# PGP Whole Disk Encryption pour Mac OS X

**Guide de démarrage rapide**
**Version 10.2**

## Présentation de PGP Whole Disk Encryption

Vous pouvez avoir recours à PGP Whole Disk Encryption (PGP WDE) pour verrouiller l'intégralité du contenu de votre système ou d'un lecteur externe ou USB Flash de votre choix.

PGP Whole Disk Encryption vous permet par ailleurs d'effectuer les opérations suivantes :

- utiliser une partie de l'espace de votre disque dur en tant que lecteur virtuel chiffré possédant sa propre lettre ;
- créer des archives Zip protégées ;
- détruire complètement les fichiers et les dossiers de sorte qu'il soit impossible de récupérer leurs données.

**Table des matières**



## Vous venez d'acheter PGP Whole Disk Encryption ?

Consultez ce guide détaillé pour vous familiariser avec le logiciel. Vous verrez qu'avec PGP Whole Disk Encryption, protéger vos données devient aussi facile que tourner la clé dans une serrure.

- Ce *guide de démarrage rapide* vous explique comment installer PGP Whole Disk Encryption et commencer à l'utiliser.
- Vous trouverez des informations plus détaillées sur PGP Whole Disk Encryption dans le *Guide de l'utilisateur de PGP Desktop*. Ce manuel vous présente les paires de clés, vous explique pourquoi il peut être utile d'en créer et décrit les procédures de création d'une clé et d'échange de clés avec des tiers en vue de chiffrer vos données et de les partager en toute sécurité.

  **Remarque :** une licence PGP Whole Disk Encryption vous donne accès à un ensemble donné de fonctionnalités PGP Whole Disk Encryption. Certaines fonctionnalités spéciales de PGP Whole Disk Encryption peuvent requérir une licence supplémentaire. Pour plus d'informations, reportez-vous à la section relative aux licences du *Guide de l'utilisateur de PGP Desktop*.
- Pour obtenir des informations sur le déploiement, la gestion et l'application des stratégies pour PGP Whole Disk Encryption, consultez le manuel *Guide de l'administrateur de PGP Universal Server*.

Après l'installation, PGP Whole Disk Encryption vous invite à créer une paire de clés PGP. Une paire de clés est constituée d'une clé privée et d'une clé publique.

- Comme son nom le suggère, la *clé privée* doit rester confidentielle, de même la phrase secrète associée. Si une personne prend possession de votre clé privée et de sa phrase secrète, elle pourra lire vos messages et emprunter votre identité pour communiquer avec des tiers. Votre clé privée est employée pour déchiffrer les messages chiffrés entrants et signer les messages sortants.
- En ce qui concerne votre *clé publique*, vous pouvez la communiquer à tous. Aucune phrase secrète ne lui est associée. Elle sert à chiffrer les messages qui ne pourront être déchiffrés qu'avec votre clé privée et à vérifier les messages signés.

Dans votre trousseau de clés sont stockées aussi bien vos paires de clés que les clés publiques de tiers ; vous utilisez ces dernières pour envoyer des messages chiffrés à leurs détenteurs. Pour afficher les clés de votre trousseau, cliquez sur le panneau de contrôle Clés PGP :

1. L'icône pour une paire de clés PGP représente deux clés (qui symbolisent la clé privée et la clé publique). Par exemple, dans l'illustration ci-dessous, Alice Cameron dispose d'une paire de clés PGP.
2. Sur les icônes des clés publiques des autres utilisateurs figure une seule clé. Par exemple, la clé publique de Ming Pa a été ajoutée au trousseau de clés illustré ici.

## Éléments installés

PGP Whole Disk Encryption utilise des licences pour octroyer l'accès aux fonctionnalités incluses dans le logiciel. Selon le type de licence dont vous disposez, les applications de la gamme PGP Whole Disk Encryption sont actives en partie ou dans leur ensemble.

Ce document contient des instructions relatives à l'affichage des fonctionnalités activées par votre licence.

**PGP Whole Disk Encryption (PGP WDE)** fait partie de la gamme PGP Desktop. Vous pouvez avoir recours à cette fonctionnalité pour verrouiller l'intégralité du contenu de votre système ou d'un lecteur externe ou USB Flash de votre choix. Les secteurs de démarrage, fichiers système et fichiers d'échange sont tous chiffrés. Lorsque vous appliquez la fonctionnalité WDE à votre lecteur de démarrage, vous n'avez pas à vous préoccuper de l'éventualité de la perte ou du vol de votre ordinateur : en effet, un pirate ne pourra accéder à vos données sans la phrase secrète adéquate. Si vous avez chiffré un dispositif USB, vous pouvez partager les données qui y sont stockées avec d'autres utilisateurs de PGP Whole Disk Encryption pour Windows ou Mac OS X.

