Kripta

用户手册

引导式加密 U 盘和分区，并可通过公司技术支持中心恢复密码。



版本 1.2 · Windows · macOS · Linux

2026 年 11 月

目录

1 Kripta 简介 — 用途与准备工作

2 首次启动 — 企业配置与组件

3 主窗口 — 指示灯、提示、托盘图标

4 加密驱动器 — 4 步向导

5 划分磁盘分区 — 加密区域与普通区域

6 使用加密驱动器 — 解锁、打开、锁定

7 更改密码

8 忘记密码 — 通过技术支持中心恢复

9 设置 — 语言、配置、更新

10 在其他计算机上使用驱动器

11 提示信息与故障排除

12 常见问题

A IT 附录 — 安装包、签名配置、语言

约定

屏幕上显示的文字（按钮、标题、菜单项）写作：**加密驱动器**。 截图来自 macOS 版本：Windows 和 Linux 上的窗口完全相同，只是设备名称不同（例如 `E:` 或 `/dev/sdb1`，而不是 `/dev/disk4s1`）。

1 Kripta 简介

Kripta 使用 AES-256 加密保护您的 **U 盘**和外置磁盘**分区**中的数据。 加密后，只有知道密码的人才能读取驱动器内容：即使 U 盘丢失，别人也无法打开。

引导式加密

四个步骤：选择驱动器、设置密码、确认、等待完成。

自动解锁

连接加密驱动器时，Kripta 会立即要求输入密码并打开它。

随处可用

同一个 U 盘可在 Windows、macOS 和 Linux 上打开（标准 VeraCrypt 格式）。

自助安装

Kripta 会自行安装和更新 VeraCrypt；企业配置通过文件导入。

九种语言

意大利语、英语、法语、西班牙语、德语、俄语、阿拉伯语、中文和日语，还可以自行添加。

通过技术支持中心恢复

忘记密码时，技术支持中心可以帮您设置新密码，数据不会丢失。

准备工作

- 计算机上已安装 **Kripta**。首次启动时，如果缺少加密引擎 **VeraCrypt**（macOS 上还需要 **FUSE-T**），Kripta 会自行安装：见第 2 章。
- 技术支持中心发送的**已签名配置文件**（`.kripta-config`），除非 IT 部门已经配置好计算机。
- 加密新驱动器时需要**连接公司网络**（或 VPN）：恢复密钥会立即发送到技术支持中心。解锁已加密的驱动器则不需要网络。
- 系统要求时，需要计算机的**管理员凭据**（见方框）。

> **授权请求**
>
> 为了直接读写驱动器、安装组件和保存配置，Kripta 需要管理员权限。 在 **Windows** 上，启动时会出现“用户帐户控制”窗口。在 **macOS** 和 **Linux** 上会出现提示“Kripta 需要管理员授权才能完成此操作”。如果 IT 部门安装了 Kripta 系统服务，则不会出现这些请求。

恢复机制简介

加密时，Kripta 会生成一个 48 位的**恢复密钥**，对其进行保护并发送到技术支持中心的存档。 您无需查看或保存它。只有技术支持中心的工作人员在验证您的身份后才能查询，每次查询都会被记录。

2 首次启动

首次启动时，Kripta 会检查两件事：是否已连接到公司的技术支持中心，以及计算机上是否安装了 VeraCrypt。 如果缺少某项，窗口顶部会出现带有修复按钮的提示。您可以自己完成所有操作。



首次启动：需要导入配置并安装 VeraCrypt。

导入企业配置

配置告诉 Kripta 将恢复密钥发送到哪个技术支持中心存档。技术支持中心会以扩展名为 `.kripta-config` 的文件提供配置， 该文件带有数字签名：任何人修改它都会被 Kripta 发现。

1. 将收到的文件保存到计算机（通过电子邮件、公司门户或 U 盘）。
2. 点击提示中的**导入配置**，或打开**设置**（右上角的齿轮），点击**导入已签名配置...**。
3. 选择文件。Kripta 会验证签名，并显示组织、技术支持中心服务器、签发日期和**签名指纹**。
4. 首次导入时，请将**指纹**与技术支持中心告知您的指纹（通过电话、内网等）**进行比对**。一致时点击**导入**。
5. 确认系统的授权请求。界面显示**配置已导入**，Help Desk 指示灯变为绿色。



确认导入并核对签名指纹。

> **指纹不一致时请勿导入**
>
> 该文件可能并非来自您的公司。请取消并联系技术支持中心。 首次导入后，Kripta 只接受使用同一密钥签名的更新：伪造的文件会被自动拒绝。

安装 VeraCrypt

Kripta 已内置 VeraCrypt 的官方安装程序（macOS 版还包含 FUSE-T）。点击提示中的**立即安装**并确认授权请求： Kripta 会验证安装程序的官方签名，然后自动完成安装，无需其他操作。



安装组件并验证官方签名。

完成后显示**安装完成**。在 Windows 上可能需要重新启动计算机。

VeraCrypt 更新

每次启动时（之后每天一次），Kripta 都会检查是否发布了更新版本的 VeraCrypt。如果有，会出现蓝色提示和 **更新** 按钮。 新版本从官方网站下载，只有在 VeraCrypt 开发者的签名有效时才会安装。



VeraCrypt 有可用更新。

更新之前

请锁定所有已打开的加密驱动器：有驱动器处于解锁状态时，Kripta 不会更新 VeraCrypt。 您可以在设置中关闭自动检查（第 9 章）。

3 主窗口

打开 Kripta 后会显示主页。您可以在这里加密新驱动器，并管理连接到计算机的加密驱动器。



主页：已连接并解锁的加密驱动器。

元素	用途
VeraCrypt	绿点：加密引擎已安装。红点：未安装（第 2 章）。鼠标悬停可查看版本。
Help Desk	绿色：可以访问密钥存档。红色：无法访问（无网络、VPN 未开启、缺少配置）。
齿轮	打开 **设置**：语言、企业配置、组件（第 9 章）。
加密驱动器	启动向导（第 4 章）。如果 Kripta 未配置或缺少 VeraCrypt，则不可用。
划分分区	将 U 盘或外置磁盘划分为多个分区（第 5 章）。
已连接的加密驱动器	已连接的 Kripta 驱动器，显示 **已锁定** 或 **已解锁** 状态及相应按钮。

提示

窗口顶部可能会出现带有解决按钮的彩色提示框：



无法连接技术支持中心服务器，且有一个恢复密钥等待发送。

- **无法连接技术支持中心服务器：**仍可解锁驱动器，但不能加密新驱动器。
- **恢复密钥等待发送：**Kripta 会自动重试；恢复联网后可点击 **立即重试**。**在提示消失前请保持 Kripta 运行。**
- **Kripta 尚未连接到技术支持中心 / 未安装 VeraCrypt / VeraCrypt … 已可用：**见第 2 章。

