ZOHO

Zoho Vault

Security specifications

Table of contents

Overview

Zoho Vault is part of Zoho's suite of products, which are trusted by more than 80 million customers around the world. Vault is a password management application that helps people manage their passwords and other sensitive data securely. This data doesn't just include personal details, but also critical customer data that 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.

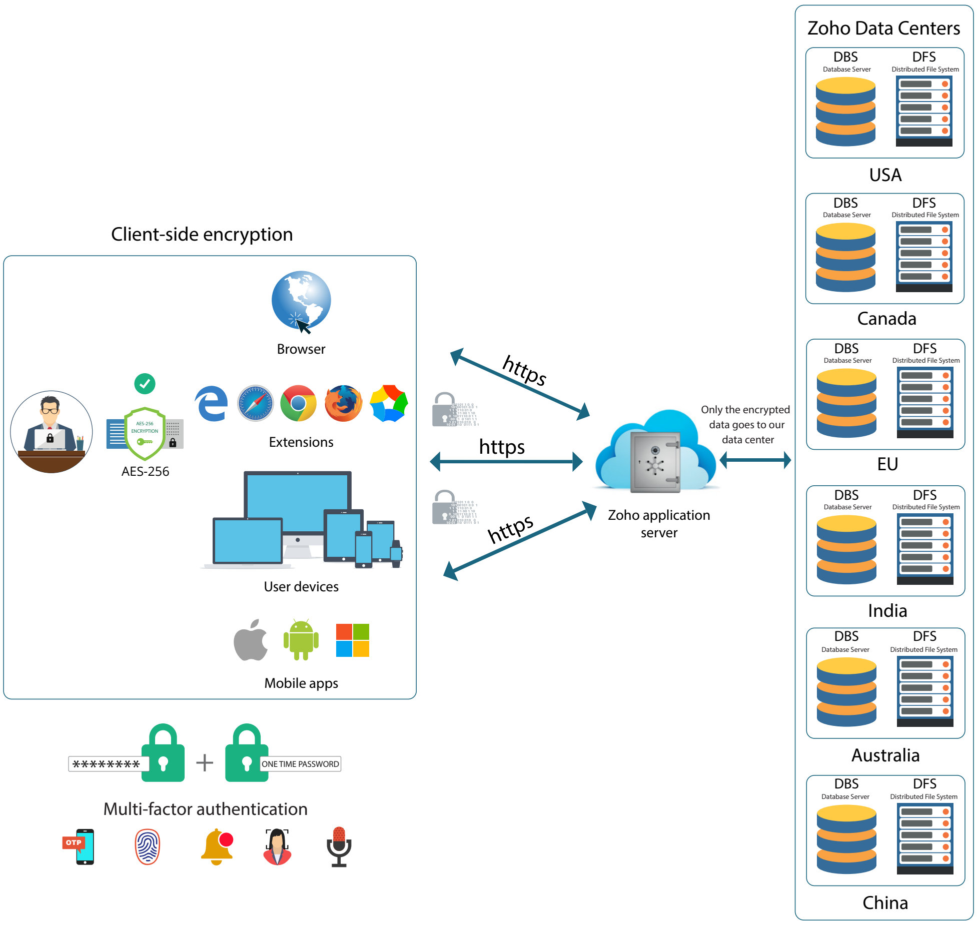
The technical architecture of the product is designed with potential threats and the current threat landscape in mind. We're equipped to handle both physical and cyberattacks at all levels in our servers, systems, and processes, ensuring that our customers' data is always secure.

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

A zero-knowledge cryptosystem

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

- All passwords and sensitive data are encrypted with an 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 decryption on the client side.
- The master key is derived with the PBKDF2 algorithm (a cryptographic key derivation function). We do not store any form of Master Password at our end/transmit it to our servers to prevent hackers from using automated tools to discover the master key.
- We encrypt all sensitive data on the client side itself and store them on our servers.
- Data is always transmitted through an HTTPS connection between the client device and Zoho Vault servers.



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.
- 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 encryption and decryption of all the data in the browser (on the 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 on 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 isn't 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 wouldn't 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 back end.

Multifactor authentication (MFA)

Multifactor 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:

- Zoho OneAuth
- SMS-based OTP
- Time-based OTP
- YubiKey
- Passkey

Users can download Zoho OneAuth, Zoho's multifactor authentication app, to add safety to their account. OneAuth provides options to use touch ID, passwordless sign-in, push notifications, and the ability to log in by scanning QR codes.

Backup verification codes aid in recovering an account without the need to reset the password.

Mark as a trusted browser

Users can mark their frequently used browsers as trusted by checking Trust this browser during the MFA process. Users won't be required to use MFA to verify their account again on the trusted browser for 180 days.

Secure password sharing

Zoho Vault helps you securely share passwords with 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 or 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 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 process, 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's no way to recover a forgotten master password because it's 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 of 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 logs, 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 least privilege

Our software components are designed and developed in line with the principle of least 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're deployed.

The role of security in the software development life cycle

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

- Members of our development team complete 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 HTTPS connection

- Verifies that you're 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 of our data centers are protected by on-site security personnel 24 hours a day.
- Access to our data centers is restricted to authorized staff only.
- Two levels of authentication, including biometric authentication, are required to enter the data centers.
- Our data centers are protected by 24-hour surveillance—including night vision camera monitors—and all activity at every data center is recorded.
- Our servers are located in unmarked, undisclosed locations to avoid attracting the attention of potential attackers.

- Our servers are protected with bulletproof walls and fire prevention systems.
- All access to the data 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 that 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 the 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've received the following security and privacy certifications from highly reputable regulatory bodies:

- SOC 2 Type II compliant—an annual evaluation is performed by the 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 27001:2022 certified for applications, systems, people, technology, and processes.
- ISO/IEC 27001:2022 certified for privacy management within the context of the organization.
- ISO/IEC 27017:2015 certified for Information technology—Security techniques— Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- SOC 2 + HIPAA—an independent third-party audit firm has examined the description of the systems for the services provided to customers from Zoho's offshore development center, based on the security, privacy, and breach requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification.

Penetration testing by third-party experts

Zoho Vault had external penetration tests performed in July 2023, and there are plans to do this periodically.

Note: Zoho has also invested in building in-house security tools. This includes our code analysis (i.e., static and interactive application security testing [SAST and IAST]) and application layer web application firewall (WAF). Our SAST/IAST tool, on the other hand, is benchmarked against Open Worldwide Application Security Project standards and has a 100% true positive score. Additionally, numerous application side frameworks, such as database frameworks, security frameworks, and other utility frameworks, are built in-house. There's a central security penetration testing team that performs testing against critical modules of all our products periodically, and we perform third-party penetration testing based on some internal metrics, which include the outcome of internal penetration test operations, code review coverage, the complexity of the application, and more.

Reporting a security issue

Zoho always respects security researchers who responsibly report legitimate vulnerabilities and help us improve the security of our services. We encourage responsible reporting of any security vulnerabilities you come across in Vault, which you can do by filing all of 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 using this online form or by calling:

- **USA: +1 973 988 3032**
- **INDIA: +91 44 6965 6118**
- **UK: +44 207 660 5003**
- **AUSTRALIA: +61 272 557 977**

Zoho Vault

www.zoho.com/vault

ZOHO

Zoho Corporation Private Limited
4141 Hacienda Drive, Pleasanton, CA 94588, USA
US +1 888 204 3539 UK : +44 (20) 35647890   Australia : +61 2 80662898