



# Security specifications



# Table of contents

## 1. Overview

## 2. Zero-knowledge cryptosystem

- a. The master password
- b. Secure user authentication
- c. Host-proof hosting
- d. Two-factor authentication
  - i. Options available
  - ii. Mark as trusted device
- e. Secure sharing of passwords
  - i. How sharing works

## 3. Zero-knowledge master password reset

## 4. Software architecture

- a. Principle of minimal privilege
- b. Cryptographic primitives used
- c. Third-party modules

## 5. Network security

- a. Secure data transfer
- b. Intrusion detection
- c. Secure operating system
- d. Virus scanning

## 6. Physical security

## 7. Redundancy and availability

## 8. Security certifications

## 9. Penetration testing by third-party experts

## 10. Reporting a security issue

## 11. Conclusion

## Overview

Zoho Vault is part of Zoho's suite of products trusted by over 50 million customers around the world. Vault is a password management application that helps people manage their passwords and other sensitive data securely. This data does not just include your personal details, but also critical customer data which must be kept secure and safeguarded at all costs. Vault is the trusted security partner for thousands of individuals, teams, and enterprises across the globe, and data security is the top priority for our research and development teams.

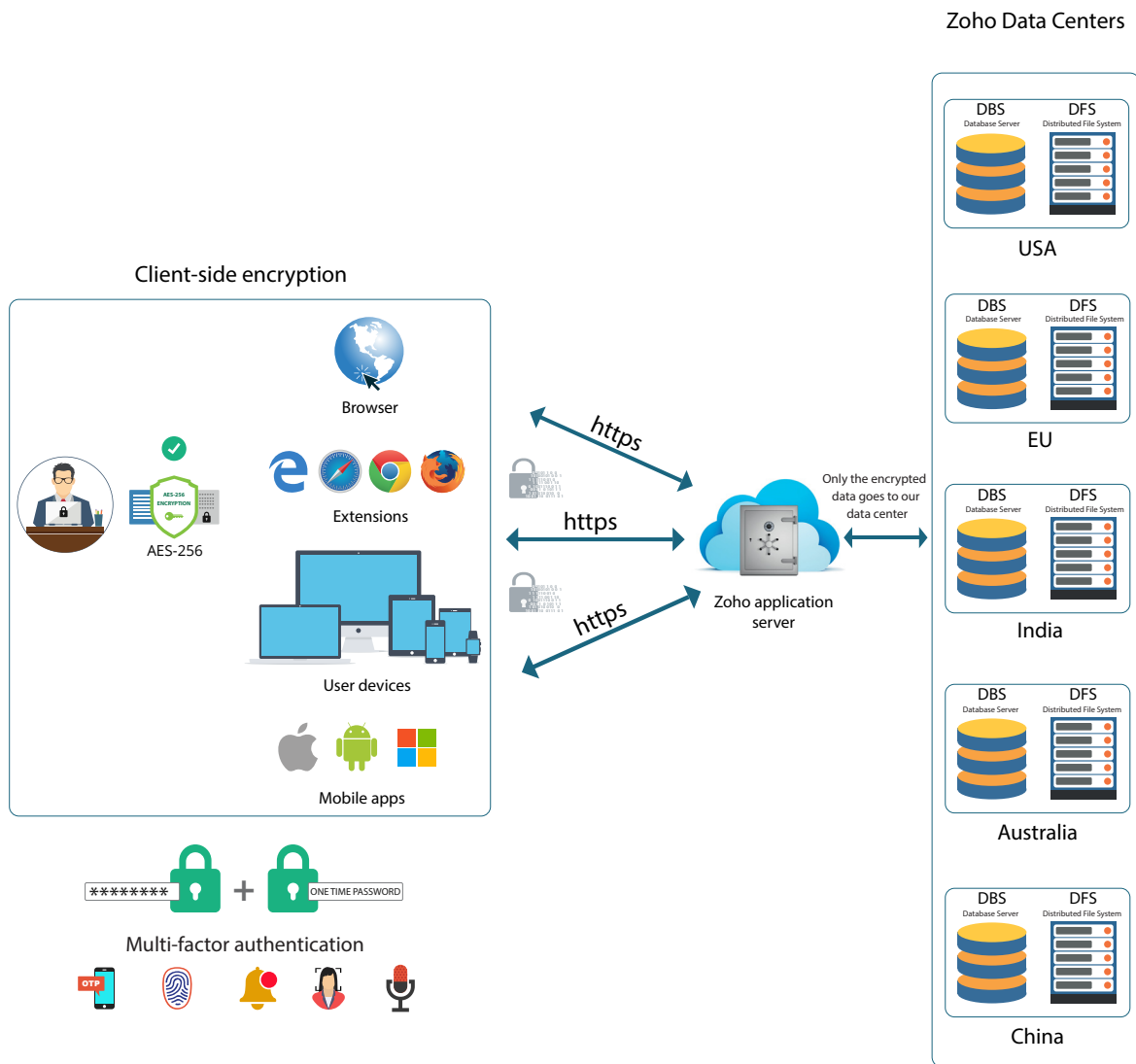
The technical architecture of the product is designed with potential threats and the current attack landscape in mind. We are equipped to handle modern cyber attacks at all levels in our servers, systems, and processes to ensure that our customers' data is always secure.