Kripta 图标：菜单栏和通知区域

Kripta 在后台运行，以便在您连接加密驱动器时及时响应；可通过带有徽标的图标进行控制：

系统	图标位置	须知
macOS	右上角的**菜单栏**中。Kripta **不会出现在程序坞中**。	在带刘海的 MacBook 上，菜单栏放满时多余的图标会被隐藏：请移除不用的图标，或按住 ⌘ 拖动它们。
Windows	右下角时钟旁的**通知区域**中。	如果图标被隐藏，点击 ^ 箭头，将徽标拖到任务栏上。
Linux	面板的**通知区域**中。	在“原生”GNOME（Fedora、Debian）上需要安装 **AppIndicator and KStatusNotifierItem Support** 扩展。

图标菜单包含 **打开 Kripta**、**加密驱动器…**、**划分分区…**、**锁定所有驱动器**、**设置…** 和 **退出 Kripta**。菜单项随所选语言显示。

> **关闭窗口不会退出 Kripta**
> Kripta 仍在菜单栏或通知区域中运行。 要重新打开窗口，请使用**打开 Kripta**，或再次启动 Kripta：将显示已在运行的窗口。

自动启动

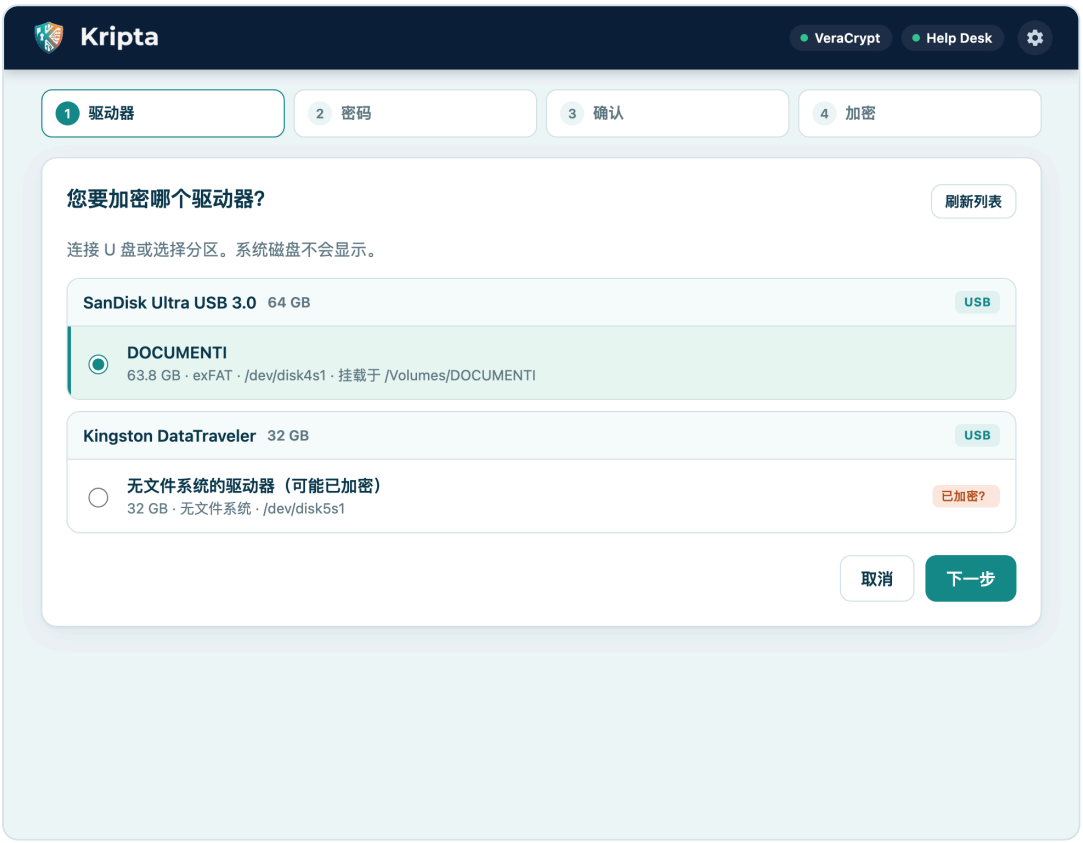
安装后，Kripta **会在每次登录时自动启动**，不打开窗口，并始终在后台监听：一旦连接加密驱动器，就会请求密码。您可以在**设置 > 自动启动**中关闭此功能（第 9 章）。**退出 Kripta**会将其关闭，直到下次登录。

