



IT technicians · Zoho One optimization



Zoho Vault

User and Administrator Manual

→ [Go to the index](#)

Prepared by Nuagix · September 2026

nuagix.ca · support@nuagix.ca

Zoom meeting: <https://nuagix.zohobookings.com/#!/andre-martin>

Index — English version

Click any title to jump directly to that section. Each chapter ends with a “Back to index” link.

PART 1 — USER GUIDE

1. Introduction and access

- 1.1 About this manual
- 1.2 What is Zoho Vault?
- 1.3 Signing in

2. Interface and navigation

- 2.1 Interface elements
- 2.2 Item types

3. Master password and first access

- 3.1 Role of the master password
- 3.2 Creating your master password
- 3.3 Automatic lock

4. Adding and managing passwords

- 4.1 Adding a password
- 4.2 Personal or enterprise
- 4.3 Importing passwords
- 4.4 Finding a password

5. Folders and organization

- 5.1 Creating a folder
- 5.2 Filing best practices

6. Sharing passwords

- 6.1 Sharing a password or folder
- 6.2 Permission levels
- 6.3 Sharing with third parties

7. Browser extension and autofill

- 7.1 Installing the extension
- 7.2 Autofill
- 7.3 Disabling the browser's password manager

8. Password generator

- 8.1 Generating a password
- 8.2 Passwords and passphrases

9. Password security audit

- 9.1 Security dashboard
- 9.2 Fixing issues

10. Emergency access and offline access

- 10.1 Emergency access
- 10.2 Offline access

11. Mobile apps

- 11.1 Features

12. Best practices

12.1 Nuagix recommendations

PART 2 — ADMINISTRATOR GUIDE

13. Users and roles

13.1 Roles

13.2 Adding a user

13.3 When an employee leaves

14. Groups and organizational sharing

14.1 Creating a user group

14.2 Sharing principles

15. Password policies

15.1 Creating a policy

15.2 Other enforced settings

16. Access control and approvals

16.1 Access control workflow

16.2 Other restrictions

17. Single sign-on to applications

17.1 Principle

17.2 Setting up an application

18. Audit logs and reports

18.1 Audit logs

18.2 Reports

19. Integrations

19.1 Zoho integrations

19.2 Other integrations

20. Security and compliance

20.1 Security controls

20.2 Privacy and Quebec Law 25

20.3 Backup

21. Editions and licenses

21.1 Editions

21.2 Tracking usage

22. Deployment checklist

22.1 Before going live

APPENDIX

A. English-French glossary

A.1 Interface terms

Part 1 — User Guide

1. Introduction and access
2. Interface and navigation
3. Master password and first access
4. Adding and managing passwords
5. Folders and organization
6. Sharing passwords
7. Browser extension and autofill
8. Password generator
9. Password security audit
10. Emergency access and offline access
11. Mobile apps
12. Best practices

[↑ Back to index](#)

1. Introduction and access

1.1 About this manual

This manual describes the Zoho Vault features available to users and the functions reserved for administrators, as available in September 2026.

Available features vary by edition (Standard, Professional, Enterprise) and by your organization's configuration. For security reasons, no example in this manual contains a real password.

1.2 What is Zoho Vault?

Zoho Vault is Zoho's password manager for teams and businesses. It stores your organization's passwords, secure notes, files and credentials in encrypted form, lets you share them without revealing them, automatically fills login forms in the browser and gives administrators full control: policies, audit, reports and single sign-on to cloud applications.

1.3 Signing in

1. Go to <https://vault.zoho.com> (or <https://vault.zohocloud.ca> if your organization is hosted in the Canadian data center).
2. Sign in with your Zoho account or your organization's single sign-on.
3. If you use Zoho One, open the app launcher and select Vault.
4. Complete multi-factor authentication with Zoho OneAuth if required.
5. Enter your master password to unlock your vault.

Nuagix tip — Install the Zoho Vault browser extension on day one: it is what will save you time every day.

