ZOHO Vault

Administrator Guide

Table of contents

8. Disaster recovery configuration

9. Audit settings

10. Reports

11. Offline access

12. Mobile access

13. Browser extensions

14. Contact details for technical assistance

Introduction

Thank you for choosing Zoho Vault to manage your enterprise passwords and other digital identities! This guide will provide you the basic information necessary to help you get started with the product.

Sign-up instructions

The first step in getting started is to create your Zoho Vault account. During the sign-up process, there are two possible scenarios which you might face:

Case-1: If you are new to Zoho
Case-2: If you already have an account with Zoho

Case-1: If you are new to Zoho

- Sign-up for Zoho Vault from here: https://www.zoho.com/vault
- For EU data center: https://www.zoho.eu/vault/
- Enter the email id, password and click the **SIGN UP FOR FREE** button. Follow the on-boarding instructions provided in the proceeding screens.
- During the account setup process, make sure you create a strong passphrase (the master-key) with which all your data will be encrypted.
- You should always remember this passphrase to access your account.
- Once you complete the account creation process, you'll see our web interface.

Case-2: If you already have an account with Zoho

- If you are the organization administrator of your account, log in to your Zoho account and click the **Access Zoho Vault** button in the top-right corner of this page.
- You will be prompted to create a passphrase (the master-password) with which all your data will be encrypted. This passphrase must be provided every time when you need to access your account.

You can find step-by-step instructions for both the cases in this section of our help documentation.

Important terminologies

We strongly recommend that you get familiarized with the following list of basic terminologies before proceeding further.

Passphrase	The master key with which your all your confidential data is encrypted and decrypted
Secrets	Passwords and other confidential data stored in Zoho Vault. There are two types of secrets: **Enterprise** and **Personal** • When you add a secret into Zoho Vault, you need to mark it either as either **Enterprise** or **Personal** • The secrets that are marked as **Enterprise** can only be shared with other users in the organization • **Personal** secrets will always re-main exclusive to you. Even your organization super administrators cannot access it
Password Policy	Password rules framed by your organization administrator.
Chamber	A group of secrets.
User	Someone who is part of your Zoho Vault account.
User Groups	A set of users from a particular domain. For example: Marketing or Finance.
Outsider	Anyone who is not part of your company's official Zoho Vault account. Such as contract workers, consultants, and other temporary workers.
Super Admin	The person who created and manages your company's Zoho Vault account. This is often the IT administrator of your company.

Basic settings

Initiate sharing

- After creating your account, you must complete the handshake process to share secrets with other users and vice versa. You can do this by navigating to the **Settings page** >> **Sharing Secrets** and clicking the **Initiate Sharing** button.
- Once the sharing process is initiated, the super-admin or any other administrators can approve the sharing requests from users.
- Both the initiate sharing and getting approval from the admin steps should be completed by the users to share secrets with others and vice-versa.

Note: The super admin (one who created the Zoho Vault account) is solely exempted from the handshake process. If any of your organization users are already having a Zoho Vault account with your company domain, they need to delete that account and join this newly set up official account.

Configure two-factor authentication (recommended)

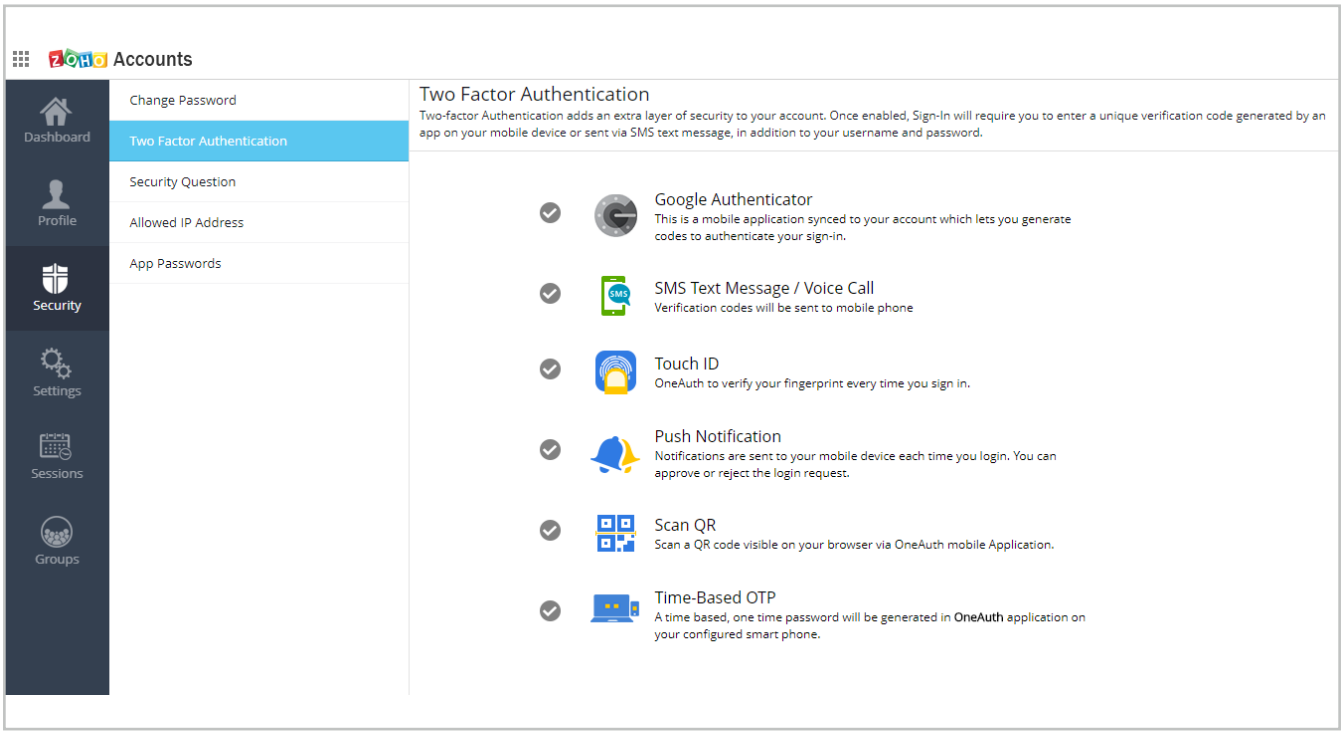
Adding an additional layer of security to your account is highly essential in the current backdrop of ever-increasing cyber attacks. You can configure two-factor authentication for your Zoho account and also enforce your enterprise users go through an additional step of authentication whenever they login.