4 加密驱动器

加密会清除驱动器上的全部内容。
开始前，请将要保留的文件复制到其他位置。加密完成后，可以将它们复制回受保护的驱动器。

连接 U 盘，确认 **Help Desk** 指示灯为绿色，然后点击**加密驱动器**。

第 1 步 — 驱动器

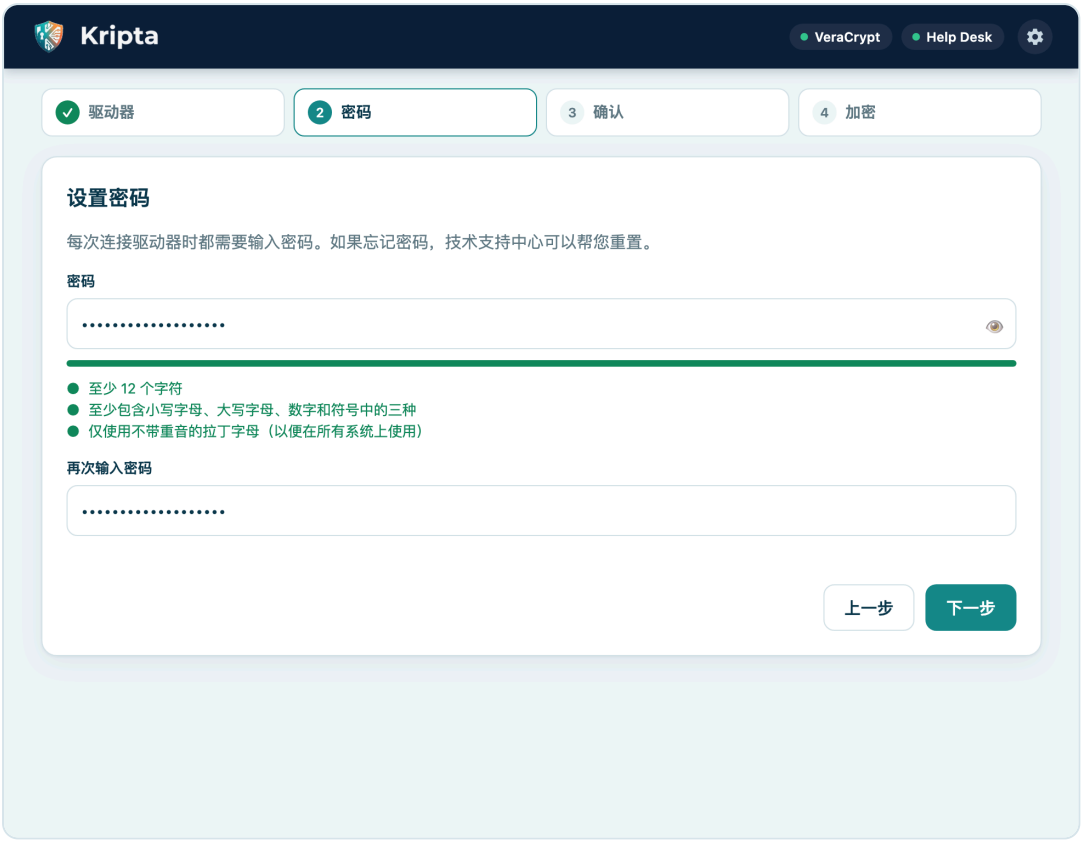


选择要加密的驱动器。

1. Kripta 会列出已连接的设备，可移动设备排在前面。**系统磁盘永远不会显示。**
2. 请仔细核对**容量和名称**，确保选择正确的驱动器。
3. 如果 U 盘没有出现，请重新插入并点击**刷新列表**。
4. 选择驱动器并点击**下一步**。

“已加密？”标签
表示驱动器没有可识别的文件系统：它很可能已经加密。如果再次加密，其当前内容将会丢失。

第 2 步 — 密码

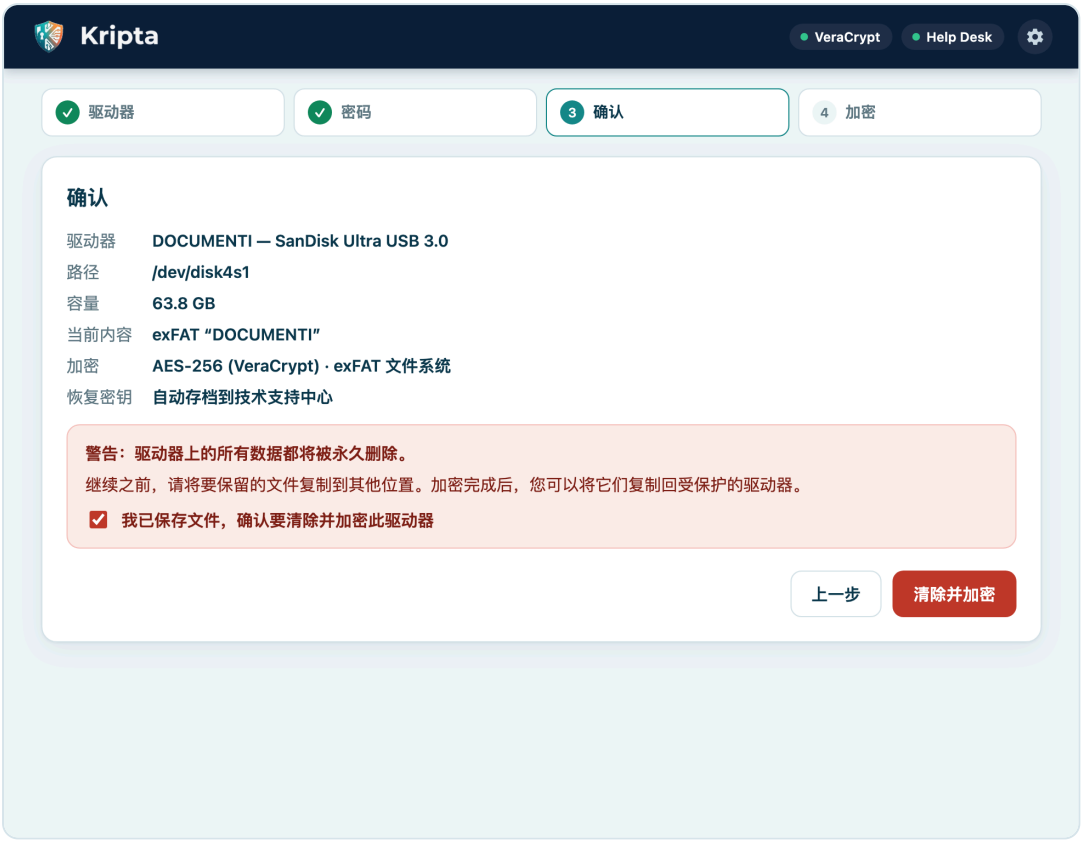


满足规则后，对应项会变成绿色。

密码必须**至少 12 个字符**，包含小写字母、大写字母、数字和符号中的**至少三种**，并且**只能使用不带重音的拉丁字母**： 中文等字符在其他系统上的输入方式可能不同。彩色条显示密码强度；👁 按钮可显示密码。在第二个输入框中再次输入，然后点击 **下一步** 。

