ZOHO

Zoho Vault

BEST PRACTICES GUIDE

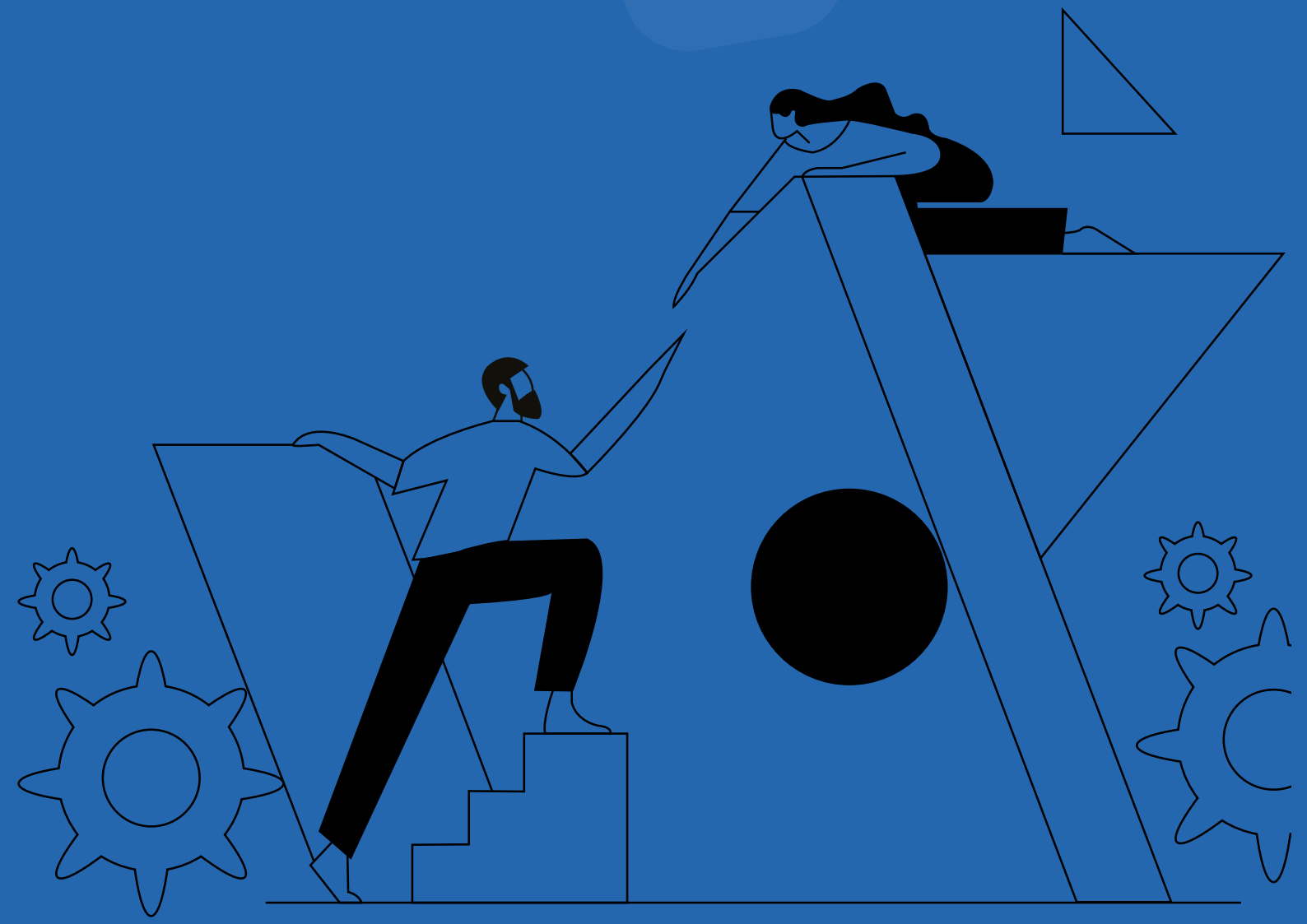

TABLE OF CONTENTS

1.0 Overview

1.1 Introduction

This guide details the best practices to be followed by super admins, admins, and end users while setting up their Zoho Vault account. Throughout this guide, end users will find tips to help them use Zoho Vault efficiently, while admins will learn the different security aspects involved in managing users and structuring Vault to satisfy their business needs.