Step 1: First level of authentication is through native or AD/LDAP

Step 2: Second level authentication through any one of the mechanisms below:

- Phone call or SMS
- Google Authenticator
- Touch ID
- Push Notification
- Scan QR
- Time-Based OTP

To configure two-factor authentication, navigate to Admin, Two-Factor Authentication settings in the web interface. More information on configuring two-factor authentication can be found in this section of our help documentation.



User provisioning and management

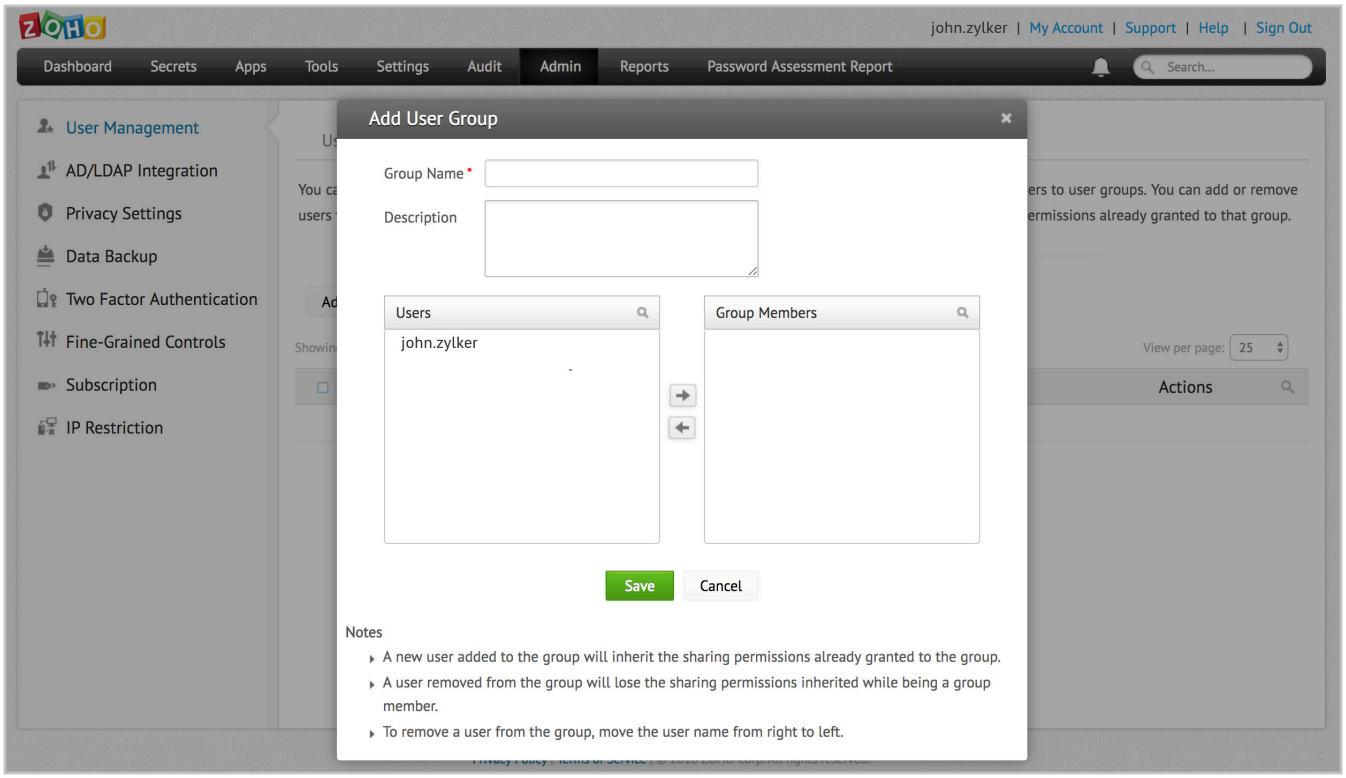
Add users

Adding users into Zoho Vault can be done in many ways. You can send an invitation to users manually via email or integrate with corporate identity stores like AD, LDAP, Azure ADAP, Office 365, or GApps. More information on adding users can be found in the following sections of our help documentation:

- Add users manually
- Import users from AD
- Azure Single Sign-on
- Import users from Office 365
- Import users from G Suite

Create user groups

After adding/importing users, you can group them based on domains, roles, geographies, etc. to carry out password operations in bulk. To create a user group(s), navigate to **Admin, User Management,** then **User Groups.** More information on creating user groups can be found in this section of our help documentation.



Assign roles

The next step is to assign role to users. There are three pre-defined roles in Zoho Vault, the Super Admin, Admin, and User. Those who have the roles of **Super Admin** and **Admin** at Zoho accounts level are automatically designated as Super Admin in Zoho Vault. You can change the role for a user at anytime. The below table explains the capabilities of each role.