> **提示**
> 用符号和数字连接几个单词组成的短语（例如 `Huoche-Hupo-Lvse-47` ）既安全又好记。请勿使用公司帐户的密码。

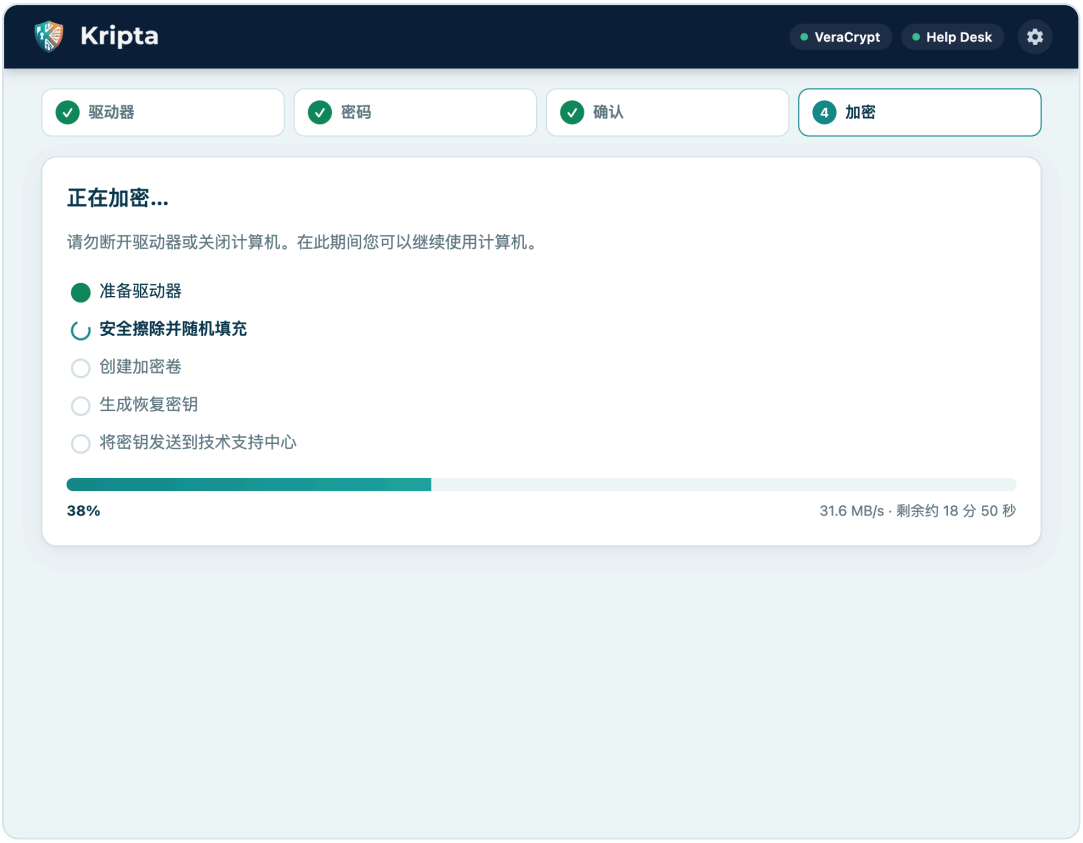
第 3 步 — 确认



摘要和清除确认。

检查摘要，勾选**我已保存文件，确认要清除并加密此驱动器**，然后点击**清除并加密**。系统可能会要求管理员授权。

第 4 步 — 加密



显示速度和剩余时间的进度。

Kripta 会准备驱动器，用随机数据完整覆盖（耗时最长的阶段），创建 exFAT 加密卷，生成恢复密钥并将其发送到技术支持中心。

> **加密期间**
> 请勿断开驱动器，也不要关闭计算机或使其进入睡眠状态。64 GB 的 U 盘大约需要 15 分钟到 1 小时。



加密完成。

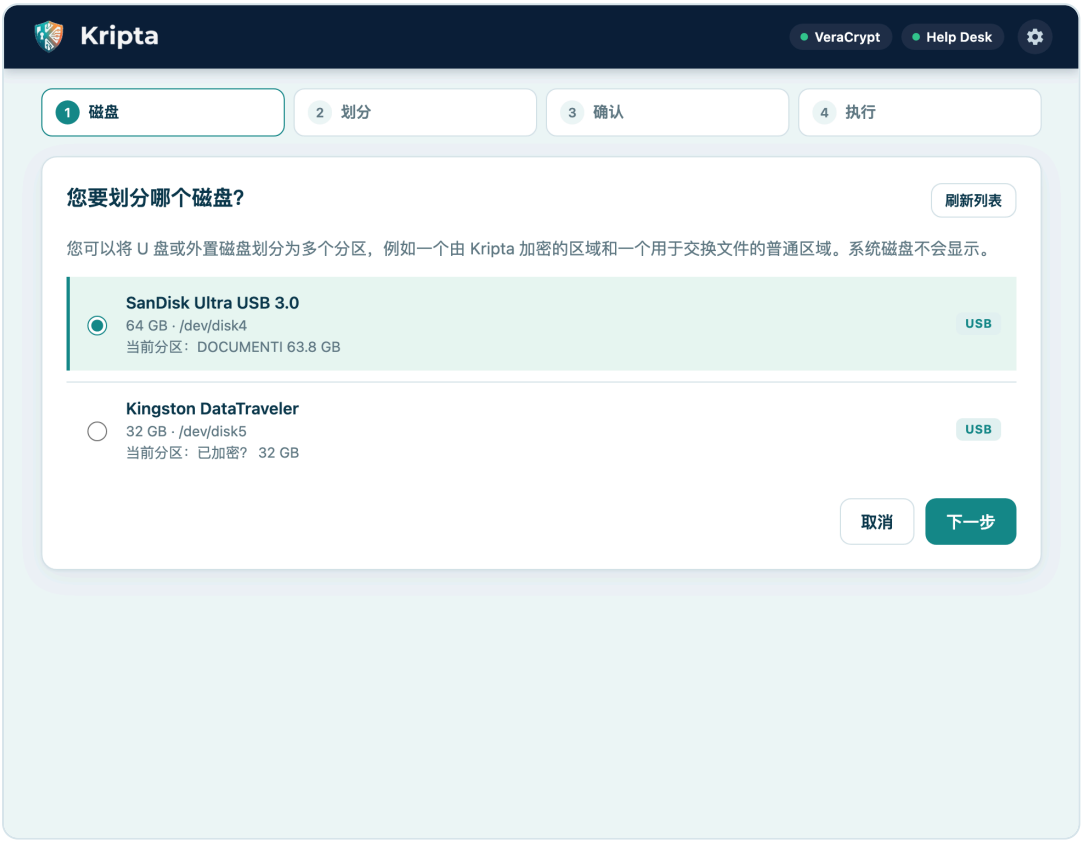
如果显示**恢复密钥尚未发送**，驱动器仍已加密并可以使用：请保持 Kripta 运行并联网，它会尽快发送密钥。如果加密失败，提示信息会说明原因（第 11 章）。

5 划分磁盘分区

使用**划分分区**，可以将 U 盘或外置磁盘划分为多个独立部分，每部分都有自己的名称和文件系统。 典型用法是：一个**加密区域**存放机密数据，一个**普通区域**用于与没有 Kripta 的计算机交换文件。

