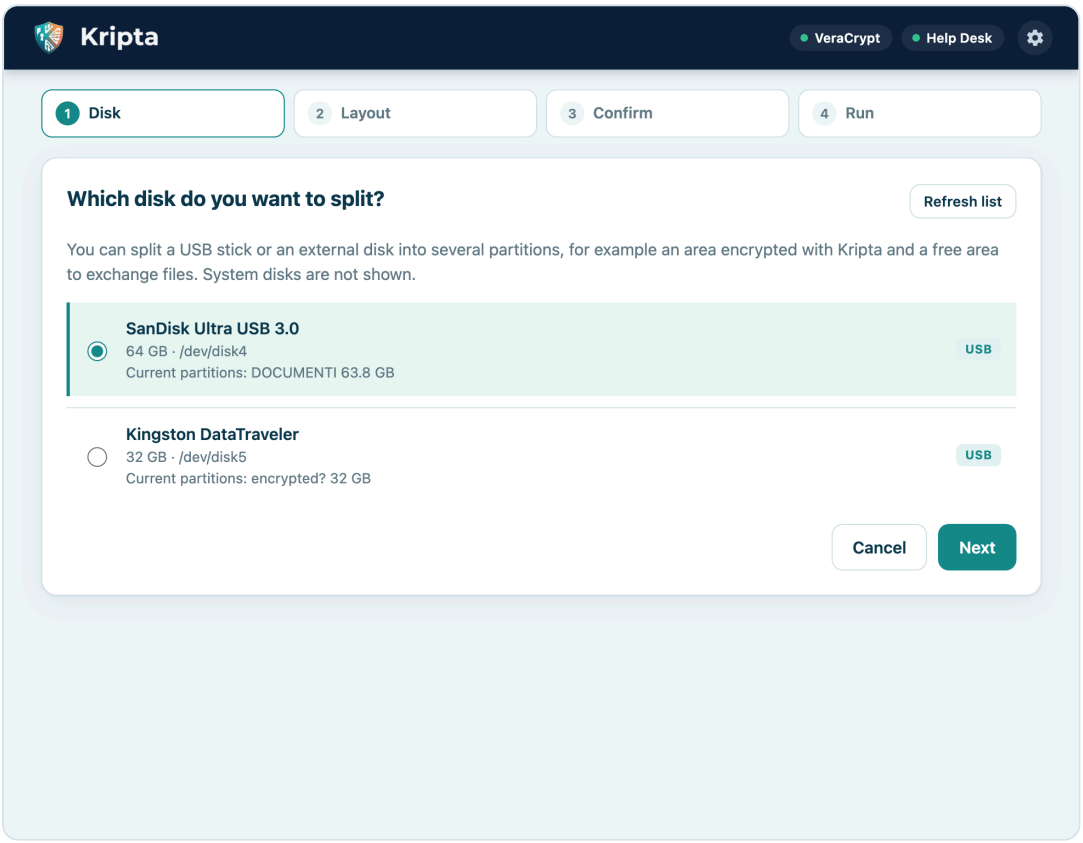
If **the recovery key has not been sent yet** appears, the drive is encrypted and usable anyway: keep Kripta running and connected, it will send the key as soon as possible. If encryption fails, the message explains why (chapter 11).

5 Splitting a disk into partitions

With **Split into partitions** you divide a USB stick or an external disk into several independent parts, each with its own name and file system. The typical use is an **encrypted area** for confidential data and a **free area** to exchange files with computers without Kripta.

