Kripta

Manuale utente

Cifratura guidata di chiavette USB e partizioni, con recupero della password tramite l'Help Desk aziendale.



Versione 1.2 · Windows · macOS · Linux

Novembre 2026

Indice

1 Cos'è Kripta — a cosa serve, cosa ti serve

2 Primo avvio — configurazione aziendale e componenti

3 La finestra principale — indicatori, avvisi, icona nella barra

4 Cifrare un'unità — la procedura guidata in 4 passi

5 Suddividere un disco in partizioni — area cifrata e area libera

6 Usare un'unità cifrata — sbloccare, aprire, bloccare

7 Cambiare la password

8 Ho dimenticato la password — recupero con l'Help Desk

9 Impostazioni — lingua, configurazione, aggiornamenti

10 Usare l'unità su altri computer

11 Messaggi e soluzione dei problemi

12 Domande frequenti

A Appendice per l'IT — pacchetti, configurazione firmata, lingue

Convenzioni

I testi che compaiono sullo schermo (pulsanti, titoli, voci) sono scritti così: **Cifra un'unità**. Le schermate provengono dalla versione macOS: su Windows e Linux la finestra è identica, cambiano solo i nomi dei dispositivi (per esempio `E:` o `/dev/sdb1` invece di `/dev/disk4s1`).

1 Cos'è Kripta

Kripta protegge i dati delle tue **chiavette USB** e delle **partizioni** di dischi esterni con una cifratura AES-256. Dopo la cifratura il contenuto dell'unità è leggibile solo da chi conosce la password: se perdi la chiavetta, nessun altro può aprirla.

Cifratura guidata
Quattro passaggi: scegli l'unità, scegli la password, conferma, attendi.

Sblocco automatico
Quando colleghi un'unità cifrata, Kripta ti chiede subito la password e la apre.

Funziona ovunque
La stessa chiavetta si apre su Windows, macOS e Linux (formato standard VeraCrypt).

Installazione autonoma
Kripta installa e aggiorna da solo VeraCrypt; la configurazione aziendale si importa con un file.

Nove lingue
Italiano, inglese, francese, spagnolo, tedesco, russo, arabo, cinese e giapponese, più quelle che aggiungi tu.

Recupero con l'Help Desk
Se dimentichi la password, l'Help Desk può aiutarti a impostarne una nuova senza perdere i dati.

Cosa ti serve

- **Kripta** installato sul computer. Al primo avvio Kripta installa da solo **VeraCrypt**, il motore di cifratura (su macOS anche **FUSE-T**), se manca: capitolo 2.
- Il **file di configurazione firmato** (`.kripta-config`) ricevuto dall'Help Desk, se l'IT non ha già configurato il computer.
- La **connessione alla rete aziendale** (o VPN) quando cifri una nuova unità: la chiave di ripristino viene inviata subito all'Help Desk. Per sbloccare un'unità già cifrata la rete non serve.
- Le **credenziali di amministratore** del computer, quando il sistema le richiede (vedi riquadro).

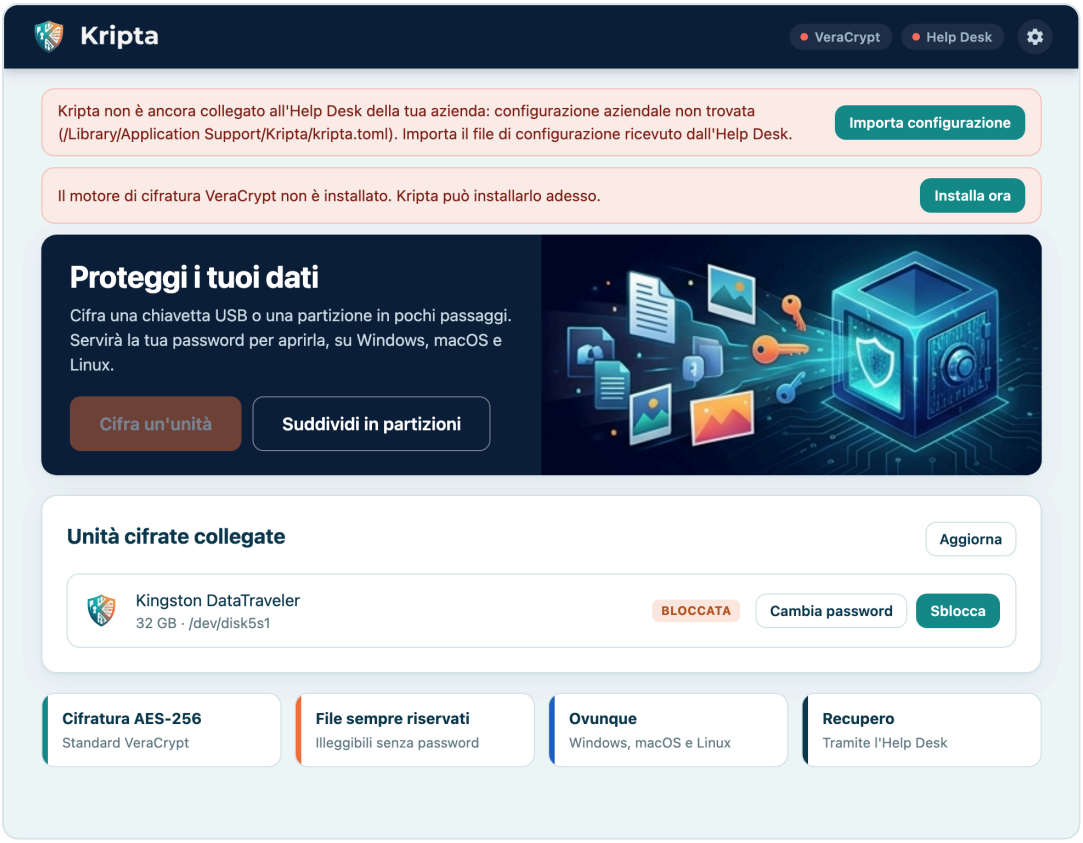
> **Richieste di autorizzazione**
> Per leggere e scrivere direttamente sull'unità, installare componenti e salvare la configurazione Kripta ha bisogno dei permessi di amministratore. Su **Windows** compare la finestra di Controllo account utente all'avvio. Su **macOS** e **Linux** compare il messaggio “Kripta richiede l'autorizzazione di un amministratore per completare l'operazione”. Se l'IT ha installato il servizio di sistema di Kripta, queste richieste non compaiono.

Come funziona il recupero, in breve

Durante la cifratura Kripta genera una **chiave di ripristino** di 48 cifre, la protegge e la invia all'archivio dell'Help Desk. Tu non devi né vederla né conservarla. Solo gli operatori dell'Help Desk possono consultarla, dopo aver verificato la tua identità, e ogni consultazione viene registrata.

2 Primo avvio

Al primo avvio Kripta controlla due cose: se è collegato all'Help Desk della tua azienda e se sul computer c'è VeraCrypt. Se manca qualcosa, in cima alla finestra compare un avviso con il pulsante per sistemarlo. Puoi fare tutto da solo.

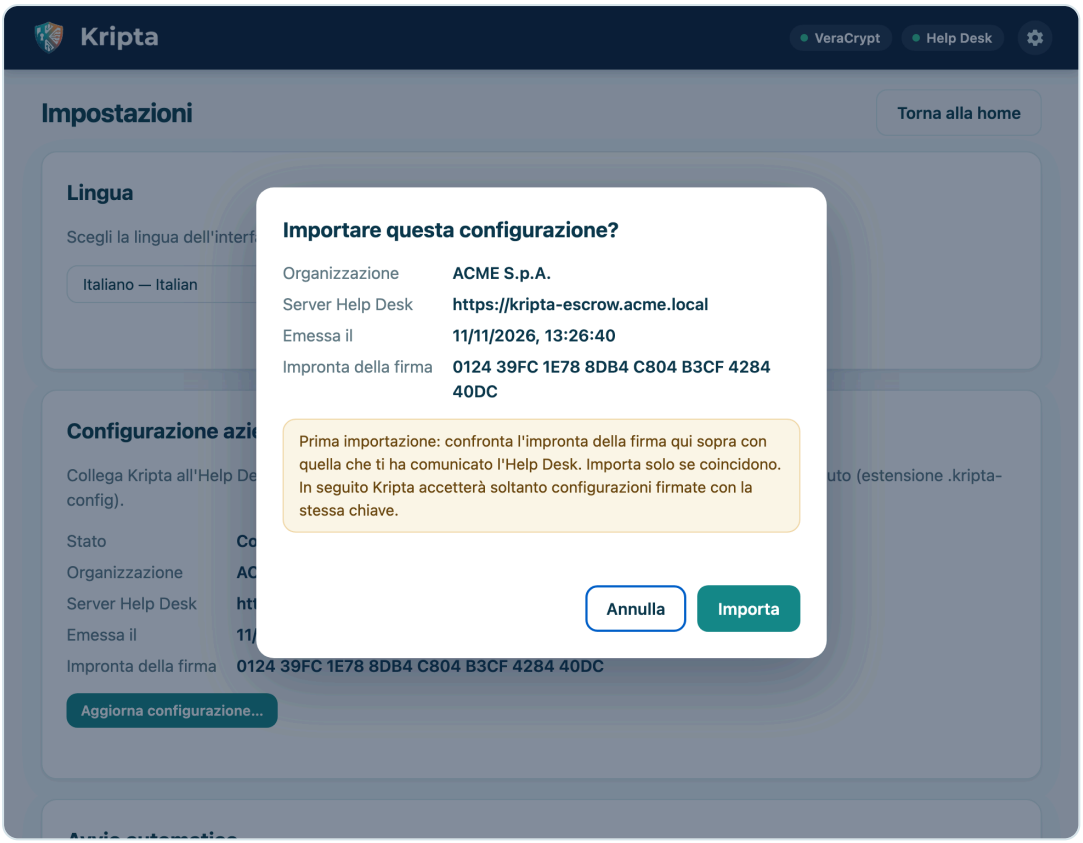


Primo avvio: configurazione da importare e VeraCrypt da installare.

Importare la configurazione aziendale

La configurazione indica a Kripta a quale archivio dell'Help Desk inviare le chiavi di ripristino. L'Help Desk te la fornisce come file con estensione `.kripta-config`, firmato digitalmente: nessuno può modificarlo senza che Kripta se ne accorga.