[↑ Back to index](#)

2. Interface and navigation

2.1 Interface elements

Element	Purpose
Passwords	List of all the secrets you can access
Folders	Groups of passwords, shareable with users or user groups
Favorites	Quick access to the passwords you use most
Security dashboard	Password strength, duplicates and old passwords
Shared with me	Passwords other users have shared with you
Trash	Deleted items, restorable for a limited time
Settings	Personal preferences; administration for administrators

2.2 Item types

- Website or application credentials (username, password, URL)
- Secure notes (recovery codes, licenses, sensitive instructions)
- Encrypted file attachments (certificates, keys, documents)
- Payment cards and banking information
- Custom types created by the administrator (e.g., server, router, Wi-Fi access point)

[↑ Back to index](#)

3. Master password and first access

3.1 Role of the master password

The master password (or passphrase) encrypts and decrypts your data directly on your device. Zoho does not know it and does not store it: this is what guarantees that no one, not even Zoho, can read your passwords.

It is separate from your Zoho account password, which is used only to authenticate you.

3.2 Creating your master password

1. On your first access, Zoho Vault asks you to create a master password.
2. Choose a long phrase made of several unrelated words, easy for you alone to remember.
3. Never reuse a phrase already used elsewhere.
4. Enter a hint that does not reveal the phrase itself, if the option is available.
5. Confirm the phrase and unlock your vault.

Caution — If you forget your master password, Zoho cannot recover it. In an organization, the administrator can reset your access, but your unshared personal passwords may be lost.

3.3 Automatic lock

- The vault locks after a set period of inactivity
- The browser extension locks when the browser closes, depending on settings
- Biometric unlock is available on compatible mobile devices
- The administrator can enforce a maximum lock timeout

[↑ Back to index](#)

4. Adding and managing passwords

4.1 Adding a password

1. Click Add Password.
2. Choose the type (website, application, card, secure note or custom type).
3. Enter the name, URL, username and password (or generate it).
4. Add tags, a description and, if needed, a file attachment.
5. File it in a folder and indicate whether it is personal or enterprise.
6. Save.

4.2 Personal or enterprise

Classification	Effect
Personal	Visible to you only; cannot be shared
Enterprise	Belongs to the organization; can be shared and is recoverable by the administrator

Nuagix tip — Classify as “Enterprise” every credential used for work (suppliers, government sites, cloud tools): the organization will not lose them when an employee leaves.

4.3 Importing passwords

1. Settings > Import Passwords.
2. Choose the source: CSV file, another password manager or a browser.
3. Map the columns to Zoho Vault fields.
4. Choose the destination folder and classification.
5. Run the import, check the imported items, then delete the source file.

Caution — An export file contains your passwords in plain text. Delete it permanently (including from the trash and downloads) as soon as the import is complete.

4.4 Finding a password

- Search by name, URL, username or tag
- Filters by folder, type, classification or owner
- Copy the username or password without displaying it
- History of a password's previous versions

[↑ Back to index](#)

5. Folders and organization

5.1 Creating a folder

1. Folders tab > Add Folder.
2. Name the folder (e.g., Accounting, IT Suppliers, Social Media).
3. Create subfolders as needed.
4. Move passwords into the folder by drag and drop or with a bulk action.

5.2 Filing best practices

- One folder per team or function rather than per person
- Clear, consistent names across the organization
- Tags for cross-cutting classifications (e.g., customer, project)
- Favorites for passwords used daily

Nuagix tip — Structure folders around the groups that need access: sharing an entire folder is much easier to manage than one-by-one shares.

[↑ Back to index](#)

6. Sharing passwords

6.1 Sharing a password or folder

1. Select the password or folder and click Share.
2. Choose the users or user groups.
3. Assign the permission level.
4. Confirm: the share is end-to-end encrypted for each recipient.

6.2 Permission levels

Permission	What the recipient can do
Login only	Sign in through the extension without seeing the password
View	See and copy the password
Modify	See and edit the password
Manage	Edit, delete and re-share

Nuagix tip — Use the Login only permission for interns, contractors and shared accounts: they work normally without ever knowing the password.

6.3 Sharing with third parties

- Share a password with an external person for a limited time, depending on edition
- Revoke the share at any time
- Change the password after an external engagement ends
- Never send a password by email, chat or text message

Caution — Never share a password outside Zoho Vault. A password sent by email remains readable in inboxes and backups.

[↑ Back to index](#)

7. Browser extension and autofill

7.1 Installing the extension

1. Install the Zoho Vault extension for Chrome, Firefox, Edge or Safari from the browser's store.
2. Click the Zoho Vault icon and sign in.
3. Unlock the vault with your master password.
4. Pin the icon to the toolbar for quick access.