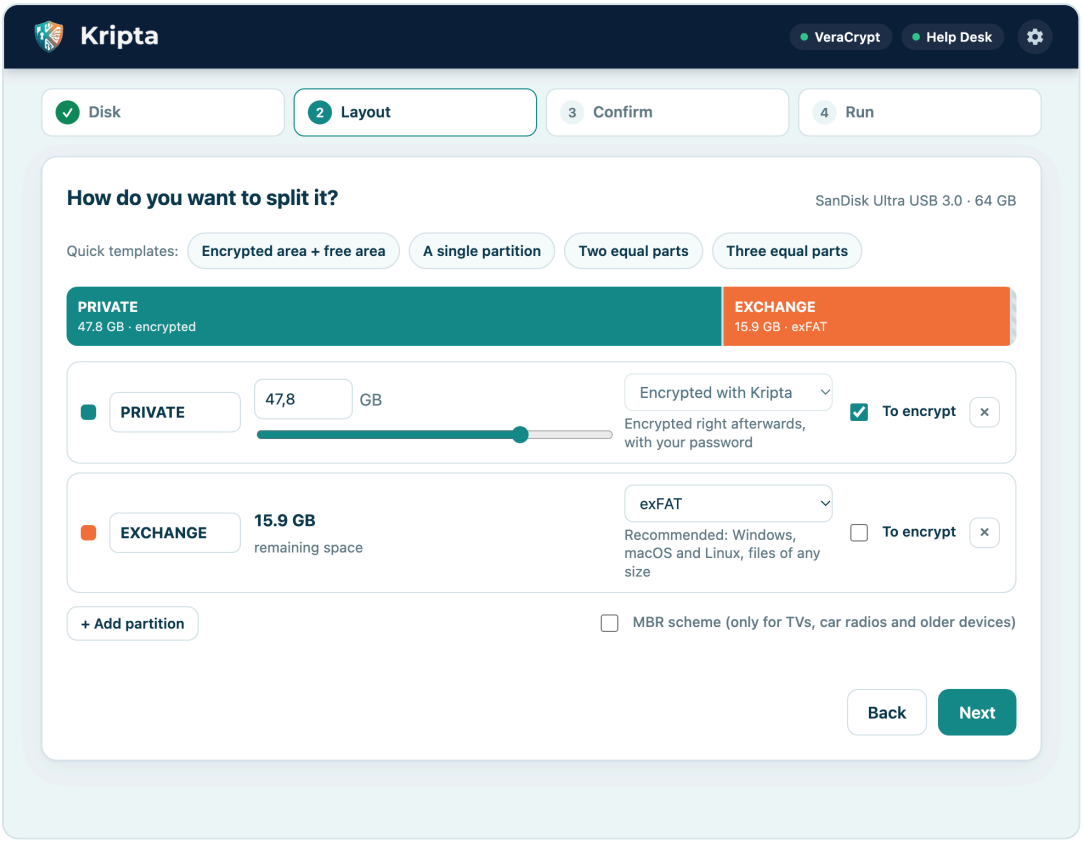
> **Splitting erases the whole disk**
> , including existing partitions and already encrypted drives. Save the files you want to keep elsewhere.

Step 1 — Disk



Choosing the disk, with its current partitions.

Step 2 — Layout



The coloured bar shows the layout in proportion.

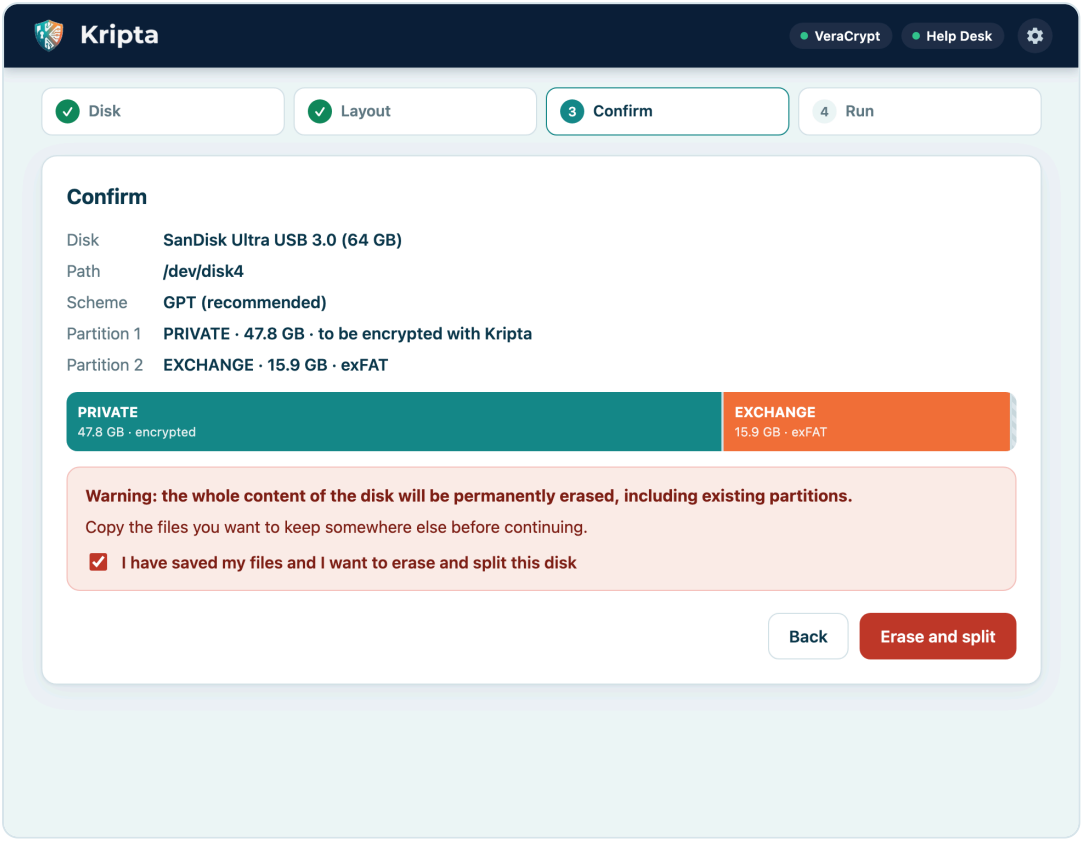
Template	Result
Encrypted area + free area	Three quarters of the disk to encrypt and the rest free in exFAT. It is the template proposed at the start.
A single partition	The whole disk in one partition.
Two / Three equal parts	The disk divided into parts of equal size.