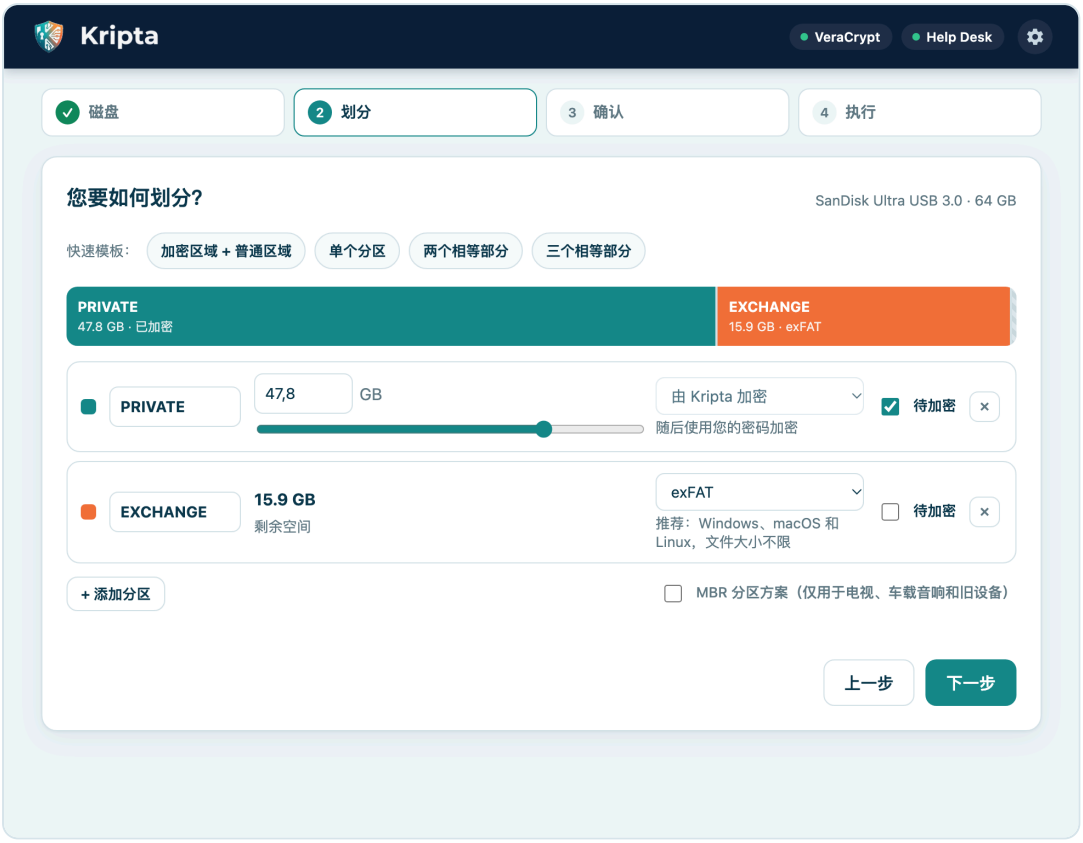
> **划分会清除整个磁盘**
> ，包括现有分区和已加密的驱动器。请将要保留的文件保存到其他位置。

第 1 步 — 磁盘



选择磁盘，并查看其当前分区。

第 2 步 — 划分



彩色条按比例显示划分结果。

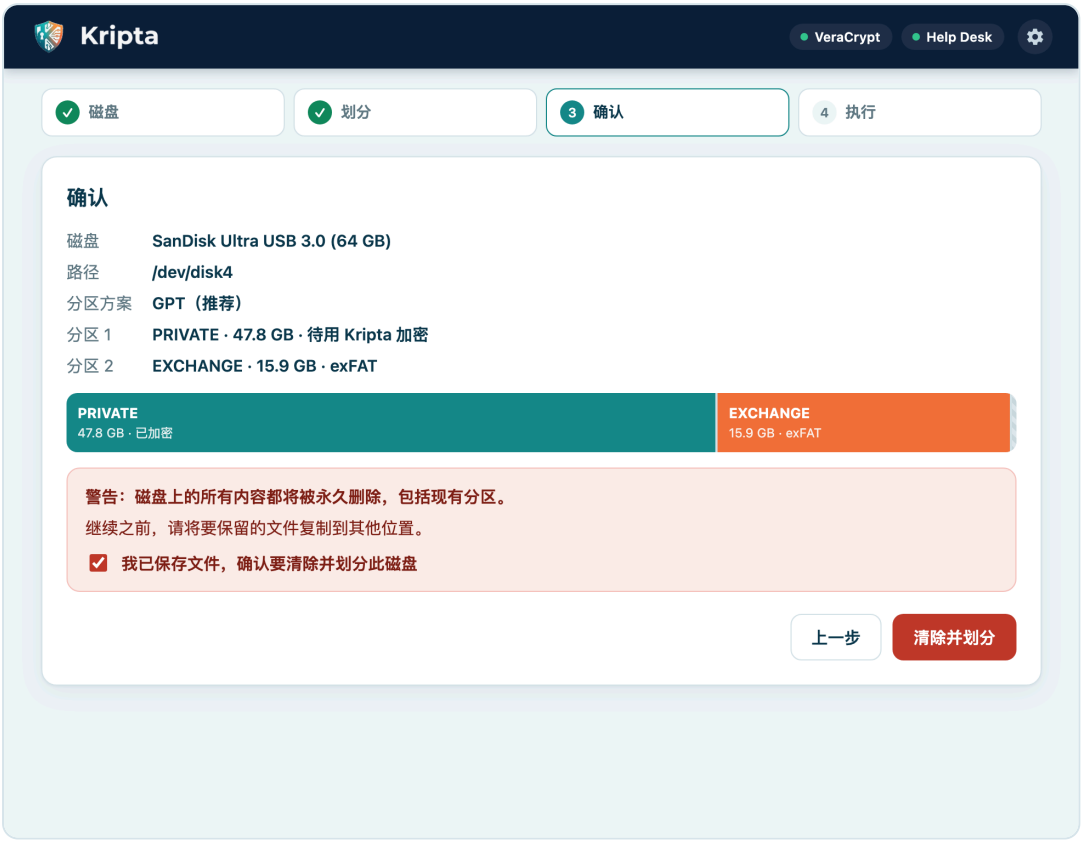
模板	结果
加密区域 + 普通区域	磁盘的四分之三用于加密，其余为 exFAT 普通区域。这是默认推荐的模板。
单个分区	整个磁盘作为一个分区。
两个 / 三个相等部分	将磁盘分为大小相同的几部分。

可为每个分区设置**名称**（最多 11 个字符：拉丁字母、数字、`_` 和 `-`）、**大小**（最后一个分区占用剩余空间）、**文件系统**以及**待加密**。**+ 添加分区**可再添加一个分区（最多 8 个）。

文件系统	可在以下系统打开	说明
exFAT（推荐）	Windows、macOS、Linux	文件大小几乎没有限制。
FAT32	几乎所有设备	单个文件最大 4 GB；在 Windows 上分区最大 32 GB。
NTFS	Windows；macOS 只读	在 Linux 上需要 `ntfs-3g`。
APFS、Mac OS 扩展	仅限 Mac	仅在 Mac 上可用。
ext4	仅限 Linux	仅在 Linux 上可用。