1. Salva sul computer il file ricevuto (per e-mail, dal portale aziendale o su una chiavetta).
2. Premi **Importa configurazione** nell'avviso, oppure apri **Impostazioni** (l'ingranaggio in alto a destra) e premi **Importa configurazione firmata…**.
3. Scegli il file. Kripta ne verifica la firma e mostra organizzazione, server dell'Help Desk, data di emissione e **impronta della firma**.
4. Alla prima importazione **confronta l'impronta** con quella che ti ha comunicato l'Help Desk (per telefono, sulla intranet…). Se coincide, premi **Importa**.
5. Conferma la richiesta di autorizzazione del sistema. Compare **Configurazione importata** e l'indicatore **Help Desk** diventa verde.

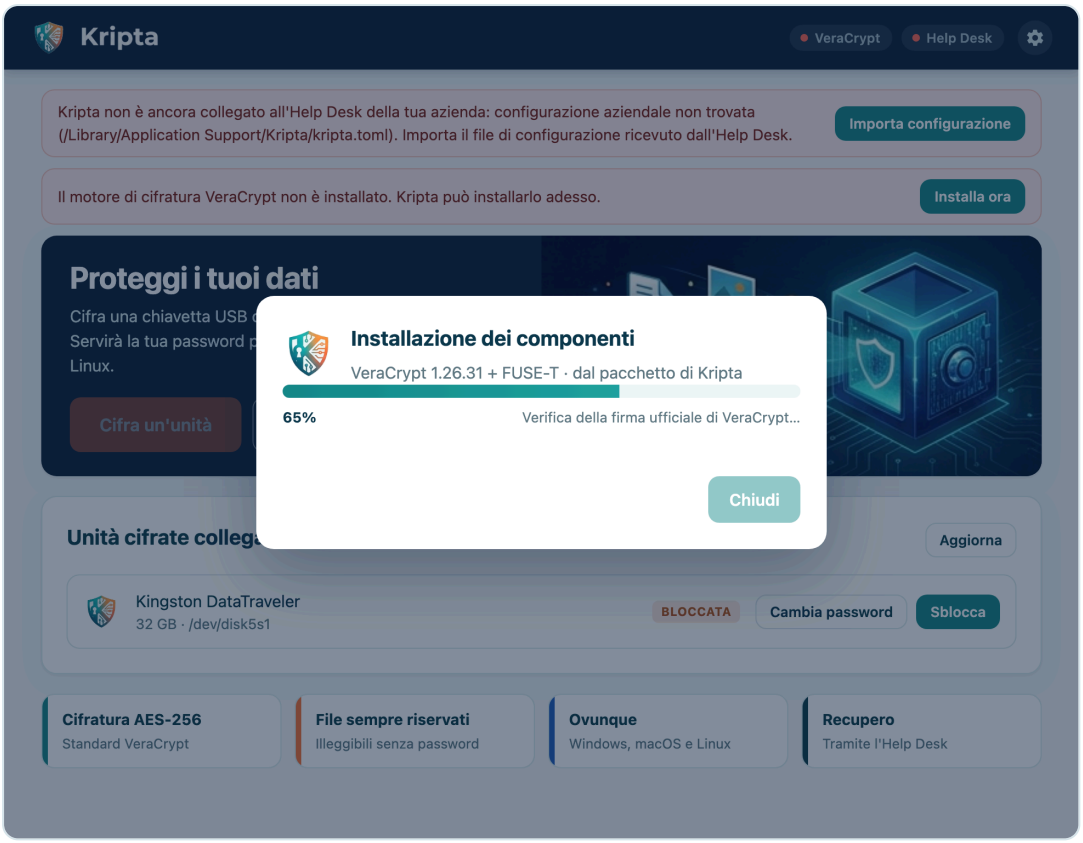


Conferma dell'importazione con l'impronta della firma.

> **Se l'impronta non coincide, non importare**
>
> Il file potrebbe non provenire dalla tua azienda. Annulla e contatta l'Help Desk. Dopo la prima importazione Kripta accetta solo aggiornamenti firmati con la stessa chiave: un file falso viene rifiutato automaticamente.

Installare VeraCrypt

Kripta contiene già l'installer ufficiale di VeraCrypt (e di FUSE-T per macOS). Premi **Installa ora** nell'avviso e conferma la richiesta di autorizzazione: Kripta verifica la firma ufficiale degli installer e li installa senza altre domande.

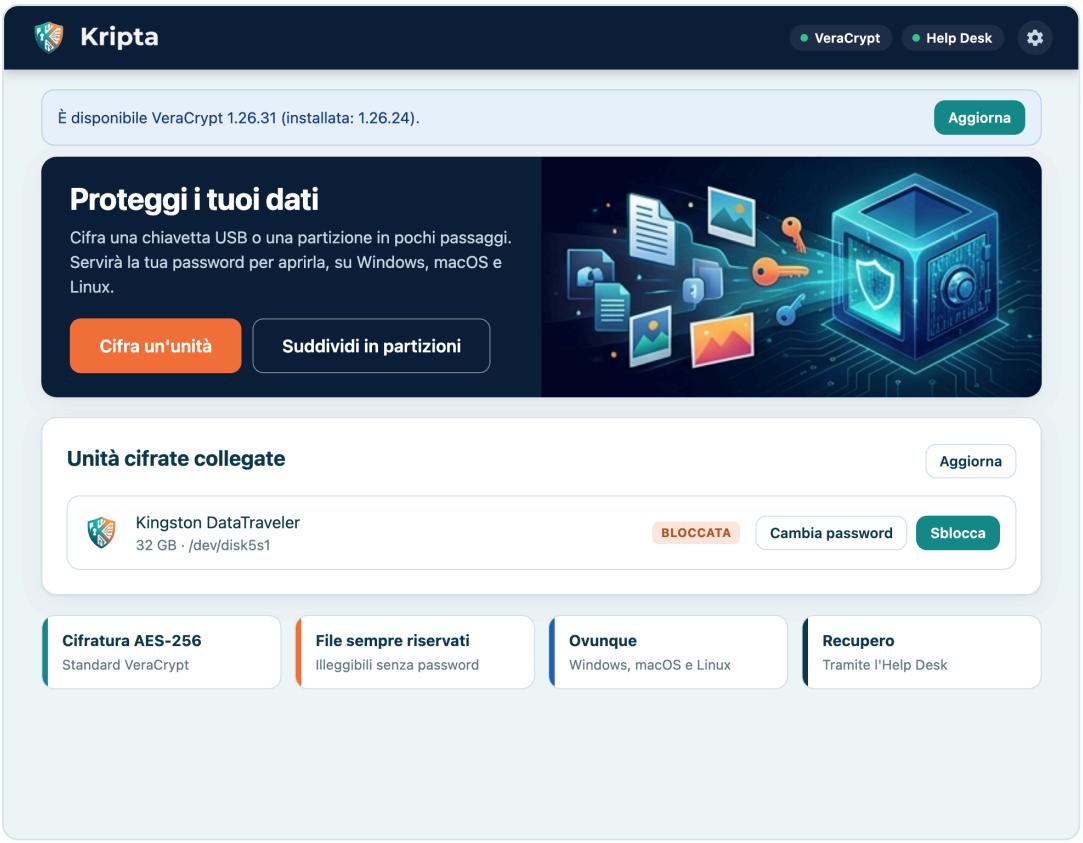


Installazione dei componenti con verifica della firma ufficiale.

Al termine compare **Installazione completata**. Su Windows può essere richiesto il riavvio del computer.

Aggiornamenti di VeraCrypt

A ogni avvio (e poi una volta al giorno) Kripta controlla se è uscita una versione più recente di VeraCrypt. Se sì, compare un avviso azzurro con il pulsante **Aggiorna**. La nuova versione viene scaricata dal sito ufficiale e installata solo se la firma degli sviluppatori di VeraCrypt è valida.



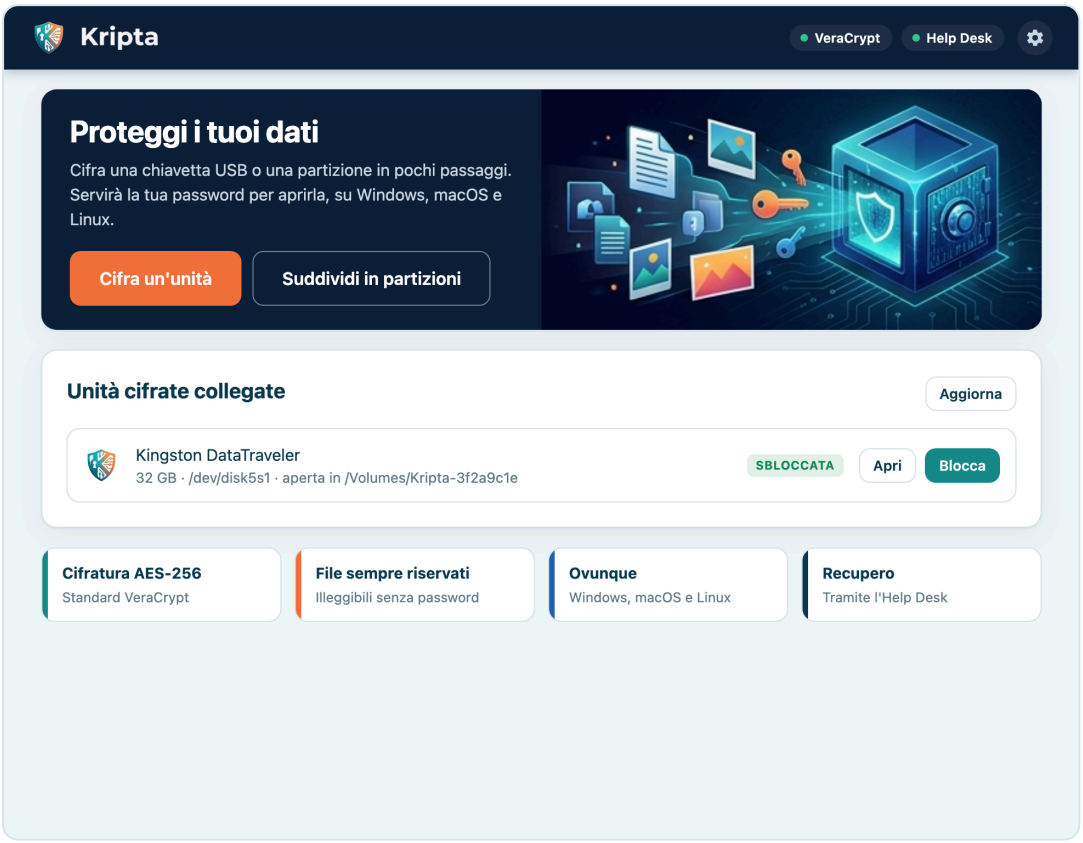
Aggiornamento di VeraCrypt disponibile.

