Encryptio User Manual

Complete Guide to the Secure Password Manager

Manual Version: 1.0
Manual Date: January 2026
Author: Encryptio Team

Encryptio Version: 0.2.4 (Secure Vault Pro)
Encryptio Release Date: January 20, 2026

Table of Contents

Introduction

What is Encryptio?

Encryptio is an enterprise-grade web-based password manager that protects your passwords and sensitive data with AES-256 encryption and Zero-Knowledge architecture. This means only you can access your passwords - not even we can see them.

Key Features

- **AES-256 Encryption**: Military-grade standard used by banks and governments
- **Zero-Knowledge Architecture**: Data is encrypted on your device before being sent
- **Enterprise Web Security**: Grade A+ Mozilla Observatory, CSP3 'strict-dynamic', HSTS Preload
- **Multi-Device**: Secure synchronization across desktop, tablet, and smartphone
- **Modern Interface**: Dark/light theme, responsive design

System Requirements

Encryptio works on any device with a modern browser:

Supported Browsers:
- Chrome 80+
- Firefox 75+
- Safari 13+
- Edge 80+
- Opera 67+
- Modern mobile browsers

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

Getting Started with Encryptio

Account Registration

1. **Visit the website**: Go to www.encryptio.it
2. **Click "Register"**: You'll find the button on the homepage
3. **Fill out the initial form**:
4. Email (will be used for login and password recovery)
5. Click "Create Account"
6. **Verify email**: Check your email inbox and click the confirmation link received
7. **Complete registration**:
8. Set your **master password** (choose a strong and memorable password)
9. Confirm the password
10. Accept the Terms of Service and Privacy Policy
11. Click "Complete Registration"
12. ⚠ **SAVE THE RECOVERY KEY**:
13. After completing registration, you'll be redirected to a special page
14. **A Recovery Key is automatically generated** for your account
15. The Recovery Key is shown **ONLY ONCE** - it won't be visible after this page
16. **COPY AND SAVE** the Recovery Key in a secure location (password manager, encrypted document, etc.)
17. The Recovery Key will allow you to recover your data if you forget your master password

⚠ **IMPORTANT**:
- The master password is required to access your passwords
- The Recovery Key is required to recover data if you forget your password
- **Losing both the password and the Recovery Key = permanent data loss** (by design, zero-knowledge architecture)
- Keep both in secure and separate locations

First Login

1. **Log in** with email and master password
2. **Verify you've saved the Recovery Key**:
3. If you haven't saved it yet, you can regenerate it from "Profile → Security → Regenerate Recovery Key"

4. ⚠ Regeneration invalidates the old Recovery Key
5. **Complete setup** (if required):
6. Configure two-factor authentication (recommended)
7. Explore the dashboard
8. **Start adding passwords**: Click "Add Password" for your first entry

Main Dashboard

The dashboard is the control center of your Encryptio account. From here you can:

- **View statistics**: Total number of passwords, recent additions
- **Quick actions**: Add password, generate password, import/export
- **Quick access**: Recently added passwords, secret notes (Premium)
- **Navigation**: Menu to access all features

Password Management

Adding a New Password

1. **From Dashboard**: Click "Add Password" or use the "Password" menu
2. **Fill out the form**:
3. **Title/Name**: Descriptive name (e.g., "Gmail Account")
4. **URL/Website**: Site address (optional but recommended)
5. **Username/Email**: Your username or email for login
6. **Password**: Enter manually or use the generator
7. **Notes**: Additional information (optional)
8. **Generate Secure Password** (recommended):
9. Click the generator icon next to the password field
10. Customize length and characters
11. Click "Copy" to insert it automatically
12. **Save**: Click "Save Password"

Viewing and Editing Passwords

1. **From password list**: Click on the password you want to view
2. **View password**:

3. Click the eye icon to show/hide the password
4. Use "Copy" to copy the password to clipboard
5. The password is automatically copied and cleared after 30 seconds
6. **Edit**:
7. Click "Edit"
8. Make necessary changes
9. Save changes
10. **Delete**:
11. Click "Delete"
12. Confirm deletion

