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 that'll help them get started with Zoho Vault, while an admin will learn the different security aspects involved in managing users and structuring Vault to satisfy the business needs.

1.2 System requirements

Zoho Vault can be accessed across all devices with a stable internet connection. Vault supports the below list of operating systems, browsers, and mobile devices.

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

1.3 Getting started

The first person to sign up for Zoho Vault becomes the super-admin by default. These super admins must be careful while choosing their data center, as other users join this primary account to start sharing passwords within their teams.

Zoho has data centers across US, Europe, and Asia, allowing you to store your data in the center from your preferred region. This will ensure your organization's data remains only in the data center of your preferred region.

You can sign up for Zoho Vault from the below regions using the corresponding links:
United States: https://www.zoho.com/vault/signup.html
Europe: https://www.zoho.eu/vault/signup.html
India: https://www.zoho.in/vault/signup.html
China: https://www.zoho.com.cn/vault/signup.html

After entering your email address and password, you will be asked if your company already has an organization created in Zoho. Proceed with **Yes** if you already are part of a Zoho organization, or select **No** to create a new organization. Finally, enter a name for the organization and create a passphrase for your Zoho Vault account. Click **Save** and proceed to finish the setup.

2.0 User onboarding and management

2.1 User onboarding

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

- Active Directory(AD) or Lightweight Directory Access Protocol(LDAP)
- GSuite
- Office 365

2.2 Enforce two-factor authentication

Setting up an additional layer of security for your password vault is critical and has to be followed across the enterprise. You can enforce two-factor authentication be followed by all users in your organization from **Admin >> Enforce TFA**. A suitable second factor can be chosen from a wide list of options like:

- Text message
- Voice call
- Time-based OTP
- Touch ID
- Push notifications
- QR scan
- Google authenticator

2.3 Set strong password policies

Enforcing a strong password policy across your organization could go a long way in improving the password strength of all your employees. It helps you keep all business passwords compliant while also helping you always stay audit-ready.

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

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

2.4 Add or import passwords

Start adding your passwords and other sensitive details to Vault manually or by importing them. To import your passwords to Vault, select **Tools >> Import Secrets**. You can immediately set up your Zoho Vault account by importing passwords from:

- Other password managers
- A standard CSV file format

3.0 Organising your vault

3.1 Modify user roles

In Zoho Vault, there are three user roles:

- Super-admin
- Admin
- End-user

The table below details the powers that come with every role.

	End-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 has the privilege to promote users to an administrator's role from **Admin >> User Management >> Change roles**. The best practice is to have only one active super-admin. Provide super-admin privileges only to authorized personnel based on your needs, and restrict the promotion of users to admin roles based on the size of your organization.

3.2 Group users together

Organize your users into different groups. You can segregate them into user groups based on their teams, circles and more. For example, you can group the finance team members together in a user group called Finance. Customise and create multiple user groups from **Admin >> User Management >> User Groups** section.

3.3 Group passwords together

Add related passwords in individual folders called Chambers. A valid example is grouping multiple social media passwords together in a single Chamber called Social media. You can also create two-levels of sub Chambers and share them with Users or Usergroups in bulk.

3.4 Sharing permissions

Secrets and Chambers can be shared with users and user groups with four different permissions. We recommend you to share Secrets and Chambers with One click login permissions as much as possible. The different levels of permissions available are:

- **One click login -** Secrets are restricted from being viewed. Allows users to just auto logon to the websites
- **View -** Users can view the Secrets in plain text
- **Edit -** Users can view and edit the Secrets
- **Manage -** Users can view, edit, share and delete the Secrets. Provides complete ownership of the Secret to users.

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

4.0 Shared password management

4.1 Configure access control for critical passwords

Restrict the access on critical enterprise passwords by setting up access control constraints to prevent unwarranted access of your crucial shared Secrets. This will mandate users to raise password access requests with valid reasons, which will then be validated by one or more admins before the users are granted access to these Secrets. All Secret accesses are audited in the Audit section. We recommend you to enable access control across all your critical Secrets from **Secrets >> More actions >> Configure access control**.

