Dell EMC MozyPro® : Technologie de cryptage Mozy

L'avantage Mozy

Simple

Gérez de manière transparente la sauvegarde, la synchronization et l'accès mobile dans les environnements de serveurs et multi-utilisateurs à partir d'une console Web unique.

Sécurisé

Vos données sont protégées grâce à un chiffrement d'entreprise, à des datacenters très avancés et à Dell EMC, une entreprise conçue pour durer.

Économique

Réalisez des économies : aucun matériel à acheter et frais supplémentaires minimes.

Contactez Mozy

mozyemeasales@dell.com
0800 91 71 34
www.mozy.fr/pro

Types de chiffrement

Mozy sécurise vos données à l'aide d'un cryptage 448 bits Blowfish ou 256 bits AES. Si vous choisissez d'utiliser le cryptage par défaut de Mozy, l'algorithme Blowfish sera utilisé. Si vous décidez de créer votre propre clé à partir d'une phrase secrète, la clé de cryptage sera créée avec AES. Vous trouverez davantage de détails sur le mode de création des clés plus loin dans ce document. Mozy prend en charge trois types de clé de cryptage, chacun disposant de différents avantages spécifiques.

- **Clé de cryptage par défaut de Mozy :** Mozy assigne une clé de cryptage à vos utilisateurs. La clé est stockée et gérée par Mozy pour simplifier l'opération au maximum.
- **Clé de chiffrement personnelle :** les utilisateurs saisissent une phrase secrète utilisée pour créer la clé de chiffrement. Chaque utilisateur crée une clé d'encryptage personnelle et unique.
- **Clé de chiffrement d'entreprise :** l'administrateur saisit une phrase secrète utilisée pour créer la clé de chiffrement. Vous pouvez créer une clé pouvant être partagée avec l'ensemble des utilisateurs de la société ou chaque groupe d'utilisateurs peut posséder la sienne. La clé professionnelle est également désignée sous le nom de c-key.

Vous déterminez le type de clé de cryptage à utiliser pendant l'installation du logiciel Mozy et ce cryptage sera associé en permanence aux fichiers stockés sur le cloud Mozy. Les clients Dell EMC MozyPro® peuvent configurer leur type de cryptage avec une configuration client pour attribuer le type de clé de cryptage aux utilisateurs. Vous pouvez également utiliser la configuration du client pour automatiser l'installation à l'aide d'une clé d'encryptage d'entreprise. Vous pourrez modifier le type de clé d'encryptage après avoir installé le logiciel. Dans ce cas, le logiciel chargera à nouveau tous vos fichiers pour leur stockage correspondant à la nouvelle clé de cryptage.

Quel que soit le type de clé de cryptage utilisé, les fichiers sont d'abord chiffrés avant d'être envoyés au cloud Mozy. Cette étape garantit leur sécurité avant qu'ils ne quittent votre ordinateur ainsi que lors de leur transit et leur stockage sur le cloud Mozy. Si vous utilisez des clés de cryptage personnelles ou d'entreprise, Mozy ne pourra pas lire ni mettre sous séquestre votre clé. Par conséquent, vos fichiers ne seront jamais décryptés avant d'être restaurés sur votre ordinateur.

Cryptage par défaut Mozy

Les clés de cryptage par défaut de Mozy sont à 448 bits construites avec l'algorithme Blowfish. Mozy stocke la clé séparément. Cela permet à Mozy de décrypter

automatiquement vos fichiers quand vous les téléchargez ou les restaurez. Mozy® Sync utilise toujours les clés de cryptage par défaut afin de garantir la mise à jour de vos fichiers sur vos ordinateurs, quel que soit le type de cryptage utilisé par les paramètres de sauvegarde.

Clés de cryptage personnelles

Les clés de cryptage personnelles utilisent un cryptage AES 256 bits créé en utilisant un mot de passe saisi par l'utilisateur. Lorsque vous téléchargez et que vous restaurez des fichiers, vous devez fournir cette clé pour les déchiffrer. Mozy n'a pas accès à votre clé de cryptage personnelle et ne peut pas décrypter les fichiers à votre place. En cas de réinstallation du logiciel Mozy ou de son installation sur un ordinateur de remplacement, vous devez utiliser la même clé pour pouvoir continuer à accéder aux fichiers précédemment sauvegardés.

Clés de cryptage d'entreprise

Les clés de cryptage d'entreprise sont créées de la même manière que les clés de cryptage personnelles. Pour protéger des accès non autorisés à la clé de cryptage, Mozy affecte un mot de passe partagé utilisé pour chiffrer la clé de cryptage d'entreprise avec l'algorithme Blowfish. Cette opération en 2 étapes garantit la sécurité de votre clé de cryptage. Comme pour les clés de cryptage personnelles, Mozy ne pourra pas vous aider à décrypter les fichiers sauvegardés car nous n'avons pas accès à votre clé. Les clés d'encryptage d'entreprise sont partagées par tous les utilisateurs ou groupe d'utilisateurs de votre organisation. Elles peuvent être affectées à des ordinateurs locaux ou bien être stockées sur un serveur réseau pour un accès par des utilisateurs.