Role	Capabilities
Super Admin	• Exclusive privilege to invite other users to join Zoho Vault, change the role of other users and acquire secrets from users • Approve secrets sharing requests from other users • Define password policies • View reports • Delete organization • Fine-grained controls

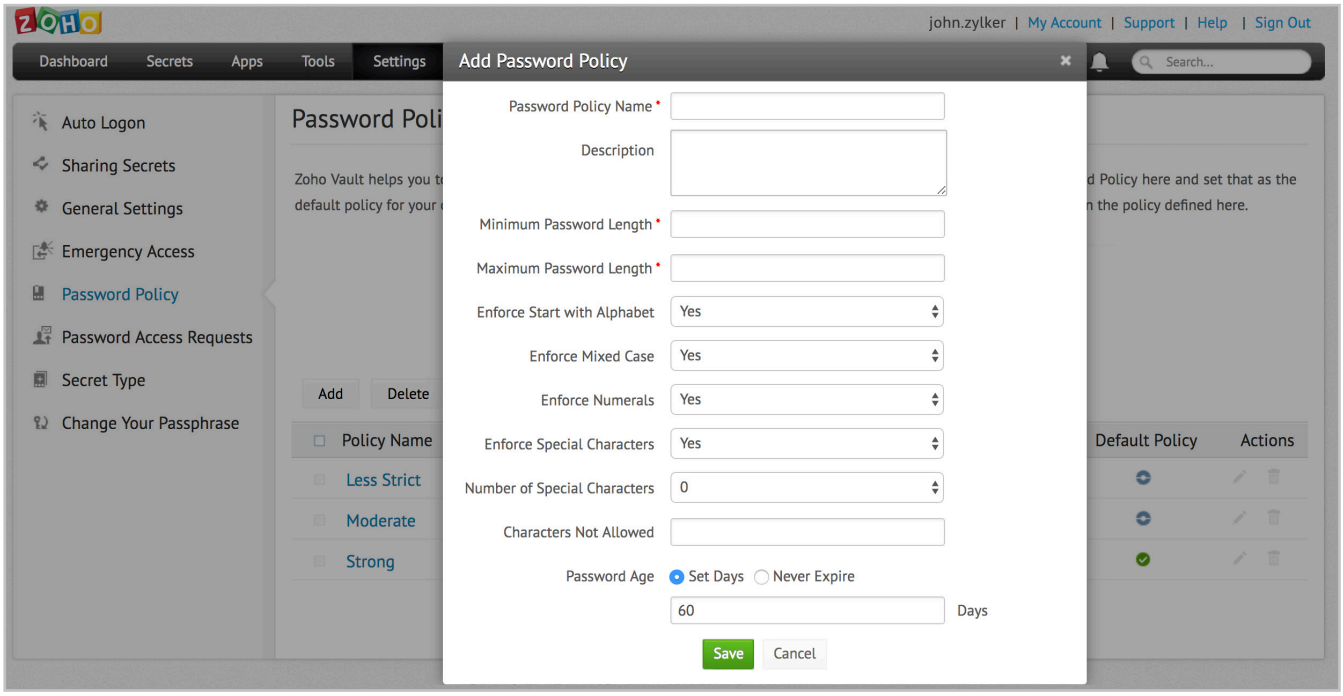
Admin	• Approve secrets sharing requests from users • Define password policies • View reports • Fine-grained controls
Users	• Cannot perform any admin operations

More information on assigning roles can be found in this section of our help documentation.

Set password policy

Zoho Vault helps you enforce usage of strong passwords across the entire organization. The built-in password generator bundled inside the product can help users generate passwords based on the complexity levels configured by you in the password policies.

You can set various conditions including minimum password length, maximum password length, enforce alphabets, numerals, special characters, age, and more. By default, you will see three types of policies there: Strong, Medium, and Less Strict. You can use any one of these or create your own password policy. Configure password policies by navigating to the Admin, Settings, then Password Policies section.



