



GUIDE DE SÉCURITÉ

Sécuriser au mieux votre installation

Protéger vos données contre la panne, le vol et les rançongiciels

À retenir

Prévoyez une heure et deux supports de sauvegarde, par exemple deux clés USB ou deux disques externes. À la fin de ce guide, votre comptabilité survivra à une panne de disque, à un vol de l'ordinateur et à un rançongiciel.

Pour toute personne qui utilise Simple ERP pour son activité professionnelle

Simple ERP Standard - Documentation utilisateur - Août 2026



Sommaire

Cliquez sur un chapitre pour y accéder directement dans votre lecteur PDF.

Avant de commencer	4
Les trois risques réels	4
Protéger la base avec une phrase de passe	4
Activer la protection	4
Choisir une phrase solide et mémorisable	5
Conserver la clé de secours	5
Organiser vos sauvegardes	5
La règle des trois copies	5
Choisir vos supports	6
Configurer la sauvegarde automatique	6
Le geste hebdomadaire	6
Si vous voulez une copie hors du local sans y penser	7
Vérifier que vos sauvegardes fonctionnent	7
Le test de restauration, deux fois par an	7
Les signes qui doivent vous alerter	7
Protéger l'accès à l'ordinateur	8
Les réglages de base	8
Les mises à jour du système	8
Utiliser la synchronisation mobile sans risque	8
Au moment de l'appairage	8
Au quotidien	8
Contrôler les appareils autorisés	9
Installer les mises à jour de Simple ERP	9
Reconnaître et traiter un rançongiciel	10
Les signes	10
Ce qu'il faut faire, dans l'ordre	10



Simple ERP

L'ERP 100 % local, privé et conforme

Pensé pour les entrepreneurs et les TPE

www.simple-erp.fr

Si des données personnelles de clients ont pu être consultées	10
Votre routine de contrôle	11
Chaque semaine	11
Chaque trimestre	11
Deux fois par an	11
Chaque année	11
Obtenir de l'aide	11



Avant de commencer

Vos données Simple ERP restent sur votre ordinateur. C'est un avantage : elles ne transitent par aucun service en ligne et personne d'autre que vous n'y accède. C'est aussi une responsabilité : leur protection dépend de vous, pas d'un prestataire.

Ce guide rassemble tout ce que vous pouvez faire pour que votre fichier client, vos devis et vos factures survivent à un incident. Aucune connaissance technique n'est nécessaire.

Les trois risques réels

Trois choses seulement peuvent vous faire perdre votre comptabilité. Elles se traitent différemment.

- **La panne.** Un disque dur meurt sans prévenir, souvent au bout de trois à cinq ans. C'est le cas le plus fréquent et le plus banal.
- **Le vol ou la perte.** Un ordinateur portable disparaît d'un véhicule ou d'un chantier. Vous perdez les données, et quelqu'un d'autre les récupère.
- **Le rançongiciel.** Un programme malveillant chiffre tous vos fichiers et réclame une rançon. Il arrive le plus souvent par une pièce jointe ou un lien dans un e-mail qui semble légitime.

La phrase de passe traite le deuxième risque. La sauvegarde traite le premier et le troisième. Vous avez besoin des deux : elles ne se remplacent pas.

Bon à savoir

Ce guide ne demande aucun abonnement et aucun service en ligne. Les protections décrites reposent uniquement sur Simple ERP, sur votre ordinateur et sur les supports que vous possédez.

Protéger la base avec une phrase de passe

C'est la première chose à faire, avant même la sauvegarde. Sans elle, n'importe qui ouvrant votre ordinateur lit l'intégralité de votre fichier client.

Activer la protection

- 1 Ouvrez **Paramètres > Sécurité**.
- 2 Choisissez l'option permettant de protéger ou chiffrer la base.
- 3 Saisissez une phrase d'au moins douze caractères.
- 4 Confirmez-la une seconde fois.
- 5 Ajoutez un indice si vous le souhaitez, sans jamais révéler la phrase.
- 6 Validez.
- 7 Lorsque la clé de secours apparaît, enregistrez-la immédiatement.



Choisir une phrase solide et mémorisable

Une bonne phrase est longue avant d'être compliquée. Quatre mots sans rapport entre eux valent mieux qu'un mot court avec des caractères spéciaux.

