



# Protection et cryptage de la sauvegarde en ligne

## Les atouts de MozyEnterprise

### Simple

Gérez les environnements multiutilisateurs, définissez des sauvegardes automatiques et planifiées, affichez le niveau d'utilisation et statistiques des comptes, tout cela à partir d'une seule console d'administration Web.

### Sécurisé

Mozy est audité SOC 1 SSAE 16 Type 2 et certifié ISO 27001 et respecte les normes de sécurité les plus strictes avec un chiffrement de classe militaire et dans des centres de données perfectionnés.

### Abordable

MozyEnterprise s'intègre simultanément dans votre infrastructure, éliminant le besoin de cassettes, DVDs et autres moyens, ce qui permet de garder les coûts informatiques au plus bas.

### Contactez MozyEnterprise

emeacorporatesales@mozy.com  
P 0800 91 71 34  
[www.mozy.fr/enterprise](http://www.mozy.fr/enterprise)

Selon IDC, parmi les services de stockage de type Cloud, la sauvegarde en ligne est devenue le segment le plus important et le plus courant des services avancés (Les avantages de la sauvegarde de type Cloud, IDC septembre 2011). L'essor des sauvegardes de type Cloud peut être attribué à la capacité de ces solutions à assurer efficacement la protection des données et la continuité des opérations de manière à renforcer la fiabilité et la cohérence, tout en réduisant considérablement les coûts informatiques et les opérations continues de maintenance et d'assistance. Toutefois, avant de profiter des avantages d'un service de sauvegarde en ligne, les entreprises doivent examiner de près les mesures de sécurité et les méthodes de cryptage employées par le prestataire de service. Considéré comme l'un des meilleurs fournisseurs de services de sauvegarde en ligne de l'industrie, Mozy prend très au sérieux la protection de vos données en identifiant trois grands domaines d'intervention en matière de protection des données dans le Cloud : la sécurité, la confidentialité et la conformité.

### Sécurité

Mozy crypte vos données avant même qu'elles ne quittent votre ordinateur, pendant leur transfert sur l'ensemble du réseau et lors de leur stockage dans nos centres de données. Les centres de données se basent sur des pratiques de sécurité physique et technique de pointe et adhèrent, le cas échéant, aux Principes de la « sphère de sécurité » de la Communauté européenne. Par ailleurs, Mozy a réussi l'audit SSAE-16 et a obtenu la certification ISO-2700. Ces audits indépendants certifient que les processus et procédures mis en œuvre par Mozy atteignent, voire dépassent, les objectifs de contrôle les plus stricts du secteur. En se soumettant volontairement à un audit SSAE-16 et en obtenant la certification ISO 27001, Mozy fait la preuve de son engagement en faveur des informations de ses clients et montre sa détermination face aux menaces croissantes auxquelles sont confrontées les informations numériques. Non seulement un grand nombre de services de sauvegarde en ligne connus négligent de mettre en œuvre ces normes de sécurité élevées, mais certains ne daignent même pas crypter vos données de manière entièrement sécurisée, sans parler de ceux qui font totalement l'impasse sur le cryptage. Plus loin dans ce document, nous passerons en revue les mesures et options complètes que Mozy propose pour s'assurer que vos données sont correctement protégées et cryptées.



## Options et normes de cryptage appliquées par Mozy

Mozy crypte vos données à l'aide d'un clé AES ou Blowfish avant même qu'elles ne quittent votre ordinateur. Blowfish est un algorithme du domaine public créé en 1993 par Bruce Schneier, un cryptographe renommé. Il s'agit d'un algorithme rapide et polyvalent qui utilise un cryptage symétrique par bloc sécurisé avec une clé de longueur variable. Mozy utilise la longueur de clé maximale égale à 448 bits pour l'algorithme de cryptage Blowfish.