4.2 Password access with help desk ticketing integration

Zoho Vault provides integration with popular help desks as an option to automate password access requests for access-control-enabled secrets. Secrets enabled with help desk approvals can be accessed when users provide a valid ticket ID from the corresponding help desks, requesting access. Vault checks if the ticket matches the criteria set by the admin, chosen from a wide range of available options. If it does, the users get instant access to the Secret. Currently Zoho Vault integrates with help desks like:

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

It would be ideal to enable this feature based on the helpdesk of your choice by selecting **Secrets >> More actions >> Configure access control >> Automatically approve access request.**

5.0 Crisis management

5.1 Periodically back up your critical information

All data stored in Zoho Vault is of critical importance to you and your organization and cannot be lost under any circumstances. Enable periodic backup for your Vault account and configure backup copies of the users to be sent either to their registered mail or to their respective cloud accounts in:

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

Users will receive an encrypted HTML file containing their Secrets that can be accessed only with their passphrase. We also recommend admins allow users to receive backup copies of only the passwords owned by them and not the ones shared with them. You can enforce this from **Admin >> Data Backup >> Include only owned Secrets >> Enable >> Save.**

5.2 Stay emergency-ready

Keep your enterprise passwords accessible 24/7 by setting up emergency contacts for your Vault account. These contacts are privileged to access all enterprise passwords during crises and emergencies when the owner of the password is unavailable. Super-admins can set up emergency contacts from **Settings >> Emergency access >> Emergency contacts >> Add.**

An emergency contact can declare an emergency from **Settings >> Emergency access >> Declare emergency**. All users will be notified whenever an emergency contact is added and when an emergency is declared. As an admin, if you believe an emergency has been declared for invalid reasons, you can revoke the declared emergency from **Settings >> Emergency access >> Emergency contacts >> Emergency declared >> Revoke emergency**. All actions performed during an emergency period are captured under 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+ readily available cloud apps for your users in bulk from **Apps >> Manage apps >> Add supported app** or configure SSO for custom apps supporting SAML 2.0 configuration from **Apps >> Manage apps >> Add custom app**. You can grant and revoke access for multiple apps for multiple users in any instance without much hassle.

7.0 Securing your enterprise data

7.1 Structure Vault to satisfy your enterprise needs

While Zoho Vault provides multiple features to enhance the user experience, you can tighten the security of your organization's Vault account by restricting users from accessing certain features. An array of customisable options are available under the **Fine-grained controls** section, found under the **Admin** tab. For enhanced levels of security for your enterprise, we suggest you to enforce the below settings:

- Restrict users from sharing Secrets with outsiders
- Restrict users from exporting Secrets shared with them
- Enable IP restriction to prevent users from accessing their Vault account outside office premises
- Hide user-defined Secret types from global view
- Restrict offline access to Secrets
- Restrict user access to Secrets through the mobile app
- Prevent users from pasting their password from elsewhere

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

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

All these settings can be managed from **Admin >> Fine-grained controls.** You can also exempt specific users from being affected by these changes by selecting **Exempt specific users** corresponding to each option under Fine-grained controls.

7.2 Track audit logs and activity reports

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

- Secrets
- Chambers
- Users
- Admin activities
- Audits and reports

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 from **Settings >> General settings >> Require passwords at the time of exporting passwords.**

Get an organizational or individual overview of all the activities performed in Vault from the multiple visual representations available under our **Reports** tab.

Use the numerous reports related to different access and sharing behavior of users to single out any suspicious activities from one or more users. Analyze the strength and patterns of the passwords set by users along with 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 alert notifications

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 deletion of Users, Secrets, or Chambers—or even any modification to the existing setup of Vault—from wherever you are.

You can turn notifications on by specifying the events you'd like to be notified for from **Audit >> Notifications >> Add.** It's ideal to monitor at least the deletion and modification of Secrets, Chambers, Users, and SSO apps.

7.4 Sharing passwords with third parties

Zoho Vault allows you to securely share your Secrets with third parties and contractors outside your organization. This time-limited password sharing option gives outsiders access to your Secrets once you share the decryption key with them. We strictly recommend you change all the passwords that are shared with outsiders right after the corresponding tasks get completed.

7.5 Dealing with former employees' data

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

A super-admin can acquire all enterprise Secrets and Chambers owned by a user and can transfer it to a user of their choice from **Admin >> User management >> User >> More actions >> Acquire Secrets, transfer ownership**, after which they can remove the user from Vault.

