Manuale Utente Encryptio

Guida Completa al Password Manager Sicuro

Versione Manuale: 1.1
Data Manuale: Marzo 2026
Autore: Team Encryptio

Versione Encryptio: 0.2.6 (Secure Vault Pro)
Data Rilascio Encryptio: 8 Marzo 2026

Indice

Introduzione

Cos'è Encryptio?

Encryptio è un password manager web-based di livello enterprise che protegge le tue password e dati sensibili con crittografia AES-256 e architettura Zero-Knowledge. Questo significa che solo tu puoi accedere alle tue password - nemmeno noi possiamo vederle.

Caratteristiche Principali

- **Crittografia AES-256**: Standard militare utilizzato da banche e governi
- **Architettura Zero-Knowledge**: I dati vengono crittografati sul tuo dispositivo prima di essere inviati
- **Sicurezza Web Enterprise**: Grade A+ Mozilla Observatory, CSP3 'strict-dynamic', HSTS Preload
- **Multi-dispositivo**: Sincronizzazione sicura su desktop, tablet e smartphone
- **Interfaccia Moderna**: Tema scuro/chiaro, design responsive

Requisiti di Sistema

Encryptio funziona su qualsiasi dispositivo con un browser moderno:

Browser Supportati:
- Chrome 80+
- Firefox 75+
- Safari 13+
- Edge 80+
- Opera 67+
- Browser mobile moderni

Dispositivi:
- Windows 10+
- macOS 10.14+
- Linux (Ubuntu, Fedora, ecc.)
- iOS 12+ (iPhone/iPad)
- Android 8.0+

Iniziare con Encryptio

Registrazione Account

1. **Visita il sito**: Vai su www.encryptio.it
2. **Clicca su "Registrati"**: Troverai il pulsante nella homepage
3. **Compila il modulo iniziale**:
4. Email (verrà utilizzata per il login e il recupero password)
5. Clicca su "Crea Account"
6. **Verifica email**: Controlla la tua casella email e clicca sul link di conferma ricevuto
7. **Completa la registrazione**:
8. Imposta la tua **password principale** (scegli una password forte e memorabile)
9. Conferma la password
10. Accetta i Termini di Servizio e la Privacy Policy
11. Clicca su "Completa Registrazione"
12. ⚠ **SALVA LA RECOVERY KEY**:
13. Dopo aver completato la registrazione, verrai reindirizzato a una pagina speciale
14. **Viene generata automaticamente una Recovery Key** per il tuo account
15. La Recovery Key viene mostrata **UNA SOLA VOLTA** - non sarà più visibile dopo questa pagina
16. **COPIA E SALVA** la Recovery Key in un luogo sicuro (password manager, documento cifrato, ecc.)
17. La Recovery Key ti permetterà di recuperare i tuoi dati se dimentichi la password principale

⚠ **IMPORTANTE**:
- La password principale è necessaria per accedere alle tue password
- La Recovery Key è necessaria per recuperare i dati se dimentichi la password
- **Perdere sia la password che la Recovery Key = perdita permanente dei dati** (by design, architettura zero-knowledge)
- Conserva entrambe in luoghi sicuri e separati

Primo Accesso

1. **Effettua il login** con email e password principale
2. **Verifica di aver salvato la Recovery Key**:
3. Se non l'hai ancora salvata, puoi rigenerarla da "Profilo → Sicurezza → Rigenera Recovery Key"

4. ⚠ La rigenerazione invalida la vecchia Recovery Key
5. **Completa il setup** (se richiesto):
6. Configura l'autenticazione a due fattori (consigliato)
7. Esplora la dashboard
8. **Inizia ad aggiungere password**: Clicca su "Aggiungi Password" per la tua prima entry

Dashboard Principale

La dashboard è il centro di controllo del tuo account Encryptio. Da qui puoi:

- **Visualizzare statistiche**: Numero totale di password, ultime aggiunte
- **Azioni rapide**: Aggiungi password, genera password, importa/esporta
- **Accesso rapido**: Ultime password aggiunte, note segrete (Premium)
- **Navigazione**: Menu per accedere a tutte le funzionalità

Estensione Browser Encryptio (Chrome, Firefox, Edge)

Con la versione 0.2.6, l'estensione browser ufficiale è disponibile negli store per Chrome, Firefox e Microsoft Edge.

Cosa puoi fare con l'estensione

- Aprire il vault direttamente dal browser.
- Cercare rapidamente credenziali e inserirle nella pagina corrente.
- Avviare autofill in modo più rapido quando navighi su siti di login.

