



Techniciens informatiques · Optimisation Zoho One



Zoho Vault

Manuel de l'utilisateur et de l'administrateur

→ [Accéder à l'index](#)

Préparé par Nuagix · Septembre 2026

nuagix.ca · support@nuagix.ca

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

Index — Version française

Cliquez sur un titre pour accéder directement à la section. Chaque chapitre se termine par un lien « Retour à l'index ».

PARTIE 1 — GUIDE DE L'UTILISATEUR

1. Introduction et accès à Zoho Vault

- 1.1 À propos de ce manuel
- 1.2 Qu'est-ce que Zoho Vault?
- 1.3 Se connecter

2. Interface et navigation

- 2.1 Éléments de l'interface
- 2.2 Types d'éléments

3. Phrase maîtresse et premier accès

- 3.1 Rôle de la phrase maîtresse
- 3.2 Créer votre phrase maîtresse
- 3.3 Verrouillage automatique

4. Ajouter et gérer les mots de passe

- 4.1 Ajouter un mot de passe
- 4.2 Personnel ou d'entreprise
- 4.3 Importer des mots de passe
- 4.4 Retrouver un mot de passe

5. Dossiers et organisation

- 5.1 Créer un dossier
- 5.2 Bonnes pratiques de classement

6. Partager des mots de passe

- 6.1 Partager un mot de passe ou un dossier
- 6.2 Niveaux de permission
- 6.3 Partage avec des tiers

7. Extension de navigateur et remplissage automatique

- 7.1 Installer l'extension
- 7.2 Remplissage automatique
- 7.3 Désactiver le gestionnaire du navigateur

8. Générateur de mots de passe

- 8.1 Générer un mot de passe
- 8.2 Mots de passe et phrases de passe

9. Audit de sécurité des mots de passe

- 9.1 Tableau de bord de sécurité
- 9.2 Corriger les problèmes

10. Accès d'urgence et accès hors ligne

- 10.1 Accès d'urgence
- 10.2 Accès hors ligne

11. Applications mobiles

11.1 Fonctions

12. Bonnes pratiques

12.1 Recommandations Nuagix

PARTIE 2 — GUIDE DE L'ADMINISTRATEUR

13. Utilisateurs et rôles

13.1 Rôles

13.2 Ajouter un utilisateur

13.3 Départ d'un employé

14. Groupes et partage organisationnel

14.1 Créer un groupe d'utilisateurs

14.2 Principes de partage

15. Politiques de mots de passe

15.1 Créer une politique

15.2 Autres paramètres imposés

16. Contrôle d'accès et approbations

16.1 Flux de contrôle d'accès

16.2 Autres restrictions

17. Authentification unique vers les applications

17.1 Principe

17.2 Configurer une application

18. Journaux d'audit et rapports

18.1 Journaux d'audit

18.2 Rapports

19. Intégrations

19.1 Intégrations Zoho

19.2 Autres intégrations

20. Sécurité et conformité

20.1 Contrôles de sécurité

20.2 Confidentialité et Loi 25

20.3 Sauvegarde

21. Éditions et licences

21.1 Éditions

21.2 Suivre l'utilisation

22. Liste de vérification du déploiement

22.1 Avant la mise en production

ANNEXES

A. Glossaire français-anglais

A.1 Correspondance des termes de l'interface

Partie 1 — Guide de l'utilisateur

1. Introduction et accès à Zoho Vault
2. Interface et navigation
3. Phrase maîtresse et premier accès
4. Ajouter et gérer les mots de passe
5. Dossiers et organisation
6. Partager des mots de passe
7. Extension de navigateur et remplissage automatique
8. Générateur de mots de passe
9. Audit de sécurité des mots de passe
10. Accès d'urgence et accès hors ligne
11. Applications mobiles
12. Bonnes pratiques

[↑ Retour à l'index](#)

1. Introduction et accès à Zoho Vault

1.1 À propos de ce manuel

Ce manuel décrit les fonctionnalités de Zoho Vault offertes aux utilisateurs et les fonctions réservées aux administrateurs, telles qu'offertes en septembre 2026.

Les fonctions disponibles varient selon l'édition (Standard, Professional, Enterprise) et selon la configuration de votre organisation. Les noms anglais des menus sont indiqués entre parenthèses. Par sécurité, aucun exemple de ce manuel ne contient de véritable mot de passe.