Password Search

Basic Search (all users):
- Use the search bar in the dashboard
- Search by title, URL, username, or notes

Advanced Search (Premium):
- Go to "Password → Advanced Search"
- Filter by:
- Title
- URL
- Username
- Custom tags
- Creation/modification date
- Password strength

Importing Passwords

Available for Premium users

1. **Prepare the file**: Export passwords from another password manager in CSV or JSON format
2. **Go to "Password → Import Passwords"**
3. **Select the file**: Choose the CSV or JSON file
4. **Verify data**: Check the preview of passwords that will be imported
5. **Confirm import**: Passwords will be encrypted and saved

Supported Formats:
- CSV (comma-separated values)
- JSON (JavaScript Object Notation)

Exporting Passwords

All users can export their passwords (GDPR right)

1. **Go to "Password → Export Passwords"**
2. **Choose format**: CSV or JSON
3. **Enter master password**: For security, you must confirm your identity
4. **Download file**: The file will be downloaded to your device

⚠ **WARNING**:
- Exported files contain **unencrypted passwords**
- Keep the file in a secure location
- Delete the file after use
- Use secure connections for download

Password Security Analysis (Premium)

Security analysis helps you identify weak or compromised passwords:

1. **Go to "Password → Security Analysis"**
2. **View report**:
3. Weak passwords (low strength)
4. Duplicate passwords
5. Old passwords (not modified for a while)
6. Compromised passwords (if found in data breaches)
7. **Take action**:
8. Modify weak passwords
9. Delete duplicate passwords
10. Update old passwords

Password History

Encryptio maintains a history of password changes:

1. **View a password**
2. **Go to "History" section**
3. **See previous versions**: Date, time, and details of changes
4. **Restore** (if needed): Return to a previous version

Secret Notes (Premium)

Secret Notes allow you to store sensitive information beyond passwords, such as software licenses, recovery codes, API keys, and more.

Creating a Secret Note

1. **From Dashboard**: Click "Add Secret Note"
2. **Fill out the form**:
3. **Title**: Descriptive name for the note
4. **Content**: Note text (up to 50,000 characters)
5. **Tags**: Custom tags to organize notes (optional, comma-separated)
6. **Save**: The note is encrypted with AES-256 before being saved

Managing Secret Notes

- **View**: Click on the note from the list
- **Edit**: Click "Edit" and make changes
- **Delete**: Click "Delete" and confirm
- **Search**: Use tags or search bar to find specific notes

Tag System

Tags help you organize notes:

- **Add tags**: Separated by comma (e.g., "licenses, software, premium")
- **Search by tag**: Use tags in search to filter notes
- **Useful tag examples**:
- `licenses`
- `recovery-codes`
- `api-keys`
- `documents`
- `personal`

Free Account Limits: Up to 5 secret notes
Premium Account: Unlimited notes

Secure File Sharing (Premium)

Secure file sharing allows you to share files securely with zero-knowledge encryption. Files are encrypted in your browser before upload.

Uploading a File

1. **Go to "File Share → Upload File"**
2. **Select file**: Choose file from your device (maximum 100 MB)
3. **Set password** (optional but recommended):
4. Create a strong password to protect the file
5. Share this password separately with the recipient
6. **Upload**: The file is encrypted and uploaded
7. **Get the link**: You'll receive a unique link for sharing

Sharing a File

1. **After upload**: Copy the sharing link
2. **Share the link**: Send the link to the recipient (email, message, etc.)
3. **Share the password**: If you set a password, send it separately
4. **Monitor downloads**: You'll receive notifications when the file is downloaded

Security Features

- **Zero-Knowledge Encryption**: Files are encrypted in the browser before upload
- **Optional Password**: Further protect files with a password
- **Automatic Expiration**: Files are automatically deleted after 48 hours
- **Download Notifications**: Receive notifications when someone downloads the file
- **Unique Link**: Each file has a unique and secure link

Downloading a Shared File

1. **Open the link**: Click on the received sharing link
2. **Enter password** (if required)
3. **Download**: The file is decrypted in the browser and downloaded

⚠ **IMPORTANT**:
- Links expire after 48 hours

- Once downloaded, the file remains available until expiration
- Don't share link and password in the same message

Security and Authentication

Recovery Key

The Recovery Key is a recovery key automatically generated during registration that allows you to recover your encrypted data if you forget your master password.