**Volumes PGP Virtual Disk** : fonctionnalité du logiciel permettant d'utiliser une partie de l'espace de votre disque dur en tant que lecteur virtuel chiffré possédant sa propre lettre. Un PGP Virtual Disk représente l'endroit idéal pour stocker vos fichiers sensibles. Cela revient à les placer dans un coffre. Lorsque la porte du coffre est ouverte (quand le volume est monté), vous pouvez modifier les fichiers qu'il contient, en sortir ou en ajouter de nouveaux. Autrement (lorsque le volume est démonté), toutes les données sont protégées.

Avec **PGP Zip**, vous pouvez regrouper différents fichiers et dossiers dans une même archive chiffrée, compressée et portable. Pour que vous puissiez créer ou ouvrir une archive PGP Zip, PGP Desktop doit être installé sur votre système. PGP Zip est un outil grâce auquel vous pouvez archiver en toute sécurité vos données sensibles, que ce soit pour les distribuer à des tiers ou bien les sauvegarder.

**PGP Shredder** détruit définitivement des fichiers et dossiers pour qu'ils ne puissent pas être récupérés, même à l'aide d'un logiciel de récupération de fichiers. Lorsque vous supprimez un fichier en le plaçant dans la corbeille (sous Windows ou Mac OS X), celui-ci n'est pas véritablement éliminé ; il demeure sur votre lecteur et finira par être écrasé. Jusqu'alors, pour un pirate, le récupérer est un jeu d'enfant. PGP Shredder, au contraire, remplace immédiatement les fichiers, à plusieurs reprises. Cette opération est très efficace, sachant que les fichiers ne peuvent pas être récupérés, même à l'aide d'un logiciel de récupération de disque élaboré. Cette fonctionnalité permet en outre de nettoyer en profondeur l'espace libre sur vos lecteurs pour empêcher la récupération des données que vous avez supprimées.

Avec la **gestion des clés**, vous pouvez gérer les clés PGP, qu'il s'agisse de vos propres paires de clés ou des clés publiques de tiers. Vous utilisez votre clé privée pour déchiffrer les messages que vous recevez et qui ont été chiffrés avec votre clé publique, et pour sécuriser vos volumes PGP Virtual Disk. Vos clés publiques, quant à elles, vous servent à chiffrer les messages que vous envoyez ou à ajouter des utilisateurs aux volumes PGP Virtual Disk.

## Configuration système requise

Pour installer PGP Whole Disk Encryption sur votre système Mac OS X, vous devez disposer de la configuration système minimale suivante :

- Apple Mac OS X10.5.x, 10.6.x, ou 10.7.x (Intel)
- 512 Mo de RAM
- 64 Mo d'espace disque dur
- PGP Whole Disk Encryption (PGP WDE) n'est pas compatible avec les logiciels tiers, autres que Apple Boot Camp, pouvant contourner la protection PGP WDE sur l'enregistrement d'amorçage principal (MBR) et écrire sur ce dernier ou le modifier. Boot Camp doit modifier le MBR avant d'installer le système d'exploitation Windows et ne peut pas être utilisé sue un système Macintosh déjà chiffré avec PGP WDE. Pour utiliser Boot Camp avec PGP WDE, consultez les instructions d'installation dans le *Guide de l'utilisateur de PGP Desktop pour Mac OS X*.

PGP Whole Disk Encryption (PGP WDE) n'est pas compatible avec les logiciels tiers, autres que Apple Boot Camp, pouvant contourner la protection PGP WDE sur l'enregistrement d'amorçage principal (MBR) et écrire sur ce dernier ou le modifier. Boot Camp doit modifier le MBR avant d'installer le système d'exploitation Windows et ne peut pas être utilisé sue un système Macintosh déjà chiffré avec PGP WDE. Pour utiliser Boot Camp avec PGP WDE, consultez les instructions d'installation.

## Installation de PGP Whole Disk Encryption

PGP Corporation vous recommande de fermer toutes les applications ouvertes avant de lancer l'installation. Ce processus peut nécessiter un redémarrage du système.