1.2 Qu'est-ce que Zoho Vault?

Zoho Vault est le gestionnaire de mots de passe de Zoho pour les équipes et les entreprises. Il conserve de façon chiffrée les mots de passe, les notes sécurisées, les fichiers et les identifiants de votre organisation, permet de les partager sans les révéler, remplit automatiquement les formulaires de connexion dans le navigateur et donne aux administrateurs un contrôle complet : politiques, audit, rapports et authentification unique vers les applications infonuagiques.

1.3 Se connecter

1. Rendez-vous sur <https://vault.zoho.com> (ou <https://vault.zohocloud.ca> si votre organisation est hébergée au centre de données canadien).
2. Connectez-vous avec votre compte Zoho ou l'authentification unique de votre organisation.
3. Si vous utilisez Zoho One, ouvrez le lanceur d'applications et sélectionnez Vault.
4. Validez l'authentification multifacteur avec Zoho OneAuth si elle est exigée.
5. Saisissez votre phrase maîtresse (master password) pour déverrouiller votre coffre.

Conseil Nuagix — Installez l'extension Zoho Vault dans votre navigateur dès le premier jour : c'est elle qui vous fera gagner du temps au quotidien.

[↑ Retour à l'index](#)

2. Interface et navigation

2.1 Éléments de l'interface

Élément	Utilité
Mots de passe (Passwords)	Liste de tous les secrets auxquels vous avez accès
Dossiers (Folders)	Regroupements de mots de passe, partageables avec des utilisateurs ou des groupes
Favoris (Favorites)	Accès rapide aux mots de passe les plus utilisés
Tableau de bord de sécurité	Force des mots de passe, doublons et mots de passe anciens
Partagés avec moi (Shared with me)	Mots de passe que d'autres utilisateurs vous ont partagés
Corbeille (Trash)	Éléments supprimés, restaurables pendant une période limitée
Paramètres (Settings)	Préférences personnelles; administration pour les administrateurs

2.2 Types d'éléments

- Identifiants de site Web ou d'application (nom d'utilisateur, mot de passe, URL)
- Notes sécurisées (codes de récupération, licences, instructions sensibles)
- Fichiers joints chiffrés (certificats, clés, documents)
- Cartes de paiement et renseignements bancaires
- Types personnalisés créés par l'administrateur (ex. : serveur, routeur, borne Wi-Fi)

[↑ Retour à l'index](#)

3. Phrase maîtresse et premier accès

3.1 Rôle de la phrase maîtresse

La phrase maîtresse (master password ou passphrase) chiffre et déchiffre vos données directement dans votre appareil. Zoho ne la connaît pas et ne la conserve pas : c'est ce qui garantit que personne, pas même Zoho, ne peut lire vos mots de passe.

Elle est distincte du mot de passe de votre compte Zoho, qui sert seulement à vous authentifier.

3.2 Créer votre phrase maîtresse

1. À votre premier accès, Zoho Vault vous demande de créer une phrase maîtresse.
2. Choisissez une phrase longue, composée de plusieurs mots sans lien entre eux, facile à retenir pour vous seul.
3. Ne réutilisez jamais une phrase déjà employée ailleurs.
4. Saisissez un indice qui ne révèle pas la phrase elle-même, si l'option est offerte.
5. Confirmez la phrase et déverrouillez votre coffre.

Attention — Si vous oubliez votre phrase maîtresse, Zoho ne peut pas la récupérer. Dans une organisation, l'administrateur peut réinitialiser votre accès, mais vos mots de passe personnels non partagés peuvent être perdus.

3.3 Verrouillage automatique

- Le coffre se verrouille après une période d'inactivité définie
- L'extension de navigateur se verrouille à la fermeture du navigateur, selon les paramètres
- Le déverrouillage par biométrie est possible sur les appareils mobiles compatibles
- L'administrateur peut imposer un délai maximal de verrouillage

[↑ Retour à l'index](#)

4. Ajouter et gérer les mots de passe

4.1 Ajouter un mot de passe

1. Cliquez sur Ajouter un mot de passe (Add Password).
2. Choisissez le type (site Web, application, carte, note sécurisée ou type personnalisé).
3. Saisissez le nom, l'URL, le nom d'utilisateur et le mot de passe (ou générez-le).
4. Ajoutez des étiquettes, une description et, au besoin, un fichier joint.
5. Classez-le dans un dossier et indiquez s'il est personnel ou d'entreprise.
6. Enregistrez.