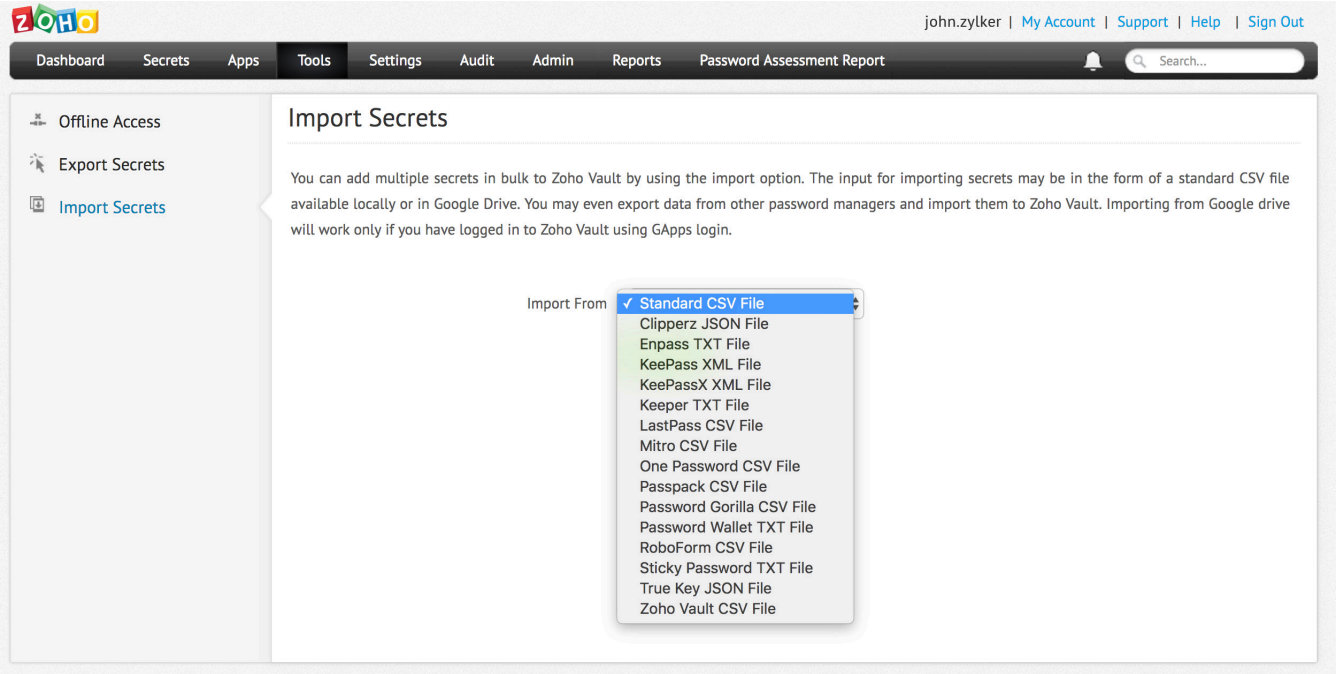
Password management

Add or import secrets

The term secret refers to passwords and other confidential data that is to be stored in Zoho Vault. You can add secrets from the **All Secrets** tab in the **Secrets** page in two ways:

- Manual addition using the **Add** button on the **All Secrets** page
- Importing them from files stored on your desktop using the Tools section. Import secrets from a standard CSV file or from files exported from other password managers.

The following links contain more information about adding secrets manually and through import tools.



Chambers and bulk sharing

Group secrets of the same type for bulk sharing purposes into folders called **Chambers** by clicking the **Add Chamber** button in the **Chambers** tab on the **Secrets** page. You can then share these secrets with other users, user groups, or with an outsider (such as contractors) using the **Share** option under Action. You can also set access privileges while sharing secrets:

One-Click Login Only	Share secrets without displaying them in plain-text. Using this method, you can restrict users to perform auto logon.
View	Share secrets with permission to view them in plain-text
Modify	Permission to view and modify the secret
Manage	Permission to view and modify the secret, modify other parameters, and share the secrets with other users

You can find more detailed information about chambers and access privileges in these help documents.

Configure access control workflow

- You can also control access for highly sensitive passwords by configuring **Access Control**, available in the **More Actions** button
- Once access control is configured for a secret, users will have to raise a request to see the secret. One or more admin(s) can approve the request. The secret will be released for view for a limited time period
- You can explore more features by clicking the **More Actions** button on the All Secrets page

You can find step-by-step instructions for configuring access-control workflow in this section of our help documentation.

Advanced Features

Direct connection to websites and applications

Launch direct connection to websites and applications from Zoho Vault's web-interface using the auto logon feature. This can be done in two ways: by native browser extensions or one-click login through installing bookmarklets on browsers. More detailed instructions can be found in the following sections of our help documentation.

- Using Browser Extensions
- Using One-Click Auto Logon

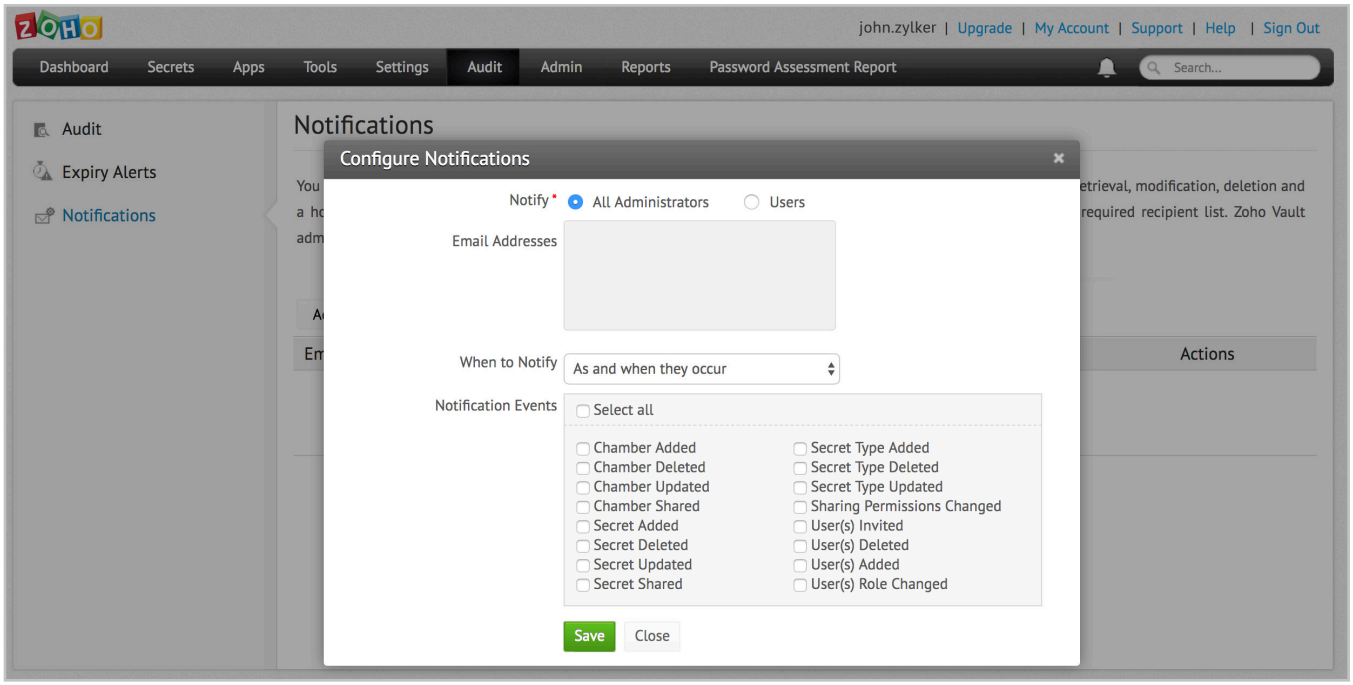
Configure single sign-on for cloud apps

Simplify password management for your users by configuring single sign-on for their most frequently used cloud apps. Navigate to **Apps >> Manage Apps >> Configure single sign-on** for your users. For more details, read this section of our help documentation.