What is the Recovery Key?

- **Recovery key**: A unique alphanumeric string automatically generated
- **Automatic generation**: Created during registration and every time you change your password
- **Shown only once**: After generation, it's shown only once and then no longer visible
- **Zero-knowledge encryption**: Allows data recovery without the server being able to access it

When is it generated?

- **During registration**: Automatically when you complete registration
- **Password change**: When you change your master password
- **Manual regeneration**: You can regenerate it from "Profile → Security → Regenerate Recovery Key"

How to save the Recovery Key

1. **During registration**:
2. After completing registration, you'll be redirected to a special page
3. The Recovery Key is shown in a highlighted box
4. Click "Copy Recovery Key" to copy it to clipboard
5. Save it immediately in a secure location
6. **Where to save it**:
7. Separate password manager
8. Encrypted document on secure cloud
9. Physical backup in safe

10. ⚠ DO NOT save it in plain text on computer or in unencrypted emails

How to use the Recovery Key

If you forget your master password:

1. **Go to "Forgot Password"**: Click the link on the login page
2. **Enter your email**: You'll receive a link to reset your password
3. **Enter the Recovery Key**: During password reset, enter the Recovery Key when requested
4. **Set new password**: Choose a new secure password
5. **Data recovery**: Your encrypted data will be automatically recovered

⚠ **IMPORTANT**:
- If you reset the password WITHOUT Recovery Key, your encrypted data will NOT be accessible
- You'll need to use the Recovery Key to recover data from "Profile → Security → Recover Data"

Regenerating the Recovery Key

If you've lost or want to change the Recovery Key:

1. **Go to "Profile → Security"**
2. **Click "Regenerate Recovery Key"**
3. **Enter master password** (and 2FA code if enabled)
4. **Save the new Recovery Key**:
5. ⚠ The old Recovery Key will no longer work
6. The new key is shown only once
7. Save it immediately

Recovering Data with Recovery Key

If you've reset your password without Recovery Key:

1. **Go to "Profile → Security → Recover Data"**
2. **Enter the Recovery Key**: The key you saved during registration or last password change
3. **Enter current password**: The password you're using now
4. **Recover**: Your data will be decrypted and made accessible

Note: If you've regenerated the Recovery Key after resetting your password, you must use the **new Recovery Key**.

Two-Factor Authentication (2FA)

Two-factor authentication adds an additional layer of security to your account.

Configuring 2FA

1. **Go to "Profile → Security"**
2. **Click "Enable 2FA"**
3. **Scan the QR Code**:
4. Open an authenticator app (Google Authenticator, Authy, Microsoft Authenticator)
5. Scan the displayed QR code
6. **Enter the code**: Enter the 6-digit code generated by the app
7. **Save Recovery Codes**:
8. ⚠ **IMPORTANT**: Save recovery codes in a secure location
9. These codes will allow you to access if you lose access to the authenticator app
10. **Confirm**: 2FA is now active

Using 2FA

Every time you log in:
1. Enter email and master password
2. Enter the 6-digit code from the authenticator app
3. Access your account

Disabling 2FA

1. **Go to "Profile → Security"**
2. **Click "Disable 2FA"**
3. **Enter master password** to confirm
4. **Confirm deactivation**

Recovery Codes

Recovery Codes are backup codes that allow you to access your account if you lose access to the authenticator app.

⚠ **IMPORTANT**:
- Save Recovery Codes in a secure location (password manager, encrypted document)
- Each code can be used only once
- You can regenerate codes from the Security page

Password Generator

The password generator creates secure and unique passwords using cryptographic algorithms.