For each partition you set **name** (up to 11 characters: letters, digits, `_` and `-`), **size** (the last one takes the remaining space), **file system** and **To encrypt**. **+ Add partition** adds another one (up to 8).

File system	Opens on	Notes
exFAT (recommended)	Windows, macOS, Linux	No practical limit on file size.
FAT32	Almost any device	Files up to 4 GB; on Windows partitions up to 32 GB.
NTFS	Windows; macOS read-only	On Linux it requires `ntfs-3g`.
APFS, **Mac OS Extended**	Mac only	Available only from a Mac.
ext4	Linux only	Available only from Linux.

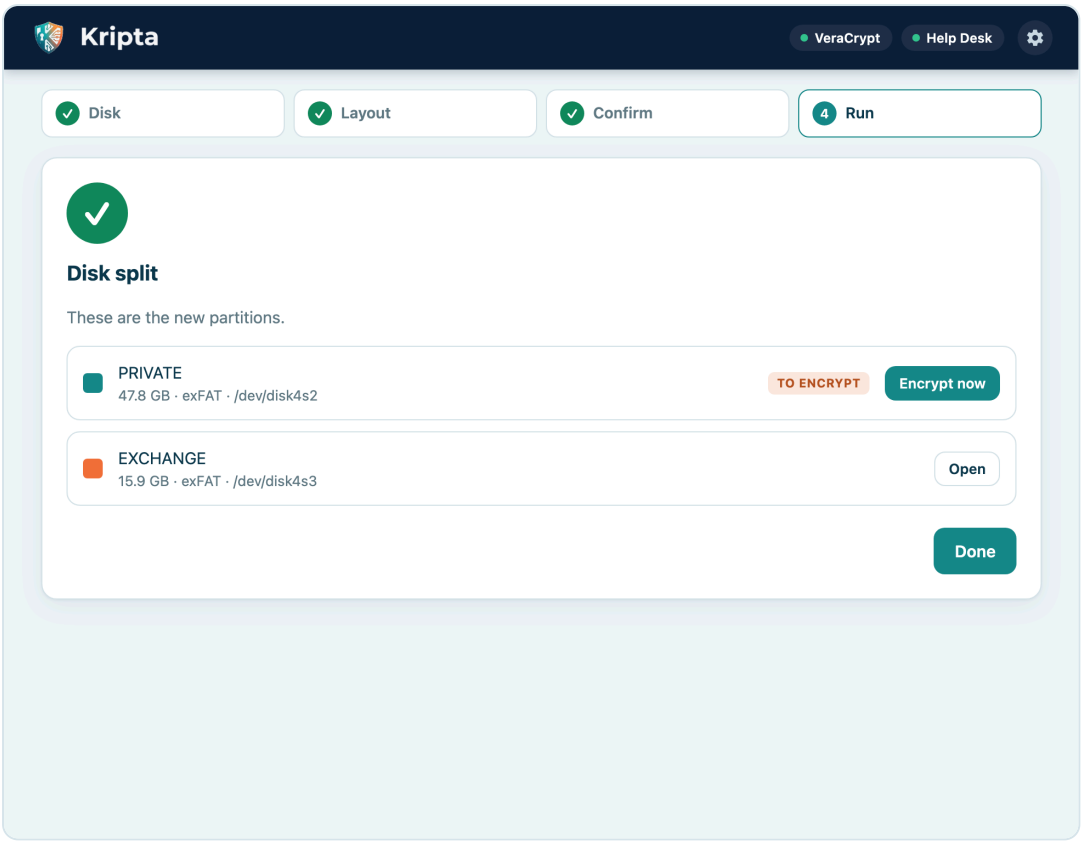
> **MBR scheme**
> Turn it on only if the stick must work with TVs, car radios or very old computers: at most 4 partitions and 2 TB.