Set notifications

Admins can choose to receive or send notifications to the list of selected recipients for specific password events, such as secret addition, retrieval, modification, deletion, and others. This can be done by navigating to **Audit > Notifications >** and clicking the **Add** button.

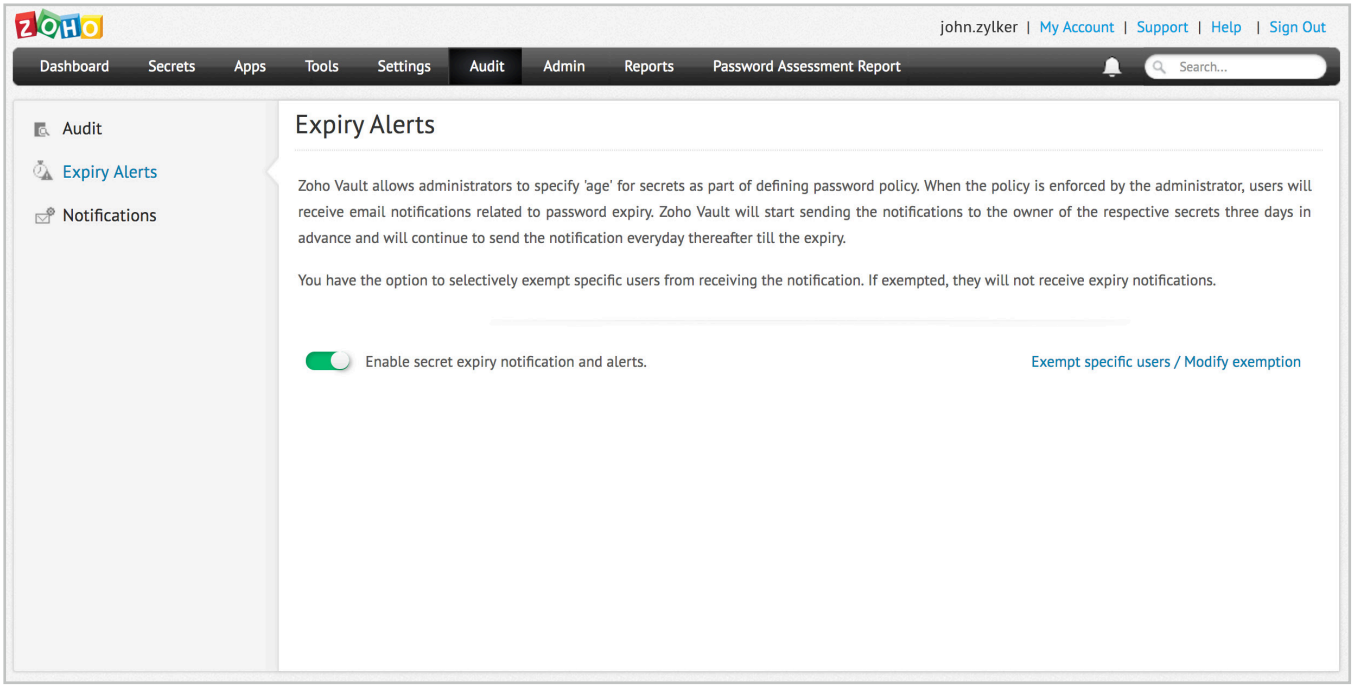
More detailed instructions on configuring notifications can be found in this section of our help documentation.



Set expiration alerts

Admins can also send email notifications to users as their password is about to expire. By default, password owners will be notified three days in advance and every day going forward until it expires. This can be done by navigating to **Audit >> Expiry Alerts >>** and clicking the **Enable secret expiry notification and alerts.**

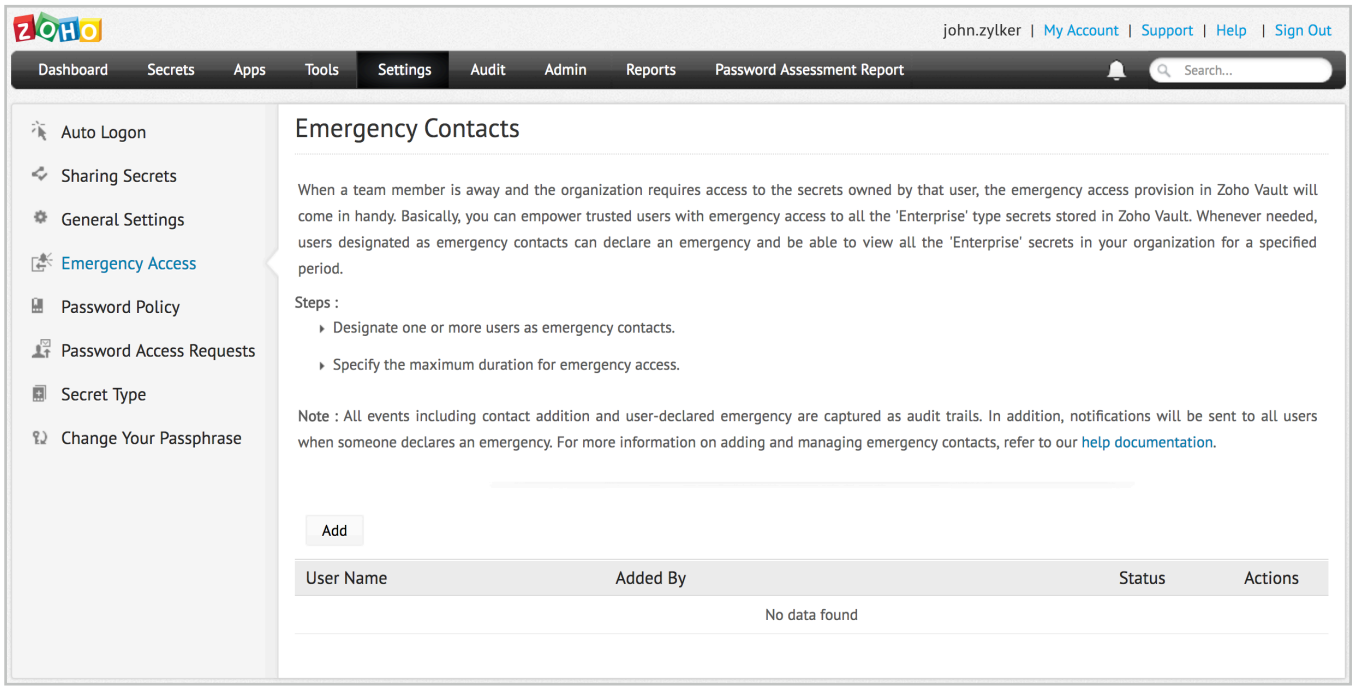
More detailed instructions on expiration alerts can be found in this section of our help documentation.