Installazione rapida

1. Vai su **Funzionalità** → **Estensione** nel sito Encryptio (oppure apri la pagina store del tuo browser).
2. Installa l'estensione ufficiale Encryptio.
3. Accedi a Encryptio nel browser.
4. Apri l'estensione dalla toolbar e verifica che il vault sia caricato.

Uso consigliato

- Mantieni una sessione attiva su encryptio.it nello stesso browser/profilo.
- Se compare un messaggio di autenticazione nell'estensione, effettua nuovamente login su encryptio.it e riapri il popup.
- Dopo aggiornamenti dell'estensione, ricarica la pagina web aperta per riallineare il contesto browser.

Gestione Password

Aggiungere una Nuova Password

1. **Dalla Dashboard**: Clicca su "Aggiungi Password" o usa il menu "Password"
2. **Compila il modulo**:
3. **Titolo/Nome**: Nome descrittivo (es. "Account Gmail")
4. **URL/Sito Web**: Indirizzo del sito (opzionale ma consigliato)
5. **Username/Email**: Il tuo username o email per il login
6. **Password**: Inserisci manualmente o usa il generatore
7. **Note**: Informazioni aggiuntive (opzionale)
8. **Genera Password Sicura** (consigliato):
9. Clicca sull'icona del generatore accanto al campo password
10. Personalizza lunghezza e caratteri
11. Clicca "Copia" per inserirla automaticamente
12. **Salva**: Clicca su "Salva Password

Visualizzare e Modificare Password

1. **Dalla lista password**: Clicca sulla password che vuoi visualizzare
2. **Visualizza password**:
3. Clicca sull'icona dell'occhio per mostrare/nascondere la password
4. Usa "Copia" per copiare la password negli appunti
5. La password viene copiata automaticamente e cancellata dopo 30 secondi
6. **Modificare**:
7. Clicca su "Modifica"
8. Apporta le modifiche necessarie
9. Salva le modifiche
10. **Eliminare**:
11. Clicca su "Elimina"
12. Conferma l'eliminazione

Ricerca Password

Ricerca Base (tutti gli utenti):
- Usa la barra di ricerca nella dashboard
- Cerca per titolo, URL, username o note

Ricerca Avanzata (Premium):
- Accedi a "Password → Ricerca Avanzata"
- Filtra per:
- Titolo
- URL
- Username
- Tag personalizzati
- Data di creazione/modifica
- Forza password

Importare Password

Disponibile per utenti Premium

1. **Prepara il file**: Esporta le password da un altro password manager in formato CSV o JSON
2. **Vai a "Password → Importa Password"**
3. **Seleziona il file**: Scegli il file CSV o JSON
4. **Verifica i dati**: Controlla l'anteprima delle password che verranno importate
5. **Conferma l'importazione**: Le password verranno crittografate e salvate

Formati Supportati:
- CSV (comma-separated values)
- JSON (JavaScript Object Notation)

Esportare Password

Tutti gli utenti possono esportare le proprie password (diritto GDPR)

1. **Vai a "Password → Esporta Password"**
2. **Scegli il formato**: CSV o JSON
3. **Inserisci la password principale**: Per sicurezza, devi confermare la tua identità
4. **Scarica il file**: Il file verrà scaricato sul tuo dispositivo

⚠ **ATTENZIONE**:
- I file esportati contengono password non crittografate**
- Conserva il file in un luogo sicuro

- Elimina il file dopo l'utilizzo
- Usa connessioni sicure per il download

Analisi Sicurezza Password (Premium)

L'analisi sicurezza ti aiuta a identificare password deboli o compromesse:

1. **Accedi a "Password → Analisi Sicurezza"**
2. **Visualizza il report**:
3. Password deboli (forza bassa)
4. Password duplicate
5. Password vecchie (non modificate da tempo)
6. Password compromesse (se trovate in data breach)
7. **Agisci**:
8. Modifica le password deboli
9. Elimina le password duplicate
10. Aggiorna le password vecchie

Cronologia modifiche (Password)

Disponibile per utenti Premium.

Encryptio registra quando ogni password viene creata o modificata. Per visualizzare la cronologia:

1. **Dalla Dashboard**: clicca su **Vedi** (icona occhio) sulla password che ti interessa, oppure clicca sulla card della password.
2. Nella pagina **Visualizza Password**, scorri in basso fino alla sezione **Cronologia modifiche**.
3. Vedrai un elenco con:
4. **Creata** – data e ora in cui la password è stata aggiunta
5. **Modificata** – data e ora di ogni successiva modifica (salvataggio, import, ecc.)

Le voci sono ordinate dalla più recente alla più antica. La cronologia viene aggiornata automaticamente a ogni creazione o modifica della password (anche in caso di import).