4.2 Personnel ou d'entreprise

Classement	Effet
Personnel (Personal)	Visible par vous seul; ne peut pas être partagé
Entreprise (Enterprise)	Appartient à l'organisation; peut être partagé et est récupérable par l'administrateur

Conseil Nuagix — Classez en « Entreprise » tous les accès qui servent au travail (fournisseurs, sites gouvernementaux, outils infonuagiques) : l'organisation ne les perdra pas au départ d'un employé.

4.3 Importer des mots de passe

1. Paramètres > Importer des mots de passe (Import Passwords).
2. Choisissez la source : fichier CSV, autre gestionnaire de mots de passe ou navigateur.
3. Associez les colonnes aux champs de Zoho Vault.
4. Choisissez le dossier et la classification de destination.
5. Lancez l'importation, vérifiez les éléments importés puis supprimez le fichier source.

Attention — Un fichier d'exportation contient vos mots de passe en clair. Supprimez-le définitivement (y compris de la corbeille et des téléchargements) dès l'importation terminée.

4.4 Retrouver un mot de passe

- Recherche par nom, URL, nom d'utilisateur ou étiquette
- Filtres par dossier, type, classification ou propriétaire
- Copier le nom d'utilisateur ou le mot de passe sans l'afficher
- Historique des versions précédentes d'un mot de passe

[↑ Retour à l'index](#)

5. Dossiers et organisation

5.1 Créer un dossier

1. Onglet Dossiers (Folders) > Ajouter un dossier.
2. Nommez le dossier (ex. : Comptabilité, Fournisseurs TI, Médias sociaux).
3. Créez des sous-dossiers au besoin.
4. Déplacez les mots de passe dans le dossier par glisser-déposer ou par action en masse.

5.2 Bonnes pratiques de classement

- Un dossier par équipe ou par fonction plutôt que par personne
- Des noms clairs et cohérents pour toute l'organisation
- Des étiquettes pour les classements transversaux (ex. : client, projet)
- Les favoris pour les mots de passe d'usage quotidien

Conseil Nuagix — Structurez les dossiers selon les groupes qui doivent y accéder : le partage d'un dossier complet est beaucoup plus simple à gérer que des partages un par un.

[↑ Retour à l'index](#)

6. Partager des mots de passe

6.1 Partager un mot de passe ou un dossier

1. Sélectionnez le mot de passe ou le dossier et cliquez sur Partager (Share).
2. Choisissez les utilisateurs ou les groupes d'utilisateurs.
3. Attribuez le niveau de permission.
4. Confirmez : le partage est chiffré de bout en bout pour chaque destinataire.

6.2 Niveaux de permission

Permission	Ce que le destinataire peut faire
Connexion seulement (Login only)	Se connecter par l'extension sans voir le mot de passe
Voir (View)	Voir et copier le mot de passe
Modifier (Modify)	Voir et modifier le mot de passe
Gérer (Manage)	Modifier, supprimer et partager à son tour

Conseil Nuagix — Utilisez la permission Connexion seulement pour les stagiaires, les contractuels et les comptes partagés : ils travaillent normalement sans jamais connaître le mot de passe.

6.3 Partage avec des tiers

- Partager un mot de passe avec une personne externe pour une durée limitée, selon l'édition
- Révoquer le partage à tout moment
- Changer le mot de passe après la fin d'un mandat externe
- Ne jamais transmettre un mot de passe par courriel, clavardage ou texto

Attention — Ne partagez jamais un mot de passe en dehors de Zoho Vault. Un mot de passe envoyé par courriel reste lisible dans les boîtes de réception et les sauvegardes.

[↑ Retour à l'index](#)

7. Extension de navigateur et remplissage automatique

7.1 Installer l'extension

1. Installez l'extension Zoho Vault pour Chrome, Firefox, Edge ou Safari depuis la boutique du navigateur.
2. Cliquez sur l'icône Zoho Vault et connectez-vous.
3. Déverrouillez le coffre avec votre phrase maîtresse.
4. Épinglez l'icône dans la barre d'outils pour y accéder rapidement.