This document contains a comprehensive list of security measures taken by our teams to ensure confidentiality, integrity, and availability of our service.

## Zero-knowledge cryptosystem

Zoho Vault uses zero-knowledge security architecture to guarantee the highest levels of information security and privacy according to the following principles:

- All passwords and sensitive data are encrypted with AES 256-bit encryption algorithm on the client side (for both browser and mobile apps).
- The master password acts as the master key for all data encryption and is not stored anywhere in our servers.
- We encrypt all sensitive data and store it in our servers.
- Data is always transmitted through an HTTPS connection.
- Even Zoho employees cannot access users' data in plain text.
- The master password is protected with PBKDF2 (a password strengthening algorithm) to prevent hackers from using automated tools to discover the master key.



## The master password

Every user is required to create a master password during account creation. This master password also acts as the user’s encryption key.

- The master password must be a minimum of eight characters long.
- Users get real-time feedback on the strength of their master password.
- Zoho does not store the master password on any of its servers.
- The master password is only known to the user and will remain secret forever.

Zoho Vault uses this master password to generate the Key Encryption Key (KEK) with a random salt value, using large iterations of a Key Derivation Function (KDF), PBKDF2 with HMAC-SHA256.

## Host-proof hosting

Zoho Vault uses the host-proof hosting technique for handling sensitive user data. Host-proof hosting is simply encrypting and decrypting all data in the browser (client side) as explained below:

- All data is encrypted with the AES-256 encryption algorithm on the client side (browser) and only the encrypted data is transmitted over HTTPS and stored in Zoho's servers.
- The master password created during the registration process acts as the master encryption key to encrypt and decrypt data. This master password is not stored anywhere on Zoho's servers.
- When the user wants to access their stored data, the application fetches the encrypted data over HTTPS from our servers.
- When the user adds, deletes, or modifies the encrypted data, Zoho Vault will encrypt the data on the client side using the same process detailed above and transmit the newly encrypted data to Zoho's servers.

Zoho's servers only hold the encrypted data, which can only be decrypted with the user's master password and the unique salt value for that user. Even if an attacker were to gain access to our servers, they would not be able to access any data in plain text.

## How authentication works?

Every user's authentication process involves the following steps:

- The user's application access request from the web, browser extension, and mobile apps will always be redirected to the Zoho Accounts login page.
- The login credentials are then passed to Zoho's server for authentication.
- When the user is successfully authenticated, cookie information is set for the user's browser session and the user's access is redirected to Vault.
- The Zoho Accounts agent on the application server validates the cookie information with Zoho Accounts Server in the backend.