Note Segrete (Premium)

Le Note Segrete ti permettono di archiviare informazioni sensibili oltre alle password, come licenze software, codici di recupero, chiavi API, e altro ancora.

Creare una Nota Segreta

1. **Dalla Dashboard**: Clicca su "Aggiungi Nota Segreta"
2. **Compila il modulo**:
3. **Titolo**: Nome descrittivo della nota
4. **Contenuto**: Il testo della nota (fino a 50.000 caratteri)
5. **Tag**: Tag personalizzati per organizzare le note (opzionale, separati da virgola)
6. **Salva**: La nota viene crittografata con AES-256 prima di essere salvata

Gestire le Note Segrete

- **Visualizzare**: Clicca sulla nota dalla lista
- **Modificare**: Clicca su "Modifica" e apporta le modifiche
- **Eliminare**: Clicca su "Elimina" e conferma
- **Cercare**: Usa i tag o la barra di ricerca per trovare note specifiche

Data di creazione e modifica (Note Segrete)

Quando apri una nota segreta (clic su **Vedi**), nella pagina di dettaglio trovi:
- **Creata il**: data e ora di creazione della nota
- **Aggiornata il**: data e ora dell'ultima modifica (se la nota è stata modificata almeno una volta)

Queste informazioni ti permettono di sapere quando la nota è stata aggiunta e quando è stata aggiornata l'ultima volta.

Cronologia modifiche (Note Segrete)

Disponibile per utenti Premium.

Come per le password, anche per le note segrete viene registrata una cronologia dettagliata (creazione e ogni modifica).

1. Apri una nota segreta (clic su **Vedi**).
2. Nella pagina di dettaglio, scorri fino alla sezione **Cronologia modifiche**.
3. Vedrai un elenco con:
4. **Creata** – data e ora in cui la nota è stata aggiunta
5. **Modificata** – data e ora di ogni successivo aggiornamento

Sistema di Tag

I tag ti aiutano a organizzare le note:

- **Aggiungi tag**: Separati da virgola (es. "licenze, software, premium")
- **Cerca per tag**: Usa i tag nella ricerca per filtrare le note
- **Esempi di tag utili**:
- `licenze`
- `codici-recupero`
- `api-keys`
- `documenti`
- `personali`

Limiti Account Gratuito: Fino a 5 note segrete
Account Premium: Note illimitate

Condivisione sicura password

La **Condivisione sicura** ti permette di condividere una password (credenziale) con un altro utente Encryptio in modo crittografato. Solo il destinatario può decifrarla; il server non vede mai la password in chiaro.

Requisiti

- Il **destinatario deve avere un account Encryptio** (registrato con la stessa installazione).
- Entrambi gli utenti devono aver effettuato almeno un accesso alla sezione Condivisione sicura (per generare le chiavi di condivisione).

Condividere una password

1. **Apri Condivisione sicura**: Dal menu **Account** → **Condivisione sicura** oppure dalla dashboard **Password** → **Condividi Password**.
2. **Condividi una password**: Clicca su "Condividi una password".
3. **Seleziona la password** da condividere (dal menu a tendina) oppure usa il pulsante **Condividi** sulla singola password in dashboard per averla già preselezionata.
4. **Inserisci l'email** del destinatario (utente Encryptio).
5. **Opzioni**: Consenti di salvare la credenziale nel vault del destinatario (consigliato); opzionalmente imposta una scadenza (7, 30 o 90 giorni).

6. **Invia**: Il destinatario riceverà un'email di notifica e potrà vedere la credenziale in **Condivisione sicura** → **Condiviso con me**.

Visualizzare una credenziale condivisa

1. **Accedi** e vai su **Account** → **Condivisione sicura** (o apri il link ricevuto per email).
2. Nella sezione **Condiviso con me** trovi l'elenco delle credenziali condivise con te.
3. Clicca **Visualizza** per aprire la credenziale (titolo, username, password, URL, note).
4. **Salva nel mio vault**: Se il mittente lo ha consentito, puoi salvare la credenziale nel tuo vault. Dopo il salvataggio puoi scegliere di rimuovere la condivisione dalla lista.
5. **Elimina**: Puoi rimuovere una condivisione dalla tua lista quando non ti serve più (la credenziale resta nel tuo vault se l'hai salvata).

Condivisioni inviate

Nella sezione **Condivisioni inviate** vedi le password che hai condiviso. Puoi **Revocare** una condivisione in qualsiasi momento: il destinatario non potrà più accedere a quella credenziale.