1.2 System requirements:

Zoho Vault can be accessed from any device with a stable internet connection. Vault supports the following operating systems, browsers, and mobile devices:

Operating systems	Browsers	Mobile devices
Mac OS	Chrome	iOS
Windows	Firefox	Android
Unix	Safari	
Ubuntu	Edge	
	Edge - Chromium	
	Opera	
	UC	
	Chromium	
	Brave	

1.3 Getting started:

The first person to sign up for Zoho Vault becomes the super admin by default. When you create a Zoho account (including a Zoho Vault account), your information will be stored in one of our datacenters (DC) based on your location, which is determined by your IP address. However, users can write an email to migrations@zohoaccounts.com to migrate from one data center to another based on their choice and our team will guide you through the process.

Zoho Vault is currently available to customers from eight distinct data centers worldwide:

United States (US) : https://vault.zoho.com/
European Union (EU) : https://vault.zoho.eu/
India (IN) : https://vault.zoho.in/
Australia (AU) : https://vault.zoho.com.au
China (CN) : https://vault.zoho.com.cn/
Japan (JP) : https://vault.zoho.jp/
Canada (CA) : https://vault.zohocloud.ca/
Saudi Arabia : https://vault.zoho.sa/

After entering your email address and password, you will be asked if your company already has an organization in Zoho. Select Yes if you're already using other Zoho services and are part of a Zoho organization. If not, select No to create a new organization. Enter a name for the organization and create a master password for your Zoho Vault account. Click Save and proceed to finish the setup.

2.0 User onboarding & management

2.1 User onboarding

There are two ways to add users in Vault. You can add them from **Settings > Users** by manually entering users' email addresses. You can also import your existing list of users from the following services:

- Active Directory (AD) or Lightweight Directory Access Protocol (LDAP)
- Azure Active Directory
- G Suite
- Office 365
- Okta

2.2 Enforce multi-factor authentication

Setting up an additional layer of security for your password vault is key to keeping your data secure, but to be effective, it must be followed by everyone in the company. You can enforce multi-factor authentication for all users in your organization by going to **Settings > Enforce MFA**. You can choose from an extensive list of options for the second authentication factor, such as:

- SMS-based OTP
- OTP authenticator
- Security Key
- Passkey
- Zoho OneAuth

2.3 Set strong password policies

Enforcing a strong password policy across your organization can go a long way to improve the strength of all your employees' passwords. It helps you keep all business passwords compliant while also helping you stay audit ready.

We recommend you either set your own customized strong password policy or enable the Strong option from our default list of password policies under **Settings > Password policy**.

If necessary, set how often users need to change their password by specifying the password age for every password policy you create to enforce password hygiene across your enterprise.

2.4 Monitor your organization's dashboard

Track your organization's cumulative password assessment score regularly and update your organization's password policies accordingly. You can also identify the number of weak passwords owned by each user and contact them individually to prompt them to reset their passwords. Get an overview of the number of passwords due for reset, actions performed in your vault, active users, power users, and security pros (the users with the highest security score) in your organization.

With Vault, users can detect compromised credentials and quickly reset them with strong, unique passwords. Super admins can enable breached password detection for every user in their organization from **Settings > Fine-grained controls**. When enabled, users can identify and reset their breached passwords from their dashboards.

2.5 Add or import passwords

Start adding your passwords and other sensitive details to Vault manually or by importing them. To import your passwords, select **Import** from the Passwords tab or select **Import Passwords** from Settings. You can set up your Zoho Vault account by importing passwords from:

- Browsers
- Other password managers
- A standard CSV file

Note:
The following fields are unencrypted in Zoho Vault to help users search for passwords, manage audits, and automatically log in to websites

- Password name
- URL
- Description
- Tags

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

3.0 Organizing your vault

3.1 Modify user roles

There are three user roles in Zoho Vault:

- Super admin
- Admin
- User

The following table gives details on the privileges that come with each role:

	User	Admin	Super admin
Add/delete users	No	No	Yes
Change roles	No	No	Yes
Approve sharing	No	Yes	Yes
Define password policies	No	Yes	Yes
View reports	No	Yes	Yes
Fine-grained controls	No	Yes	Yes
Basic operations	Yes	Yes	Yes

A Zoho Vault super admin can promote users to an admin role by going to **Settings > Users > Change role.** The best practice is to have only one active super admin. Only provide super admin privileges to authorized personnel based on your needs, and restrict the number of users with admin roles based on the size of your organization.