Prima di aggiornare

Blocca tutte le unità cifrate aperte: Kripta non aggiorna VeraCrypt mentre un'unità è sbloccata. Puoi disattivare il controllo automatico nelle Impostazioni (capitolo 9).

3 La finestra principale

All'apertura Kripta mostra la schermata iniziale. Da qui puoi cifrare una nuova unità e gestire quelle già cifrate collegate al computer.

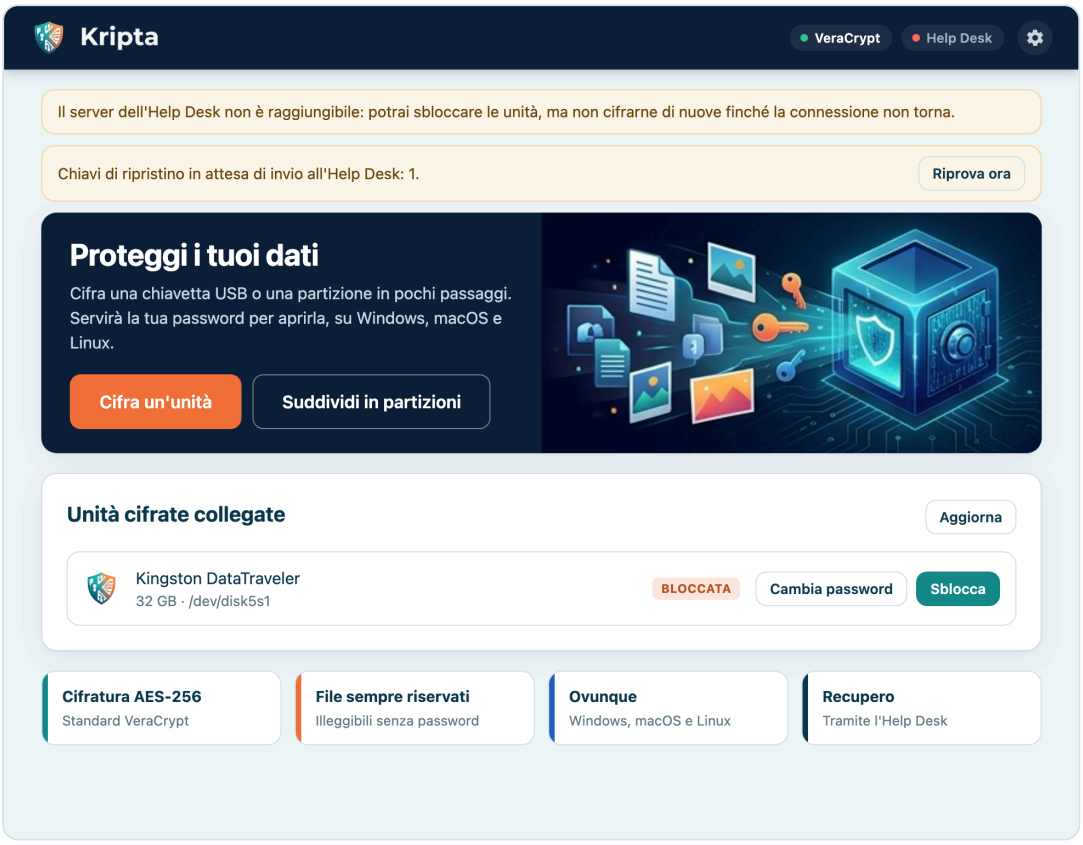


Schermata iniziale con un'unità cifrata collegata e sbloccata.

Elemento	A cosa serve
VeraCrypt	Pallino **verde**: il motore di cifratura è installato. **Rosso**: non è installato (capitolo 2). Passando con il mouse vedi la versione.
Help Desk	Verde: l'archivio delle chiavi è raggiungibile. Rosso: non lo è (rete assente, VPN spenta, configurazione mancante).
Ingranaggio	Apre le **Impostazioni**: lingua, configurazione aziendale, componenti (capitolo 9).
Cifra un'unità	Avvia la procedura guidata (capitolo 4). È disattivato se Kripta non è configurato o se manca VeraCrypt.
Suddividi in partizioni	Divide una chiavetta o un disco esterno in più partizioni (capitolo 5).
Unità cifrate collegate	Le unità Kripta collegate, con lo stato **Bloccata** o **Sbloccata** e i relativi pulsanti.

Avvisi

In cima alla finestra possono comparire riquadri colorati con un pulsante per risolvere il problema:



Server dell'Help Desk non raggiungibile e una chiave di ripristino in attesa di invio.

- **Server dell'Help Desk non raggiungibile:** puoi continuare a sbloccare le unità, ma non a cifrarne di nuove.
- **Chiavi di ripristino in attesa di invio:** Kripta riprova da solo; puoi premere **Riprova ora** quando torni in rete. **Tieni Kripta aperto finché l'avviso non scompare.**
- **Kripta non è ancora collegato all'Help Desk / VeraCrypt non è installato / è disponibile VeraCrypt…:** vedi capitolo 2.

L'icona di Kripta: barra dei menu e area di notifica

Kripta lavora in background per accorgersi di quando colleghi un'unità cifrata, e si controlla da un'icona con l'emblema:

Sistema	Dove si trova l'icona	Da sapere
macOS	Nella **barra dei menu** in alto a destra. Kripta **non compare nel Dock**.	Sui MacBook con la tacca, se la barra è piena le icone in eccesso restano nascoste: togli quelle che non usi o trascinale tenendo premuto ⌘.
Windows	Nell'**area di notifica** in basso a destra, vicino all'orologio.	Se è tra le icone nascoste, clicca la freccia ^ e trascina l'emblema sulla barra.

Sistema	Dove si trova l'icona	Da sapere
Linux	Nell'**area di notifica** del pannello.	Su GNOME “puro” (Fedora, Debian) serve l'estensione **AppIndicator and KStatusNotifierItem Support**.

Il menu dell'icona contiene **Apri Kripta**, **Cifra un'unità…**, **Suddividi in partizioni…**, **Blocca tutte le unità**, **Impostazioni…** e **Esci da Kripta**. Le voci seguono la lingua scelta.

> **Chiudere la finestra non chiude Kripta**
>
> Kripta resta attivo nella barra dei menu o nell'area di notifica. Per riaprire la finestra usa **Apri Kripta**, oppure avvia di nuovo Kripta: verrà mostrata la finestra già attiva.

Avvio automatico

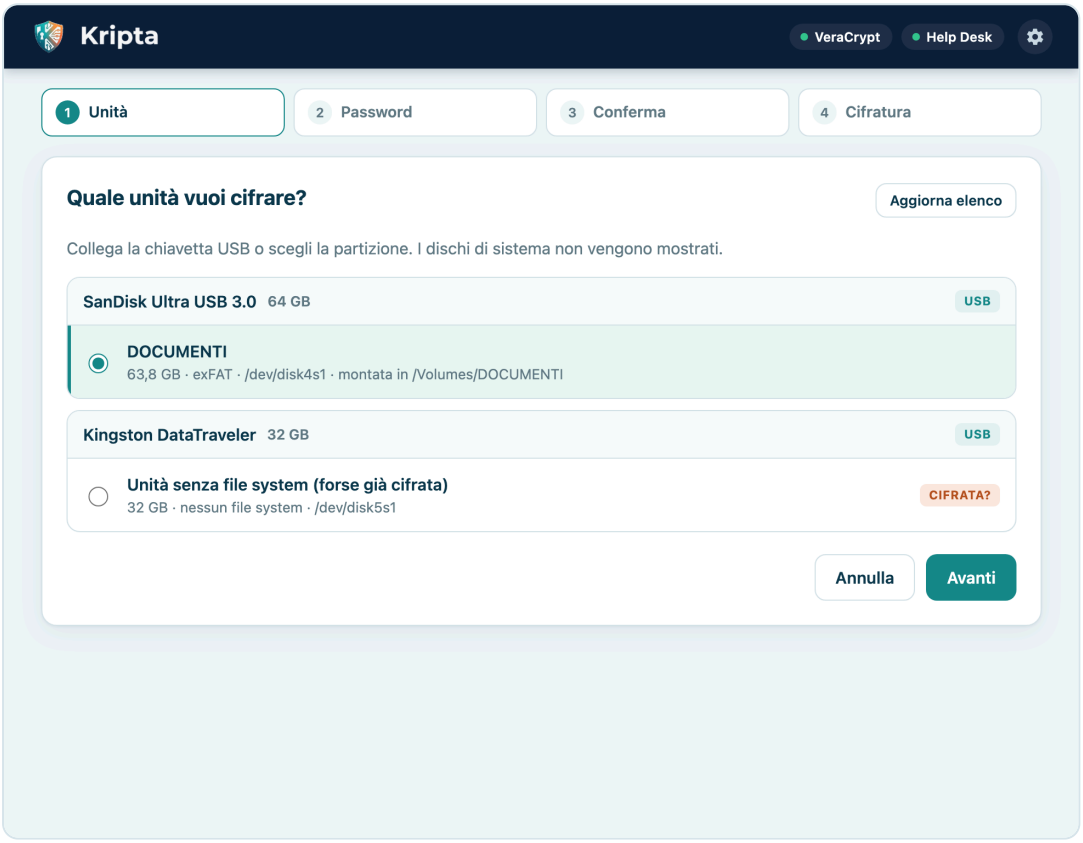
Dopo l'installazione Kripta **si avvia da solo a ogni accesso**, senza aprire la finestra, e resta sempre in ascolto: appena colleghi un'unità cifrata ti chiede la password. Puoi disattivarlo in **Impostazioni › Avvio automatico** (capitolo 9). **Esci da Kripta** lo chiude fino al prossimo accesso.

4 Cifrare un'unità

La cifratura cancella tutto il contenuto dell'unità.
Prima di iniziare copia altrove i file che vuoi conservare. Dopo la cifratura potrai ricopiarli sull'unità protetta.

Collega la chiavetta, verifica che l'indicatore **Help Desk** sia verde e premi **Cifra un'unità**.