7.2 Remplissage automatique

- Remplissage des identifiants en un clic sur les pages de connexion reconnues
- Connexion automatique aux sites configurés
- Proposition d'enregistrer les nouveaux identifiants saisis
- Mise à jour proposée lorsque vous changez un mot de passe sur un site
- Remplissage des cartes de paiement et des formulaires, selon l'édition
- Ouverture directe d'un site à partir de l'extension

Note — Si un site n'est pas reconnu, vérifiez que l'URL enregistrée correspond bien à la page de connexion.

7.3 Désactiver le gestionnaire du navigateur

Pour éviter que les mots de passe soient enregistrés à deux endroits, désactivez l'enregistrement des mots de passe dans le navigateur (Chrome, Edge, Firefox ou Safari), puis importez dans Zoho Vault les mots de passe qui y étaient conservés.

[↑ Retour à l'index](#)

8. Générateur de mots de passe

8.1 Générer un mot de passe

1. Dans le formulaire d'ajout ou dans l'extension, cliquez sur l'icône du générateur.
2. Choisissez la longueur (16 caractères ou plus recommandés).
3. Incluez majuscules, minuscules, chiffres et caractères spéciaux, selon les exigences du site.
4. Cliquez sur Générer, puis utilisez le mot de passe proposé.

8.2 Mots de passe et phrases de passe

Type	Quand l'utiliser
Mot de passe aléatoire	Sites et applications, puisque Zoho Vault s'en souvient pour vous
Phrase de passe (passphrase)	Ce que vous devez saisir de mémoire : phrase maîtresse, session d'ordinateur
Mot de passe conforme à une politique	Mot de passe généré selon la politique définie par l'administrateur

Conseil Nuagix — Avec un gestionnaire de mots de passe, vous n'avez plus besoin de retenir vos mots de passe : générez-les longs et uniques pour chaque site.

[↑ Retour à l'index](#)

9. Audit de sécurité des mots de passe

9.1 Tableau de bord de sécurité

Indicateur	Signification
Mots de passe faibles	Trop courts ou trop simples
Mots de passe réutilisés	Même mot de passe utilisé sur plusieurs sites
Mots de passe anciens	Pas changés depuis longtemps
Non conformes à la politique	Ne respectent pas la politique de l'organisation
Mots de passe compromis	Détectés dans des fuites de données connues, selon l'édition

9.2 Corriger les problèmes

1. Ouvrez le tableau de bord de sécurité et triez par gravité.
2. Commencez par les mots de passe compromis et réutilisés.
3. Changez le mot de passe sur le site, puis mettez-le à jour dans Zoho Vault (ou utilisez la réinitialisation en un clic si elle est offerte pour ce site).
4. Vérifiez que votre score de sécurité s'améliore.

Conseil Nuagix — Réservez 15 minutes chaque mois pour corriger les mots de passe signalés : c'est l'une des mesures de cybersécurité les plus rentables pour une PME.

[↑ Retour à l'index](#)

10. Accès d'urgence et accès hors ligne

10.1 Accès d'urgence

L'accès d'urgence (Emergency Access) permet à des personnes désignées par l'organisation d'accéder à des mots de passe critiques en cas d'absence ou d'incident, au moyen d'un compte d'urgence (break-glass). Chaque déclaration d'urgence est journalisée et les administrateurs en sont avisés.

Selon l'édition, l'accès d'urgence est configuré par le super administrateur.

10.2 Accès hors ligne

- Fichier de sauvegarde hors ligne chiffré, protégé par une phrase distincte, selon les paramètres
- Consultation dans les applications mobiles sans connexion Internet
- Utile en cas de panne réseau ou pour les situations de continuité des activités
- L'administrateur peut autoriser ou interdire l'accès hors ligne

Attention — Conservez tout fichier hors ligne dans un emplacement sûr et chiffré. Ne le copiez jamais sur une clé USB non chiffrée ni dans un dossier partagé.

