

Encryptio — Manuale utente

Web e estensione browser · aggiornato 2026-09-24

Guida pratica allo stato attuale del prodotto.

Sommario

- 1. Cos'è Encryptio
- 2. Registrazione e accesso
- 3. Password principale e blocco automatico
- 4. Vault: password e note
- 5. Recovery key
- 6. Autenticazione a due fattori (2FA)
- 7. Condivisione monouso (Premium)
- 8. Digital Legacy (Premium)
- 9. Piani e prezzi
- 10. Estensione del browser
- 11. Strumenti pubblici
- 12. Profilo e preferenze
- 13. Assistenza e buone pratiche
- 14. Backup sul server (policy di sicurezza)

1. Cos'è Encryptio

Encryptio è un gestore di password e note segrete a conoscenza zero: la cifratura avviene sul tuo dispositivo. Il server conserva solo il vault già chiuso e non può leggerlo.

Usi l'app web su qualsiasi browser moderno. Su Chrome, Firefox ed Edge puoi anche installare l'estensione (sblocco, Compila, Apri dal vault). Su Safari usa il sito: non c'è un'estensione nello store. Non esistono app native per telefono: sullo smartphone apri lo stesso sito nel browser.

Senza account puoi usare gli Strumenti pubblici (generatore di password e Cifra testo). Il vault richiede registrazione.

2. Registrazione e accesso

Registrazione: inserisci un'email che controlli e accetta Termini e Privacy. Ricevi un link monouso (valido 30 minuti). Poi scegli la password principale (almeno 12 caratteri) e conferma di nuovo Termini e Privacy: solo allora viene creato il vault. Non esiste un account senza vault.

Subito dopo la creazione Encryptio ti propone di creare una recovery key (puoi saltare e farlo dopo in Profilo → Sicurezza).

Accesso: email + password principale. Se hai la 2FA, inserisci anche il codice dell'app autenticatore o un codice di backup.

Sessione e vault sono due cose diverse. La sessione (cookie) può restare attiva per alcune ore anche se chiudi il browser: risulti ancora "entrato". La chiave del vault invece vive solo in memoria: dopo un blocco per inattività, un ricaricamento o la chiusura del browser va reinserita la password principale su Sblocca.

In Profilo (vault sbloccato) puoi cambiare l'email dell'account: reinserisci la password principale e conferma il nuovo indirizzo con un link monouso. Il vault non viene modificato; sugli altri dispositivi dovrai accedere di nuovo.

Eliminare l'account (Profilo) richiede sessione, conferma dell'email e la parola DELETE. Cancella in modo permanente la riga utente e il ciphertext sul server. Prima esporta un backup locale se ti serve una copia.

3. Password principale e blocco automatico

La password principale non lascia mai il dispositivo. Encryptio non può reimpostarla né aprire i dati senza di essa (o senza recovery key).

Dal browser derivano due materiali: la chiave del vault (resta in memoria solo mentre è sbloccato) e un segreto di autenticazione usato solo per dimostrare l'accesso al server.

Dopo un periodo di inattività (predefinito 15 minuti, modificabile in Profilo → Preferenze; 0 = mai) il vault si blocca da solo: la chiave esce dalla memoria e serve di nuovo la password principale. Restare connessi non basta.

In Profilo puoi anche scegliere dove andare dopo lo sblocco (elenco combinato, solo password o solo note).

4. Vault: password e note

Dopo lo sblocco trovi l'elenco combinato in Vault, le password in Vault → Password e le note in Vault → Note segrete (o dalle scorciatoie del menu).

Ogni password può avere titolo, utente, password, URL del sito e tag. Le note segrete sono testo lungo (licenze, codici, appunti riservati) con titolo e tag.

Puoi cercare, ordinare e paginare. Sulle password puoi filtrare quelle a rischio (deboli, riutilizzate, obsolete) e aprire la scheda dal badge.

Import ed export JSON o CSV avvengono solo sul tuo computer, a vault sbloccato. Non esiste un export lato server. Il file di export è in chiaro: conservalo in un posto sicuro ed eliminalo quando non serve più. Puoi anche importare export del vecchio Encryptio o file comuni, sempre nel browser.

Con l'estensione installata, un clic sull'URL di una password apre il sito e può compilare i campi di login. Senza estensione il link si apre comunque in una nuova scheda.

Piano Starter (gratuito): fino a 15 password e 15 note. Premium toglie quei limiti. Se torni a Starter oltre il limite, le 15 più vecchie per tipo restano modificabili; le più recenti in eccesso sono solo visualizzazione ed eliminazione finché non riduci l'elenco o torni a Premium. L'export locale include comunque tutto.

5. Recovery key

La recovery key è il piano B se dimentichi la password principale. Ti viene proposta dopo la registrazione e puoi crearla (o ricrearla) in Profilo → Sicurezza.

Viene mostrata una sola volta: copiala o stampala e conservala offline in un posto sicuro. Encryptio non te la reinvià e non offre un download JSON della chiave.

Per usarla: Password dimenticata → apri il link email (valido 24 ore) → inserisci la recovery key e scegli una nuova password principale. Senza recovery key, se perdi la password principale i dati restano chiusi per sempre — anche per noi.

Dopo un recupero o un cambio password principale, Digital Legacy va riconfigurato (nuove chiavi ai

contatti).

6. Autenticazione a due fattori (2FA)

Opzionale. Protegge solo l'accesso all'account (login), non sostituisce la password principale per sbloccare il vault.