7.2 Autofill

- One-click credential filling on recognized login pages
- Automatic login to configured sites
- Prompt to save newly entered credentials
- Update prompt when you change a password on a site
- Filling of payment cards and forms, depending on edition
- Open a site directly from the extension

Note — If a site is not recognized, check that the saved URL matches the login page.

7.3 Disabling the browser's password manager

To avoid storing passwords in two places, turn off password saving in the browser (Chrome, Edge, Firefox or Safari), then import the passwords stored there into Zoho Vault.

[↑ Back to index](#)

8. Password generator

8.1 Generating a password

1. In the add form or in the extension, click the generator icon.
2. Choose the length (16 characters or more recommended).
3. Include uppercase, lowercase, numbers and special characters, according to the site's requirements.
4. Click Generate, then use the suggested password.

8.2 Passwords and passphrases

Type	When to use it
Random password	Websites and applications, since Zoho Vault remembers it for you
Passphrase	What you must type from memory: master password, computer session
Policy-compliant password	Password generated according to the administrator's policy

Nuagix tip — With a password manager, you no longer need to remember your passwords: generate long, unique ones for every site.

[↑ Back to index](#)

9. Password security audit

9.1 Security dashboard

Indicator	Meaning
Weak passwords	Too short or too simple
Reused passwords	Same password used on several sites
Old passwords	Not changed for a long time
Policy non-compliant	Do not meet the organization's policy
Compromised passwords	Found in known data breaches, depending on edition

9.2 Fixing issues

1. Open the security dashboard and sort by severity.
2. Start with compromised and reused passwords.
3. Change the password on the site, then update it in Zoho Vault (or use one-click reset if available for that site).
4. Check that your security score improves.

Nuagix tip — Set aside 15 minutes each month to fix flagged passwords: it is one of the most cost-effective cybersecurity measures for a small business.

[↑ Back to index](#)

10. Emergency access and offline access

10.1 Emergency access

Emergency Access lets people designated by the organization reach critical passwords in case of absence or incident, through a break-glass account. Every emergency declaration is logged and administrators are notified.

Depending on edition, emergency access is configured by the Super Admin.

10.2 Offline access

- Encrypted offline backup file, protected by a separate phrase, depending on settings
- Viewing in the mobile apps without an Internet connection
- Useful during network outages or for business continuity situations
- The administrator can allow or prohibit offline access

Caution — Keep any offline file in a safe, encrypted location. Never copy it to an unencrypted USB key or a shared folder.

[↑ Back to index](#)

11. Mobile apps

11.1 Features

- View, add and edit passwords on iOS and Android
- Unlock with Face ID, Touch ID or fingerprint
- Autofill in mobile apps and browsers
- Built-in password generator
- Offline access according to organization settings
- Smartwatch access to favorite items, depending on the device

[↑ Back to index](#)

12. Best practices

12.1 Nuagix recommendations

- Choose a long, unique master password and never write it down in plain text
- Use a different password, generated by Zoho Vault, for every site
- Turn on multi-factor authentication on every site that offers it and keep recovery codes in a secure note
- Classify every work-related credential as “Enterprise”
- Share only through Zoho Vault, with the lowest possible permission
- Fix passwords flagged by the security dashboard every month
- Lock your vault when you leave your workstation

[↑ Back to index](#)

Part 2 — Administrator Guide

- 13. Users and roles
- 14. Groups and organizational sharing
- 15. Password policies
- 16. Access control and approvals
- 17. Single sign-on to applications
- 18. Audit logs and reports
- 19. Integrations
- 20. Security and compliance
- 21. Editions and licenses
- 22. Deployment checklist

[↑ Back to index](#)

13. Users and roles

13.1 Roles

Role	Controls
Super Admin	Full access: user management, roles, MFA, privacy, integrations, ownership transfer
Admin	All administration operations except user management; approves critical activities
User	Manages their own passwords and those shared with them
Custom roles	Permissions tailored to specific functions, depending on edition

Note — Even a Super Admin does not automatically see every password: they see those classified as “Enterprise” and shared with them, or reach them through emergency access.