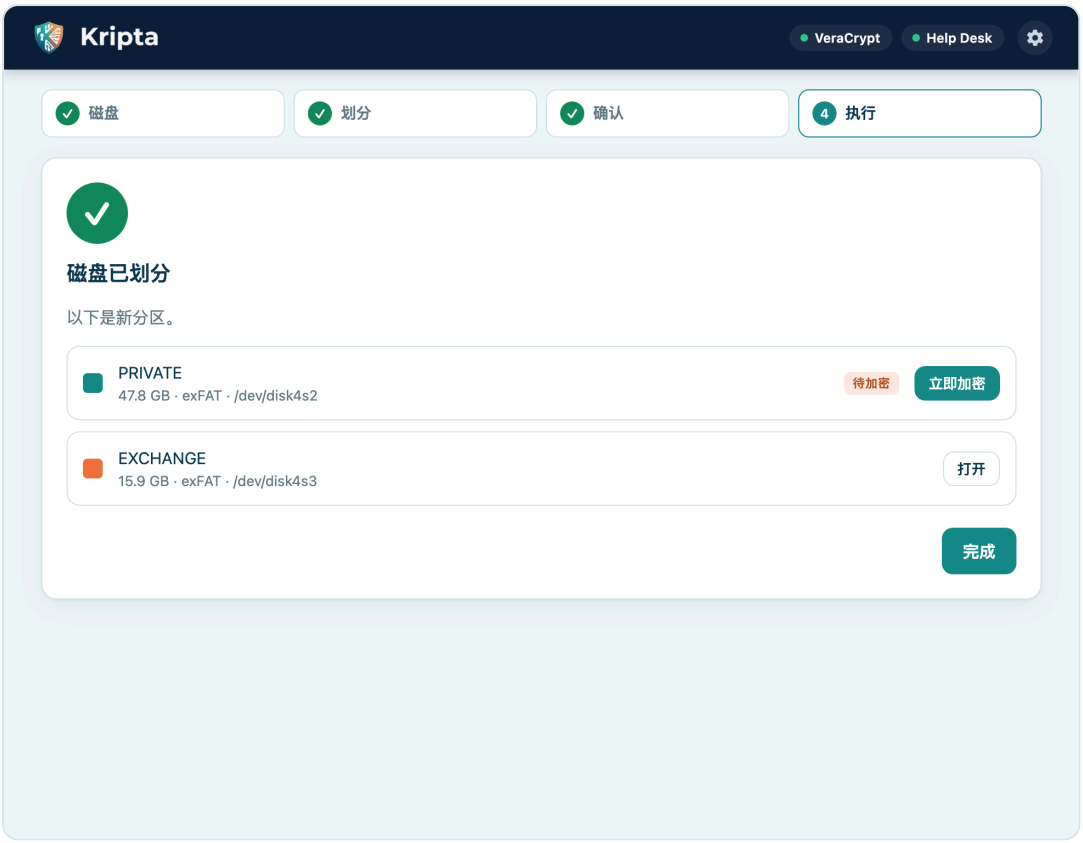
> **MBR 方案**
> 仅当 U 盘需要在电视、车载音响或非常旧的计算机上使用时才启用：最多 4 个分区，磁盘最大 2 TB。

第 3 步 — 确认和第 4 步 — 执行



清除前的摘要。

勾选确认框并点击 **清除并划分** 。通常不到一分钟即可完成。



分区已创建：待加密区域旁有“立即加密”按钮。

在待加密分区旁点击**立即加密**：加密向导（第 4 章）会以已选好的分区开始。

> **加密前，“待加密”区域不受保护**
> 完成加密前，请勿在其中存放机密文件。

6 使用加密驱动器

解锁

在 Kripta 运行时连接加密驱动器，会自动出现密码输入框。



插入驱动器时要求输入密码。

1. 输入密码并点击 **解锁**（或按回车键）。
2. 驱动器会像普通磁盘一样在文件资源管理器、访达或 Linux 文件管理器中打开。
3. 点击 **忽略**，可以稍后在主窗口中解锁。

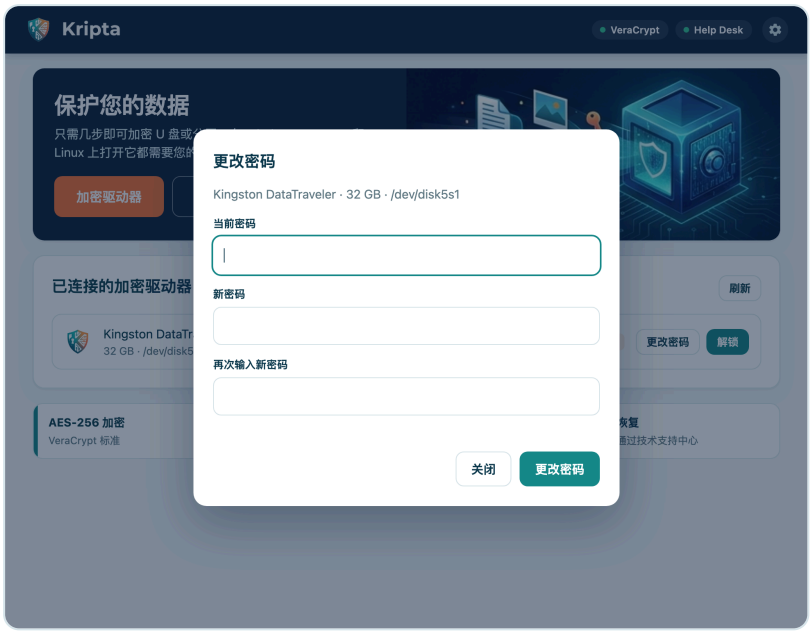
使用文件和锁定

驱动器解锁后可正常使用文件：写入的所有内容都会被透明加密。使用完毕后，关闭打开的文件，点击 **锁定**，然后断开驱动器。

> **请勿在未锁定的情况下断开已解锁的驱动器**
> 否则可能丢失正在复制的文件。

7 更改密码

只要知道当前密码，就可以随时更改密码。驱动器上的数据不受影响。



“更改密码”窗口。

1. 如果驱动器已解锁，请先点击 **锁定** 。
2. 点击驱动器旁的 **更改密码** 。
3. 输入当前密码，再输入两次新密码（规则与第 4 章相同），然后确认。

> **恢复密钥怎么办?**
> 它仍然有效：更改密码后，技术支持中心依然可以帮助您。

8 忘记密码

技术支持中心可以向您提供驱动器的恢复密钥：用它可以设置新密码并找回所有文件。



通过技术支持中心恢复。

1. 在密码输入框中选择**我忘记了密码**。
2. 窗口显示计算机名称和驱动器名称；点击**显示**还会显示驱动器标识符。
3. **联系技术支持中心**并提供这些信息。验证身份后，工作人员会向您口述 **48 位密钥**。
4. 在**恢复密钥**框中输入该密钥，设置新密码，然后点击**重置密码**。