3.2 Group users

Organize your users into different groups. You can segregate them into user groups based on their teams. For example, you can group all the finance team members in a user group called Finance. Customize and create user groups from the User Group section under Settings.

3.3 Group passwords

Organize and manage your passwords in individual folders. For example, group your social media passwords together in a single folder called Social media. You can also create multiple levels of subfolders and share them in bulk with users or user groups.

3.4 Sharing permissions

Passwords and folders can be shared with users and user groups with four different permissions. We recommend you share passwords and folders with one-click login permissions as much as possible. The different levels of permissions available are:

- **One-click login only:** Passwords cannot be viewed in plain text. Only allows users to auto log on to the websites.
- **View:** Users can view the passwords in plain text.
- **Modify:** Users can view and modify the passwords.
- **Manage:** Users can view, edit, share, and delete the passwords. Provides users with complete ownership of the password.

Think twice before sharing passwords with the Manage permission as this gives the user complete control of your passwords.

4.0 Shared password management

4.1 Configure access control for critical passwords

Restrict access to critical enterprise passwords by setting up access control constraints to prevent unwarranted access to your most confidential shared passwords. This will make users submit password access requests with valid reasons, which will then be validated by one or more admins before the users are granted access to these passwords. All password access requests are audited in the Audit section. We recommend you enable access control for all your confidential passwords by going to **Passwords > More > Enable access control**.

4.2 Password access with help desk ticketing integration

Zoho Vault provides integrations with popular help desks to automate password access requests for passwords enabled with access control. With help desk approvals, the passwords can be accessed when users provide a valid ticket ID from the corresponding help desks and request access. Vault checks if the ticket matches the criteria set by the admin, which can be chosen from a wide range of available options. If it does, users get instant access to the password. Currently, Zoho Vault is integrated with the following help desks:

- Jira
- Service Desk Plus OnDemand
- Service Now
- Zendesk
- Zoho Desk

You can enable this feature for the help desk of your choice by navigating to **Passwords > More > Enable access control > Automatically approve access requests**.

5.0 Crisis management

5.1 Periodically back up your critical information

All data stored in Zoho Vault is important to you and your organization and must not be lost under any circumstances. Enable periodic backup of your Vault account and configure backup copies of the users' data to either be sent to their registered email address or added to their cloud accounts in:

- Amazon S3
- Box
- Dropbox
- Google Drive
- OneDrive
- Zoho WorkDrive

Users will receive an encrypted file containing all their data from Zoho Vault which can only be unlocked with their master password. We also recommend admins only allow users to receive backup copies of the passwords owned by them and not the ones shared with them. You can enforce this by navigating to **Settings > Data Back-up > Include only user-owned Passwords**

5.2 Stay emergency-ready

Keep your enterprise passwords accessible 24/7 by setting up emergency contacts for your Vault account. These contacts can access all enterprise passwords during crises and emergencies when the owner of the password is unavailable. Super admins can set up emergency contacts by navigating to **Settings > Emergency Access > Add**. A newly added contact cannot declare an emergency until 24 hours after they are added by going to **Settings > Emergency Access > Declare Emergency**. All users will be notified whenever an emergency contact is added and when an emergency is declared. As a super admin, if you believe an emergency has been declared for invalid reasons, you can end the declared emergency by going to **Settings > Emergency Access > Emergency Declared > End Emergency**. All actions performed during an emergency period are captured in the audit logs.

6.0 Single sign-on (SSO) for cloud applications

6.1 Configure single sign-on

Enable SSO services for cloud applications that support SAML 2.0 configuration to increase your users' productivity. Provide SSO instantly for over 100 cloud apps for your users in bulk by navigating to Apps and then Manage apps and clicking Add supported app or configure SSO for custom apps which support SAML 2.0 configuration by going to Apps and then Manage apps and clicking Add custom app. You can easily grant and revoke access for multiple apps for multiple users in any instance.