## Multi-factor authentication (MFA)

Multi-factor authentication adds an additional layer of security to user accounts. When configured, users will need to set a second level of authentication from the following list of options:

- Google Authenticator
- SMS or voice call
- Touch ID
- Push notification
- Scan QR code
- Time-based OTP

Users can also download [Zoho OneAuth](#), Zoho's multi-factor authentication app to add safety to their account.

## Mark as trusted device

Users can mark their frequently used devices as trusted by checking Trust this browser during the MFA process. The cryptographic authentication material created will be used to identify the device. Users will not be required to use TFA to verify their account again on the verified browser for the next 180 days.

## Secure sharing of passwords

Zoho Vault helps you securely share passwords with the members of your company while maintaining the highest level of security and privacy standards. Every new user except the first super admin is required to complete a one-time handshake process to start sharing passwords and view the passwords that have been shared with them.

## How sharing works?

- An RSA public-private key is generated for each user during the sign-up process.
- A new org key (AES 256-bit) is also created for the organization during setup.
- The super administrator's private key is encrypted using the master password and is stored in our database.
- The org key is also encrypted using the super administrator's public key and stored in our database.
- During the handshake period, the encrypted org key stored in the database is decrypted using the super administrator's private key. The org key is then encrypted using the user's RSA public key and the newly encrypted org key is shared and stored in the user's database.
- When the user tries to share a password, the user's private key, which is stored in encrypted form in the database, is retrieved and decrypted using the user's master password. The newly encrypted org key shared by the super administrator is then retrieved. The encrypted org key is decrypted using the user's private key. The password to be shared is now encrypted using the org key.

## Zero-knowledge master password reset

As a zero-knowledge service provider, Zoho Vault provides a completely secure mechanism for resetting the master password. To reset a forgotten master password, click the **Forgot Master Password** option on the Authentication screen. There is no way to recover a forgotten master password, since it is not stored anywhere. When users reset a forgotten master password, all personal passwords will be lost and an encrypted file containing the data from their account will be sent to their registered email address. If the user remembers their forgotten master password in the future, they can access and decrypt the encrypted data from the file. The enterprise passwords, however, can be recovered in a multi-user environment where at least one user has access to the org key. In these cases, after the master password is reset, users can access all their enterprise passwords when an admin or super admin approves their password sharing request (handshake).



## Field encryption

Zoho Vault rigorously encrypts all sensitive fields. Some fields, however, are left unencrypted to help users search for passwords, manage audit log, and automatically log in to websites. The unencrypted fields are:

- Password Name
- URL
- Description
- Tags

All custom fields and the fields in all custom categories are encrypted by default. The label names of the associated fields, however, are unencrypted.

## Software architecture

### Principle of minimal privilege

Our software components are designed and developed in line with the principle of minimal privilege for better security. This means that each module is independent and can only access the data it requires. This eliminates communication with unwanted or insecure external hostile codes.

### Cryptographic primitives used

Zoho Vault uses only the strongest cryptographic primitives, regarded as the gold standard within the industry:

- AES 256-bit encryption
- PBKDF2 with HMAC-SHA256
- ECDHE\_RSA

## Third-party modules

Zoho Vault uses the best third-party software modules and code libraries available in the industry. These modules are subjected to a program of rigorous internal testing and reviewing before they are deployed.

## Role of security in SDLC

Zoho Vault is designed and developed within a security-focused software development life cycle framework by our engineering and security experts:

- Members of our development team take regular, industry-standard security training to keep up with the recent advancements and threats.
- Security processes are rigorously applied at each stage of design, development, and validation.
- No module is excluded from our internal validation procedures.
- Modules are only rolled out to production if they meet our internal security standards and pass the validation tests set by our panel of experts.