Using the Generator

1. **From Dashboard**: Click "Generate Password" or go to "Tools → Password Generator"
2. **Customize settings**:
3. **Length**: Choose length (recommended: 16+ characters)
4. **Include uppercase**: Uppercase letters (A-Z)
5. **Include lowercase**: Lowercase letters (a-z)
6. **Include numbers**: Numbers (0-9)
7. **Include symbols**: Special characters (!@#$%^&*)
8. **Generate**: Click "Generate Password"
9. **Copy**: Click "Copy" to copy the password
10. **Use**: Paste the password where needed

Tips for Strong Passwords

- **Minimum length**: 16 characters (recommended: 20+)
- **Variety**: Use uppercase, lowercase, numbers, and symbols
- **Uniqueness**: Use a different password for each account
- **Don't reuse**: Don't reuse old passwords

Breach Checker

The Breach Checker verifies if your email has been involved in public data breaches.

1. **Go to "Tools → Breach Checker"**
2. **Enter your email**
3. **Verify**: The system checks if the email has been found in known data breaches
4. **Results**:
5. If your email has been compromised, you'll receive an alert
6. Immediately change passwords for affected accounts

Device Management

Encryptio allows you to view and manage devices that have access to your account.

1. **Go to "Profile → Devices"**
2. **View devices**:
3. Device name
4. Type (desktop, mobile, tablet)

5. Last access
6. IP address
7. Approximate location
8. **Manage**:
9. **Disconnect device**: Remove access from a specific device
10. **Disconnect all**: Disconnect all devices except the current one

Login History

Monitor all access to your account:

1. **Go to "Profile → Login History"**
2. **View**:
3. Date and time of access
4. Device used
5. IP address
6. Location
7. Outcome (success/failed)
8. **Detect suspicious activity**: If you notice access from unknown devices or locations, immediately change your password

Audit Log

The Audit Log records all important activities on your account:

- Password creation/modification/deletion
- Security settings changes
- Subscription changes
- Access from new devices

Available for Premium users

Advanced Tools and Features

Encryption Tool

Encryptio includes a tool to encrypt text directly in the browser:

1. **Go to "Tools → Encryption"**
2. **Enter text**: The text you want to encrypt
3. **Set password**: Choose a password to encrypt the text
4. **Encrypt**: Click "Encrypt"
5. **Copy result**: The encrypted text can be copied and shared
6. **Decrypt**: Use the same tool with the password to decrypt

⚠ **IMPORTANT**:
- The password is required to decrypt
- If you lose the password, the text cannot be recovered
- This tool works completely in the browser - no data is sent to the server

Backup and Restore

Creating a Backup

1. **Go to "Profile → Backup"**
2. **Click "Create Backup"**
3. **Enter master password** to confirm
4. **Download file**: The backup is downloaded in encrypted JSON format

Restoring from Backup

1. **Go to "Profile → Backup"**
2. **Click "Restore from Backup"**
3. **Select backup file**
4. **Enter master password**
5. **Confirm restore**: ⚠ This will overwrite current data

⚠ **IMPORTANT**:
- Backups contain encrypted data
- Keep backups in a secure location
- Create regular backups to protect your data

Data Recovery

If you've lost access to your account but have a backup:

1. **Go to "Profile → Recover Data"**
2. **Follow instructions** to restore data from backup
3. **Contact support** if you need assistance

Account Management

User Profile

Manage your profile information:

1. **Go to "Profile → Profile Settings"**
2. **Edit**:
3. Email (requires verification)
4. Name (optional)
5. Notification preferences
6. **Save changes**

Changing Master Password

⚠ **IMPORTANT**: Changing the master password requires encrypting all data with the new key.

1. **Go to "Profile → Change Password"**
2. **Enter**:
3. Current password
4. New password
5. Confirm new password
6. **Confirm**: All data will be re-encrypted with the new password
7. **Wait for completion**: The process may take a few minutes

Deleting Account

⚠ **WARNING**: Account deletion is permanent and irreversible.