Sicurezza

- Le credenziali sono crittografate con una chiave che solo il destinatario può decifrare (crittografia RSA + AES).
- Il server non ha accesso alle password in chiaro.
- Scadenza opzionale e revoca immediata dal mittente.

Condivisione File Sicura (Premium)

La condivisione file sicura ti permette di condividere file in modo sicuro con crittografia zero-knowledge. I file vengono crittografati nel tuo browser prima dell'upload.

Caricare un File

1. **Vai a "File Share → Carica File"**
2. **Seleziona il file**: Scegli il file dal tuo dispositivo (massimo 100 MB)
3. **Imposta password** (opzionale ma consigliato):
4. Crea una password forte per proteggere il file
5. Condividi questa password separatamente con il destinatario

6. **Carica**: Il file viene crittografato e caricato
7. **Ottieni il link**: Riceverai un link univoco per la condivisione

Condividere un File

1. **Dopo il caricamento**: Copia il link di condivisione
2. **Condividi il link**: Invia il link al destinatario (email, messaggio, ecc.)
3. **Condividi la password**: Se hai impostato una password, inviala separatamente
4. **Monitora i download**: Riceverai notifiche quando il file viene scaricato

Caratteristiche Sicurezza

- **Crittografia Zero-Knowledge**: I file sono crittografati nel browser prima dell'upload
- **Password Opzionale**: Proteggi ulteriormente i file con una password
- **Scadenza Automatica**: I file vengono eliminati automaticamente dopo 48 ore
- **Notifiche Download**: Ricevi notifiche quando qualcuno scarica il file
- **Link Unico**: Ogni file ha un link univoco e sicuro

Scaricare un File Condiviso

1. **Apri il link**: Clicca sul link di condivisione ricevuto
2. **Inserisci la password** (se richiesta)
3. **Scarica**: Il file viene decrittografato nel browser e scaricato

⚠ **IMPORTANTE**:
- I link scadono dopo 48 ore
- Una volta scaricato, il file rimane disponibile fino alla scadenza
- Non condividere link e password nello stesso messaggio

Sicurezza e Autenticazione

Recovery Key

La Recovery Key è una chiave di recupero generata automaticamente durante la registrazione che ti permette di recuperare i tuoi dati crittografati se dimentichi la password principale.

Cos'è la Recovery Key?

- **Chiave di recupero**: Una stringa alfanumerica univoca generata automaticamente
- **Generazione automatica**: Viene creata durante la registrazione e ogni volta che cambi la password
- **Mostrata una sola volta**: Dopo la generazione, viene mostrata una sola volta e poi non è più visibile
- **Crittografia zero-knowledge**: Permette di recuperare i dati senza che il server possa accedervi

Quando viene generata?

- **Durante la registrazione**: Automaticamente quando completi la registrazione
- **Cambio password**: Quando cambi la password principale
- **Rigenerazione manuale**: Puoi rigenerarla da "Profilo → Sicurezza → Rigenera Recovery Key"

Come salvare la Recovery Key

1. **Durante la registrazione**:
2. Dopo aver completato la registrazione, verrai reindirizzato a una pagina speciale
3. La Recovery Key viene mostrata in una scatola evidenziata
4. Clicca su "Copia Recovery Key" per copiarla negli appunti
5. Salvala immediatamente in un luogo sicuro
6. **Dove salvarla**:
7. Password manager separato
8. Documento cifrato su cloud sicuro
9. Backup fisico in cassaforte
10. ⚠ NON salvarla in chiaro sul computer o in email non cifrate

Come usare la Recovery Key

Se dimentichi la password principale:

1. **Vai a "Password dimenticata"**: Clicca sul link nella pagina di login
2. **Inserisci la tua email**: Riceverai un link per reimpostare la password
3. **Inserisci la Recovery Key**: Durante il reset password, inserisci la Recovery Key quando richiesto
4. **Imposta nuova password**: Scegli una nuova password sicura
5. **Recupero dati**: I tuoi dati crittografati verranno recuperati automaticamente

⚠ **IMPORTANTE**:
- Se reimposti la password SENZA Recovery Key, i tuoi dati crittografati NON saranno accessibili
- Dovrai usare la Recovery Key per recuperare i dati da "Profilo → Sicurezza → Recupera Dati"

Rigenerare la Recovery Key

Se hai perso o vuoi cambiare la Recovery Key:

1. **Vai a "Profilo → Sicurezza"**
2. **Clicca su "Rigenera Recovery Key"**
3. **Inserisci la password principale** (e codice 2FA se abilitato)
4. **Salva la nuova Recovery Key**:
5. ⚠ La vecchia Recovery Key non funzionerà più
6. La nuova chiave viene mostrata una sola volta
7. Salvala immediatamente

Recuperare Dati con Recovery Key

Se hai reimpostato la password senza Recovery Key:

1. **Vai a "Profilo → Sicurezza → Recupera Dati"**
2. **Inserisci la Recovery Key**: La chiave che avevi salvato durante la registrazione o l'ultimo cambio password
3. **Inserisci la password corrente**: La password che stai usando ora
4. **Recupera**: I tuoi dati verranno decrittografati e resi accessibili

Nota: Se hai rigenerato la Recovery Key dopo aver reimpostato la password, devi usare la **nuova Recovery Key**.