Configure emergency access

The “break glass” account for emergency access helps you proactively tackle crucial situations and enterprise passwords owned by any user at any point of time. This can be configured in the **Settings >> Emergency Access** tab.

More detailed instructions on configuring emergency access can be found in this section of our help documentation.



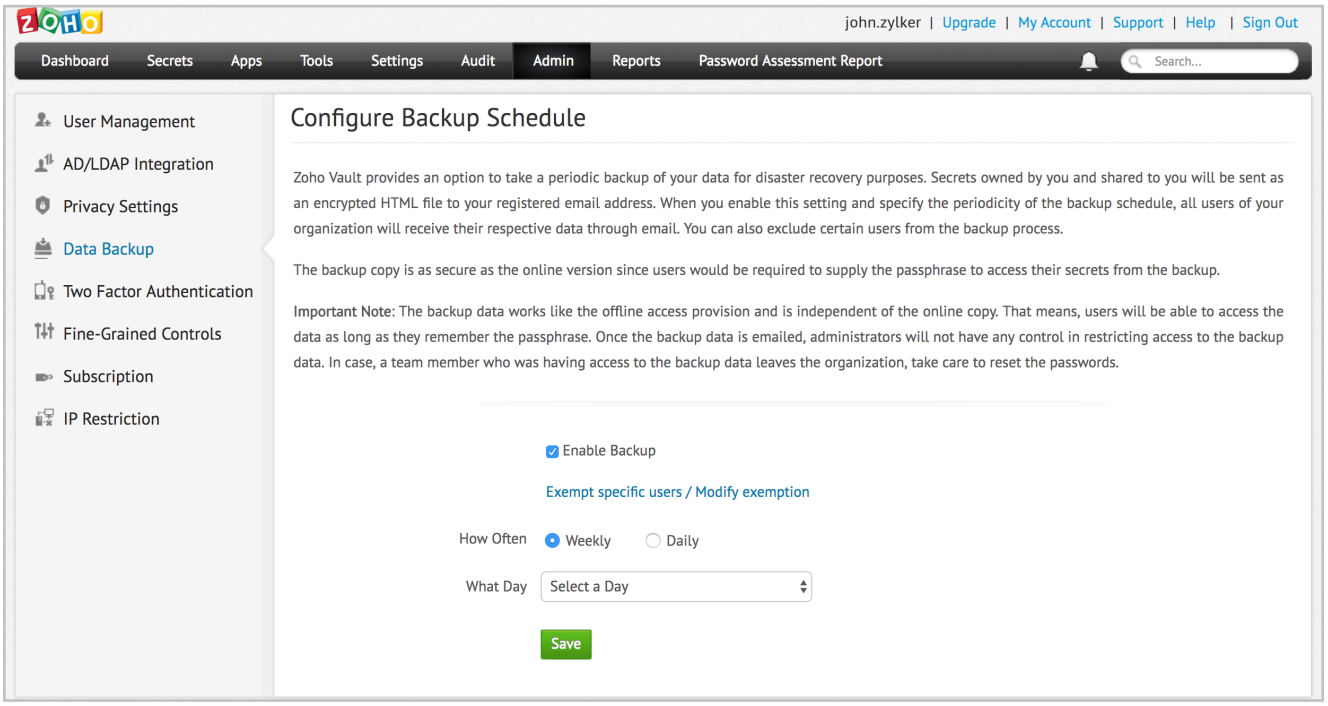
Fine-grained controls

You can enforce some features across the organization and also selectively exempt users when needed. Navigate to **Admin >> Fine-Grained Controls** to perform this operation. You can go through this section of our help documentation to learn more.

Disaster recovery configuration

Configure periodic backup of your data to recover in the event of disasters. The list of secrets owned by you and shared with you will be sent as an encrypted HTML file to your email address at configured intervals. The backup copy can be accessed only after supplying the passphrase every time.

To configure periodic data backup, navigate to **Admin >> General >> Data Back-up.** More detailed instructions on data back up can be found in this section of help documentation.