Passo 1 — Unità

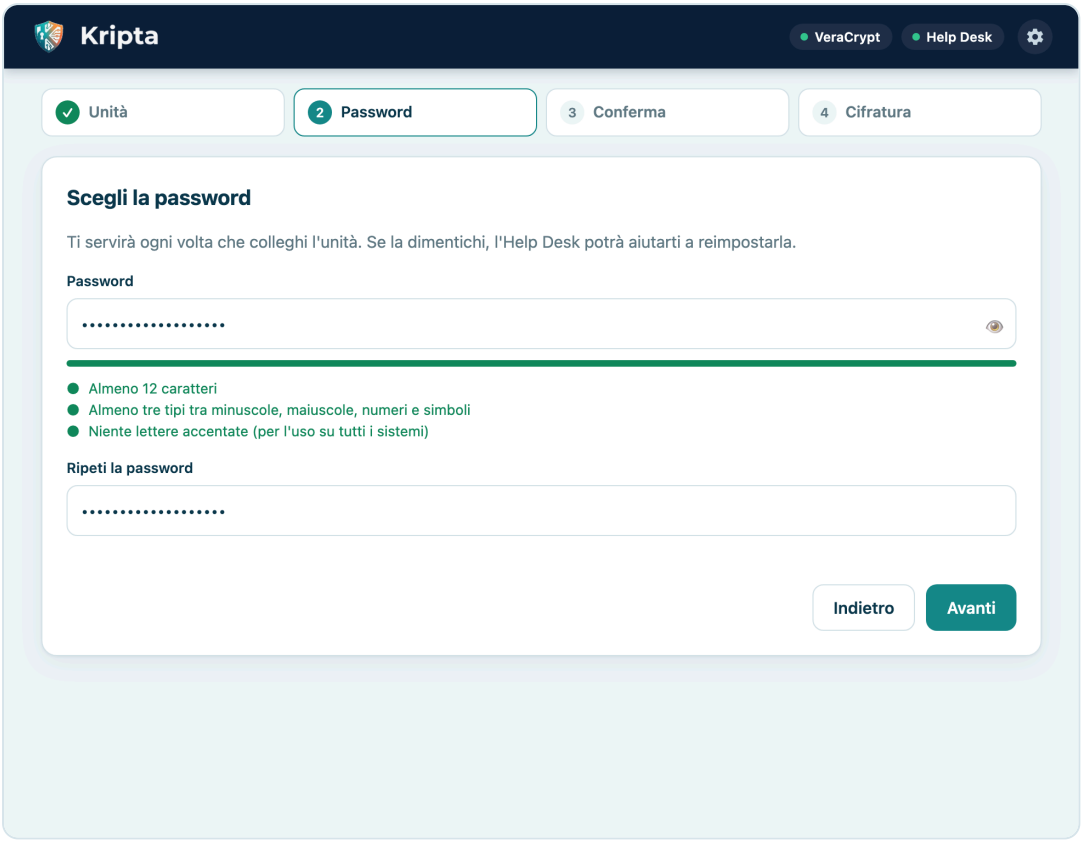


Scelta dell'unità da cifrare.

1. Kripta elenca i dispositivi collegati, prima quelli rimovibili. I **dischi di sistema non vengono mai mostrati**.
2. Controlla con attenzione **capacità e nome** per essere sicuro di scegliere l'unità giusta.
3. Se la chiavetta non compare, ricollegala e premi **Aggiorna elenco**.
4. Seleziona l'unità e premi **Avanti**.

Etichetta “Cifrata?”
Indica un'unità senza file system riconoscibile: probabilmente è già cifrata. Se la cifri di nuovo, il suo contenuto attuale andrà perso.

Passo 2 — Password

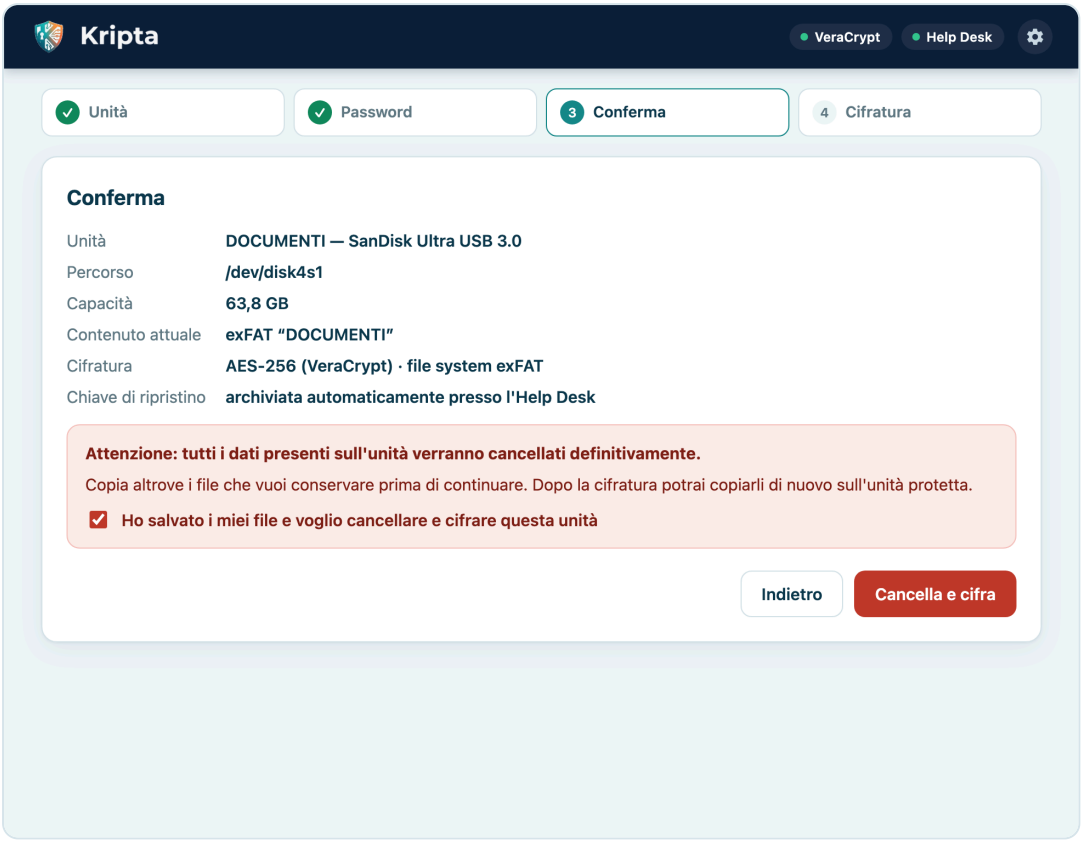


Le regole diventano verdi man mano che vengono rispettate.

La password deve avere **almeno 12 caratteri**, **almeno tre tipi** tra minuscole, maiuscole, numeri e simboli, e **nessuna lettera accentata** (à, è, ü…), che su altri sistemi potrebbe essere digitata in modo diverso. La barra colorata indica la robustezza; il pulsante 👁 mostra la password. Ripetila nel secondo campo e premi **Avanti**.

> **Consiglio**
> Una frase di più parole unite da simboli e numeri (per esempio `Treno-Lago-Verde-47`) è sicura e facile da ricordare. Non usare la password del tuo account aziendale.

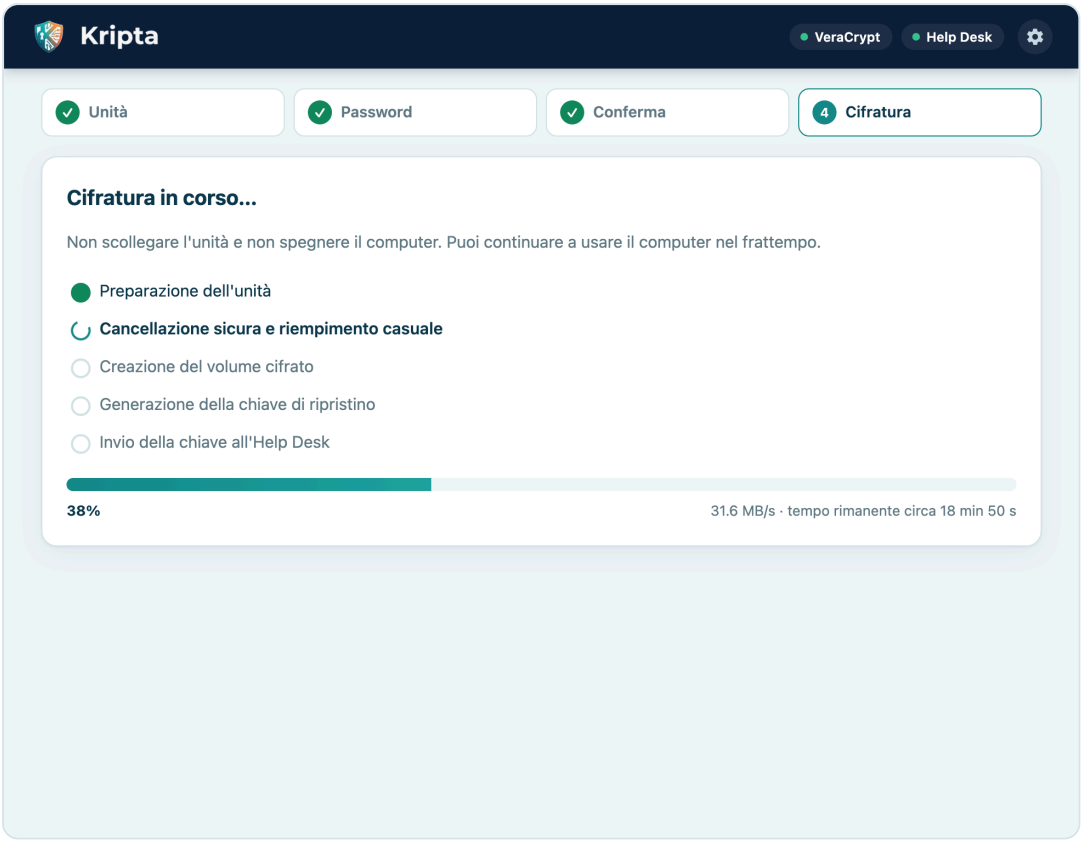
Passo 3 — Conferma



Riepilogo e conferma della cancellazione.

Controlla il riepilogo, seleziona **Ho salvato i miei file e voglio cancellare e cifrare questa unità** e premi **Cancella e cifra**. Il sistema può chiederti l'autorizzazione di amministratore.