Autenticazione a Due Fattori (2FA)

L'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza al tuo account.

Configurare 2FA

1. **Vai a "Profilo → Sicurezza"**
2. **Clicca su "Abilita 2FA"**
3. **Scansiona il QR Code**:
4. Apri un'app authenticator (Google Authenticator, Authy, Microsoft Authenticator)
5. Scansiona il codice QR mostrato
6. **Inserisci il codice**: Inserisci il codice a 6 cifre generato dall'app

7. **Salva i Recovery Codes**:
8. ⚠ **IMPORTANTE**: Salva i codici di recupero in un luogo sicuro
9. Questi codici ti permetteranno di accedere se perdi l'accesso all'app authenticator
10. **Conferma**: Il 2FA è ora attivo

Usare 2FA

Ogni volta che accedi:
1. Inserisci email e password principale
2. Inserisci il codice a 6 cifre dall'app authenticator
3. Accedi al tuo account

Disabilitare 2FA

1. **Vai a "Profilo → Sicurezza"**
2. **Clicca su "Disabilita 2FA"**
3. **Inserisci la password principale** per confermare
4. **Conferma la disattivazione**

Recovery Codes

I Recovery Codes sono codici di backup che ti permettono di accedere al tuo account se perdi l'accesso all'app authenticator.

⚠ **IMPORTANTE**:
- Salva i Recovery Codes in un luogo sicuro (password manager, documento cifrato)
- Ogni codice può essere usato una sola volta
- Puoi rigenerare i codici dalla pagina Sicurezza

Generatore di Password

Il generatore di password crea password sicure e uniche usando algoritmi crittografici.

Usare il Generatore

1. **Dalla Dashboard**: Clicca su "Genera Password" o accedi a "Strumenti → Generatore Password"
2. **Personalizza le impostazioni**:
3. **Lunghezza**: Scegli la lunghezza (consigliato: 16+ caratteri)
4. **Includi maiuscole**: Lettere maiuscole (A-Z)
5. **Includi minuscole**: Lettere minuscole (a-z)

6. **Includi numeri**: Numeri (0-9)
7. **Includi simboli**: Caratteri speciali (!@#$%^&*)
8. **Genera**: Clicca su "Genera Password"
9. **Copia**: Clicca su "Copia" per copiare la password
10. **Usa**: Incolla la password dove necessario

Suggerimenti per Password Forti

- **Lunghezza minima**: 16 caratteri (consigliato: 20+)
- **Varietà**: Usa maiuscole, minuscole, numeri e simboli
- **Unicità**: Usa una password diversa per ogni account
- **Non riutilizzare**: Non riutilizzare password vecchie

Breach Checker

Il Breach Checker verifica se la tua email è stata coinvolta in violazioni di dati pubbliche.

1. **Vai a "Strumenti → Breach Checker"**
2. **Inserisci la tua email**
3. **Verifica**: Il sistema controlla se l'email è stata trovata in data breach noti
4. **Risultati**:
5. Se la tua email è stata compromessa, riceverai un avviso
6. Cambia immediatamente le password degli account interessati

Gestione Dispositivi

Encryptio ti permette di vedere e gestire i dispositivi che hanno accesso al tuo account.

1. **Vai a "Profilo → Dispositivi"**
2. **Visualizza i dispositivi**:
3. Nome dispositivo
4. Tipo (desktop, mobile, tablet)
5. Ultimo accesso
6. Indirizzo IP
7. Posizione approssimativa
8. **Gestisci**:
9. **Disconnetti dispositivo**: Rimuovi l'accesso da un dispositivo specifico
10. **Disconnetti tutti**: Disconnetti tutti i dispositivi tranne quello corrente

Cronologia Accessi

Monitora tutti gli accessi al tuo account:

1. **Vai a "Profilo → Cronologia Accessi"**
2. **Visualizza**:
3. Data e ora dell'accesso
4. Dispositivo utilizzato
5. Indirizzo IP
6. Posizione
7. Esito (successo/fallito)
8. **Rileva attività sospetta**: Se noti accessi da dispositivi o luoghi sconosciuti, cambia immediatamente la password