13.2 Adding a user

1. Admin > User Management > Users > Invite Users.
2. Enter email addresses or sync from your directory (Microsoft Entra ID, Active Directory, Google Workspace, Okta).
3. Choose the role and add the user to the appropriate groups.
4. The user accepts the invitation and creates their master password.
5. Approve their access to pending shares (awaiting users), if applicable.

Note — In Zoho One, first add the user in the Zoho One console and assign them the Vault app.

13.3 When an employee leaves

1. Transfer ownership of their enterprise passwords to another user (Transfer Ownership).
2. Remove them from groups and revoke their shares.
3. Change the critical passwords they had access to (bank, government, IT administrator).
4. Deactivate and then delete the user to free the license.

Caution — Changing shared passwords when an employee leaves is essential: revoking Zoho Vault access does not erase what the person may have seen or copied.

[↑ Back to index](#)

14. Groups and organizational sharing

14.1 Creating a user group

1. Admin > User Management > User Groups > Create Group.
2. Name the group after the team or function (e.g., Finance, IT, Management).
3. Add members, or sync the group from the directory.
4. Share the team's folders with the group, with the appropriate permission.

14.2 Sharing principles

- Share folders with groups rather than passwords with individuals
- Grant the minimum permission needed (login only when possible)
- Review shares every quarter
- Designate an owner for each team folder

Nuagix tip — Match Zoho Vault groups to your real teams and sync them with the directory: when an employee joins or leaves, their access updates automatically.

[↑ Back to index](#)

15. Password policies

15.1 Creating a policy

1. Admin > Password Policies > Add Policy.
2. Set the minimum and maximum length.
3. Require uppercase, lowercase, numbers and special characters.
4. Prohibit certain characters or reuse of recent passwords.
5. Set a renewal period (e.g., 90 days for critical credentials).
6. Apply the policy by default or to specific types or folders.

15.2 Other enforced settings

Setting	Effect
Master password complexity	Minimum length and complexity required
Lock timeout	Lock after a period of inactivity
Multi-factor authentication	Mandatory for all users
Offline access	Allowed or prohibited
Export and print	Allowed or prohibited by role
Password reset alerts	Reminders when a password reaches its expiry date

Nuagix tip — Enforce a 16-character minimum for generated passwords and multi-factor authentication for everyone: these two measures block most common attacks.

[↑ Back to index](#)

16. Access control and approvals

16.1 Access control workflow

1. Enable Access Control on a sensitive password or folder.
2. Designate the approvers.
3. The user submits an access request, with a reason and a duration.
4. The approver accepts or rejects; access is granted for the set duration and then revoked.
5. If needed, the password is reset automatically after use, depending on edition.

16.2 Other restrictions

- IP restriction: access allowed only from your offices or VPN
- Device and browser restrictions, depending on edition
- Approval of critical activities (export, bulk deletion)
- Email alerts on sensitive events

Note — Approval workflows suit highly privileged credentials: bank accounts, government portals (e.g., Revenu Québec, CRA), administration consoles.

[↑ Back to index](#)

17. Single sign-on to applications

17.1 Principle

Zoho Vault can act as an identity provider (SAML) for your cloud applications. Users sign in to these applications from Zoho Vault without knowing a separate password, and the administrator grants or removes access to each application from a single console.

17.2 Setting up an application

1. Admin > Single Sign-On > Add Application.
2. Choose the application from the catalogue (e.g., Microsoft 365, Google Workspace, Slack) or add a custom SAML application.
3. Copy the Zoho Vault metadata into the application, and the application's metadata into Zoho Vault.
4. Assign the application to users or groups.
5. Test the login with a pilot account before rolling it out.

Caution — Keep a backup administrator account in each SSO-connected application so you do not lose access if the configuration fails.

[↑ Back to index](#)

18. Audit logs and reports

18.1 Audit logs

- Real-time history of access, views, copies, changes and shares
- Administrative operations and policy changes
- Emergency access declarations
- Filters by user, password, action and period
- Forwarding to a SIEM (Syslog) for centralized monitoring, depending on edition

18.2 Reports

Report	Content
Password report	Strength, age, policy compliance
Sharing report	Who has access to what, with which permissions
User activity report	Each user's logins and actions
Access report	Passwords viewed and access requests
Compliance reports	Audit-ready reports, depending on edition

Nuagix tip — Schedule a monthly delivery of the sharing report to managers: they confirm that their team's access is still justified.