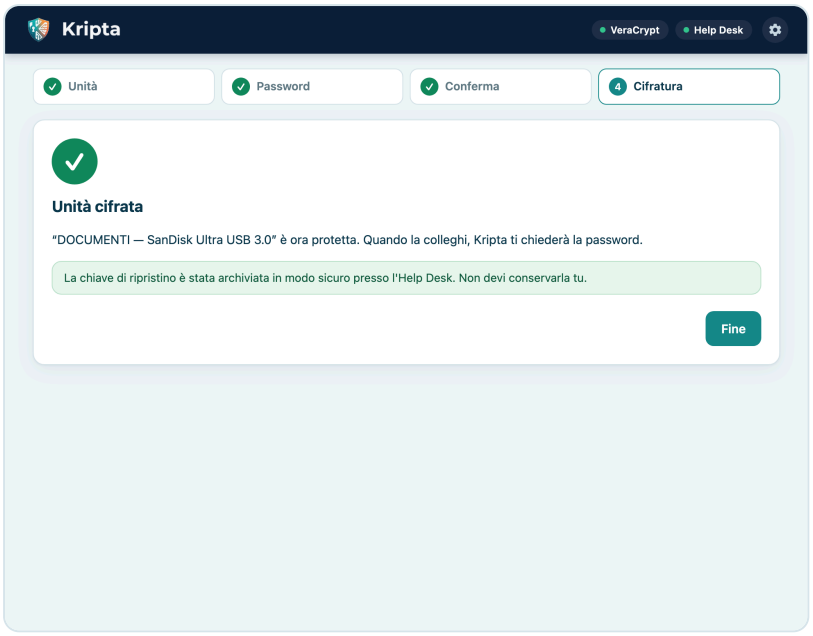
Passo 4 — Cifratura



Avanzamento con velocità e tempo residuo.

Kripta prepara l'unità, la riscrive interamente con dati casuali (la fase più lunga), crea il volume cifrato exFAT, genera la chiave di ripristino e la invia all'Help Desk.

> **Durante la cifratura**
> Non scollegare l'unità e non spegnere né sospendere il computer. Una chiavetta da 64 GB richiede indicativamente da 15 minuti a un'ora.



Cifratura completata.

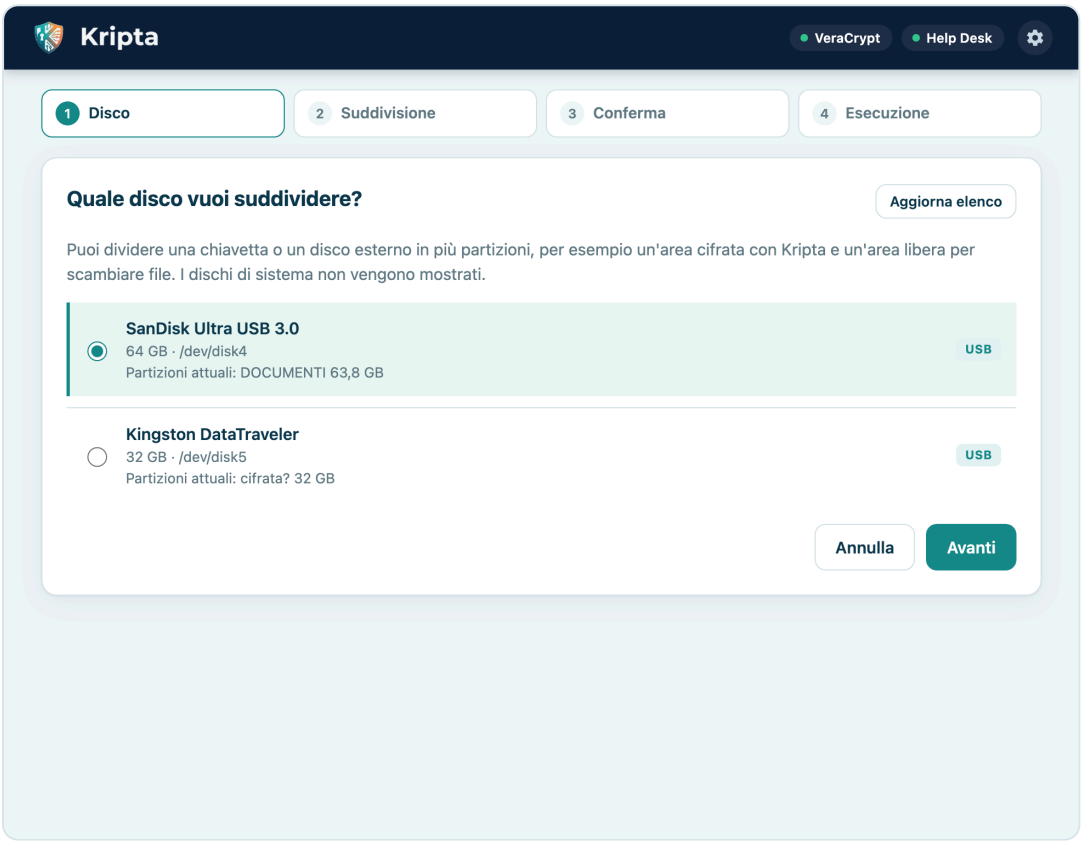
Se compare **la chiave di ripristino non è ancora stata inviata**, l'unità è comunque cifrata e utilizzabile: lascia Kripta aperto e connesso, invierà la chiave appena possibile. Se la cifratura non riesce, il messaggio spiega il motivo (capitolo 11).

5 Suddividere un disco in partizioni

Con **Suddividi in partizioni** dividi una chiavetta USB o un disco esterno in più parti indipendenti, ognuna con il proprio nome e file system. L'uso tipico è un'**area cifrata** per i dati riservati e un'**area libera** per scambiare file con computer senza Kripta.

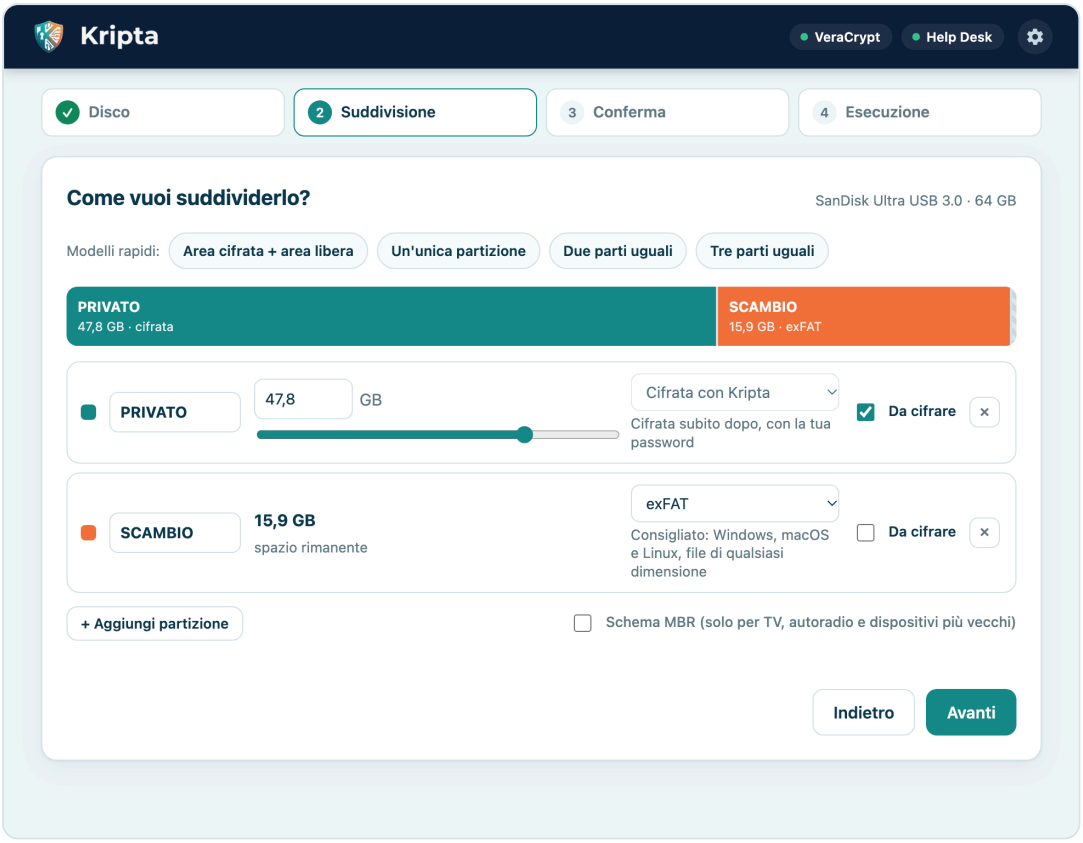
> **La suddivisione cancella tutto il disco**
> , comprese le partizioni esistenti e le unità già cifrate. Salva altrove i file da conservare.

Passo 1 — Disco



Scelta del disco, con le partizioni attuali.

Passo 2 — Suddivisione



La barra colorata mostra in proporzione la suddivisione.

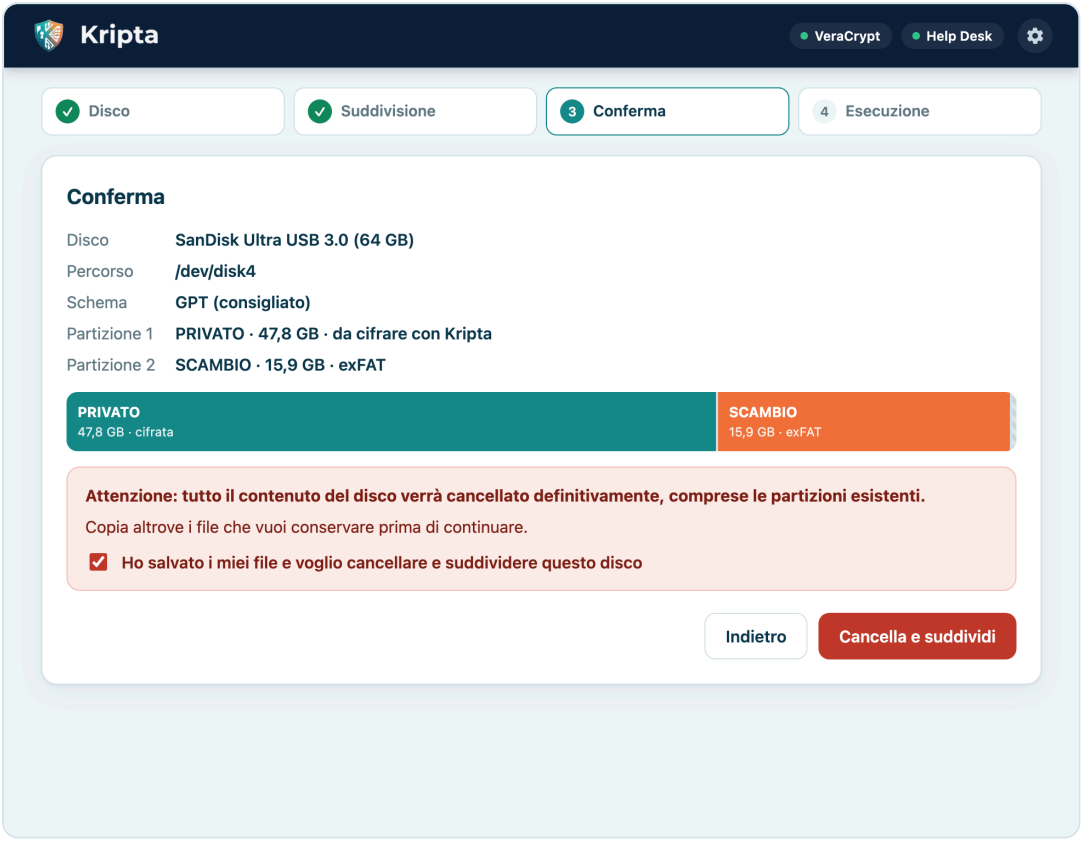
Modello	Risultato
Area cifrata + area libera	Tre quarti del disco da cifrare e il resto libero in exFAT. È il modello proposto all'inizio.
Un'unica partizione	Tutto il disco in una sola partizione.
Due / Tre parti uguali	Il disco diviso in parti di uguale dimensione.