- Assemblez plusieurs mots qui n'ont rien à voir, par exemple **charpente vélo mandarine 1987**.
- Comptez au moins douze caractères, idéalement plus de seize.
- N'utilisez pas le nom de l'entreprise, un prénom, une date de naissance ou une plaque d'immatriculation.
- N'utilisez pas la même phrase que votre messagerie ou votre banque.
- Notez-la dans un gestionnaire de mots de passe, ou sur papier dans un endroit fermé à clé.

Conserver la clé de secours

La clé de secours permet de rouvrir la base si vous oubliez la phrase. Elle doit être conservée **ailleurs que sur l'ordinateur**.

- 1 Imprimez-la ou recopiez-la à la main.
- 2 Rangez-la dans un endroit fermé, à un autre endroit que l'ordinateur.
- 3 Placez une seconde copie chez un proche de confiance, chez votre comptable ou dans un coffre.
- 4 Notez dans votre agenda, une fois par an, de vérifier que vous savez toujours où elle se trouve.

Danger

Si vous perdez à la fois la phrase de passe et la clé de secours, la base est définitivement illisible. Le support Simple ERP ne possède aucune clé universelle et aucune porte dérobée. Personne ne pourra rouvrir vos données.

Organiser vos sauvegardes

C'est le chapitre le plus important du guide. Une sauvegarde mal organisée donne un faux sentiment de sécurité et ne sert à rien le jour de l'incident.

La règle des trois copies

Retenez trois chiffres : **3, 2, 1**.

- **3 copies** de vos données : celle de travail sur l'ordinateur, plus deux sauvegardes.
- **2 supports différents** : le disque de l'ordinateur et un support externe.
- **1 copie hors du local** : chez vous si l'ordinateur est à l'atelier, ou l'inverse.

La troisième ligne est celle qu'on oublie, et c'est celle qui vous sauve en cas d'incendie, de dégât des eaux ou de cambriolage.



Choisir vos supports

Prévoyez **deux supports**, pas un seul. Vous les utiliserez en alternance.

- Une clé USB de bonne qualité suffit pour la plupart des activités. Comptez 32 Go.
- Un petit disque externe convient mieux si vous conservez beaucoup de documents et de photos de chantier.
- Étiquetez-les physiquement **Sauvegarde A** et **Sauvegarde B**.
- N'utilisez pas ces supports pour autre chose. Pas de photos de famille, pas de transfert de fichiers, pas de prêt à un client.

À retenir

Deux supports ne coûtent pas beaucoup plus cher qu'un seul, et c'est précisément ce qui vous protège du rançongiciel. Un support resté branché en permanence sera chiffré en même temps que votre ordinateur.

Configurer la sauvegarde automatique

- 1 Ouvrez **Paramètres > Sauvegardes**.
- 2 Activez la sauvegarde automatique.
- 3 Choisissez le dossier de destination sur votre support externe.
- 4 Vérifiez que la conservation de l'historique est activée.
- 5 Enregistrez.

Simple ERP conserve plusieurs versions successives plutôt qu'une seule copie écrasée à chaque fois. C'est essentiel : cela vous permet de revenir à une version antérieure si un problème n'est découvert que plusieurs jours plus tard.

Le geste hebdomadaire

Une seule habitude à prendre, et tout le reste en découle.

- 1 Chaque vendredi, branchez le support qui n'était pas utilisé la semaine passée.
- 2 Ouvrez Simple ERP et laissez la sauvegarde se faire.
- 3 Vérifiez le message de confirmation.
- 4 **Débranchez le support** et rangez-le.
- 5 Emportez régulièrement l'un des deux supports hors du local.

Attention

Un support branché en permanence n'est pas une sauvegarde. C'est un deuxième disque, et un rançongiciel le chiffrera aussi sûrement que le premier. Le geste qui protège, c'est de débrancher.



Si vous voulez une copie hors du local sans y penser

Vous pouvez déposer une copie de votre sauvegarde sur un espace de stockage en ligne qui vous appartient : celui inclus dans votre messagerie, un espace loué chez un hébergeur, ou un boîtier de stockage installé à votre domicile.

Le fichier de sauvegarde est déjà chiffré par Simple ERP avant de quitter votre ordinateur. Le prestataire qui l'héberge ne peut pas le lire, et Simple ERP n'y a pas accès non plus. Vos données restent les vôtres.