[↑ Back to index](#)

19. Integrations

19.1 Zoho integrations

Application	Typical use
Zoho One / Zoho Directory	User provisioning and single sign-on
Zoho Desk	Secure credential access for support agents
Zoho Cliq	View or share a password from Cliq
Zoho Assist	Use credentials during remote support sessions
Zoho WorkDrive	Store encrypted backups

19.2 Other integrations

- Directories: Microsoft Active Directory, Microsoft Entra ID, Google Workspace, Okta, OneLogin
- IT help desk: ServiceNow, Zendesk, Jira Service Management
- SIEM via Syslog for security monitoring
- Extensions for Chrome, Firefox, Edge and Safari
- REST API and command-line interface for automation
- iOS, Android and smartwatch apps

[↑ Back to index](#)

20. Security and compliance

20.1 Security controls

- Local AES-256 encryption: data is encrypted before it leaves the device (zero-knowledge architecture)
- Mandatory multi-factor authentication and single sign-on (SAML) via Zoho Accounts / Zoho Directory
- Access restriction by IP address
- Audit log of all operations
- Scheduled encrypted backups
- Hosting in the Canadian data center (zohocloud.ca)

20.2 Privacy and Quebec Law 25

- Zoho Vault helps demonstrate reasonable security measures to protect personal information
- Limit access to systems containing personal information on a need-to-know basis
- Keep audit logs to document access in case of a confidentiality incident
- Build access revocation into the employee departure procedure
- Document your password policies in your governance policies

Note — This manual is not legal advice. Confirm your obligations with your legal advisor.

20.3 Backup

1. Admin > Backup.
2. Schedule an encrypted backup of enterprise passwords.
3. Choose a secure, restricted-access location.
4. Test restoration at least once a year.

Caution — An unencrypted export exposes all of the organization's passwords. Reserve exporting to the Super Admin and always prefer the encrypted backup.

[↑ Back to index](#)

21. Editions and licenses

21.1 Editions

Edition	For whom
Free (Personal)	Personal use, single user
Standard	Small teams: sharing, folders, basic policies
Professional	Growing teams: groups, reports, emergency access, integrations
Enterprise	Organizations: SSO to applications, access control, SIEM, directories
Zoho One / Workplace	Vault included with the suite's other apps, depending on the plan

Note — Features by edition change over time. See Zoho's pricing page for the current list.

21.2 Tracking usage

Admin > Subscription shows the edition, the number of licenses used and awaiting users. Remove licenses from departed users after transferring their passwords.

[↑ Back to index](#)

22. Deployment checklist

22.1 Before going live

- ☐ Backup Super Admin designated
- ☐ Multi-factor authentication made mandatory
- ☐ Password and master password policies defined
- ☐ Users invited or synced from the directory
- ☐ User groups created by team
- ☐ Team folders created and shared with the right groups
- ☐ Existing passwords imported and source files destroyed
- ☐ Browser extension installed on every workstation
- ☐ Browsers' built-in password managers disabled
- ☐ Emergency access and encrypted backup configured
- ☐ IP restrictions and approval workflows enabled for critical credentials
- ☐ Employee departure procedure updated
- ☐ Users trained and documentation delivered

Nuagix tip — Nuagix can support your team with Zoho Vault setup, integration and training.
Book a Zoom meeting: <https://nuagix.zohobookings.com/#!/andre-martin>

[↑ Back to index](#)

Appendix

A. English-French glossary

[↑ Back to index](#)

A. English-French glossary

A.1 Interface terms

English (interface)	French
Master Password / Passphrase	Phrase maîtresse
Password	Mot de passe
Folder	Dossier
Secure Note	Note sécurisée
Personal	Personnel
Enterprise	Entreprise
Share	Partager
Login only	Connexion seulement
User Group	Groupe d'utilisateurs
Autofill	Remplissage automatique
Password Generator	Générateur de mots de passe
Password Policy	Politique de mots de passe
Emergency Access	Accès d'urgence
Access Control	Contrôle d'accès
Transfer Ownership	Transfert de propriété
Single Sign-On (SSO)	Authentification unique
Audit Log	Journal d'audit
Super Admin	Super administrateur
Backup	Sauvegarde
Trash	Corbeille

[↑ Back to index](#)