[↑ Retour à l'index](#)

11. Applications mobiles

11.1 Fonctions

- Consulter, ajouter et modifier des mots de passe sur iOS et Android
- Déverrouillage par Face ID, Touch ID ou empreinte digitale
- Remplissage automatique dans les applications et les navigateurs mobiles
- Générateur de mots de passe intégré
- Accès hors ligne selon les paramètres de l'organisation
- Montre connectée pour les éléments favoris, selon l'appareil

[↑ Retour à l'index](#)

12. Bonnes pratiques

12.1 Recommandations Nuagix

- Choisissez une phrase maîtresse longue et unique et ne la notez nulle part en clair
- Utilisez un mot de passe différent, généré par Zoho Vault, pour chaque site
- Activez l'authentification multifacteur sur tous les sites qui l'offrent et conservez les codes de récupération dans une note sécurisée
- Classez en « Entreprise » tous les accès liés au travail
- Partagez uniquement par Zoho Vault, avec la permission la plus faible possible
- Corrigez chaque mois les mots de passe signalés par le tableau de bord de sécurité
- Verrouillez votre coffre lorsque vous quittez votre poste

[↑ Retour à l'index](#)

Partie 2 — Guide de l'administrateur

- 13. Utilisateurs et rôles
- 14. Groupes et partage organisationnel
- 15. Politiques de mots de passe
- 16. Contrôle d'accès et approbations
- 17. Authentification unique vers les applications
- 18. Journaux d'audit et rapports
- 19. Intégrations
- 20. Sécurité et conformité
- 21. Éditions et licences
- 22. Liste de vérification du déploiement

[↑ Retour à l'index](#)

13. Utilisateurs et rôles

13.1 Rôles

Rôle	Contrôle
Super administrateur (Super Admin)	Accès complet : gestion des utilisateurs, rôles, MFA, confidentialité, intégrations, transfert de propriété
Administrateur (Admin)	Toutes les opérations d'administration sauf la gestion des utilisateurs; approuve les activités critiques
Utilisateur (User)	Gère ses propres mots de passe et ceux qu'on lui partage
Rôles personnalisés	Permissions ajustées à des fonctions précises, selon l'édition

Note — Même un super administrateur ne voit pas automatiquement tous les mots de passe : il voit ceux qui sont classés « Entreprise » et partagés avec lui, ou y accède par l'accès d'urgence.

13.2 Ajouter un utilisateur

1. Administration (Admin) > Gestion des utilisateurs (User Management) > Utilisateurs > Inviter des utilisateurs.
2. Saisissez les adresses courriel ou synchronisez depuis votre annuaire (Microsoft Entra ID, Active Directory, Google Workspace, Okta).
3. Choisissez le rôle et ajoutez l'utilisateur aux groupes appropriés.
4. L'utilisateur accepte l'invitation et crée sa phrase maîtresse.
5. Approuvez son accès aux partages en attente (utilisateurs en attente), s'il y a lieu.

Note — Dans Zoho One, ajoutez d'abord l'utilisateur dans la console Zoho One et attribuez-lui l'application Vault.

13.3 Départ d'un employé

1. Transférez la propriété de ses mots de passe d'entreprise à un autre utilisateur (Transfer Ownership).
2. Retirez-le des groupes et révoquez ses partages.
3. Changez les mots de passe critiques auxquels il avait accès (banque, gouvernement, administrateur TI).
4. Désactivez puis supprimez l'utilisateur pour libérer la licence.

Attention — Changer les mots de passe partagés au départ d'un employé est essentiel : révoquer l'accès à Zoho Vault n'efface pas ce que la personne a pu voir ou copier.

[↑ Retour à l'index](#)

14. Groupes et partage organisationnel

14.1 Créer un groupe d'utilisateurs

1. Administration > Gestion des utilisateurs > Groupes d'utilisateurs (User Groups) > Créer un groupe.
2. Nommez le groupe selon l'équipe ou la fonction (ex. : Finances, TI, Direction).
3. Ajoutez les membres, ou synchronisez le groupe depuis l'annuaire.
4. Partagez les dossiers de l'équipe avec le groupe, avec la permission appropriée.

14.2 Principes de partage

- Partager des dossiers avec des groupes plutôt que des mots de passe avec des personnes
- Accorder la permission minimale nécessaire (connexion seulement si possible)
- Réviser les partages chaque trimestre
- Désigner un responsable pour chaque dossier d'équipe

Conseil Nuagix — Faites correspondre les groupes Zoho Vault à vos équipes réelles et synchronisez-les avec l'annuaire : l'arrivée ou le départ d'un employé met ses accès à jour automatiquement.

[↑ Retour à l'index](#)

15. Politiques de mots de passe

15.1 Créer une politique

1. Administration > Politiques de mots de passe (Password Policies) > Ajouter une politique.
2. Définissez la longueur minimale et maximale.
3. Exigez majuscules, minuscules, chiffres et caractères spéciaux.
4. Interdisez certains caractères ou la réutilisation des derniers mots de passe.
5. Fixez une période de renouvellement (ex. : 90 jours pour les accès critiques).
6. Appliquez la politique par défaut ou à des types ou dossiers précis.