1. **Go to "Profile → Delete Account"**
2. **Read the warning**: Understand the consequences

3. **Enter master password** to confirm
4. **Confirm deletion**: All data will be permanently deleted

Before deleting:
- Export all passwords
- Download backups
- Cancel active subscriptions

Privacy Settings

1. **Go to "Profile → Privacy"**
2. **Manage**:
3. Analytics data sharing (optional)
4. Cookie preferences
5. Email notifications

Dark/Light Theme

Encryptio supports dark and light themes:

1. **Theme toggle**: Click the theme icon in the navigation bar
2. **System preferences**: The theme can automatically follow operating system preferences
3. **Settings**: Go to "Profile → Settings" to configure preferred theme

---

Subscriptions and Plans

Available Plans

Free Plan (Starter)

Cost: Free forever

Included:
- Up to 5 saved passwords
- AES-256 encryption
- Unlimited password generator
- Multi-device synchronization
- Basic email support

Premium Plan

Cost:
- Monthly: €3.99/month
- Semi-annual: €3.39/month (15% savings)
- Annual: €2.79/month (30% savings)

Included (everything from Starter +):
- Unlimited passwords
- Encrypted secret notes (unlimited)
- Secure file sharing
- Two-factor authentication (2FA)
- Advanced password search
- Password security analysis
- Automatic backup
- Audit log
- Priority support
- Import passwords from other managers

Upgrading to Premium

1. **From Dashboard**: Click "Upgrade to Premium" or go to "Subscriptions"
2. **Choose plan**: Monthly, semi-annual, or annual
3. **Choose payment method**: PayPal
4. **Complete payment**: Follow PayPal instructions
5. **Activate Premium**: Your account will be updated immediately

Managing Subscription

1. **Go to "Subscriptions → Manage"**
2. **View**:
3. Current plan
4. Expiration date
5. Payment history
6. **Modify**:
7. Change plan (monthly/semi-annual/annual)
8. Cancel subscription
9. Update payment method

Canceling Subscription

1. **Go to "Subscriptions → Manage"**
2. **Click "Cancel Subscription"**
3. **Confirm**: Subscription will remain active until the end of the paid period
4. **After expiration**: Account will return to free plan

⚠ **NOTE**:
- Existing passwords will remain accessible
- Premium features will be disabled
- Secret notes beyond free limit (5) will not be accessible until Premium is restored

Payment History

View all payments made:

1. **Go to "Subscriptions → Payment History"**
2. **View**:
3. Payment date
4. Amount
5. Payment method
6. Status (completed/pending/failed)
7. **Download receipts**: Download receipts for your records

Frequently Asked Questions

Security

Q: How does encryption work in Encryptio?
A: Encryptio uses AES-256 encryption, the same standard used by banks and governments. Data is encrypted on your device before being sent to servers (Zero-Knowledge architecture).

Q: What happens if I forget my master password?
A: You can reset your password using the "Forgot Password" link on the login page. **IMPORTANT**:
- If you have the **Recovery Key**, enter it during password reset to recover all your encrypted data
- If you DON'T have the Recovery Key, you can reset the password but encrypted data won't be accessible until you use the Recovery Key to recover them from "Profile → Security → Recover Data"

- We recommend enabling 2FA and saving both Recovery Codes and Recovery Key in secure locations

Q: Are my data safe?
A: Yes. Your data is encrypted with AES-256 and we use Zero-Knowledge architecture. Not even we can see your passwords. Servers are certified and GDPR compliant.

Q: What happens if Encryptio is breached?
A: Even in case of server breach, your data remains inaccessible thanks to end-to-end encryption. Passwords are encrypted on your device before being sent.

Q: What is the Recovery Key and when is it generated?
A: The Recovery Key is a recovery key automatically generated during registration and every time you change your master password. It allows you to recover your encrypted data if you forget your password. It's shown only once after generation - it's essential to save it immediately in a secure location (password manager, encrypted document, physical backup). If you lose both the password and the Recovery Key, data cannot be recovered (by design, zero-knowledge architecture).