Audit Log

L'Audit Log registra tutte le attività importanti del tuo account:

- Creazione/modifica/eliminazione password
- Modifiche alle impostazioni di sicurezza
- Cambiamenti all'abbonamento
- Accessi da nuovi dispositivi

Disponibile per utenti Premium

Strumenti e Funzionalità Avanzate

Strumento di Crittografia

Encryptio include uno strumento per crittografare testo direttamente nel browser:

1. **Vai a "Strumenti → Crittografia"**
2. **Inserisci il testo**: Il testo che vuoi crittografare
3. **Imposta password**: Scegli una password per crittografare il testo
4. **Crittografa**: Clicca su "Crittografa"
5. **Copia il risultato**: Il testo crittografato può essere copiato e condiviso
6. **Decrittografa**: Usa lo stesso strumento con la password per decrittografare

⚠ **IMPORTANTE**:
- La password è necessaria per decrittografare
- Se perdi la password, il testo non può essere recuperato
- Questo strumento funziona completamente nel browser - nessun dato viene inviato al server

Backup e Ripristino

Creare un Backup

1. **Vai a "Profilo → Backup"**
2. **Clicca su "Crea Backup"**
3. **Inserisci la password principale** per confermare
4. **Scarica il file**: Il backup viene scaricato in formato JSON cifrato

Ripristinare da Backup

1. **Vai a "Profilo → Backup"**
2. **Clicca su "Ripristina da Backup"**
3. **Seleziona il file di backup**
4. **Inserisci la password principale**
5. **Conferma il ripristino**: ⚠ Questo sovrascriverà i dati attuali

⚠ **IMPORTANTE**:
- I backup contengono dati crittografati
- Conserva i backup in un luogo sicuro
- Crea backup regolari per proteggere i tuoi dati

Recupero Dati

Se hai perso l'accesso al tuo account ma hai un backup:

1. **Vai a "Profilo → Recupera Dati"**
2. **Segui le istruzioni** per ripristinare i dati dal backup
3. **Contatta il supporto** se hai bisogno di assistenza

Gestione Account

Profilo Utente

Gestisci le informazioni del tuo profilo:

1. **Vai a "Profilo → Impostazioni Profilo"**
2. **Modifica**:
3. Email (richiede verifica)
4. Nome (opzionale)
5. Preferenze notifiche
6. **Salva le modifiche**

Cambiare la Password Principale

⚠ **IMPORTANTE**: Cambiare la password principale richiede la crittografia di tutti i dati con la nuova chiave.

1. **Vai a "Profilo → Cambia Password"**
2. **Inserisci**:
3. Password attuale
4. Nuova password
5. Conferma nuova password
6. **Conferma**: Tutti i dati verranno ricrittografati con la nuova password
7. **Attendi il completamento**: Il processo può richiedere alcuni minuti

Eliminare l'Account

⚠ **ATTENZIONE**: L'eliminazione dell'account è permanente e irreversibile.

1. **Vai a "Profilo → Elimina Account"**
2. **Leggi l'avviso**: Comprendi le conseguenze
3. **Inserisci la password principale** per confermare
4. **Conferma l'eliminazione**: Tutti i dati verranno eliminati permanentemente

Prima di eliminare:
- Esporta tutte le password
- Scarica i backup
- Annulla gli abbonamenti attivi

Impostazioni Privacy

1. **Vai a "Profilo → Privacy"**
2. **Gestisci**:
3. Condivisione dati analitici (opzionale)
4. Preferenze cookie
5. Notifiche email

Tema Scuro/Chiaro

Encryptio supporta temi scuro e chiaro:

1. **Toggle tema**: Clicca sull'icona del tema nella barra di navigazione
2. **Preferenze sistema**: Il tema può seguire automaticamente le preferenze del sistema operativo
3. **Impostazioni**: Vai a "Profilo → Impostazioni" per configurare il tema preferito

---

Abbonamenti e Piani

Piani Disponibili

Piano Gratuito (Starter)

Costo: Gratuito per sempre

Incluso:
- Fino a 5 password salvate
- Crittografia AES-256
- Generatore password illimitato
- Sincronizzazione multi-dispositivo
- Autenticazione a due fattori (2FA)
- Supporto base via email

Piano Premium

Costo:
- Mensile: €3,99/mese
- Semestrale: €3,39/mese (risparmio 15%)
- Annuale: €2,79/mese (risparmio 30%)