15.2 Autres paramètres imposés

Paramètre	Effet
Complexité de la phrase maîtresse	Longueur et complexité minimales exigées
Délai de verrouillage	Verrouillage après une période d'inactivité
Authentification multifacteur	Obligatoire pour tous les utilisateurs
Accès hors ligne	Autorisé ou interdit
Exportation et impression	Autorisées ou interdites selon le rôle
Alertes de réinitialisation	Rappels lorsqu'un mot de passe atteint sa date d'expiration

Conseil Nuagix — Imposez 16 caractères minimum pour les mots de passe générés et l'authentification multifacteur pour tous : ces deux mesures bloquent la majorité des attaques courantes.

[↑ Retour à l'index](#)

16. Contrôle d'accès et approbations

16.1 Flux de contrôle d'accès

1. Activez le contrôle d'accès (Access Control) sur un mot de passe ou un dossier sensible.
2. Désignez les approbateurs.
3. L'utilisateur soumet une demande d'accès, avec un motif et une durée.
4. L'approbateur accepte ou refuse; l'accès est accordé pour la durée prévue puis révoqué.
5. Au besoin, le mot de passe est réinitialisé automatiquement après usage, selon l'édition.

16.2 Autres restrictions

- Restriction par adresse IP : accès permis seulement depuis vos bureaux ou votre RPV
- Restriction des appareils et des navigateurs, selon l'édition
- Approbation des activités critiques (exportation, suppression en masse)
- Alertes par courriel sur les événements sensibles

Note — Les flux d'approbation conviennent aux accès à privilèges élevés : comptes bancaires, portails gouvernementaux (ex. : Revenu Québec, ARC), consoles d'administration.

[↑ Retour à l'index](#)

17. Authentification unique vers les applications

17.1 Principe

Zoho Vault peut servir de fournisseur d'identité (SAML) pour vos applications infonuagiques. Les utilisateurs se connectent à ces applications depuis Zoho Vault sans connaître de mot de passe distinct, et l'administrateur accorde ou retire l'accès à chaque application depuis une seule console.

17.2 Configurer une application

1. Administration > Authentification unique (Single Sign-On) > Ajouter une application.
2. Choisissez l'application dans le catalogue (ex. : Microsoft 365, Google Workspace, Slack) ou ajoutez une application SAML personnalisée.
3. Copiez les métadonnées Zoho Vault dans l'application, et celles de l'application dans Zoho Vault.
4. Attribuez l'application aux utilisateurs ou aux groupes.
5. Testez la connexion avec un compte pilote avant de l'étendre.

Attention — Conservez un compte administrateur de secours dans chaque application reliée par SSO pour ne pas perdre l'accès en cas de problème de configuration.

[↑ Retour à l'index](#)

18. Journaux d'audit et rapports

18.1 Journaux d'audit

- Historique en temps réel des accès, consultations, copies, modifications et partages
- Opérations administratives et changements de politiques
- Déclarations d'accès d'urgence
- Filtres par utilisateur, par mot de passe, par action et par période
- Envoi vers un SIEM (Syslog) pour la surveillance centralisée, selon l'édition

18.2 Rapports

Rapport	Contenu
Rapport sur les mots de passe	Force, âge, conformité aux politiques
Rapport de partage	Qui a accès à quoi, avec quelles permissions
Rapport d'activité des utilisateurs	Connexions et actions de chaque utilisateur
Rapport sur les accès	Mots de passe consultés et demandes d'accès
Rapports de conformité	Rapports prêts pour les vérifications, selon l'édition

Conseil Nuagix — Planifiez un envoi mensuel du rapport de partage aux gestionnaires : ils valident ainsi que les accès de leur équipe sont toujours justifiés.