Step 3 — Confirm and step 4 — Run



Summary before erasing.

Tick the confirmation box and press **Erase and split**. It usually takes less than a minute.



Partitions created: the area to encrypt has the “Encrypt now” button.

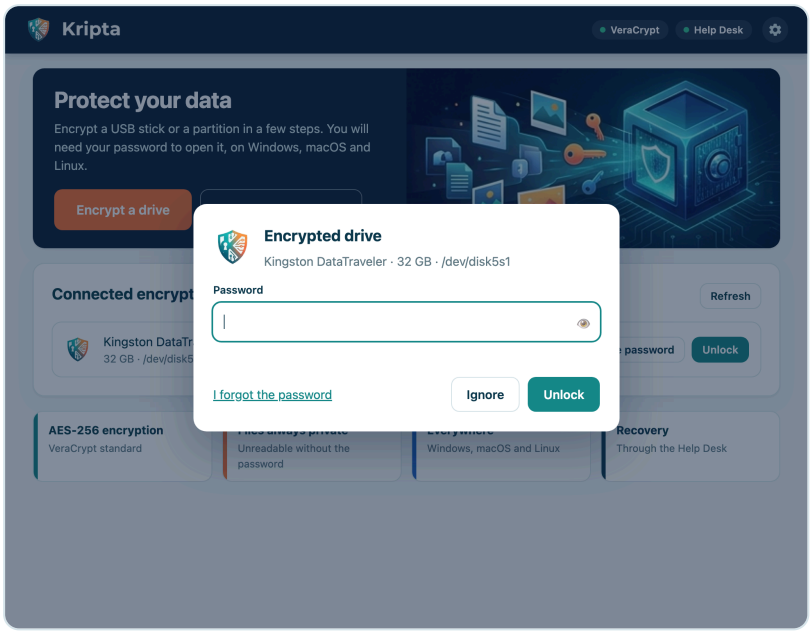
Next to the partitions to encrypt press **Encrypt now**: encryption (chapter 4) starts with the partition already selected.

> **Until you encrypt it, the “to encrypt” area is not protected**
> Do not copy confidential files to it before encryption is complete.

6 Using an encrypted drive

Unlocking

When you connect an encrypted drive while Kripta is running, the password request appears automatically.



Password request when the drive is inserted.

1. Type the password and press **Unlock** (or Enter).
2. The drive opens like a normal disk in File Explorer, Finder or the Linux file manager.
3. With **Ignore** you unlock it later from the main window.

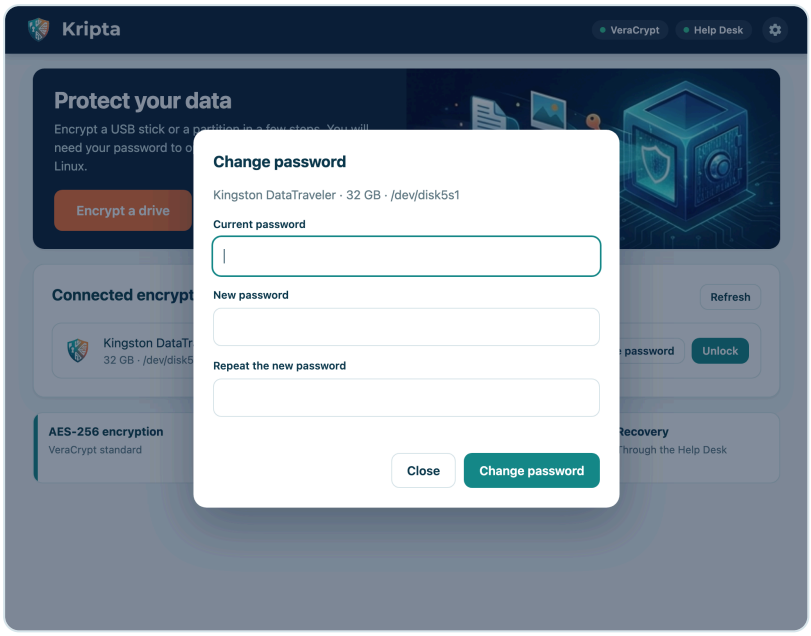
Working with files and locking

With the drive unlocked you use files normally: everything you write is encrypted transparently. When you are done, close the open files, press **Lock** and disconnect the drive.

> **Do not disconnect an unlocked drive without locking it**
> You might lose the files you were copying.

7 Changing the password

You can change the password whenever you like, if you know the current one. The data on the drive is not touched.