We also recommend you delete the data of users removed from Vault right after they're deleted. You can access this from **Admin >> Privacy settings >> Immediately**, corresponding to "How long should the user data be retained after deletion?" field.

8.0 Best practices for users

TABLE OF CONTENTS

1.0 Getting started

2.0 Setting up your vault

3.0 Keeping track of your account

4.0 Things to remember

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 passphrase

Your passphrase will be the key that unlocks your data stored in Zoho Vault. This will be the only password you'll need to remember in the future. Ensure you set a strong, unique passphrase for your account to stay compliant.

1.3 Enable two-factor authentication

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

You can enable this by selecting My account >> Dashboard >> Two-factor authentication. You can select a second factor of authentication from a wide list of options like text message, voice call, time-based OTP, touch ID, push notifications, QR scan, and Google authenticator.

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 >> General Settings.

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 **Tools >> Import Secrets** to select the type of file you'd like to import.

Custom file formats of password managers like Lastpass, 1Password, Keepass, Keeper, and many others are available for seamless migration to Zoho Vault. You can also import your passwords from a standard CSV file format to immediately set up your Zoho Vault account.

2.2 Download the browser extensions and mobile apps

Simplify your online login process with Zoho Vault browser extensions. You can download our extensions for:

- Chrome
- Safari
- Firefox
- Edge

Use these extensions to auto log in to online accounts and to generate secure passwords on signup pages. Download our mobile apps to access your passwords from anywhere. We support mobile applications for:

- iOS
- Android
- Windows

You can also find the download link to all the extensions and apps from the **Dashboard** of your Zoho Vault account.

2.3 Group passwords together

Add related passwords in individual folders called Chambers. A good example is grouping multiple social media passwords together in a single Chamber called Social media. You can also create multiple sub-Chambers and share them with Users or Usergroups in bulk.

2.4 Sharing permissions

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

- **One-click login:** Secrets are restricted from being viewed. Allows users to just auto log on to the websites
- **View:** Users can view the Secrets in plain text
- **Edit:** Users can view and edit the Secrets
- **Manage:** Users can view, edit, share, and delete the Secrets. Provides complete ownership of the Secret to users.

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

3.0 Keeping track of your account

3.1 Adhere to the password policy

Set strong passwords to satisfy the constraints of your organizational password policy. If this policy requires you to recycle your passwords after x number of days, do so well within the mentioned period. Strong passwords help improve your average password strength under the Password assessment report, and this in turn reflects on your **Dashboard**, keeping you in the secure green zone.

3.2 Monitor your Dashboard

Apart from your password strength score, you can also single out the weak passwords from the Dashboard. Find out the number of less-complex, reused, and recycled passwords, along with the number of unchanged passwords. Passwords that are part of the username or are dictionary words found in your account are also listed here. Replace all these weak passwords with secure, strong passwords from Zoho Vault.

3.3 Back up your critical details

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

4.0 Things to remember

4.1 Initiate proper handover of Secrets before leaving the organization

Alert your admins and super-admins well before you leave your organization to initiate the proper handover of Secrets and Chambers owned by you.

Select the enterprise Secrets you own from the **Secrets** tab and select **More Actions >> Transfer ownership** to select the user to whom you wish to transfer the Secrets. Once all enterprise Secrets are transferred, you can export all the personal Secrets owned by you before the super-admin deactivates your profile.

4.2 Add our support e-mail to your trusted list

Mark our support email address (support@zohovault.com) under the trusted e-mail address list to receive all our updates in your inbox. This includes support response, product updates, security notices, and details about education webinars.

About Zoho Vault

Zoho Vault is an online password manager for teams. It helps securely store, share, and manage passwords from anywhere. Zoho Vault leverages the host-proof hosting (zero-knowledge architecture) to provide the highest levels of data security and privacy. The software is available in three editions and two languages. Zoho Vault offers three licensing options—Standard, Professional, and Enterprise—priced per user, per month. For more information on Zoho Vault, please visit https://www.zoho.com/vault/pricing.html.

Useful links:

Product demo
Getting started
Upcoming webinars
Testimonials
Resources

Contact:

Australia: +61 291654046 - 6400

USA: +1 3123402567 - 6400

UK: +44 2039012997 - 6400

India: +91 044 67447048 - 6400

Vault

Zoho Corporation
4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539 UK : +44 (20) 35647890 Australia : +61 2 80662898
www.zoho.com/vault