**Remarque :** pour pouvoir installer la mise à jour, vous devez disposer de droits d'administration sur votre système.

Le programme d'installation de PGP Whole Disk Encryption vous guide tout au long de la procédure d'installation du logiciel.

#### Pour installer PGP Whole Disk Encryption sur votre système Mac OS X

1. Fermez toutes les autres applications.
2. Montez l'image DiskCopy PGP.
3. Cliquez deux fois sur `PGP.pkg`.
4. Suivez les instructions affichées à l'écran.
5. Si vous y êtes invité, redémarrez le système.

**Remarque :** si votre ordinateur se trouve dans un domaine protégé par un PGP Universal Server, votre administrateur

PGP aura peut-être prédéfini des fonctions ou paramètres du programme d'installation de PGP Whole Disk Encryption. En outre, si votre administrateur PGP a configuré une inscription automatisée, votre mot de passe de domaine Windows sera utilisé pour toutes les conditions requises de phrase secrète dans PGP Whole Disk Encryption. Si la stratégie le spécifie, PGP Whole Disk Encryption peut démarrer automatiquement pour chiffrer le contenu de votre disque au moment où votre mot de passe Windows est saisi.

## Gestion des licences

Pour connaître les fonctionnalités prises en charge par votre licence, ouvrez PGP Whole Disk Encryption et sélectionnez **PGP > Licence**. Cliquez sur **Détails**. Les détails relatifs à votre licence sont alors affichés.

## Démarrage de PGP Whole Disk Encryption

Quatre modes d'accès sont proposés :

- Écran principal de PGP Whole Disk Encryption
- Utilisation de l'icône PGP Whole Disk Encryption dans la barre de menus
- Utilisation de l'icône PGP Dock
- Utilisation du Finder sous Mac OS X

### Écran principal de PGP Whole Disk Encryption

L'écran principal de PGP Whole Disk Encryption représente votre premier mode d'interaction avec le produit.


L'écran principal de PGP Whole Disk Encryption comporte les éléments suivants :

| | |
|---|---|
| 1 | **Le champ de recherche** : vous permet de rechercher des clés figurant dans le trousseau de clés local. Saisissez simplement un nom ou une adresse de courrier électronique sur le trousseau de clés local et appuyez sur Entrée. Pour utiliser d'autres critères de recherche, cliquez sur **Recherche avancée**. |
| 2 | **La zone de travail de PGP Whole Disk Encryption** : affiche les options de PGP Disk et décrit la fonction de chaque option. |
| 3 | **La barre d'outils** : permet d'accéder aux fonctions fréquemment utilisées. Vous pouvez :<br>• créer une archive PGP Zip ;<br>• créer un volume PGP Virtual Disk ;<br>• monter un volume PGP Virtual Disk existant ;<br>• synchroniser des clés ;<br>• décomposer des fichiers. |
| 4 | **L'élément Clés** : vous permet de contrôler les clés PGP que PGP Whole Disk Encryption gère pour vous. |
| 5 | **L'élément PGP Zip** vous permet d'afficher et de gérer les archives PGP Zip. |
| 6 | **L'élément PGP Disk** : vous permet d'afficher et de gérer les volumes PGP Virtual Disk. Vous pouvez également l'utiliser pour créer d'autres volumes de ce type, ainsi que pour chiffrer un disque entier ou gérer le chiffrement de disques amovibles à l'aide de la fonction PGP Whole Disk Encryption. |
| 7 | **L'élément Serveurs de clés** : vous permet d'afficher et de gérer les serveurs de clés. |

## Chiffrement d'un lecteur à l'aide de PGP WDE

Utilisez la fonction PGP WDE pour chiffrer intégralement le disque d'amorçage (ordinateurs Macintosh avec processeur Intel uniquement) et les disques externes sur les systèmes Mac OS X. Cette fonction permet également de chiffrer intégralement les disques externes formatés Windows.

Avant de chiffrer votre disque, assurez-vous de sauvegarder son contenu afin de ne perdre aucune donnée en cas de perte ou de vol de l'ordinateur ou d'incapacité à déchiffrer le disque.

Le logiciel de sauvegarde fonctionne normalement avec PGP WDE ; les fichiers qu'il sauvegarde sont déchiffrés *avant* d'être sauvegardés.

1 Ouvrez PGP Whole Disk Encryption et cliquez sur l'élément PGP Disk. L'écran PGP Disk s'affiche.


2 Cliquez sur **Chiffrer un disque**. L'écran Chiffrer le disque complet apparaît et présente la liste des disques de votre système pouvant être protégés.