Attivala in Profilo, scansiona il QR o inserisci il secret nell'app autenticatore, poi conserva i codici di backup monouso mostrati una sola volta.

7. Condivisione monouso (Premium)

Da Vault → Condividi in modo sicuro (o dalle Mie condivisioni) puoi creare un link monouso: il testo o una voce del vault viene cifrato sul dispositivo; la chiave resta nel frammento dell'URL (dopo #). Encryptio memorizza solo il ciphertext.

Chi apre il link lo può usare una volta sola (o fino a scadenza). Poi la condivisione non è più disponibile. Non serve un account Encryptio per aprire il link.

Disponibile con Premium o prova attiva. Non confonderla con Digital Legacy (emergenza a lungo termine) né con Cifra testo (strumento pubblico senza vault).

8. Digital Legacy (Premium)

In Profilo → Digital Legacy puoi nominare fino a cinque contatti di fiducia, in ordine di priorità, per un accesso di emergenza in sola lettura.

Quando aggiungi un contatto, il browser crea una chiave di accesso Legacy e un wrap della vault key. La chiave viene mostrata una sola volta: consegnala al contatto fuori banda (stampa o canale sicuro). Encryptio non la invia via email.

Il contatto richiede l'accesso dalla pagina pubblica `/legacy/request`. Parte un periodo di attesa (configurabile); puoi annullare in qualsiasi momento da Profilo.

Dopo il grant riceve un link: deve confermare (protezione da prefetch delle email) e inserire la chiave Legacy. Apre una vista in sola lettura e a tempo: niente modifiche, export o nuove condivisioni.

Con più contatti, se la finestra scade senza che il delegato apra l'accesso, il sistema passa al contatto successivo (escalation).

Opzionale: trigger di inattività. Dopo i giorni impostati ricevi un avviso in grazia; se non torni attivo, il contatto prioritario può ricevere il grant. Resta zero-knowledge: Encryptio non tiene mai la vault key in chiaro né in escrow.

Senza Premium (o prova attiva) non puoi configurare Digital Legacy; le richieste dei contatti non partono.

9. Piani e prezzi

Starter: gratuito (limiti 15 + 15). Premium: 3,99 €/mese oppure 2,79 €/mese con fatturazione annuale (totale annuo sulla pagina Prezzi). Prova Premium di 30 giorni una sola volta, senza carta.

Premium toglie i limiti di voci e sblocca la condivisione monouso e Digital Legacy.

L'abbonamento a pagamento passa da PayPal (checkout sul server, senza SDK PayPal nella

pagina). Dettagli e cosa succede se torni a Starter: pagina Prezzi e Profilo → Piano.

10. Estensione del browser

Chrome, Firefox ed Edge: installa Encryptio dalla pagina Estensione del sito (o dagli store collegati). Non usare l'estensione del vecchio prodotto Flask.

Dal popup: sblocca con la password principale (e 2FA al login se attiva), cerca anche per tag, ordina, Compila sulla scheda aperta oppure Apri per andare al sito e compilare.

Dal vault web, con l'estensione attiva, il clic sull'URL della password apre e compila. La chiave resta in memoria nel service worker e si blocca dopo circa 15 minuti di inattività (come sul web).

Safari e i browser mobili: usa l'app web; non c'è estensione store.

11. Strumenti pubblici

Dal menu Strumenti: Generatore — password casuali o frasi memorabili (IT/EN) con generatore crittografico nel browser. Nulla viene inviato al server. È anche incorporato quando aggiungi una password al vault.

Cifra testo (/tools/cipher) — sigilla o apre un testo con una password scelta da te, sempre nel browser. Non è collegato al vault né alla recovery key: se dimentichi quella password, il testo sigillato non si recupera.

12. Profilo e preferenze

In Profilo puoi impostare nome visualizzato e dati anagrafici opzionali (restano dentro il vault cifrato), dimensioni pagina, lingua, destinazione dopo lo sblocco e minuti di blocco automatico.

Consenso email di prodotto/servizio: è un'impostazione account sul server (opt-in, predefinita disattivata). Puoi attivarla in registrazione o in Profilo. Encryptio non allega mai il contenuto del vault alle email.

13. Assistenza e buone pratiche

Nel menu Supporto trovi questo manuale PDF, le FAQ e Contatti. Novità e Come funziona sono sotto Prodotto. Per idee sul prodotto usa Suggerimenti (dopo l'accesso): non incollare password o contenuti del vault.

Conserva offline la recovery key e, se usi Digital Legacy, le chiavi Legacy dei contatti. Non condividere la password principale. Dopo un export locale, tratta il file come materiale sensibile.

14. Backup sul server (policy di sicurezza)

Encryptio esegue backup automatici notturni del database del servizio: copia globale, con retention tipica di circa 30 giorni. Nei backup c'è solo dati del vault sigillati e metadati account — mai la password principale né la vault key in chiaro.

Da quel backup globale un operatore può, se serve, ripristinare anche un singolo account cancellato per errore (entro la retention). Non è uno storico versioni del vault che ripristini da solo in Profilo, e non sostituisce l'export JSON/CSV sul tuo computer.

Punto di ripristino: sia disaster recovery sia ripristino di un singolo account riportano i dati solo allo stato dell'ultimo backup notturno riuscito (di norma la notte precedente). Le modifiche successive

non rientrano in quel ripristino. Lo accetti esplicitamente in registrazione insieme a Termini e Privacy.

Se dimentichi la password principale senza recovery key, né i backup né Encryptio possono riaprire il vault. Dettagli in Informativa privacy e FAQ.