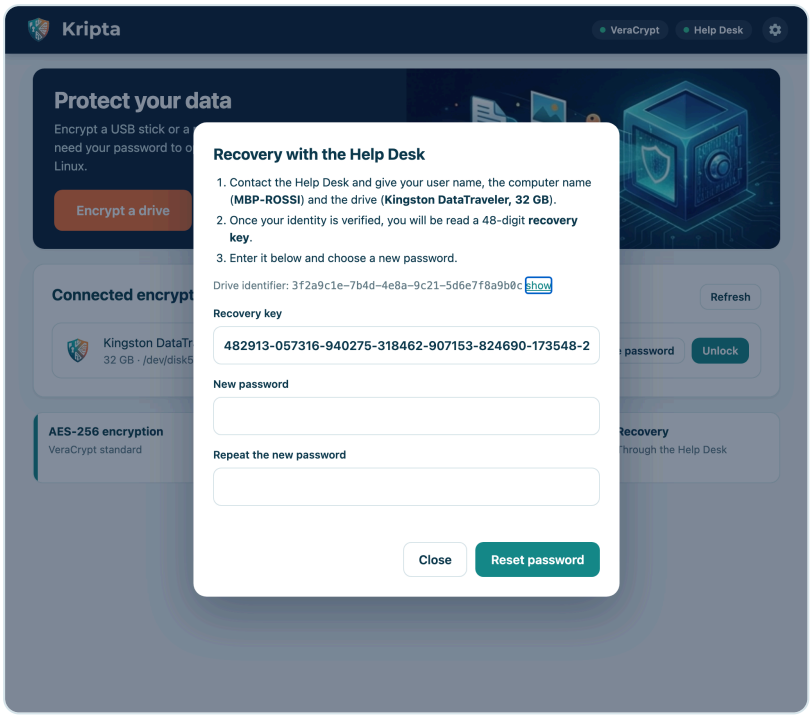
The Change password window.

1. If the drive is unlocked, press **Lock** first.
2. Press **Change password** next to the drive.
3. Enter the current password and the new one twice (same rules as chapter 4), then confirm.

> **What about the recovery key?**
> It stays valid: the Help Desk can help you even after a password change.

8 I forgot the password

The Help Desk can give you the drive's recovery key: with it you set a new password and get all your files back.



Recovery with the Help Desk.

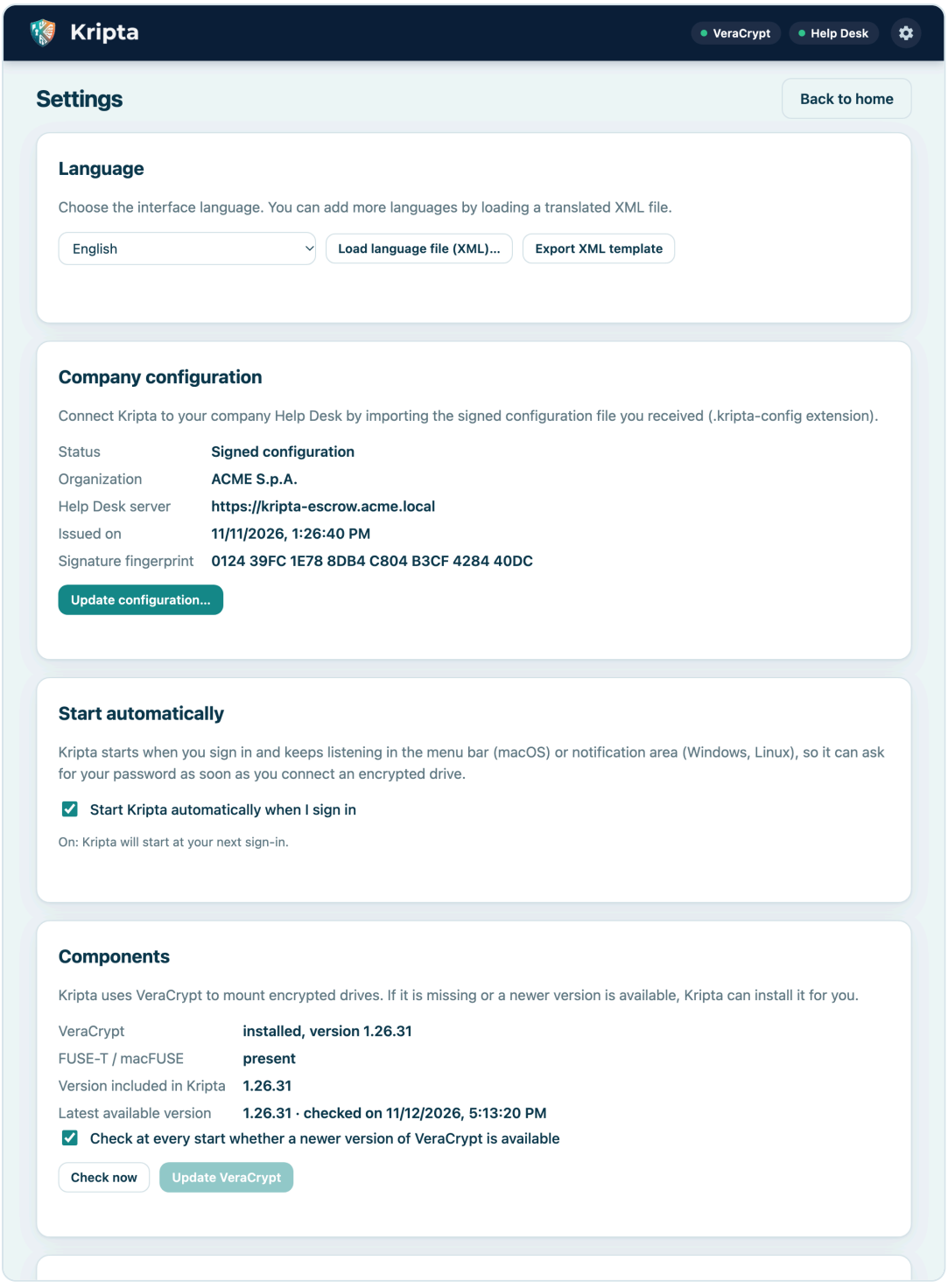
1. In the password request choose **I forgot the password**.
2. The window shows the computer and drive names; **show** also displays the drive identifier.
3. **Contact the Help Desk** and give these details. Once your identity is verified, you will be read the **48-digit key**.
4. Type it in the **Recovery key** field, choose a new password and press **Reset password**.