3 Dans la liste **Sélectionnez un disque, sélectionnez le disque à protéger.**

4 Dans la section **Sécuriser avec**, précisez la méthode d'accès au disque protégé. Sélectionnez l'utilisateur **Clé publique** ou **Phrase secrète**.

**Remarque :** si vous chiffrez un disque de démarrage, vous pouvez uniquement utiliser l'authentification par phrase secrète. PGP Whole Disk Encryption sélectionne donc **Utilisateur de phrase secrète** pour vous et passe directement à l'écran Ajout d'un utilisateur de PGP Whole Disk.

- Pour protéger votre disque avec une clé publique, sélectionnez **Clé publique**, puis cliquez sur **Continuer**. L'écran Ajout d'un utilisateur de PGP Whole Disk s'affiche. Sélectionnez une clé dans la liste fournie et cliquez sur **Continuer**. La boîte de dialogue Saisissez la phrase secrète PGP s'affiche. Tapez la phrase secrète de la clé sélectionnée, puis cliquez sur **OK**. L'écran Récapitulatif de PGP Whole Disk Encryption apparaît, présentant un récapitulatif de la façon dont le disque sera chiffré. Cette option est disponible uniquement si vous chiffrez un disque amovible.
- Pour protéger votre disque avec une phrase secrète, sélectionnez **Phrase secrète**, puis cliquez sur **Continuer.** L'écran Ajout d'un utilisateur de PGP Whole Disk s'affiche. Complétez le champ **Nom** (ou acceptez le nom par défaut), puis saisissez la phrase secrète souhaitée dans le champ **Saisissez votre phrase secrète**, puis tapez-la à nouveau dans le champ **Confirmez votre phrase secrète. Pour que la phrase secrète s'affiche à mesure que vous saisissez les caractères, sélectionnez Afficher les frappes**. Cliquez sur **Continuer**. L'écran Récapitulatif de PGP Whole Disk Encryption apparaît, présentant un récapitulatif de la façon dont le disque sera chiffré.

L'indicateur de qualité de la phrase secrète fournit une indication de base sur la force de la phrase secrète que vous créez en comparant le degré d'entropie de cette phrase par rapport à une véritable chaîne aléatoire 128 bits (même degré d'entropie que dans une clé AES128). Pour plus d'informations, reportez-vous à la section Indicateur de qualité de la phrase secrète (du *Guide de l'utilisateur de PGP Desktop pour Mac OS X).*

5 Vérifiez les informations, puis cliquez sur **Chiffrer.** Le processus de chiffrement commence et l'écran Progression du chiffrement apparaît.

6 Cliquez sur **Fermer**. La fenêtre de l'application PGP Whole Disk Encryption s'affiche tandis que le processus de chiffrement se poursuit en arrière-plan. Une barre indique l'avancée du processus de chiffrement.

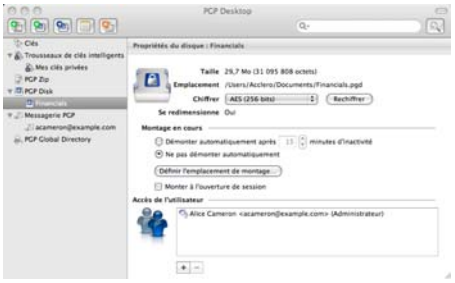
**Remarque :** le processus de chiffrement continue même si vous fermez l'écran Progression du chiffrement. Vous ne pouvez cependant pas voir la barre de progression tant que vous ne fermez pas cet écran.

7 Au cours du processus de chiffrement, vous pouvez effectuer les opérations suivantes :

- Pour interrompre temporairement le processus de chiffrement, cliquez sur **Arrêter**. La boîte de dialogue Chiffrement non terminé s'affiche.
- Cliquez sur **Pause** pour interrompre le processus de chiffrement, sur **Déchiffrer** pour déchiffrer la partie du disque déjà chiffrée ou sur **Annuler** pour fermer la boîte de dialogue et poursuivre le processus de chiffrement.

**Remarque :** si le processus s'interrompt pour signaler une erreur de lecture/écriture du disque, cela signifie que PGP Whole Disk Encryption a identifié des secteurs défectueux sur le disque au cours du chiffrement<>. Inversez immédiatement le processus de chiffrement en *déchiffrant* la partie du disque déjà chiffrée. Utilisez ensuite les outils de vérification de disque pour déterminer et résoudre le problème.