[↑ Retour à l'index](#)

19. Intégrations

19.1 Intégrations Zoho

Application	Utilisation typique
Zoho One / Zoho Directory	Provisionnement des utilisateurs et authentification unique
Zoho Desk	Accès sécurisé aux identifiants pour les agents de soutien
Zoho Cliq	Consulter ou partager un mot de passe depuis Cliq
Zoho Assist	Utiliser les identifiants lors de sessions de soutien à distance
Zoho WorkDrive	Stocker les sauvegardes chiffrées

19.2 Autres intégrations

- Annuaires : Microsoft Active Directory, Microsoft Entra ID, Google Workspace, Okta, OneLogin
- Soutien TI : ServiceNow, Zendesk, Jira Service Management
- SIEM par Syslog pour la surveillance de sécurité
- Extensions pour Chrome, Firefox, Edge et Safari
- API REST et interface en ligne de commande pour l'automatisation
- Applications iOS, Android et montre connectée

[↑ Retour à l'index](#)

20. Sécurité et conformité

20.1 Contrôles de sécurité

- Chiffrement AES-256 local : les données sont chiffrées avant de quitter l'appareil (architecture à connaissance nulle)
- Authentification multifacteur obligatoire et authentification unique (SAML) via Zoho Accounts / Zoho Directory
- Restriction des accès par adresse IP
- Journal d'audit de toutes les opérations
- Sauvegardes chiffrées planifiées
- Hébergement au centre de données canadien (zohocloud.ca)

20.2 Confidentialité et Loi 25

- Zoho Vault aide à démontrer des mesures de sécurité raisonnables pour protéger les renseignements personnels
- Limitez l'accès aux systèmes contenant des renseignements personnels selon le principe du besoin de savoir
- Conservez les journaux d'audit pour documenter les accès en cas d'incident de confidentialité
- Intégrez la révocation des accès à la procédure de départ des employés
- Documentez vos politiques de mots de passe dans vos politiques de gouvernance

Note — Ce manuel n'est pas un avis juridique. Validez vos obligations avec votre conseiller juridique.

20.3 Sauvegarde

1. Administration > Sauvegarde (Backup).
2. Planifiez une sauvegarde chiffrée des mots de passe d'entreprise.
3. Choisissez un emplacement sécurisé et à accès restreint.
4. Testez la restauration au moins une fois par année.

Attention — Une exportation non chiffrée expose tous les mots de passe de l'organisation. Réservez l'exportation au super administrateur et privilégiez toujours la sauvegarde chiffrée.

[↑ Retour à l'index](#)

21. Éditions et licences

21.1 Éditions

Édition	Pour qui
Gratuite (Personal)	Usage personnel, un seul utilisateur
Standard	Petites équipes : partage, dossiers, politiques de base
Professional	Équipes en croissance : groupes, rapports, accès d'urgence, intégrations
Enterprise	Organisations : SSO vers les applications, contrôle d'accès, SIEM, annuaires
Zoho One / Workplace	Vault inclus avec les autres applications de la suite, selon l'offre

Note — Les fonctions offertes par édition évoluent. Consultez la page des tarifs de Zoho pour la liste à jour.

21.2 Suivre l'utilisation

Administration > Abonnement (Subscription) affiche l'édition, le nombre de licences utilisées et les utilisateurs en attente. Retirez les licences des utilisateurs partis après le transfert de leurs mots de passe.

[↑ Retour à l'index](#)

22. Liste de vérification du déploiement

22.1 Avant la mise en production

- ☐ Super administrateur de secours désigné
- ☐ Authentification multifacteur rendue obligatoire
- ☐ Politiques de mots de passe et de phrase maîtresse définies
- ☐ Utilisateurs invités ou synchronisés depuis l'annuaire
- ☐ Groupes d'utilisateurs créés selon les équipes
- ☐ Dossiers d'équipe créés et partagés avec les bons groupes
- ☐ Mots de passe existants importés et fichiers sources détruits
- ☐ Extension de navigateur installée sur tous les postes
- ☐ Gestionnaire de mots de passe des navigateurs désactivé
- ☐ Accès d'urgence et sauvegarde chiffrée configurés
- ☐ Restrictions IP et flux d'approbation activés pour les accès critiques
- ☐ Procédure de départ des employés mise à jour
- ☐ Utilisateurs formés et documentation remise

Conseil Nuagix — Nuagix peut accompagner votre équipe dans la configuration, l'intégration et la formation Zoho Vault. Réservez une rencontre Zoom :
<https://nuagix.zohobookings.com/#!/andre-martin>

[↑ Retour à l'index](#)

Annexes

A. Glossaire français-anglais

[↑ Retour à l'index](#)

A. Glossaire français-anglais

A.1 Correspondance des termes de l'interface

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

[↑ Retour à l'index](#)