一个密钥只能使用一次

每次恢复后，Kripta 都会生成新密钥并发送到技术支持中心。

谨防诈骗

技术支持中心绝不会索要您的密码。应由您主动联系技术支持中心，而不是相反。

9 设置

点击右上角的齿轮，或在图标菜单中选择 **设置...** 即可打开。



设置：语言、企业配置、组件、关于。

语言

从列表中选择语言：界面、图标菜单和授权请求会立即切换。选择 **自动** 时，Kripta 使用系统语言。内置语言：

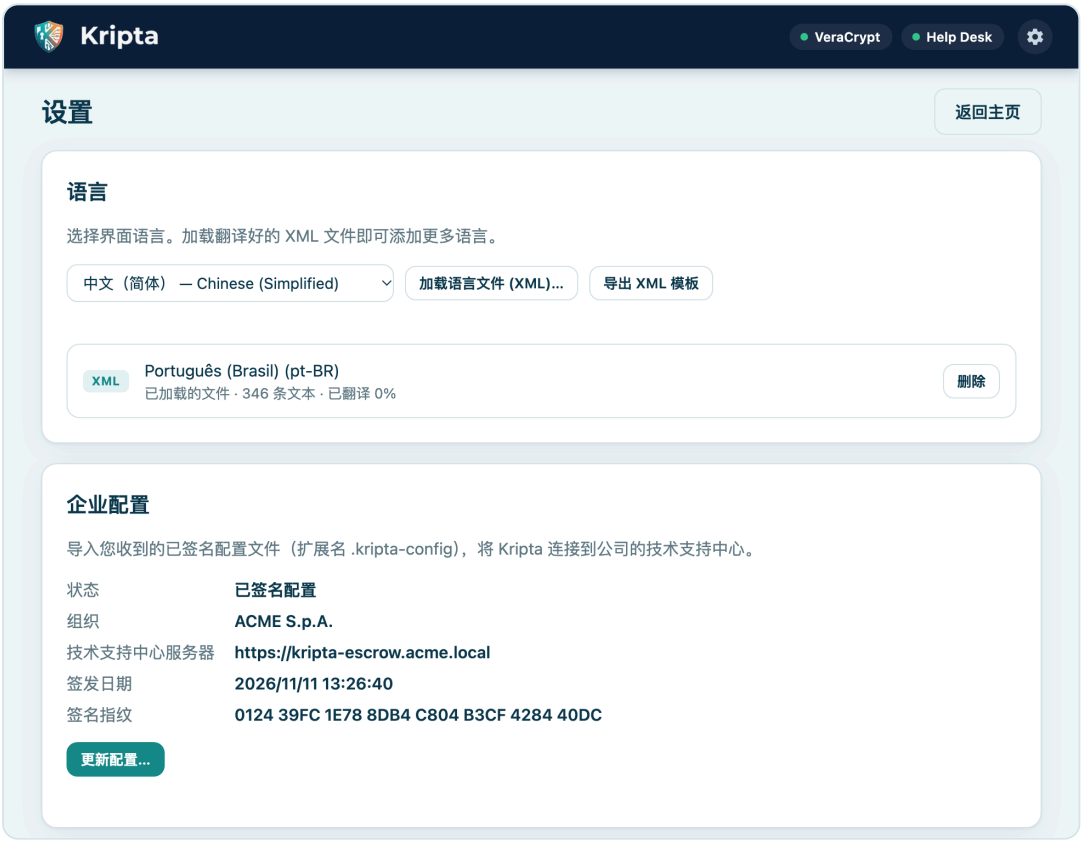
Italiano English Français Español Deutsch Русский العربية 中文 日本語

添加语言

翻译是简单的 XML 文件，每种语言一个。添加方法：

1. 点击 **导出 XML 模板**：当前语言的文件会保存到“下载”文件夹。
2. 翻译每个 `<string>` 元素的文本，保持 `id` 属性和占位符 `{1}`、`{2}` 不变。
3. 在文件开头设置 `code`（例如 `pt` 或 `pt-BR`）、`name`、`english-name` 和 `dir`（从右到左书写的语言用 `rtl`）。
4. 点击 **加载语言文件 (XML)...** 并选择该文件：语言会出现在列表中，并显示已翻译文本的百分比。缺少的文本以英文显示。

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



从 XML 文件加载的语言，带有“删除”按钮。

加载与内置语言代码相同的文件会替换该语言（便于修正某个术语）；**删除** 可恢复原始语言。 九种内置语言的文件位于本手册旁边的 `lang` 文件夹中。

企业配置

显示已安装配置的组织、技术支持中心服务器、日期和指纹。**更新配置...** 可导入技术支持中心提供的新文件（第 2 章）。

组件

显示已安装的 VeraCrypt 版本、Kripta 内置版本和最新可用版本。**立即检查**会立刻检查，**安装** / **更新 VeraCrypt** 开始安装。**每次启动时检查…** 复选框用于开启或关闭自动检查。

自动启动

登录时自动启动 Kripta 复选框默认开启。其下方显示自动启动是否已在系统中注册。如果关闭，在您打开 Kripta 之前它不会检测加密驱动器。

10 在其他计算机上使用驱动器

Kripta 加密的驱动器使用标准 **VeraCrypt** 格式和 **exFAT** 文件系统：可在 Windows、macOS 和 Linux 上打开。

计算机	插入驱动器时会发生什么
已配置 Kripta	出现密码输入框：一切自动完成。
已安装 Kripta 但**没有企业配置**（例如在家中）	仍会出现密码输入框，驱动器可以解锁。 如果缺少 VeraCrypt，Kripta 会提供 **立即安装** 。没有配置时无法加密新驱动器，也无法恢复密码。
仅安装了 VeraCrypt	打开 VeraCrypt，选择一个空闲槽位，点击**选择设备**，选择 U 盘的分区，然后点击**加载**并输入密码。
既没有 Kripta 也没有 VeraCrypt	不会出现任何提示：操作系统不会从 U 盘自动启动程序。 系统可能会提示**格式化**驱动器：**请始终拒绝**。请安装 Kripta（从公司网站获取），然后重新连接驱动器。

管理员权限

在任何计算机上打开加密驱动器都需要管理员权限，因为 VeraCrypt 使用系统驱动程序。 在您没有管理员凭据的计算机上无法打开驱动器。

用于交换的普通区域

如果经常使用没有 Kripta 的计算机，可以用 **加密区域 + 普通区域** 模板划分 U 盘（第 5 章）： 还可以将 Kripta 安装程序复制到普通区域中。