> **One key, one use**
> After every recovery Kripta generates a new key and sends it to the Help Desk.

> **Beware of scams**
> The Help Desk will never ask for your password. You contact the Help Desk, not the other way round.

9 Settings

They open with the gear at the top right or with **Settings…** in the icon menu.



Settings: language, company configuration, components, about.

Language

Choose the language from the list: the interface, the icon menu and the authorization requests change immediately. With **Automatic** Kripta uses the system language. Included languages:

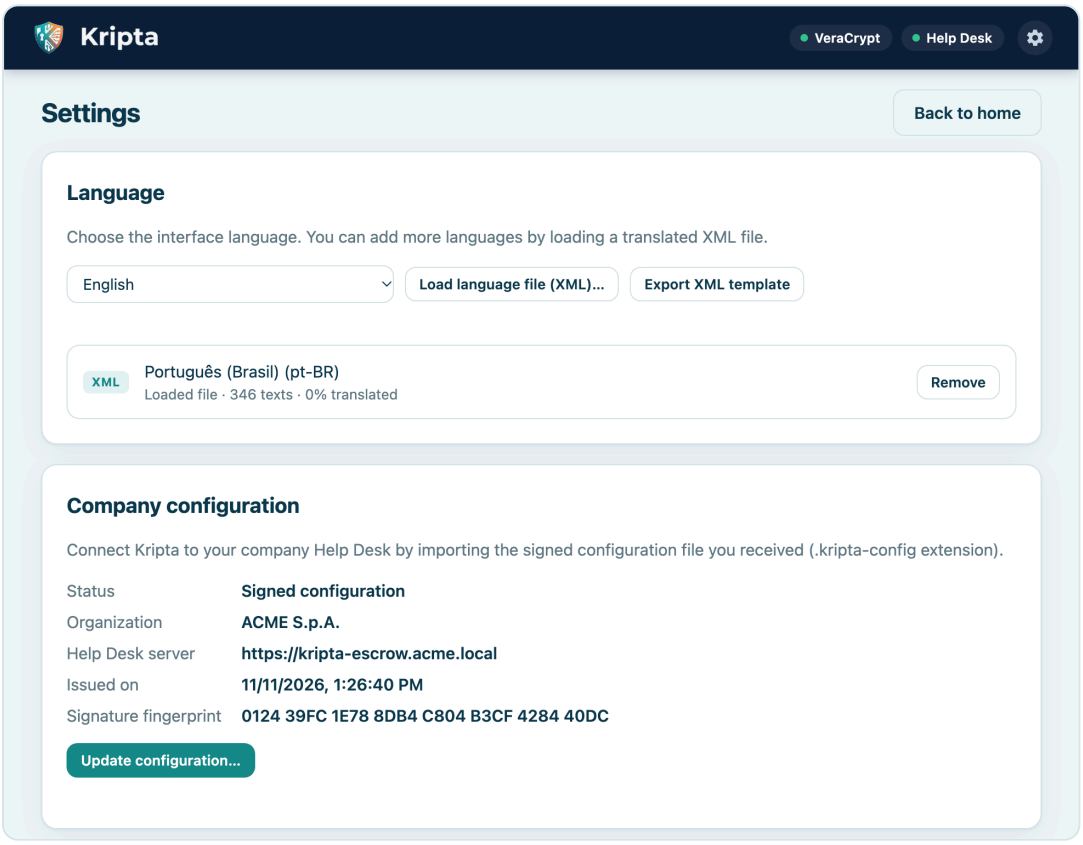
Italiano English Français Español Deutsch Русский العربية 中文 日本語