Per ogni partizione imposti **nome** (fino a 11 caratteri: lettere, numeri, `_` e `-`), **dimensione** (l'ultima occupa lo spazio rimanente), **file system** e **Da cifrare**. Con **+ Aggiungi partizione** ne aggiungi un'altra (fino a 8).

File system	Si apre su	Note
exFAT (consigliato)	Windows, macOS, Linux	Nessun limite pratico sulla dimensione dei file.
FAT32	Quasi ogni dispositivo	File fino a 4 GB; su Windows partizione fino a 32 GB.
NTFS	Windows; macOS solo in lettura	Su Linux richiede `ntfs-3g`.
APFS, **Mac OS esteso**	Solo Mac	Disponibili solo da un Mac.
ext4	Solo Linux	Disponibile solo da Linux.

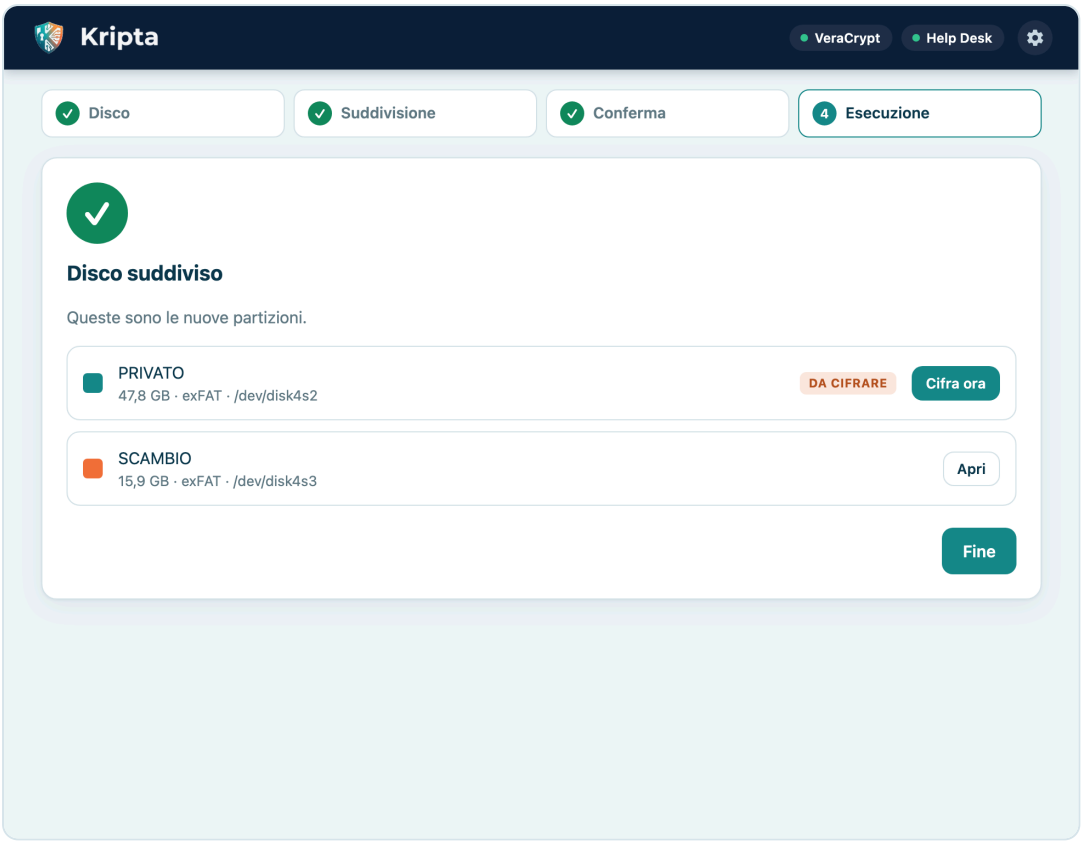
Schema MBR
Attivalo solo se la chiavetta deve funzionare con TV, autoradio o computer molto vecchi: al massimo 4 partizioni e 2 TB.

Passo 3 — Conferma e passo 4 — Esecuzione



Riepilogo prima della cancellazione.

Seleziona la casella di conferma e premi **Cancella e suddividi**. Di solito basta meno di un minuto.



Partizioni create: l'area da cifrare ha il pulsante “Cifra ora”.

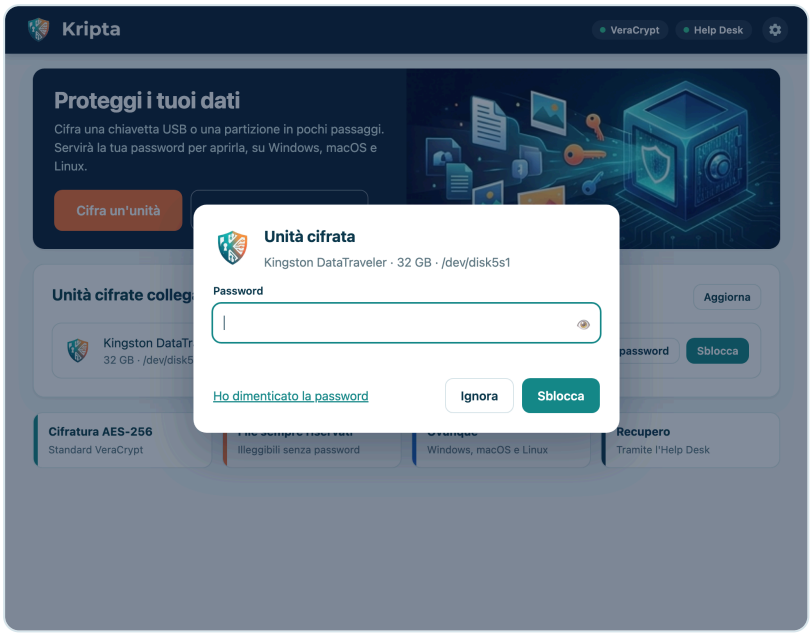
Accanto alle partizioni da cifrare premi **Cifra ora**: la cifratura (capitolo 4) parte con la partizione già selezionata.

> **Finché non la cifri, l'area “da cifrare” non è protetta**
> Non copiarci file riservati prima di aver completato la cifratura.

6 Usare un'unità cifrata

Sbloccare

Quando colleghi un'unità cifrata con Kripta in esecuzione, compare automaticamente la richiesta della password.



Richiesta della password all'inserimento.

1. Scrivi la password e premi **Sblocca** (o Invio).
2. L'unità si apre come un normale disco in Esplora file, nel Finder o nel file manager di Linux.
3. Con **Ignora** la sblocchi più tardi dalla finestra principale.

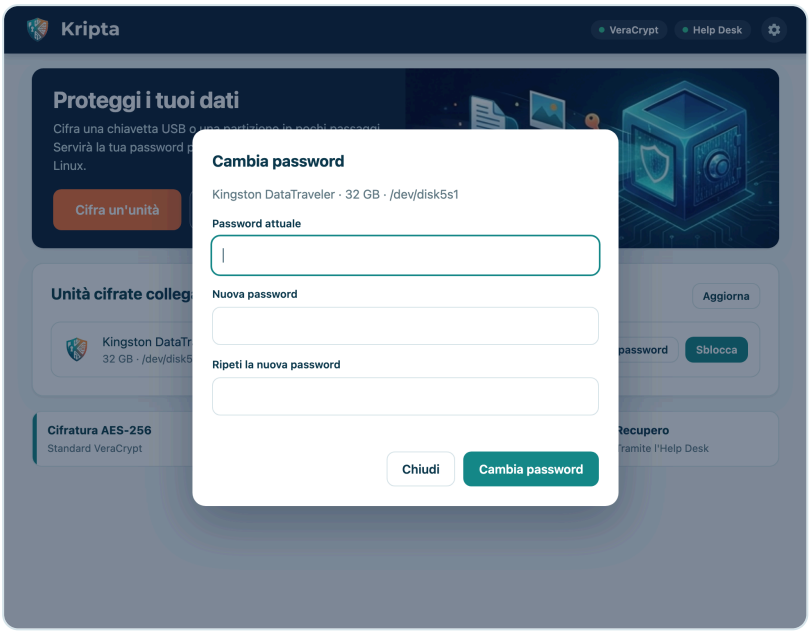
Lavorare con i file e bloccare

Con l'unità sbloccata usi i file normalmente: tutto ciò che scrivi viene cifrato in modo trasparente. Quando hai finito, chiudi i file aperti, premi **Blocca** e scollega l'unità.

> **Non scollegare un'unità sbloccata senza bloccarla**
> Potresti perdere i file che stavi copiando.

7 Cambiare la password

Puoi cambiare la password quando vuoi, se conosci quella attuale. I dati sull'unità non vengono toccati.