## Network security

Our network and infrastructure are designed to combat the most sophisticated cyber attacks.

## Secure data transfer

All communication between the application and our servers is fully encrypted and tunneled through an HTTPS connection. Transferring data through a secure channel like HTTPS enhances security and safeguards the user data from eavesdroppers, man-in-the-middle attacks, and other common hacking techniques.

## Advantages of SSL connection

- Verifies that you are sending and receiving data from our servers every time.
- Only encrypted data is transmitted between the client and the server.
- Ensures that only our servers can receive your requests and only you receive the response.
- Even if an attacker intercepts your data during the exchange with our servers, they cannot read or decrypt data without your master password.

## Intrusion detection

Our network is screened and gated with powerful and certified intrusion detection and intrusion prevention systems to protect user data from the latest electronic attacks.

## Secure operating system

The application runs inside a secured, sliced-down operating system for maximum protection against vulnerabilities.

## Virus scanning

Traffic flowing into our servers is scanned for viruses using state-of-the-art virus scanning protocols which are updated regularly.

## Physical security

Our data centers are located in various locations around the world and use highly sophisticated security features to protect all customer data:

- All our data centers are protected by on-site security personnel 24 hours a day.
- Access to data centers is restricted to authorized staff only.
- Two-levels of authentication, including biometric authentication, are required to enter the data centers.
- 24-hour surveillance including a night vision camera monitor record all activity at every data center.

- Our servers are located in unmarked, undisclosed locations to avoid the attention of potential attackers.
- The servers are protected with bulletproof walls and fire prevention systems.
- All access to the centers is logged and passwords are strictly regulated.
- Audits are carried out at regular intervals and all security processes are reviewed by management.

## Redundancy and availability

Our distributed infrastructure ensures users can always access their data from anywhere in the world. If the primary data center becomes inaccessible, users will be connected to the secondary data center. The application offers read-only access from the secondary data center during the mission-critical period. There will be no data loss during the process as data sync will be completed when the primary data center is back online. Users can also configure periodic data backup for disaster recovery purposes. Passwords and other confidential data will be sent to their registered email address or to their cloud account at regular intervals as an encrypted file. This encrypted file is as secure as the online version. Users can only access their passwords from the backup by entering their master password.

## Security Certifications

We have received the following security and privacy certifications from highly reputed regulatory bodies:

- SOC 2 Type II compliant: an annual evaluation is performed by AICPA, which covers all essential security and privacy controls, including availability, processing integrity, and confidentiality.
- Compliant with US-EU and US-Swiss Safe Harbor Frameworks and certified by TRUSTe.
- ISO/IEC 27001:2013 certified for our applications, systems, people, technology, and processes.

## Penetration testing by third-party experts

Zoho Vault has not currently undergone third-party expert testing. We are planning to be reviewed by some of the industry's best third-party experts in the near future.

## Reporting a security issue

Zoho always respects security researchers who responsibly report legitimate vulnerabilities and help us improve the security of our service. We encourage responsible reporting of any security vulnerabilities you come across in Vault, which you can do by filing all your bugs and issues via our [bug bounty program](#). If your reported bug is eligible for an award, it will be sent to you.

## Conclusion

Our research and development teams constantly work to keep your digital lives simple and secure. This document provides a detailed overview of how we keep your data safe. If you still have unanswered questions, please don't hesitate to contact us.

You can reach out to us over:

**Email:** [support@zohovault.com](mailto:support@zohovault.com)

**Phone:**

**Australia:** +61 291654046 - 6400

**USA:** +1 312 340 2567 - 6400

**UK:** +44 20 3901 2997 - 6400

**India:** +91 044 67447048 - 6400

[www.zoho.com/vault](http://www.zoho.com/vault)



Zoho Corporation Private Limited

4141 Hacienda Drive, Pleasanton, CA 94588, USA

US +1 888 204 3539 UK : +44 (20) 35647890 Australia : +61 2 80662898