Adding a language

Translations are simple **XML** files, one per language. To add one:

1. Press **Export XML template**: the file of the current language is saved in the Downloads folder.
2. Translate the text of every `<string>` element, keeping the `id` attributes and the `{1}`, `{2}` placeholders unchanged.
3. At the top of the file set `code` (for example `pt` or `pt-BR`), `name`, `english-name` and `dir` (`rtl` for right-to-left languages).
4. Press **Load language file (XML)...** and choose the file: the language appears in the list with the percentage of translated texts. Missing texts are shown in English.

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



A language loaded from an XML file, with the Remove button.

Loading a file with the same code as an included language replaces it (useful to fix a term); **Remove** restores the original. The files of the nine included languages are next to this manual, in the `lang` folder.

Company configuration

Shows organization, Help Desk server, date and fingerprint of the installed configuration. **Update configuration...** imports a new file received from the Help Desk (chapter 2).

Components

Shows the installed VeraCrypt version, the one included in Kripta and the latest available. **Check now** checks immediately, **Install** / **Update VeraCrypt** starts the installation. The **Check at every start…** box turns the automatic check on or off.

Start automatically

The **Start Kripta automatically when I sign in** box is on by default. Below it you can see whether automatic start is registered in the system. If you turn it off, Kripta does not detect encrypted drives until you open it.

10 Using the drive on other computers

Drives encrypted by Kripta use the standard **VeraCrypt** format with the **exFAT** file system: they open on Windows, macOS and Linux.

Computer	What happens when you insert the drive
With Kripta configured	The password request appears: everything is automatic.
With Kripta installed but **without company configuration** (for example at home)	The password request still appears and the drive unlocks. If VeraCrypt is missing, Kripta offers **Install now**. Without configuration you cannot encrypt new drives or recover passwords.
With VeraCrypt only	Open VeraCrypt, choose a free slot, **Select Device**, choose the stick's partition, then **Mount** and enter the password.
Without Kripta or VeraCrypt	No request appears: operating systems do not start programs from USB sticks. The system may offer to **format** the drive: **always refuse**. Install Kripta (from the company site) and connect the drive again.

Administrator rights

Opening an encrypted drive on any computer requires administrator rights, because VeraCrypt uses a system driver. On a computer whose credentials you do not have, the drive cannot be opened.

Free area for exchange

If you often use computers without Kripta, split the stick with the **Encrypted area + free area** template (chapter 5): you can also copy the Kripta installer to the free area.

11 Messages and troubleshooting

Message or situation	What to do
Kripta is not yet connected to your company Help Desk	Import the `.kripta-config` file received from the Help Desk (chapter 2).
The package signature is not valid	The file has been modified or damaged: ask the Help Desk for it again.
The package is signed with a different key / not with an approved key	The file does not come from your company. Do not use it and contact the Help Desk.
The configuration is managed by IT and cannot be replaced	The computer is configured centrally: nothing to import.
The VeraCrypt encryption engine is not installed	Press **Install now**. If there is no button, contact the Help Desk.
The official VeraCrypt signature is not valid / the file does not match the signed version	The download was altered or incomplete: installation was cancelled. Try again later.
Lock all encrypted drives before updating VeraCrypt	Press **Lock** on the open drives, then repeat the update.
Restart the computer to complete the update (Windows)	Save your work and restart.
The Help Desk server cannot be reached. Encryption has not started.	Connect to the company network or VPN and try again. The data on the drive has not been touched.
Recovery keys waiting to be sent	Connect to the network and press **Retry now**. Keep Kripta running until the alert disappears.
No drive available	Reconnect the stick (try another USB port) and press **Refresh list**.
Administrator authorization cancelled / Timed out	Repeat the operation and confirm the system request.
Cannot unmount / lock the volume	Close the documents and windows opened from the drive, then try again.
Wrong password	Check Caps Lock and the keyboard layout. If you do not remember it, see chapter 8.
Wrong recovery key	Check the digits with the operator again: you need the **most recent** key.
The disk contains an unlocked Kripta drive	Lock it on the home screen, then repeat the splitting.
The system did not detect the new partitions	Disconnect and reconnect the drive.