Incluso (tutto di Starter +):
- Password illimitate
- Note segrete cifrate (illimitate)
- Condivisione file sicura
- Ricerca avanzata password
- Analisi sicurezza password
- Backup automatico
- Audit log
- Supporto prioritario
- Import password da altri manager

Passare a Premium

1. **Dalla Dashboard**: Clicca su "Passa a Premium" o vai a "Abbonamenti"
2. **Scegli il piano**: Mensile, semestrale o annuale
3. **Scegli il metodo di pagamento**: PayPal
4. **Completa il pagamento**: Segui le istruzioni di PayPal
5. **Attiva Premium**: Il tuo account verrà aggiornato immediatamente

Gestire l'Abbonamento

1. **Vai a "Abbonamenti → Gestisci"**
2. **Visualizza**:
3. Piano attuale
4. Data di scadenza
5. Storico pagamenti
6. **Modifica**:
7. Cambia piano (mensile/semestrale/annuale)
8. Annulla abbonamento
9. Aggiorna metodo di pagamento

Annullare l'Abbonamento

1. **Vai a "Abbonamenti → Gestisci"**
2. **Clicca su "Annulla Abbonamento"**
3. **Conferma**: L'abbonamento rimarrà attivo fino alla fine del periodo pagato
4. **Dopo la scadenza**: L'account tornerà al piano gratuito

⚠ **NOTA**:
- Le password esistenti rimarranno accessibili
- Le funzionalità Premium saranno disabilitate
- Le note segrete oltre il limite gratuito (5) non saranno accessibili fino al ripristino Premium

Storico Pagamenti

Visualizza tutti i pagamenti effettuati:

1. **Vai a "Abbonamenti → Storico Pagamenti"**
2. **Visualizza**:
3. Data pagamento
4. Importo
5. Metodo di pagamento
6. Stato (completato/pendente/fallito)
7. **Scarica ricevute**: Scarica le ricevute per i tuoi record

---

Domande Frequenti

Sicurezza

Q: Come funziona la crittografia in Encryptio?
A: Encryptio utilizza crittografia AES-256, lo stesso standard utilizzato da banche e governi. I dati vengono crittografati sul tuo dispositivo prima di essere inviati ai server (architettura Zero-Knowledge).

Q: Cosa succede se dimentico la password principale?
A: Puoi reimpostare la password usando il link "Password dimenticata" nella pagina di login. **IMPORTANTE**:
- Se hai la **Recovery Key**, inseriscila durante il reset password per recuperare tutti i tuoi dati crittografati
- Se NON hai la Recovery Key, potrai reimpostare la password ma i dati crittografati non saranno accessibili fino a quando non userai la Recovery Key per recuperarli da "Profilo → Sicurezza → Recupera Dati"
- Ti consigliamo di abilitare 2FA e salvare sia i Recovery Codes che la Recovery Key in luoghi sicuri

Q: I miei dati sono al sicuro?
A: Sì. I tuoi dati sono crittografati con AES-256 e utilizziamo architettura Zero-Knowledge.

Nemmeno noi possiamo vedere le tue password. I dati sono ospitati in Italia e il servizio è conforme al GDPR.

Q: Cosa succede se Encryptio viene violato?
A: Anche in caso di violazione dei server, i tuoi dati rimangono inaccessibili grazie alla crittografia end-to-end. Le password vengono crittografate sul tuo dispositivo prima dell'invio.

Q: Cos'è la Recovery Key e quando viene generata?
A: La Recovery Key è una chiave di recupero generata automaticamente durante la registrazione e ogni volta che cambi la password principale. Ti permette di recuperare i tuoi dati crittografati se dimentichi la password. Viene mostrata una sola volta dopo la generazione - è fondamentale salvarla immediatamente in un luogo sicuro (password manager, documento cifrato, backup fisico). Se perdi sia la password che la Recovery Key, i dati non possono essere recuperati (by design, architettura zero-knowledge).

Funzionalità

Q: Quante password posso salvare?
A:
- Account gratuito: Fino a 5 password
- Account Premium: Password illimitate

Q: Posso esportare le mie password?
A: Sì, tutti gli utenti possono esportare le proprie password in formato CSV o JSON (diritto GDPR). Vai a "Password → Esporta Password".

Q: Posso importare password da altri password manager?
A: Sì, gli utenti Premium possono importare password da altri manager in formato CSV o JSON. Vai a "Password → Importa Password".

Q: Su quali dispositivi posso usare Encryptio?
A: Encryptio funziona su qualsiasi dispositivo con un browser moderno: desktop (Windows, macOS, Linux), tablet e smartphone (iOS, Android).

Q: Le password si sincronizzano tra dispositivi?
A: Sì, le password si sincronizzano automaticamente tra tutti i tuoi dispositivi quando accedi al tuo account.