7.0 Securing your enterprise data

7.1 Structure Vault to meet your enterprise needs

While Zoho Vault provides a range of features to tighten the security of your organization's Vault account by restricting users from accessing certain features. An array of customizable options are available in the Fine-grained controls section of the Settings tab. To increase security for your enterprise, we suggest you enforce the following settings:

- Prevent users from sharing passwords with outsiders
- Prevent users from exporting passwords shared with them
- Enable IP restriction to prevent users from accessing their Vault from outside the office premises.
- Hide user-defined password categories from global view
- Restrict offline access to passwords
- Restrict user access to passwords through the mobile app
- Prevent users from copying and pasting their passwords

Enterprises that require users to only be able to access the passwords shared by the admins can enforce further restrictions:

- Prevent users from adding new passwords
- Prevent users from storing personal passwords
- Prevent users from sharing passwords
- Prevent users from exporting passwords
- Prevent users from receiving backup data when they forget their password
- Enable IP restriction for mobile apps

All these settings can be managed by going to **Settings** and then **Fine-grained controls**. You can also exempt specific users from being affected by these changes by selecting **Manage Exemptions** for each option under Fine-grained controls.

7.2 Track audit logs and activity reports

Every action performed in Vault is tracked in the Audit section as logs with complete details of who accessed which password at what time, along with their browser and IP details. These logs are tracked for all sensitive activities performed on:

- Passwords
- Folders
- Users and groups
- Other activities
- Super audit

You can use the **Advanced search** option to narrow down the event you're looking for. These logs can also be exported for further analysis. Enable password protection before allowing admins to export these audit logs by navigating to **Settings** and then **Personalization** and selecting **Set constraints while exporting Audits and Reports**.

Get an overview of all the activities performed in Vault at an organizational or individual level from the visual representations available on our Reports tab.

Use the reports related to different access and sharing behaviors of users to identify any suspicious activities from users. Analyze the strength and patterns of the passwords set by users and get an overview of the number of unchanged passwords. Use these visual reports to set strict password policies across your organization to ensure your users set strong passwords for their accounts.

7.3 Configure custom alerts

We highly recommend you configure alerts to be sent to your registered email for critical events that occur in Vault. This helps you track important activities like the deletion of users, passwords, or folders or any modification to the setup in Vault, wherever you are. You can configure notifications for specific events by going to **Settings** and then **Alerts** and selecting **Create Alert**. We recommend you monitor at least the deletion and modification of passwords, folders, users, and SSO applications.

7.4 Sharing passwords with third parties

Zoho Vault allows you to securely share your passwords with third parties and contractors outside your organization. This options gives these third parties quick access to your passwords for a limited time once you share the decryption key with them. We strongly recommend that you change all the passwords that are shared with outsiders as soon as the reason for giving them access is complete.

7.5 Dealing with the data of former employees

If an employee decides to leave your organization, ensure you acquire all enterprise passwords owned by them. Once you acquire them, we strongly recommend that you change them to keep your accounts secure.

A super admin can acquire all enterprise passwords and folders owned by a user and transfer them to a different user of their choice by going to **Settings > Users > More > Transfer Ownership**. When all passwords and folders are acquired, the user can be removed from Vault.

We also recommend that you delete the data of users removed from Vault right after they're deleted. You can access this by going to **Settings** and then **Privacy settings** and selecting **Immediately** for the Retain user data after user deletion field.

8.0 Best practices for users

TABLE OF CONTENTS

1.0 Getting started

1.1 Avoid creating duplicate accounts

Avoid creating a separate account with Zoho Vault. Join the account your admin has invited you to in order to prevent any delay in getting added to your team's centralized vault. If you face any difficulties, reach out to your organization's admin or write to **support@zohovault.com**.

1.2 Set a strong master password

Your master password will be the key that unlocks your data stored in Zoho Vault. This will be the only password you'll need to remember. Set a strong, unique master password for your account to keep your vault safe and protected.

1.3 Enable multi-factor authentication

Even if your admin has not enforced multi-factor authentication for all users, we highly recommend you safeguard your account with a second factor of authentication.