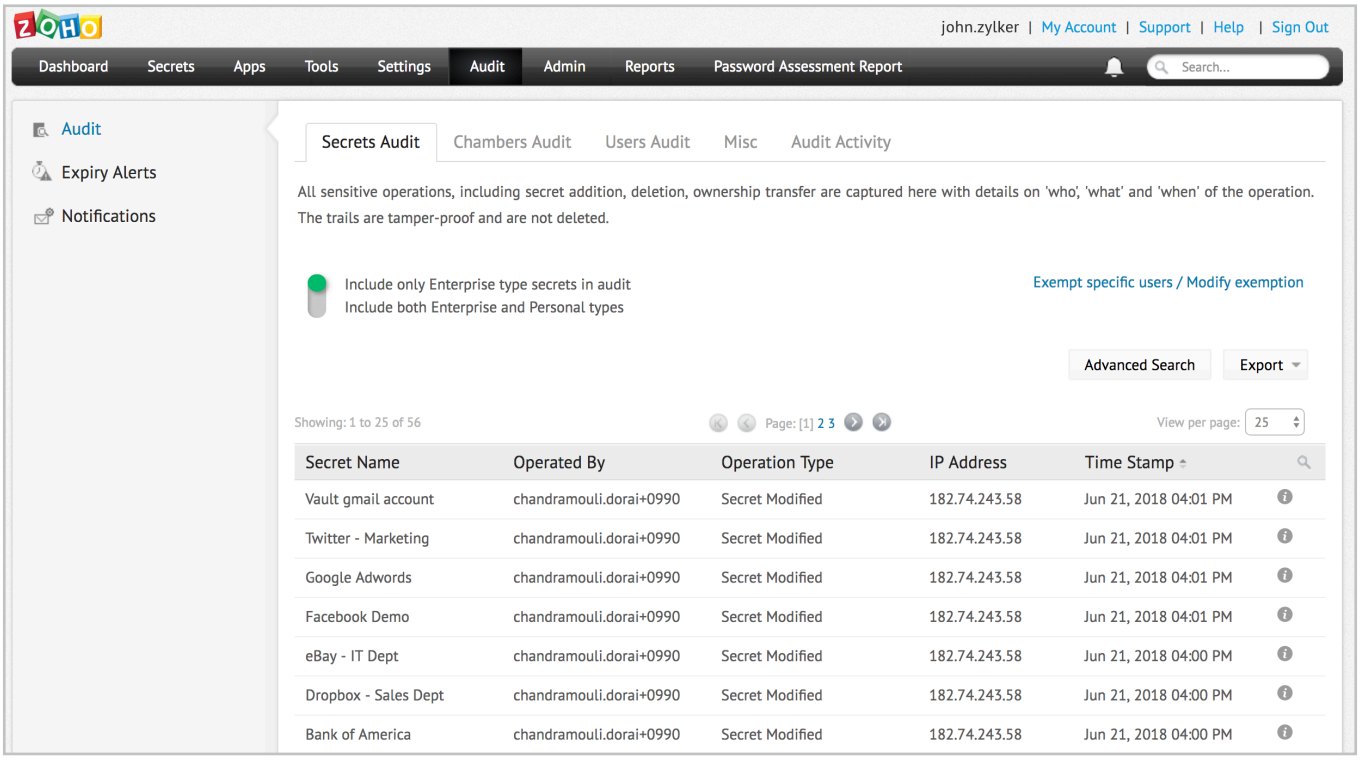


Audit settings

Zoho Vault is designed with an effective auditing mechanism that records every single action performed by users. All operations are audited along with the time stamp and IP address from which the user accesses the product. There are four types of audit in Zoho Vault.

- **Secrets audit:** All operations pertaining to secrets addition, deletion, and ownership transfer are captured with details on the 'who', 'what', and 'when' of the operation
- **Chambers audit:** Includes all operations related to chamber addition, and deletion with details on the 'who', 'what', and 'when' of the operation
- **Users audit:** All operations performed in Zoho Vault by a Zoho Vault user
- **Misc:** Records of the fine-grained access controls, password policy, and the 'who', 'what', and 'when' of the operation

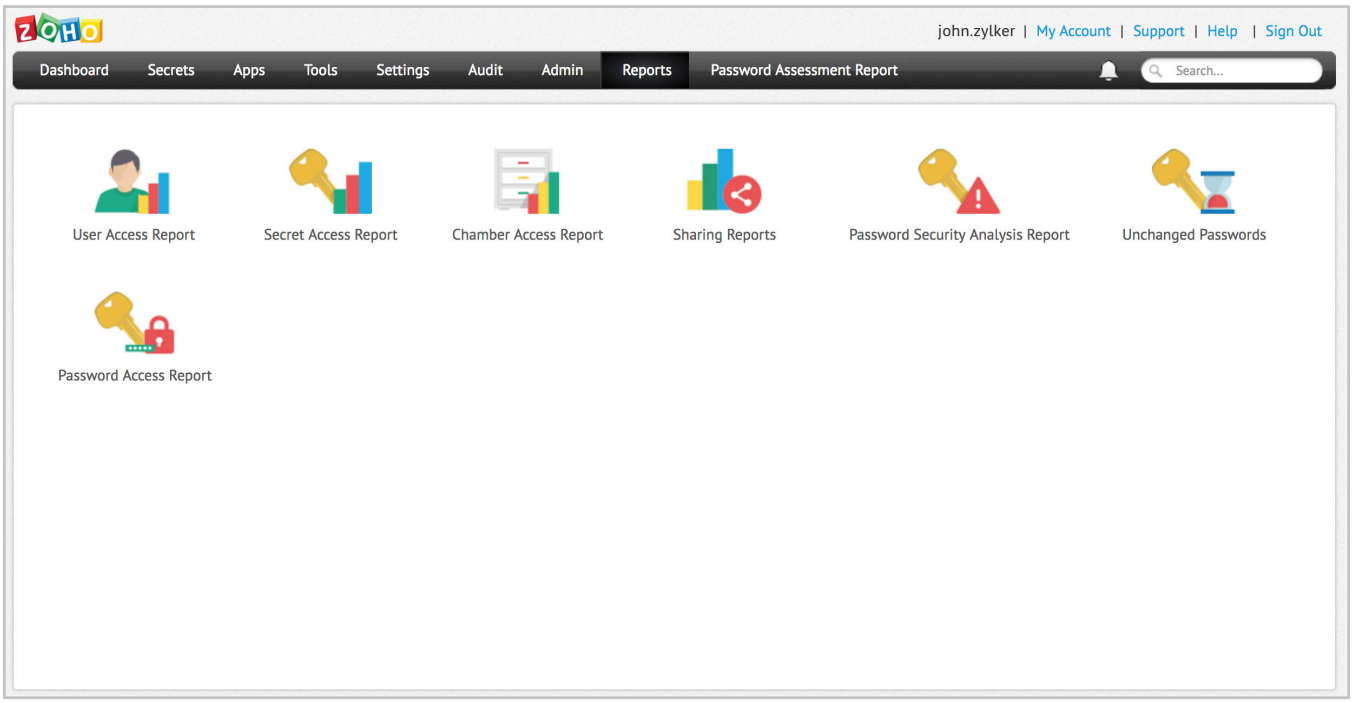
You can view the audits on the **Audit** tab in the web interface. More detailed instructions on audit can be found in this section of our help documentation.