Dérivé des clés d'encryptage pour des clés personnalisées

Lors de la personnalisation d'une clé de cryptage personnelle ou d'entreprise, Mozy procède à plusieurs passages du mot de passe entré dans l'algorithme SHA-512 pour créer un hachage du code. La clé d'encryptage 256 bits AES est créée à partir du hachage obtenu. Mozy n'a jamais accès à votre clé de cryptage et ne peut pas vous aider à décrypter vos fichiers si vous égarez votre clé.

Clés d'encryptage personnelles

Une fois créée, la clé d'encryptage subit un hachage avec des passages multiples dans l'algorithme SHA-512 puis stockée dans le système local.

- Sur Windows, la clé de chiffrement hachée est stockée dans le registre. De plus, cette clé est protégée par l'API de protection des données de Microsoft et ne peut pas être lue par les utilisateurs ni les administrateurs de la machine.
- Sur Mac OSX, la clé de cryptage hachée est stockée dans state.db.

Le hachage du résultat garantit la sécurité de la clé de chiffrement sur le système local. Vous pouvez également sauvegarder la clé au format de fichier .dat en cas de besoin de la réinstallation future du logiciel.

Clés de cryptage d'entreprise

Lors de la création de clés de cryptage d'entreprise, Mozy ajoute la clé à un fichier.ckey puis le crypte avec un mot de passe partagé. Le mot de passe partagé garantit, en cas de fichier .ckey compromis, que votre clé de cryptage ne pourra pas être lue ni utilisée pour décrypter vos fichiers. N'oubliez pas que le mot de passe partagé ne sert pas à chiffrer ni à déchiffrer vos données. Le mot de passe partagé sert à chiffrer votre clé d'encryptage en rajoutant un autre niveau de sécurité à vos données.

Lorsque vous installez le logiciel Mozy sur vos points d'extrémité, Mozy décrypte le fichier de la clé de cryptage d'entreprise pour pouvoir stocker le mot de passe crypté dans le système local. La clé d'encryptage subit un hachage par plusieurs passages dans l'algorithme SHA-512, elle est chiffrée par un algorithme Blowfish en mode CBC avec une clé symétrique brouillée et masquée dans le fichier binaire client puis stockée dans le système local.

- Sur Windows, la clé de chiffrement hachée est stockée dans le registre. L'entrée d'enregistrement est limitée par des contrôles d'accès à SYSTEM. De plus, la clé est protégée par l'API de protection des données de Microsoft avec une clé spécifique à chaque utilisateur, et ne peut pas être lue par les utilisateurs ni les administrateurs de la machine.
- Sur Mac OSX, la clé de cryptage hachée est stockée dans state.db.

Quelle est la clé adaptée à mes besoins ?

Le tableau suivant vous aidera à comprendre la manière dont les différents types de cryptage agissent sur les fonctions client disponibles du service Mozy.

Fonctions	Clé par défaut	Clé personnelle	Clé d'entreprise
Restaurer les fichiers en utilisant le logiciel de sauvegarde sans fournir de clé de cryptage ou prendre d'autres mesures manuelles pour le décryptage.	Oui	Oui	Oui
Utilisez l'application mobile Mozy pour accéder aux fichiers sauvegardés.	Oui	Oui	Oui ; le fichier.ckey doit être stocké sur un serveur Web accessible aux appareils mobiles.
Utiliser la prévisualisation du fichier dans l'application mobile Mozy.	Oui	Oui	Oui
Utiliser Mozy sur le web pour télécharger ou restaurer.	Oui	Oui, doit être déchiffré manuellement avec un utilitaire de décryptage.	Oui, seul l'administrateur peut le décrypter manuellement avec un utilitaire de décryptage.
Utilisez le Gestionnaire de restauration de Mozy pour restaurer des fichiers.	Oui	Oui	Oui, si le gestionnaire de restauration a accès au fichier.ckey à partir de l'emplacement spécifié dans la configuration client.
Utiliser l'aperçu du fichier, la vignette photo, et la recherche de nom de fichier dans Mozy sur le Web.	Oui	Non, la recherche par nom de fichier est prise en charge mais il n'y a pas l'aperçu des fichiers ni les vignettes.	Non, la recherche par nom de fichier est prise en charge, mais il n'y a pas l'aperçu des fichiers ni les vignettes.
Utilisez Mozy Sync pour mettre à jour les fichiers sur les ordinateurs associés et pour prévisualiser les vignettes des fichiers et des photos.	Oui	Oui	Oui, cependant Sync sur mobile n'est pas pris en charge.

05/17, Brochure, H15545-FR