Conseil

C'est la façon la plus simple de satisfaire la troisième règle sans avoir à transporter un support. Elle ne remplace pas les deux supports physiques : elle s'y ajoute.

Vérifier que vos sauvegardes fonctionnent

Une sauvegarde jamais testée n'est pas une sauvegarde. C'est une hypothèse.

Le test de restauration, deux fois par an

- 1 Branchez l'un de vos supports.
- 2 Ouvrez **Paramètres > Données & sync.**
- 3 Restaurez la sauvegarde **sous un autre nom de base**, par exemple **TEST-restauration**.
- 4 Déverrouillez-la avec votre phrase de passe.
- 5 Ouvrez trois ou quatre factures récentes et vérifiez leur contenu.
- 6 Vérifiez que vos clients et vos produits sont bien présents.
- 7 Supprimez la base de test une fois le contrôle terminé.

Ce test vérifie trois choses d'un coup : le support fonctionne, le fichier n'est pas corrompu, et vous connaissez toujours votre phrase de passe.

Attention

Restaurez toujours sous un nouveau nom. Ne restaurez jamais par-dessus votre base de travail pour faire un test : une erreur de manipulation écraserait vos données réelles.

Les signes qui doivent vous alerter

- Simple ERP signale qu'un support n'a pas été vu depuis plus de deux semaines.
- Une sauvegarde échoue deux fois de suite.
- Le support met anormalement longtemps à répondre, ou fait un bruit inhabituel.
- Le nombre de sauvegardes conservées n'augmente plus.



Dans tous ces cas, remplacez le support sans attendre. Une clé USB est un consommable, pas un équipement définitif.

Protéger l'accès à l'ordinateur

La meilleure phrase de passe ne sert à rien si l'ordinateur reste ouvert et accessible.

Les réglages de base

- 1 Mettez un mot de passe sur votre session Windows, macOS ou Linux. Pas de session sans mot de passe.
- 2 Réglez le verrouillage automatique de l'écran sur cinq minutes d'inactivité.
- 3 Prenez l'habitude de verrouiller manuellement en quittant votre poste. Sur Windows, appuyez sur la touche Windows et sur L.
- 4 Activez le chiffrement du disque proposé par votre système : BitLocker sur Windows Professionnel, FileVault sur macOS.
- 5 Si plusieurs personnes utilisent l'ordinateur, créez une session distincte pour chacune.

Les mises à jour du système

Laissez les mises à jour de sécurité de Windows ou de macOS s'installer. La très grande majorité des rançongiciels exploitent des failles corrigées depuis des mois sur les machines à jour.

Sur Windows, activez également la protection contre les rançongiciels intégrée : ouvrez **Sécurité Windows**, puis **Protection contre les virus et menaces**, puis **Gérer la protection contre les rançongiciels**, et activez **Accès contrôlé aux dossiers**. Autorisez ensuite Simple ERP lorsque le système le demande.

Conseil

Un antivirus payant n'est pas nécessaire. Celui intégré à Windows est efficace s'il est à jour et si vous ne le désactivez pas.

Utiliser la synchronisation mobile sans risque

L'application mobile communique avec votre ordinateur par le réseau local. Quelques précautions suffisent.

Au moment de l'appairage

- 1 Réalisez l'appairage chez vous ou dans votre local, sur **votre** réseau Wi-Fi.
- 2 Ne réalisez jamais un appairage sur un réseau public : gare, hôtel, café, réseau d'un client ou d'un chantier.
- 3 Vérifiez que le QR code affiché provient bien de votre ordinateur.
- 4 Confirmez l'appairage sur l'ordinateur quand Simple ERP vous le demande.

Au quotidien



- Protégez le téléphone par un code, une empreinte ou une reconnaissance faciale.
- Synchronisez de préférence sur votre réseau habituel.
- N'utilisez pas la synchronisation sur un Wi-Fi ouvert sans mot de passe.

Contrôler les appareils autorisés

- 1 Ouvrez **Paramètres > Données & sync.**
- 2 Consultez la liste des appareils appairés.
- 3 Vérifiez que vous reconnaissez chacun d'eux et sa date de dernière utilisation.
- 4 Révoquez immédiatement tout appareil inconnu, vendu, perdu ou appartenant à un ancien salarié.