You can enable this by selecting your profile picture on the header and going to **My account** and then **Dashboard** and selecting **Two-factor authentication**. You can select a second factor of authentication from a wide list of options like SMS-based OTP, OTP authenticator, Security Key, Passkey, Zoho OneAuth

1.4 General security

Your Zoho Vault account times out after 15 minutes by default. We strongly recommend you set this time to be as low as possible from **Settings > Personalization.**

2.0 Setting up your vault

2.1 Add or import passwords

Start adding your passwords and other sensitive details to Vault manually or by importing them. If you're moving to Vault from another password manager, select Import from the Passwords tab or click Import Passwords from Settings to select the type of file you'd like to import.

Custom file formats from password managers like LastPass, 1Password, Dashlane, Bitwarden, KeePass, and many others can be seamlessly migrated to Zoho Vault. You can also import your passwords from a standard CSV file format to set up your Zoho Vault account.

2.2 Download our browser extensions

Simplify online authentication with Zoho Vault's browser extensions. You can download our extensions for:

- **Ulaa**
- **Chrome**
- **Firefox**
- **Microsoft Edge**
- **Safari**
- **Brave**
- **Vivaldi**
- **Opera**

You can use the extensions to automatically log in to online accounts and generate secure passwords for new signups. The extensions will also help you save passwords of new signups to your vault.

Note:
By default, the extension will be locked after 10 minutes. Set the right timeout period to keep your extension active for as long as you need from the extension's Settings tab.

Install our mobile apps

Download our mobile apps to access your passwords from anywhere. We support mobile applications for:

- iOS
- Android

You can also find the download link for all the extensions and apps by clicking your your profile picture in the header of your account.

Group passwords

Organize and manage your passwords from individual folders. For example, group all your social media passwords together in a single folder called Social media. You can also create multiple subfolders and share them in bulk with users or user groups.

2.3 Sharing permissions

Passwords and folders can be shared with users and user groups with four different permissions. We recommend you share passwords and folders with one-click login only permission as much as possible. The different levels of permissions available are:

- **One-click login only:** Passwords cannot be viewed and copied. Only allows users to auto log on to websites
- **View:** Users can view the passwords in plain text
- **Modify:** Users can view and modify the passwords.
- **Manage:** Users can view, edit, share, and delete the passwords. Provides users complete ownership of the passwords.

Think twice before you share passwords with Manage permissions as this gives complete control of the password to the user.

3.0 Keeping track of your account

3.1 Adhere to the password policy

Use strong passwords for all your accounts to satisfy your organization's password policy. Strong passwords keep your accounts safe from potential cyber threats and also improve your password assessment score displayed in the Dashboard.

3.2 Monitor your dashboard

In addition to the password assessment score, you can also identify weak passwords from the Dashboard. From this page, you can identify:

- Passwords that have been reused
- Passwords that have been recycled
- Passwords that contain the username
- Passwords that contain dictionary words
- Old and weak passwords

Replace all these weak passwords with secure, strong passwords in Zoho Vault. You can also keep an eye on passwords that need to be reset soon and stay compliant with your company's security policies.

With Vault, users can detect compromised credentials and quickly reset them with strong, unique passwords. Super admins can enable breached password detection for every user in their organization from **Settings > Fine-grained controls**. When enabled, users can identify and reset their breached passwords from their dashboards.

3.3 Back up your critical details

If your administrator has enabled cloud backup for your organization, ensure you link your cloud account with Zoho Vault from **Settings > Cloud backup** to periodically receive backup copies of your passwords from Zoho Vault. This will help you organize all your critical information and access or restore them during crisis and emergencies.

4.0 Things to remember

4.1 Initiate proper handover of passwords before leaving the organization

Alert your admins and super admins before you leave your organization to initiate the proper handover of all business passwords and folders you own.

Select the enterprise passwords you own from the Passwords tab and select **More** and then **Transfer Ownership** to select the user you wish to transfer the passwords to. When you have transferred all your enterprise passwords to another users, you can export all your personal passwords before the super admin deactivates your profile.

4.2 Add our support email address to your trusted list

Add our support email address (support@zohovault.com) to the trusted email address list to ensure you receive all our updates in your inbox. This includes support responses, product updates, security notices, and details about education webinars.

Contact support when you need help

You can contact support from within Zoho Vault's interface by selecting **Request Assistance**. You can also share your feedback with us by selecting **Share Feedback**. Alternatively, you can contact our support by phone or email. Our support team is available 24 hours a day, Monday to Friday.

Contact us:

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

Email:
support@zohovault.com

www.zoho.com/vault

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