Reports

Information on the password management operations are showcased in the form of intuitive reports in Zoho Vault. The snapshot of various activities such as user access, secret access, chamber access, and unchanged passwords are provided in the form of intuitive reports that help IT administrators make better decisions on password management.

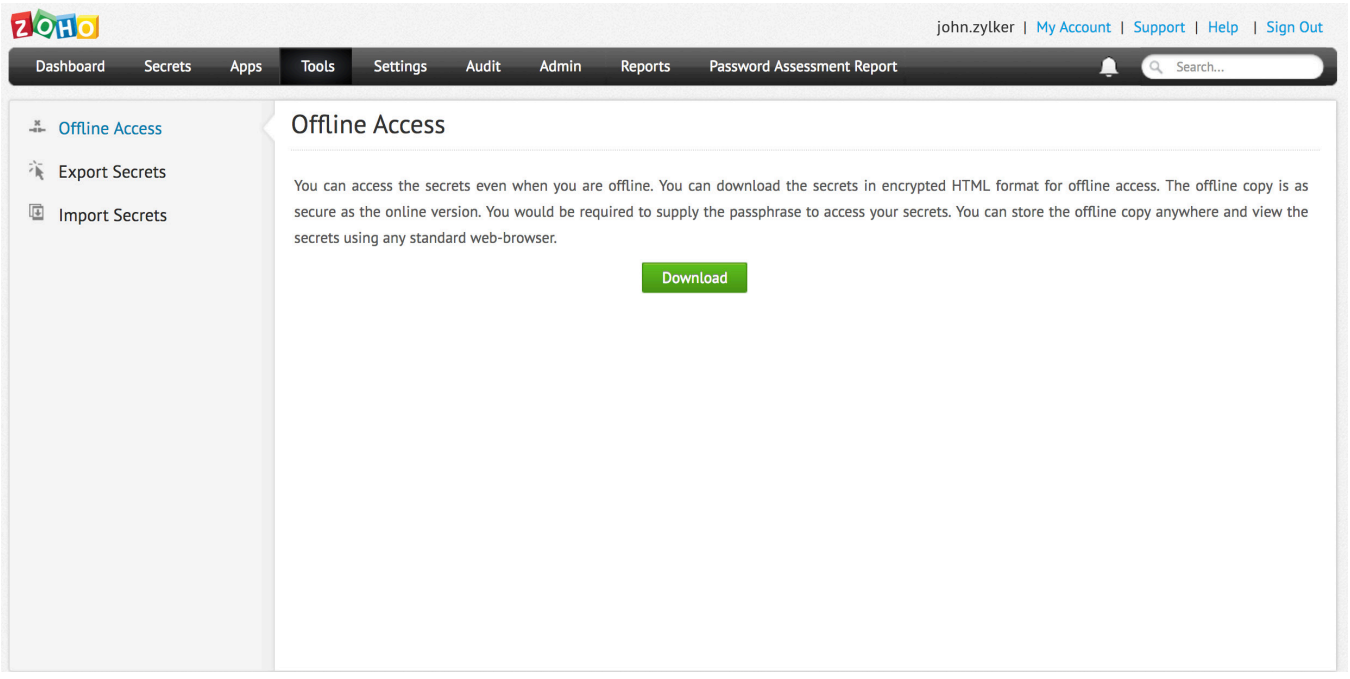
To access reports, navigate to the Reports tab in the web interface. More detailed information on reports can be found in this section of our help documentation.



Offline access

Zoho Vault offers a secure provision to access your passwords even without a standard internet connection. You can download your passwords in the form of a secure, encrypted HTML file and carry it in any removable media. Navigate to Tools >> Offline Access and click the Download button to get an offline copy on your machine.

More detailed information on offline access can be found in [this section of our help documentation.]



Mobile access

Our native mobile apps help you view and manage passwords on the go. The list of supported mobile operating systems and detailed instructions for each are given below.

- Android
- iOS
- Windows

Browser extensions

To simplify day-to-day password management operations and make users more productive, Zoho Vault provides the option to securely synchronize passwords through native browser extensions. The extension helps you auto-fill passwords and automatically log in to websites and web applications in a single click. In addition, you can also add new secrets, share them with colleagues, approve access requests, and more.

After deploying an extension, you can perform most of the password management operations directly from the browser extension without logging into the web interface every single time. Currently, extensions are available for Chrome, Firefox, and Safari.

Contact details for technical assistance

If you are facing any issues in getting started with the product or if you are stuck somewhere, feel free to contact us for immediate assistance.

Email: support@zohovault.com
Toll-free number: +1 (888) 900 9646

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