AES est un algorithme de cryptage à 256 bits de classe militaire qui est devenu le standard de facto du gouvernement américain pour le cryptage de renseignements classés Secret et Très secret. AES est également l'algorithme de cryptage standard utilisé par la NSA (National Security Agency). Il est devenu l'un des algorithmes de cryptage les plus largement répandus et pris en charge. De plus, l'algorithme AES est accepté par la FIPS (Federal Information Processing Standard) 140-2 en matière de cryptographie. Par conséquent, le cryptage AES permet aux entreprises de se conformer pleinement aux normes gouvernementales strictes sur la protection des données et les administrations publiques et les filiales réglementées peuvent donc toutes utiliser les options de cryptage AES de Mozy pour protéger leurs données.

AES est jugé plus sécurisé et plus robuste que Blowfish, même si les deux algorithmes sont réputés pour leur niveau de protection très élevé. D'un autre côté, si AES peut atteindre des vitesses de cryptage élevées, Blowfish reste le plus rapide.

Bien que l'algorithme Blowfish soit jugé sûr, aucune cryptanalyse le concernant n'est accessible au public. Cela ne signifie pas que l'algorithme lui-même a été brisé, mais simplement que les vulnérabilités qu'il pourrait présenter ne sont pas encore connues. Cela montre aussi que d'autres algorithmes qui ont fait l'objet de davantage d'attention sont susceptibles de bénéficier d'une plus grande longévité du point de vue de leur utilisation industrielle et de leur prise en charge générale. D'un autre côté, AES a subi plusieurs séries d'analyses approfondies, la première ayant consisté en un examen sur 5 ans mené dans le cadre de sa propre adoption en tant que norme de cryptage avancée AES (Advanced Encryption Standard). Depuis l'année 2000, plusieurs autres cryptanalyses accessibles au public ont été

réalisées sur AES, qui ont entraîné sa large diffusion et sa distinction comme l'un des algorithmes de cryptages le plus sécurisés.

L'utilisation du cryptage AES ou Blowfish avec le service MozyEnterprise est déterminée en fonction de votre choix parmi les trois options de cryptage Mozy suivantes :

- Clé par défaut - utilise Blowfish
- Clés personnelles - utilise AES
- Clé d'encryption entreprise - utilise AES

En plus du cryptage AES ou Blowfish, au cours du transfert de vos données Mozy utilise une connexion SSL certifiée avec vérification de certificat bidirectionnelle pour les communications entre vos ordinateurs et le service MozyEnterprise. Il s'agit de la technologie utilisée par les banques pour sécuriser les transactions en ligne. De plus, tous les utilisateurs sont tenus de s'authentifier auprès de Mozy à l'aide d'un nom d'utilisateur et d'un mot de passe.

## Cryptage à l'aide de la clé par défaut

La clé par défaut, également appelée clé standard, recourt à l'algorithme Blowfish pour crypter vos données. Outre le fait qu'elle utilise un algorithme de cryptage à la fois très sûr et très rapide, l'un des principaux avantages de la clé par défaut est que Mozy en assure la maintenance. Inutile de vous soucier de mémoriser la phrase de passe de la clé pour crypter ou décrypter vos données. Mozy se charge automatiquement de tout cela pour vous, tout en s'assurant que vos données sont cryptées de manière sécurisée avant leur transfert au cours de la procédure de sauvegarde.

Par ailleurs, les fonctions Web et de mobilité incluses dans Mozy bénéficient d'une prise en charge intégrée de la clé par défaut. Autrement dit, vous pouvez afficher, rechercher ou télécharger des fichiers de sauvegarde à partir de votre périphérique mobile ou d'un navigateur Web, et ce de manière transparente et sécurisée. La clé par défaut fournit une solution de cryptage prête à l'emploi et facile à utiliser pour toutes vos sauvegardes. Bien que la clé par défaut offre un cryptage convivial et sécurisé, certaines entreprises préfèrent gérer leur propre phrase de passe de cryptage plutôt que de permettre à Mozy d'avoir connaissance de cette clé. Comme son nom l'indique, cette clé est utilisée par défaut sauf si vous sélectionnez l'une des autres options de cryptage.