Features

Q: How many passwords can I save?
A:
- Free account: Up to 5 passwords
- Premium account: Unlimited passwords

Q: Can I export my passwords?
A: Yes, all users can export their passwords in CSV or JSON format (GDPR right). Go to "Password → Export Passwords".

Q: Can I import passwords from other password managers?
A: Yes, Premium users can import passwords from other managers in CSV or JSON format. Go to "Password → Import Passwords".

Q: On which devices can I use Encryptio?
A: Encryptio works on any device with a modern browser: desktop (Windows, macOS, Linux), tablet and smartphone (iOS, Android).

Q: Do passwords sync between devices?
A: Yes, passwords automatically sync across all your devices when you log into your account.

Account and Subscriptions

Q: Is Encryptio free?
A: Yes, we offer a free plan that allows saving up to 5 passwords. For advanced features, a Premium subscription is available.

Q: How can I upgrade to Premium?
A: Go to "Subscriptions" from the dashboard and choose the plan you prefer. Payment is made via PayPal.

Q: Can I cancel my subscription at any time?
A: Yes, you can cancel your subscription at any time. The subscription will remain active until the end of the paid period.

Q: What happens if I cancel Premium?
A: Existing passwords will remain accessible, but Premium features will be disabled. The account will return to the free plan after expiration.

Privacy and GDPR

Q: Is Encryptio GDPR compliant?
A: Yes, Encryptio is fully GDPR compliant (EU Regulation 2016/679). You have the right to access, rectify, delete, and portability of data.

Q: Where are my data stored?
A: Data is stored in certified data centers in Europe (Germany and Netherlands), compliant with security and privacy regulations.

Q: What data is collected?
A: We only collect data strictly necessary to provide the service: email, master password (hash), and encrypted data of saved passwords.

Support and Contacts

Email Support

For assistance, contact support:
- **Email**: supporto@encryptio.it
- **Response time**:
- Premium account: 24-48 hours
- Free account: 3-5 business days

Support Center

Visit the support center for:
- Detailed guides
- Video tutorials
- Frequently asked questions
- Updates and news

Reporting Issues

If you encounter a problem:
1. Go to "Contacts" from the main menu
2. Fill out the contact form
3. Describe the problem in detail
4. Include screenshots if possible
5. Send the report

Suggestions and Feedback

We appreciate your feedback! Share:
- Suggestions for improvements
- New features you'd like to see
- General user experience

Social Media

Follow us for updates and news:
- Twitter: @encryptio
- Blog: blog.encryptio.it

Conclusion

Thank you for choosing Encryptio as your password manager! This manual covers all the main features of the platform.

Next Steps

1. **Verify you've saved the Recovery Key**: Make sure you've saved the Recovery Key generated during registration in a secure location
2. **Add your first passwords**: Start saving passwords for your most important accounts

3. **Enable 2FA**: Add an additional layer of security
4. **Explore features**: Try the password generator, secret notes (Premium), and other tools
5. **Create a backup**: Protect your data by creating regular backups
6. **Upgrade to Premium**: If you need more features, consider upgrading to Premium

Additional Resources

- **FAQ**: www.encryptio.it/faq
- **Features**: www.encryptio.it/features
- **Security**: www.encryptio.it/security
- **Privacy Policy**: www.encryptio.it/privacy
- **Terms of Service**: www.encryptio.it/terms

Manual Updates

This manual is regularly updated to reflect new features and improvements. Check periodically for the latest versions.

Encryptio - Your Security, Your Privacy

Version Information

This manual refers to **Encryptio version 0.2.4 (Secure Vault Pro)**, released on **January 20, 2026**.

To verify the installed version:
- Check the website footer
- Go to "Changelog" from the main menu
- Check the "Information" page in your profile

Note: Some features described in this manual may vary slightly between versions. If you notice differences, consult the changelog for the latest updates.

Last manual update: January 2026
Encryptio version reference: 0.2.4 (Secure Vault Pro) - Released on January 20, 2026