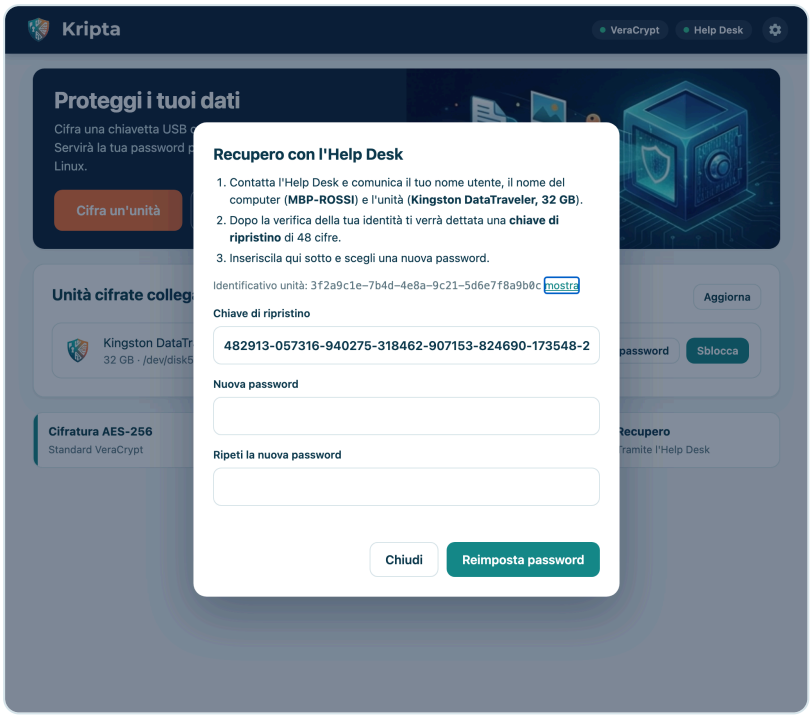
Finestra Cambia password.

1. Se l'unità è sbloccata, premi prima **Blocca**.
2. Premi **Cambia password** accanto all'unità.
3. Inserisci la password attuale e due volte quella nuova (stesse regole del capitolo 4), poi conferma.

> **E la chiave di ripristino?**
> Resta valida: l'Help Desk potrà aiutarti anche dopo un cambio di password.

8 Ho dimenticato la password

L'Help Desk può fornirti la chiave di ripristino dell'unità: con quella imposti una nuova password e ritrovi tutti i file.



Recupero con l'Help Desk.

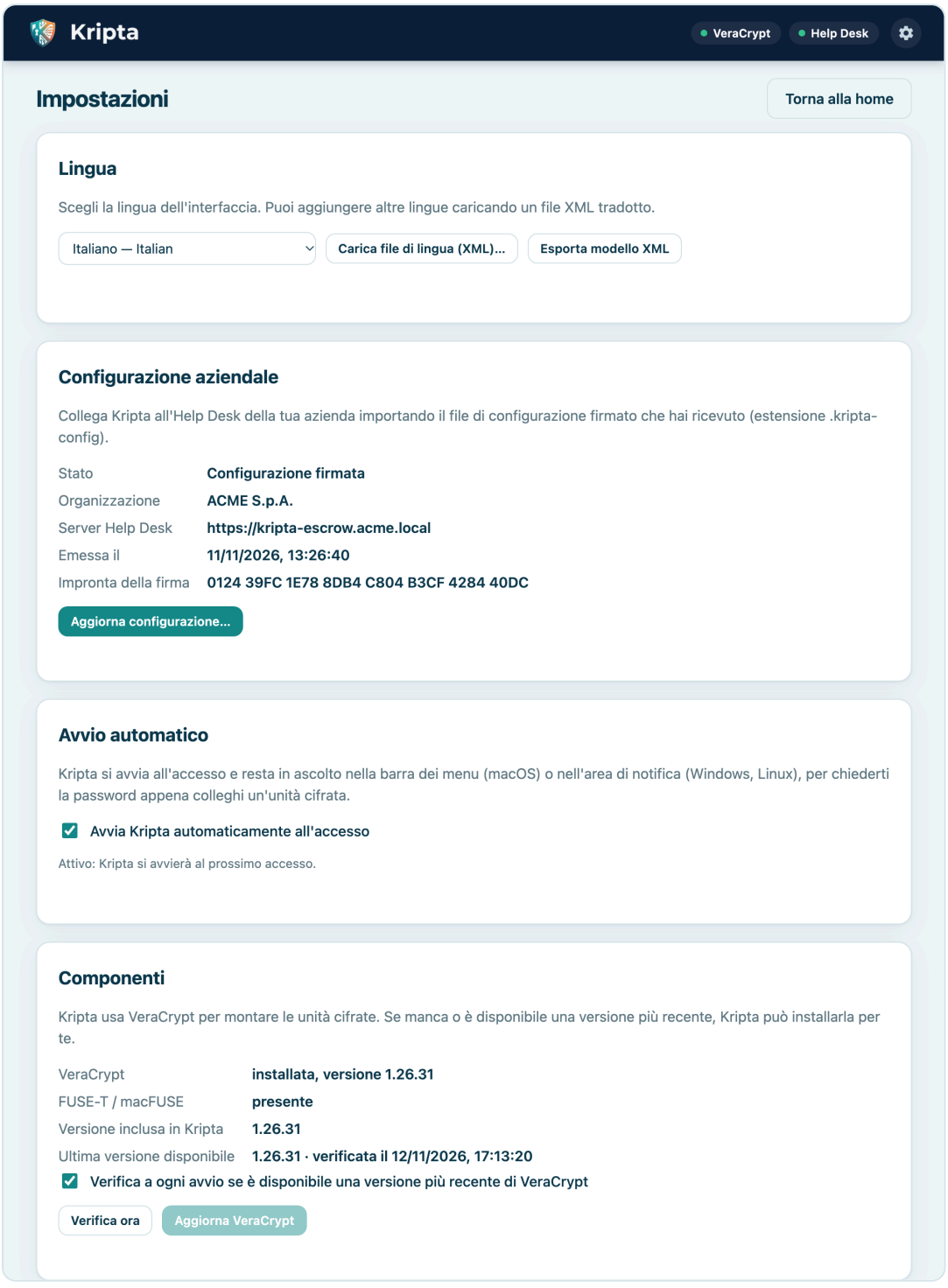
1. Nella richiesta di password scegli **Ho dimenticato la password**.
2. La finestra mostra nome del computer e dell'unità; con **mostra** compare anche l'identificativo dell'unità.
3. **Contatta l'Help Desk** e comunica questi dati. Dopo la verifica della tua identità ti verrà dettata la **chiave di 48 cifre**.
4. Scrivila nel campo **Chiave di ripristino**, scegli una nuova password e premi **Reimposta password**.

> **Una chiave, un solo uso**
> Dopo ogni recupero Kripta genera una nuova chiave e la invia all'Help Desk.

> **Attenzione alle truffe**
> L'Help Desk non ti chiederà mai la tua password. Sei tu a contattare l'Help Desk, non il contrario.

9 Impostazioni

Si aprono con l'ingranaggio in alto a destra o con **Impostazioni…** dal menu dell'icona.



Le Impostazioni: lingua, configurazione aziendale, componenti, informazioni.

Lingua

Scegli la lingua dall'elenco: l'interfaccia, il menu dell'icona e le richieste di autorizzazione cambiano subito. Con **Automatica** Kripta usa la lingua del sistema. Lingue incluse:

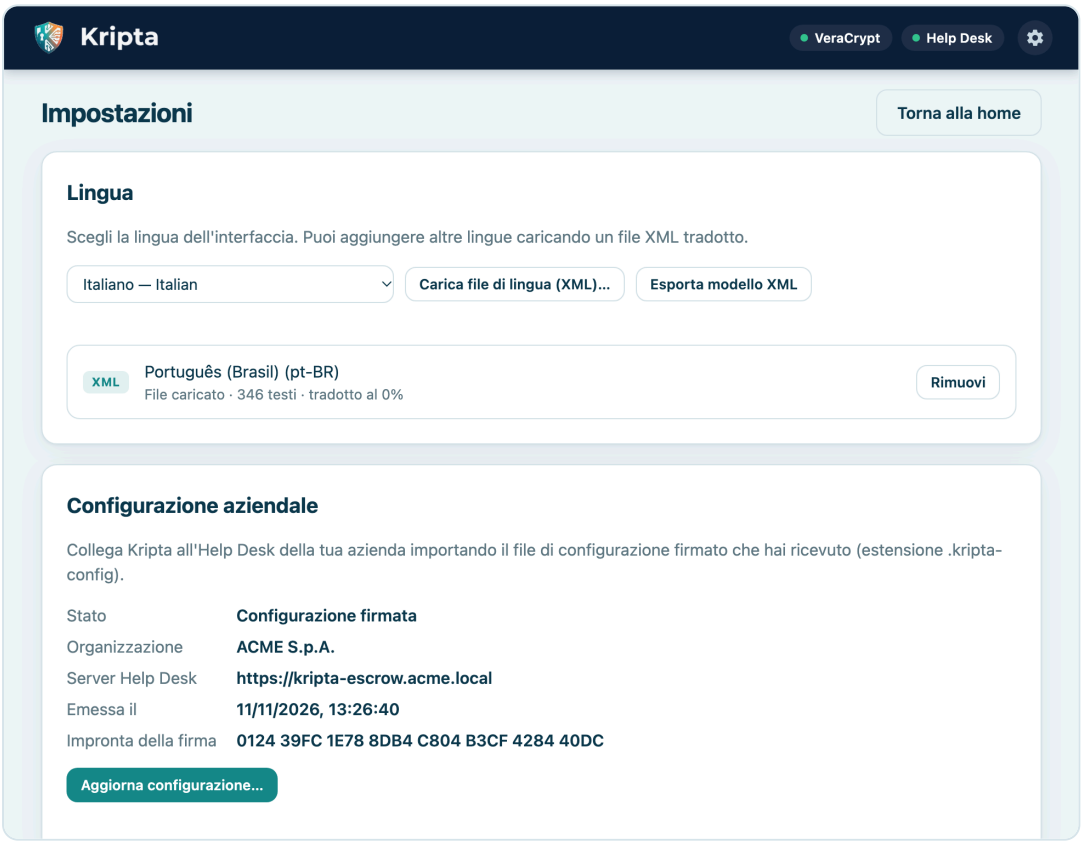
Italiano English Français Español Deutsch Русский العربية 中文 日本語

Aggiungere una lingua

Le traduzioni sono semplici file **XML**, uno per lingua. Per aggiungerne una:

1. Premi **Esporta modello XML**: nella cartella Download viene salvato il file della lingua attuale.
2. Traduci il testo di ogni elemento `<string>` lasciando invariati gli attributi `id` e i segnaposto `{1}`, `{2}`.
3. In cima al file imposta `code` (per esempio `pt` o `pt-BR`), `name`, `english-name` e `dir` (`rtl` per le lingue scritte da destra a sinistra).
4. Premi **Carica file di lingua (XML)…** e scegli il file: la lingua compare nell'elenco con la percentuale di testi tradotti. I testi mancanti vengono mostrati in inglese.