Message or situation	What to do
The language file is not valid XML / element not allowed	Fix the file indicated in the message: only `<string>` elements with plain text are allowed.
The unlock window does not appear when inserting the drive	Check that Kripta is running (icon in the bar) and use **Unlock** in the main window.

12 Frequently asked questions

Can I encrypt a stick that already contains files without losing them?

No. Encryption erases the drive. Copy the files elsewhere, encrypt the drive and then copy them back.

Can I encrypt my computer's internal disk?

No. Kripta is designed for sticks and external disks; system disks are not shown.

Can the Help Desk read my files?

The Help Desk only keeps the recovery key and can look it up only at your request, with every access logged.

Do I need to write down the recovery key?

No. You never see it and do not need to keep it: it is stored at the Help Desk.

Does Kripta install programs on my computer?

Only VeraCrypt (and FUSE-T on macOS), after your confirmation and only if the developers' official signature is valid.

Can I use the stick on a home computer?

Yes, by installing Kripta or VeraCrypt (chapter 10). Always follow company rules on using data off-site.

The language I need is missing. What can I do?

You can translate the XML template and load it from Settings (chapter 9), or ask IT to distribute one.

Why can't I use accented letters in the password?

Windows, macOS and Linux may encode them differently: the same password typed on another system might not be recognized.

How much space do I lose with encryption?

Very little: a few hundred kilobytes for the volume headers.

A Appendix for IT

Packages

System	Package	Notes
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	Contains the official VeraCrypt MSIs (x64 and ARM64). The app starts with administrator rights.
macOS 11+	`Kripta_1.2.0_universal.dmg`	Contains VeraCrypt (FUSE-T and macFUSE builds) and FUSE-T, which needs no kernel extension.
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	Contains VeraCrypt for Ubuntu 22.04/24.04 and Debian 12/13; for other versions Kripta downloads the verified package.
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	Contains VeraCrypt for Fedora 44; also install `exfatprogs`.
Other distributions	`Kripta_1.2.0_amd64.AppImage`	Portable executable.

Signed configuration

On the escrow server, once, generate the signing key; then sign the client configuration (template in `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 Ltd" acme.kripta-config
```

Distribute `acme.kripta-config` to users and publish the **fingerprint** on a trusted channel (intranet, Help Desk phone). Kripta saves the configuration in the system location (`%ProgramData%\Kripta`, `/Library/Application Support/Kripta`, `/etc/kripta`) through the privileged process, together with the signer's key: later updates must carry the same signature. To avoid relying on users checking the fingerprint, build Kripta with `KRIPTA_PROVISIONING_KEYS=<public key>`: only those keys will be accepted. A configuration copied by hand by IT (unsigned) cannot be replaced by a package.

VeraCrypt installation and updates

- The included installers are prepared with `scripts/fetch-veracrypt.py` at build time.
- Before installing, the privileged process verifies the OpenPGP signature of the official SHA-256 list with the embedded IDRIX key (fingerprint `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`) and the file hash.
- Options in `kripta.toml`: `veracrypt_update_check = false` turns off the update check; `veracrypt_release_api = "https://mirror.internal/…"` uses an internal mirror with the same format as the GitHub API.

Languages

The language XML files are in `app/ui/lang/` (included in the app) and in `docs/manuale/lang/`. Languages loaded by users are saved in the user data folder (`languages/`). To distribute a new language to everyone, add the file to `app/ui/lang/` and its code to the list in `app/ui/i18n.js`.

Optional components

- **Start at sign-in** in the menu bar / notification area (`kripta --background`): **automatic**. Kripta registers it at every start (macOS: `~/Library/LaunchAgents/com.kripta.agent.plist`, restarted if it terminates abnormally; Windows: scheduled task “Kripta” at logon with highest privileges, also created by the installer and removed on uninstall; Linux: `/etc/xdg/autostart/kripta.desktop` from the .deb/.rpm packages, `~/.config/autostart/kripta.desktop` for the AppImage). It can be turned off in Settings.
- **Privileged helper** as a service (no password requests): `deploy/macos/com.kripta.helper.plist`, `deploy/linux/kripta-helper.service`.