## Cryptage à l'aide de clés personnelles

Les clés personnelles constituent l'une des deux options proposées par Mozy aux entreprises et aux particuliers qui souhaitent profiter des avantages du cryptage AES. Elles permettent aux utilisateurs individuels de gérer leur propre clé de cryptage, en laissant chacun d'eux spécifier sa propre clé de cryptage pour les données de son ordinateur. Par conséquent, en plus de la sécurité renforcée que fournit le cryptage AES, la protection est encore améliorée par le fait que chaque clé personnelle est connue seulement de l'utilisateur. Le service Mozy n'assure pas la maintenance et n'a pas connaissance de cette clé. De fait, même sous l'action de la loi, Mozy ne peut pas décrypter vos fichiers si vous choisissez le cryptage personnel.

Pour créer leur clé personnelle exclusive, les utilisateurs sont invités à entrer une phrase de passe, de longueur quelconque, composée de caractères, de symboles et de chiffres. Pour assurer la sécurité de la clé, le logiciel client Mozy utilise une empreinte numérique de la phrase de passe stockée dans l'ordinateur de l'utilisateur.

Étant donné que le service Mozy ne stocke pas votre clé de cryptage personnelle et qu'il n'est pas capable de la décrypter, les fonctions Web et mobiles de Mozy permettant de consulter, rechercher et télécharger directement les fichiers que vous avez sauvegardés nécessitent de saisir la phrase de passe appropriée.

De plus, en tant qu'administrateur Mozy, si vous souhaitez effectuer une restauration pour le compte de vos utilisateurs ou pour récupérer les fichiers de personnes ayant quitté l'entreprise, vous devrez connaître les clés personnelles de ces utilisateurs ou y avoir accès.

De même, si des utilisateurs individuels oublient leur phrase de passe, ils ne pourront pas décrypter ou restaurer leurs données sur un poste de travail. Pour se prémunir des phrases de passe oubliées, Mozy fournit de option d'exportation. L'option de dépôt permet à l'utilisateur d'enregistrer sa phrase de passe de cryptage dans un fichier texte sur un partage réseau ou un lecteur USB amovible. Il est également possible d'enregistrer le fichier sur le disque dur de l'ordinateur local. Cette solution n'est toutefois pas recommandée car il serait inaccessible si l'ordinateur rencontrait une défaillance système. Il est recommandé aux entreprises qui ont choisi l'option d'exportation d'établir une stratégie de sécurité quant à l'emplacement dans lequel ces fichiers de phrases de passe sont stockés.

Pour les entreprises qui veulent bénéficier des avantages du cryptage AES mais qui ne souhaitent pas que les utilisateurs gèrent leur propre phrase de passe, Mozy propose l'option Clé d'encryption entreprise.

## Cryptage à l'aide de la clé d'entreprise (Clé d'encryption entreprise)

La clé d'entreprise Mozy (Clé d'encryption entreprise) permet aux entreprises de profiter de la force de l'algorithme AES pour le cryptage de leurs données et propose par ailleurs une gestion simplifiée et renforcée des phrases de passe. L'option Clé d'encryption entreprise permet à une personne de créer une phrase de passe pour l'ensemble de l'entreprise. Le choix de cette personne vous appartient. Il peut s'agir par exemple, d'un directeur, d'un gestionnaire ou d'un administrateur de la sécurité ou du service informatique. À partir de la console d'administration de Mozy, vous définissez la phrase de passe Clé d'encryption entreprise et choisissez un emplacement dans lequel la stocker (par exemple, un partage réseau, un serveur Web ou dans le cadre d'un package d'installation du logiciel Mozy sur des ordinateurs clients). Puisque Mozy est installé sur différents ordinateurs, chacun d'eux aura accès à cet emplacement pour crypter et décrypter des fichiers à l'aide de la clé.

Comme la phrase de passe Clé d'encryption entreprise sera probablement stockée sur un partage réseau ou un serveur Web, pour empêcher tout accès non autorisé à cette clé, Mozy recourt à la fonction Secret partagé qui crypte la phrase de passe. Lors de l'installation de Mozy sur vos ordinateurs clients, le cryptage de cette phrase de passe est automatiquement programmé au niveau de chaque client. Vos postes de travail qui exécutent le client de sauvegarde Mozy pourront ainsi utiliser cette phrase de passe pour crypter ou décrypter des fichiers le cas échéant.