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



Una lingua caricata da file XML, con il pulsante Rimuovi.

Caricando un file con lo stesso codice di una lingua inclusa la sostituisci (utile per correggere un termine); **Rimuovi** ripristina la lingua originale. I file delle nove lingue incluse si trovano accanto a questo manuale, nella cartella `lang`.

Configurazione aziendale

Mostra organizzazione, server dell'Help Desk, data e impronta della configurazione installata. Con **Aggiorna configurazione…** importi un nuovo file ricevuto dall'Help Desk (capitolo 2).

Componenti

Mostra la versione di VeraCrypt installata, quella inclusa in Kripta e l'ultima disponibile. **Verifica ora** controlla subito, **Installa** / **Aggiorna VeraCrypt** avvia l'installazione. La casella **Verifica a ogni avvio…** attiva o disattiva il controllo automatico.

Avvio automatico

La casella **Avvia Kripta automaticamente all'accesso** è attiva di serie. Sotto la casella è indicato se l'avvio automatico è registrato nel sistema. Se la disattivi, Kripta non rileva le unità cifrate finché non lo apri.

10 Usare l'unità su altri computer

Le unità cifrate da Kripta usano il formato standard di **VeraCrypt** con file system **exFAT**: si aprono su Windows, macOS e Linux.

Computer	Cosa succede inserendo l'unità
Con Kripta configurato	Compare la richiesta della password: è tutto automatico.
Con Kripta installato ma **senza configurazione aziendale** (per esempio a casa)	Compare comunque la richiesta della password e l'unità si sblocca. Se manca VeraCrypt, Kripta propone **Installa ora**. Senza configurazione non puoi cifrare nuove unità né fare il recupero.
Con solo VeraCrypt	Apri VeraCrypt, scegli uno slot libero, **Seleziona dispositivo**, scegli la partizione della chiavetta, poi **Monta** e inserisci la password.
Senza Kripta né VeraCrypt	Non compare nessuna richiesta: i sistemi operativi non avviano programmi dalle chiavette. Il sistema potrebbe proporti di **formattare** l'unità: **rifiuta sempre**. Installa Kripta (dal sito aziendale) e collega di nuovo l'unità.

Diritti di amministratore
Per aprire un'unità cifrata su qualsiasi computer servono i diritti di amministratore, perché VeraCrypt usa un driver di sistema. Su un computer di cui non hai le credenziali l'unità non si può aprire.

Area libera per lo scambio
Se devi spesso usare computer senza Kripta, suddividi la chiavetta con il modello **Area cifrata + area libera** (capitolo 5): nell'area libera puoi copiare anche l'installer di Kripta.

11 Messaggi e soluzione dei problemi

Messaggio o situazione	Cosa fare
Kripta non è ancora collegato all'Help Desk della tua azienda	Importa il file `.kripta-config` ricevuto dall'Help Desk (capitolo 2).
La firma del pacchetto non è valida	Il file è stato modificato o danneggiato: richiedilo di nuovo all'Help Desk.
Il pacchetto è firmato con una chiave diversa / non è firmato con una chiave approvata	Il file non proviene dalla tua azienda. Non usarlo e contatta l'Help Desk.
La configurazione è gestita dall'IT e non può essere sostituita	Il computer è configurato centralmente: non serve importare nulla.
Il motore di cifratura VeraCrypt non è installato	Premi **Installa ora**. Se il pulsante non c'è, contatta l'Help Desk.
La firma ufficiale di VeraCrypt non è valida / il file non corrisponde alla versione firmata	Il download è stato alterato o è incompleto: l'installazione è stata annullata. Riprova più tardi.
Blocca tutte le unità cifrate prima di aggiornare VeraCrypt	Premi **Blocca** sulle unità aperte, poi ripeti l'aggiornamento.
Riavvia il computer per completare l'aggiornamento (Windows)	Salva il lavoro e riavvia.
Il server Help Desk non è raggiungibile. La cifratura non è stata avviata.	Collegati alla rete aziendale o alla VPN e riprova. I dati sull'unità non sono stati toccati.
Chiavi di ripristino in attesa di invio	Connettiti alla rete e premi **Riprova ora**. Tieni Kripta aperto finché l'avviso non scompare.
Nessuna unità disponibile	Ricollega la chiavetta (prova un'altra porta USB) e premi **Aggiorna elenco**.
Autorizzazione amministratore annullata / Tempo scaduto	Ripeti l'operazione e conferma la richiesta del sistema.
Impossibile smontare / bloccare il volume	Chiudi i documenti e le finestre aperti dall'unità, poi riprova.
Password non corretta	Controlla Bloc Maiusc e il layout di tastiera. Se non la ricordi, vedi il capitolo 8.
Chiave di ripristino non corretta	Ricontrolla le cifre con l'operatore: serve la chiave **più recente**.
Sul disco c'è un'unità Kripta sbloccata	Bloccala nella schermata iniziale, poi ripeti la suddivisione.
Il sistema non ha rilevato le nuove partizioni	Scollega e ricollega l'unità.
Il file di lingua non è un XML valido / elemento non ammesso	Correggi il file indicato nel messaggio: sono ammessi solo elementi `<string>` con testo semplice.

Messaggio o situazione	Cosa fare
La finestra di sblocco non compare all'inserimento	Verifica che Kripta sia in esecuzione (icona nella barra) e usa **Sblocca** dalla finestra principale.

12 Domande frequenti

Posso cifrare una chiavetta che contiene già dei file senza perderli?

No. La cifratura cancella l'unità. Copia i file altrove, cifra l'unità e poi ricopiali.

Posso cifrare il disco interno del mio computer?

No. Kripta è pensato per chiavette e dischi esterni; i dischi di sistema non vengono mostrati.

L'Help Desk può leggere i miei file?

L'Help Desk conserva solo la chiave di ripristino e può consultarla soltanto su tua richiesta, con registrazione di ogni accesso.

Devo annotare la chiave di ripristino?

No. Non la vedi mai e non devi conservarla: è archiviata presso l'Help Desk.

Kripta installa programmi sul mio computer?

Solo VeraCrypt (e FUSE-T su macOS), dopo la tua conferma e soltanto se la firma ufficiale degli sviluppatori è valida.

Posso usare la chiavetta su un computer di casa?

Sì, installando Kripta o VeraCrypt (capitolo 10). Rispetta comunque le regole aziendali sull'uso dei dati fuori sede.

La lingua che mi serve non c'è. Cosa posso fare?

Puoi tradurre il modello XML e caricarlo dalle Impostazioni (capitolo 9), oppure chiedere all'IT di distribuirne uno.

Perché non posso usare lettere accentate nella password?

Windows, macOS e Linux possono codificarle in modo diverso: la stessa password digitata su un altro sistema potrebbe non essere riconosciuta.

Quanto spazio perdo con la cifratura?

Pochissimo: alcune centinaia di kilobyte per le intestazioni del volume.

A Appendice per l'IT

Pacchetti

Sistema	Pacchetto	Note
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	Contiene gli MSI ufficiali di VeraCrypt (x64 e ARM64). L'app si avvia con privilegi di amministratore.
macOS 11+	`Kripta_1.2.0_universal.dmg`	Contiene VeraCrypt (versioni FUSE-T e macFUSE) e FUSE-T, che non richiede estensioni del kernel.
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	Contiene VeraCrypt per Ubuntu 22.04/24.04 e Debian 12/13; per le altre versioni Kripta scarica il pacchetto verificato.
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	Contiene VeraCrypt per Fedora 44; installare anche `exfatprogs`.
Altre distribuzioni	`Kripta_1.2.0_amd64.AppImage`	Eseguibile portabile.

Configurazione firmata

Sul server escrow, una volta sola, generare la chiave di firma; poi firmare la configurazione client (modello in `deploy/client/kripta.toml.example`):

```
kripta-escrow keygen-sign            # chiave privata (da custodire offline) + pubblica + impronta
kripta-escrow sign-config client.toml firma.key "ACME S.p.A." acme.kripta-config
```

Distribuire `acme.kripta-config` agli utenti e pubblicare l'**impronta** su un canale affidabile (intranet, telefono dell'Help Desk). Kripta salva la configurazione nella posizione di sistema (`%ProgramData%\Kripta`, `/Library/Application Support/Kripta`, `/etc/kripta`) tramite il processo privilegiato, insieme alla chiave del firmatario: gli aggiornamenti successivi devono avere la stessa firma. Per non dipendere dalla verifica dell'impronta da parte dell'utente, compilare Kripta con `KRIPTA_PROVISIONING_KEYS=<chiave pubblica>`: saranno accettate solo quelle chiavi. Una configurazione copiata a mano dall'IT (senza firma) non può essere sostituita da un pacchetto.

Installazione e aggiornamento di VeraCrypt

- Gli installer inclusi sono preparati con `scripts/fetch-veracrypt.py` al momento della build.
- Prima di installare, il processo privilegiato verifica la firma OpenPGP della lista SHA-256 ufficiale con la chiave IDRIX incorporata (impronta `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`) e l'hash del file.
- Opzioni in `kripta.toml`: `veracrypt_update_check = false` disattiva il controllo degli aggiornamenti; `veracrypt_release_api = "https://mirror.interno/…"` usa un mirror interno con lo stesso formato dell'API GitHub.

Lingue

I file XML delle lingue sono in `app/ui/lang/` (inclusi nell'app) e in `docs/manuale/lang/`. Le lingue caricate dagli utenti vengono salvate nella cartella dati dell'utente (`languages/`). Per distribuire una nuova lingua a tutti, aggiungere il file in `app/ui/lang/` e il codice nell'elenco di `app/ui/i18n.js`.

Componenti facoltativi

- **Avvio all'accesso** in barra dei menu / area di notifica (`kripta --background`): **automatico**. Kripta lo registra a ogni avvio (macOS: `~/Library/LaunchAgents/com.kripta.agent.plist`, riavviato se termina in modo anomalo; Windows: attività pianificata «Kripta» all'accesso con privilegi massimi, creata anche dall'installer e rimossa alla disinstallazione; Linux: `/etc/xdg/autostart/kripta.desktop` dai pacchetti .deb/.rpm, `~/.config/autostart/kripta.desktop` per AppImage). Si disattiva dalle Impostazioni.
- **Helper privilegiato** come servizio (nessuna richiesta di password): `deploy/macos/com.kripta.helper.plist`, `deploy/linux/kripta-helper.service`.