11 提示信息与故障排除

提示信息或情况	处理方法
Kripta 尚未连接到公司的技术支持中心	导入从技术支持中心收到的 `.kripta-config` 文件（第 2 章）。
配置包签名无效	文件已被修改或损坏：请向技术支持中心重新索取。
配置包的签名密钥不同 / 未经批准	该文件并非来自您的公司。请勿使用，并联系技术支持中心。
配置由 IT 部门管理，不能替换	计算机已集中配置：无需导入。
未安装 VeraCrypt 加密引擎	点击 **立即安装** 。如果没有该按钮，请联系技术支持中心。
VeraCrypt 官方签名无效 / 文件与签名版本不一致	下载内容被篡改或不完整：已取消安装。请稍后重试。
更新 VeraCrypt 前请锁定所有加密驱动器	在已打开的驱动器上点击 **锁定** ，然后重新更新。
请重新启动计算机以完成更新（Windows）	保存工作并重新启动。
无法连接技术支持中心服务器。加密未开始。	连接公司网络或 VPN 后重试。驱动器上的数据未受影响。
恢复密钥等待发送	联网后点击 **立即重试** 。在提示消失前请保持 Kripta 运行。
没有可用的驱动器	重新插入 U 盘（尝试其他 USB 端口），然后点击 **刷新列表** 。
管理员授权已取消 / 超时	重复操作并确认系统请求。
无法卸载 / 锁定卷	关闭从驱动器打开的文档和窗口，然后重试。
密码不正确	检查大写锁定键和键盘布局。如果忘记了密码，请参阅第 8 章。
恢复密钥不正确	与工作人员再次核对数字：需要使用**最新**的密钥。
该磁盘上有已解锁的 Kripta 驱动器	在主页上锁定它，然后重新划分。
系统未检测到新分区	断开并重新连接驱动器。
语言文件不是有效的 XML / 包含不允许的元素	修正提示中指出的文件：只允许包含纯文本的 `<string>` 元素。
插入驱动器时没有出现解锁窗口	确认 Kripta 正在运行（任务栏中有图标），然后在主窗口中使用 **解锁** 。

12 常见问题

能否在不丢失文件的情况下加密已有文件的 U 盘?

不能。加密会清除驱动器。请先将文件复制到其他位置，加密驱动器后再复制回来。

能否加密计算机的内置磁盘?

不能。Kripta 专为 U 盘和外置磁盘设计；系统磁盘不会显示。

技术支持中心能读取我的文件吗?

技术支持中心只保存恢复密钥，并且只能应您的请求查询，每次访问都会被记录。

需要记下恢复密钥吗?

不需要。您永远看不到它，也无需保存：它存档在技术支持中心。

Kripta 会在我的计算机上安装程序吗?

只会安装 VeraCrypt（macOS 上还有 FUSE-T），且需经您确认，并且只在开发者官方签名有效时安装。

可以在家用计算机上使用 U 盘吗?

可以，安装 Kripta 或 VeraCrypt 即可（第 10 章）。请始终遵守公司关于在办公场所外使用数据的规定。

没有我需要的语言，怎么办?

您可以翻译 XML 模板并在设置中加载（第 9 章），或请 IT 部门统一分发。

为什么密码中不能使用中文或带重音的字母?

Windows、macOS 和 Linux 对这些字符的编码可能不同：在另一个系统上输入同一密码可能无法识别。

加密会占用多少空间?

非常少：卷头仅占几百 KB。

A IT 附录

安装包

系统	安装包	说明
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	包含 VeraCrypt 官方 MSI（x64 和 ARM64）。应用以管理员权限启动。
macOS 11+	`Kripta_1.2.0_universal.dmg`	包含 VeraCrypt（FUSE-T 和 macFUSE 版本）以及无需内核扩展的 FUSE-T。
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	包含适用于 Ubuntu 22.04/24.04 和 Debian 12/13 的 VeraCrypt；其他版本由 Kripta 下载经验证的软件包。
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	包含适用于 Fedora 44 的 VeraCrypt；还需安装 `exfatprogs`。
其他发行版	`Kripta_1.2.0_amd64.AppImage`	便携式可执行文件。

签名配置

在 escrow 服务器上一次性生成签名密钥，然后对客户端配置进行签名（模板见 `deploy/client/kripta.toml.example`）：

```
kripta-escrow keygen-sign            # 私钥（离线保存）+ 公钥 + 指纹
kripta-escrow sign-config client.toml signing.key "ACME" acme.kripta-config
```

将 `acme.kripta-config` 分发给用户，并通过可信渠道（内网、技术支持中心电话）公布**指纹**。 Kripta 通过特权进程将配置保存到系统位置（`%ProgramData%\Kripta`、`/Library/Application Support/Kripta`、`/etc/kripta`），同时保存签名者的密钥：之后的更新必须使用相同的签名。 如不希望依赖用户核对指纹，可在构建 Kripta 时设置 `KRIPTA_PROVISIONING_KEYS=<公钥>`：只接受这些密钥。 IT 部门手动复制的（未签名）配置不能被配置包替换。

VeraCrypt 的安装与更新

- 内置安装程序在构建时通过 `scripts/fetch-veracrypt.py` 准备。
- 安装前，特权进程会使用内置的 IDRIX 密钥（指纹 `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`） 验证官方 SHA-256 列表的 OpenPGP 签名以及文件哈希。
- `kripta.toml` 中的选项：`veracrypt_update_check = false` 关闭更新检查；`veracrypt_release_api = "https://mirror.internal/…"` 使用与 GitHub API 格式相同的内部镜像。

语言

语言 XML 文件位于 `app/ui/lang/`（随应用提供）和 `docs/manuale/lang/`。用户加载的语言保存在用户数据文件夹（`languages/`）中。要向所有人分发新语言，请将文件添加到 `app/ui/lang/`，并将其代码加入 `app/ui/i18n.js` 的列表。

可选组件

- **登录时启动**到菜单栏 / 通知区域（`kripta --background`）：**自动**。Kripta 每次启动时都会注册（macOS：`~/Library/LaunchAgents/com.kripta.agent.plist`，异常终止时自动重启；Windows：登录时以最高权限运行的计划任务“Kripta”，安装程序也会创建，卸载时删除；Linux：.deb/.rpm 包提供 `/etc/xdg/autostart/kripta.desktop`，AppImage 使用 `~/.config/autostart/kripta.desktop`）。可在设置中关闭。
- **特权助手**作为服务运行（不再请求密码）：`deploy/macos/com.kripta.helper.plist`、`deploy/linux/kripta-helper.service`。