Pour effectuer une restauration à l'aide de la clé Clé d'encryption entreprise, il est nécessaire de recourir à l'utilitaire de cryptage Mozy pour décrypter les fichiers à restaurer. L'utilitaire de cryptage Mozy vous invite à entrer le chemin d'accès du fichier Clé d'encryption entreprise, du secret partagé et des fichiers téléchargés depuis la restauration Web pour décrypter et restaurer les fichiers sur votre ordinateur local.

Comme pour les clés personnelles, vous êtes responsable de la gestion et du stockage de la phrase de passe Clé d'encryption entreprise, Mozy ne la connaît pas. Con-



trairement à d'autres fournisseurs de sauvegarde en ligne, Mozy n'exige pas que la clé soit transférée ou déposée sur son système. Par conséquent, Mozy n'a pas la possibilité de décrypter vos fichiers si vous choisissez l'option Clé d'encryption entreprise. Puisque ni le service Mozy ni la plupart des utilisateurs de votre organisation n'ont accès à votre phrase de passe Clé d'encryption entreprise, vous avez la garantie que vos données d'entreprise sont protégées contre tout accès non autorisé, même s'il s'agit d'un employé qui tente de télécharger des fichiers sur un ordinateur domestique.

## Confidentialité

Pour protéger la confidentialité de vos données, Mozy intègre un ensemble de contrôles techniques, administratifs et physiques standard du secteur qui protègent vos informations personnelles. Mozy a également mis en place son propre engagement de confidentialité pour mener ses activités selon les principes suivants :

- Vos informations sont les vôtres et non les nôtres.
- Nous ne vendons pas vos informations à qui que ce soit, ni ne vendons vos coordonnées.
- Nous ne passons pas au crible vos informations pour créer votre profil ou vous cibler commercialement.
- Vous pouvez toujours reprendre possession de vos informations. Nous n'avons aucun droit sur vos informations si vous annulez le service.

## Conformité

Mozy considère la conformité comme un élément essentiel de la protection de vos données. Nos clients souhaitent souvent savoir si nos solutions de sauvegarde leur permettent de demeurer conformes à un large éventail de normes internationales, américaines et européennes, notamment PCI DSS, SOX, HIPAA, GLBA, Directive 95/46/CE Protection des données à caractère personnel, Directive 2002/58/CE Vie privée et communications électroniques et Sphère de sécurité. Les principes qui sous-tendent ces normes visent à permettre au propriétaire des données de conserver la maîtrise de ses informations confidentielles et d'avoir la garantie que seules les personnes autorisées y aient accès.

Lorsque vous sauvegardez des informations sur Mozy, vous gardez le contrôle de vos données par le biais des schémas d'authentification et du cryptage du système. Chaque fichier est crypté avant d'être transmis à l'infrastructure Mozy pour y être stocké. Autrement dit, les informations à caractère personnel et confidentiel demeurent privées pendant que nous les conservons pour vous. Nous ne transigeons pas avec les contrôles de sécurité internes gérés par nos clients pour se conformer aux diverses réglementations. Mozy prend également des mesures proactives pour se protéger des attaques, des risques et des violations d'accès qui pourraient menacer la sécurité, la confidentialité et l'intégrité de vos données.

## Protéger vos données, protéger votre entreprise

Mozy a pour mission de protéger vos données et votre entreprise. Vous pouvez compter sur les stratégies de sécurité strictes de Mozy, sur son cryptage de classe militaire et sur ses centres de données d'envergure internationale pour une protection optimale de vos données d'entreprise dans le respect de toutes les exigences requises en matière de disponibilité, de sécurité, de confidentialité et de conformité. Mozy est le nom le plus digne de confiance dans la sauvegarde en ligne, aussi bien pour les grandes entreprises que les petites entreprises. Élément d'EMC, le géant du stockage, Mozy possède l'expérience et l'infrastructure nécessaires pour conserver vos données en toute sécurité.