Account e Abbonamenti

Q: Encryptio è gratuito?
A: Sì, offriamo un piano gratuito che permette di salvare fino a 5 password. Per funzionalità avanzate, è disponibile un abbonamento Premium.

Q: Come posso passare a Premium?
A: Vai a "Abbonamenti" dalla dashboard e scegli il piano che preferisci. Il pagamento avviene tramite PayPal.

Q: Posso annullare l'abbonamento in qualsiasi momento?
A: Sì, puoi annullare l'abbonamento in qualsiasi momento. L'abbonamento rimarrà attivo fino alla fine del periodo pagato.

Q: Cosa succede se annullo Premium?
A: Le password esistenti rimarranno accessibili, ma le funzionalità Premium saranno disabilitate. L'account tornerà al piano gratuito dopo la scadenza.

Privacy e GDPR

Q: Encryptio è conforme al GDPR?
A: Sì, Encryptio è pienamente conforme al GDPR (Regolamento UE 2016/679). Hai il diritto di accesso, rettifica, cancellazione e portabilità dei dati.

Q: Dove sono memorizzati i miei dati?
A: I dati sono memorizzati in datacenter in Italia, conformi alle normative di sicurezza e privacy. Encryptio rispetta privacy by design e le normative applicabili; al momento non possiede certificazioni ufficiali.

Q: Quali dati vengono raccolti?
A: Raccogliamo solo i dati strettamente necessari per fornire il servizio: email, password principale (hash), e dati crittografati delle password salvate.

Supporto e Contatti

Supporto Email

Per assistenza, contatta il supporto:
- **Email**: supporto@encryptio.it
- **Tempo di risposta**:
- Account Premium: 24-48 ore
- Account gratuito: 3-5 giorni lavorativi

Centro Assistenza

Visita il centro assistenza per:
- Guide dettagliate

- Video tutorial
- Domande frequenti
- Aggiornamenti e novità

Segnalazione Problemi

Se riscontri un problema:
1. Vai a "Contatti" dal menu principale
2. Compila il modulo di contatto
3. Descrivi il problema in dettaglio
4. Includi screenshot se possibile
5. Invia la segnalazione

Suggerimenti e Feedback

Apprezziamo il tuo feedback! Condividi:
- Suggerimenti per miglioramenti
- Nuove funzionalità che vorresti vedere
- Esperienza d'uso generale

Social Media

Seguici per aggiornamenti e novità:
- Twitter: @encryptio
- Blog: blog.encryptio.it

Conclusione

Grazie per aver scelto Encryptio come tuo password manager! Questo manuale copre tutte le funzionalità principali della piattaforma.

Prossimi Passi

1. **Verifica di aver salvato la Recovery Key**: Assicurati di aver salvato la Recovery Key generata durante la registrazione in un luogo sicuro
2. **Aggiungi le tue prime password**: Inizia a salvare le password dei tuoi account più importanti
3. **Abilita 2FA**: Aggiungi un ulteriore livello di sicurezza

4. **Esplora le funzionalità**: Prova il generatore password, le note segrete (Premium), e altri strumenti
5. **Crea un backup**: Proteggi i tuoi dati creando un backup regolare
6. **Passa a Premium**: Se hai bisogno di più funzionalità, considera l'upgrade a Premium

Risorse Aggiuntive

- **FAQ**: www.encryptio.it/faq
- **Caratteristiche**: www.encryptio.it/features
- **Sicurezza**: www.encryptio.it/security
- **Privacy Policy**: www.encryptio.it/privacy
- **Termini di Servizio**: www.encryptio.it/terms

Aggiornamenti del Manuale

Questo manuale viene aggiornato regolarmente per riflettere le nuove funzionalità e miglioramenti. Controlla periodicamente per le versioni più recenti.

Encryptio - La Tua Sicurezza, La Tua Privacy

Informazioni Versione

Questo manuale fa riferimento a **Encryptio versione 0.2.4 (Secure Vault Pro)**, rilasciata il **20 Gennaio 2026**.

Per verificare la versione installata:
- Controlla il footer del sito web
- Vai a "Changelog" dal menu principale
- Controlla la pagina "Informazioni" nel tuo profilo

Nota: Alcune funzionalità descritte in questo manuale potrebbero variare leggermente tra versioni. Se riscontri differenze, consulta il changelog per gli aggiornamenti più recenti.

Ultimo aggiornamento manuale: Gennaio 2026
Versione Encryptio di riferimento: 0.2.4 (Secure Vault Pro) - Rilasciata il 20 Gennaio 2026