À retenir

Faites ce contrôle tous les trois mois, et systématiquement après la perte ou le remplacement d'un téléphone. Un appareil révoqué perd instantanément tout accès.

Installer les mises à jour de Simple ERP

Chaque mise à jour est signée électroniquement par Simple ERP. Votre ordinateur vérifie cette signature avant d'installer quoi que ce soit, et refuse toute mise à jour qui ne serait pas authentique.

- 1 Acceptez les mises à jour lorsque Simple ERP vous les propose.
- 2 Ne téléchargez jamais Simple ERP ailleurs que depuis le site officiel **simple-erp.fr** ou depuis l'application elle-même.
- 3 Méfiez-vous de tout e-mail vous invitant à installer une mise à jour depuis une pièce jointe ou un lien. Simple ERP ne procède jamais ainsi.
- 4 Faites une sauvegarde avant une mise à jour importante, par prudence.

Attention

Aucun message légitime de Simple ERP ne vous demandera votre phrase de passe, votre clé de secours ou votre mot de passe de session. Le support n'en a jamais besoin.



Reconnaître et traiter un rançongiciel

Les signes

- Vos fichiers ont changé de nom ou d'extension et ne s'ouvrent plus.
- Un message à l'écran réclame un paiement pour récupérer vos données.
- Un fichier texte inhabituel apparaît dans plusieurs dossiers.
- L'ordinateur ralentit fortement et le disque travaille en permanence sans raison.

Ce qu'il faut faire, dans l'ordre

- 1 **Débranchez le câble réseau et coupez le Wi-Fi immédiatement.** C'est le geste le plus urgent : il empêche la propagation.
- 2 **Débranchez tout support de sauvegarde encore connecté.**
- 3 **N'éteignez pas l'ordinateur brutalement** si vous envisagez une analyse ultérieure.
- 4 **Ne payez pas la rançon.** Le paiement ne garantit rien, finance l'activité criminelle et vous désigne comme cible pour la suite.
- 5 **Ne rebranchez aucun support de sauvegarde sur la machine touchée.** Il serait chiffré à son tour.
- 6 Faites nettoyer ou réinstaller complètement l'ordinateur avant toute restauration.
- 7 Restaurez votre sauvegarde **seulement** sur une machine saine.
- 8 Déposez plainte et signalez l'incident sur **cybermalveillance.gouv.fr**.

Danger

L'erreur la plus coûteuse consiste à brancher la clé de sauvegarde sur l'ordinateur infecté pour « vérifier si elle va bien ». C'est ce geste qui transforme un incident gênant en perte définitive.

Si des données personnelles de clients ont pu être consultées

Vos fichiers contiennent des noms, adresses et coordonnées de clients. En cas de fuite avérée, la réglementation impose une notification à la CNIL sous 72 heures. Conservez la date, l'heure et la description de l'incident dès le premier jour : ces informations vous seront demandées.



Votre routine de contrôle

Chaque semaine

- Brancher le support de sauvegarde de la semaine, lancer la sauvegarde, débrancher.

Chaque trimestre

- Vérifier la liste des appareils mobiles appairés.
- Vérifier que les deux supports fonctionnent toujours.
- Emporter un support hors du local.

Deux fois par an

- Réaliser un test de restauration complet sous un autre nom de base.
- Vérifier que vous savez où se trouve la clé de secours.
- Vérifier que Simple ERP et votre système sont à jour.

Chaque année

- Remplacer les clés USB de plus de trois ans.
- Relire ce guide et vérifier que votre organisation n'a pas dérivé.

Obtenir de l'aide

Si vous avez un doute sur la sécurité de votre installation, contactez le support en indiquant :

- Votre système : Windows, macOS ou Linux.
- La version de Simple ERP affichée dans le menu.
- Ce que vous avez observé exactement, et depuis quand.
- Les protections déjà en place : phrase de passe, sauvegardes, supports utilisés.

En cas de suspicion de rançongiciel, appliquez d'abord les étapes du chapitre précédent, puis contactez le support depuis un **autre** appareil.

Bon à savoir

Le support Simple ERP ne vous demandera jamais votre phrase de passe ni votre clé de secours. Si quelqu'un vous les réclame en se présentant comme le support, il ne s'agit pas de nous.