Lorsque le processus de chiffrement est terminé, les propriétés du disque chiffré s'affichent.



## Meilleures pratiques avec PGP WDE

Avant de chiffrer votre disque, vous devez effectuer certaines tâches afin de garantir un chiffrement initial correct.

- **Déterminer si le disque concerné est pris en charge** : pour plus de détails concernant les types de disques pris en charge, reportez-vous à la section « Types de disques pris en charge » du *Guide de l'utilisateur de PGP Desktop.*
- **Vérifier que les caractères que vous avez utilisés pour votre phrase secrète sont tous pris en charge** : pour connaître la liste des caractères acceptés pour les phrases secrètes, reportez-vous à la section « Caractères pris en charge » du *Guide de l'utilisateur de PGP Desktop.*
- **Vérifier le bon fonctionnement du disque avant de commencer son chiffrement** : si PGP WDE rencontre des erreurs sur le disque lors du chiffrement, le processus sera interrompu afin que vous puissiez les corriger. Il est cependant plus efficace de les résoudre avant de commencer le chiffrement. Reportez-vous à la section *Vérification du bon fonctionnement du disque avant le chiffrement* (à la page 5).
- **Effectuer une sauvegarde du disque avant le chiffrement** : avant de chiffrer votre disque, assurez-vous de sauvegarder son contenu afin de ne perdre aucune donnée en cas de perte ou de vol de l'ordinateur, ou

d'incapacité à déchiffrer le disque. Pensez également à effectuer des sauvegardes régulières.

- **Évaluer le temps nécessaire pour chiffrer le disque** et se préparer en conséquence. Reportez-vous à la section *Calcul de la durée du chiffrement* (à la page 5).
- **Effectuer un test pilote afin de vérifier la compatibilité du logiciel** : pour plus de sécurité, PGP Corporation conseille de tester PGP WDE sur quelques ordinateurs afin de vérifier qu'il n'existe aucun conflit avec d'autres logiciels installés avant un déploiement sur un grand nombre d'ordinateurs. Ce test peut s'avérer particulièrement utile dans les environnements utilisant une image COE (Corporate Operating Environment) standardisée. Certains logiciels de protection des disques sont incompatibles avec PGP WDE et peuvent causer de graves problèmes, tels que la perte de données. Reportez-vous à la section *Effectuer un test pilote afin de vérifier la compatibilité du logiciel* (Consultez "*Réalisation d'un test pilote afin de vérifier la compatibilité du logiciel*" à la page 6), qui répertorie les problèmes d'interopérabilité connus, ainsi que les *Notes de publication de PGP Whole Disk Encryption* contenant les mises à jour apportées à cette liste.
- **Vérifier que le mode veille a été désactivé**. PGP Whole Disk Encryption n'est pas compatible avec le mode mise en veille prolongée des systèmes Mac OS X.
- **Utilisation d'Apple Boot Camp**. Si vous utilisez Apple Boot Camp, PGP Corporation vous recommande d'effectuer toutes les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X. Assurez-vous que vous avez installé PGP Whole Disk Encryption sur les partitions Mac OS X et Windows avant d'effectuer les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X.

## Vérification du bon fonctionnement du disque avant le chiffrement

PGP Corporation adopte délibérément une attitude prudente lors du chiffrement des disques afin d'éviter la perte de données. Il n'est pas rare que des erreurs de contrôle de redondance cyclique (CRC) se produisent au cours du processus. Si PGP WDE rencontre un disque dur comportant des secteurs défectueux, il interrompt, par défaut, le processus de chiffrement. Vous pouvez ainsi résoudre le problème avant de reprendre le chiffrement afin d'éliminer les risques d'endommagement du disque et de perte de données.

Pour éviter toute interruption lors du chiffrement, PGP Corporation vous recommande de corriger les erreurs du disque avant de commencer le processus.

**Remarque :** si vous utilisez PGP Whole Disk Encryption dans un environnement géré, les secteurs défectueux identifiés lors du chiffrement sont consignés sur le serveur de gestion et le processus se poursuit.

## Recommandations

Avant d'utiliser PGP Desktop pour chiffrer votre disque, il est recommandé d'exécuter un utilitaire tiers d'analyse du disque capable d'effectuer une vérification de base de l'intégrité des données et de corriger les incohérences pouvant engendrer des erreurs de contrôle de redondance cyclique (CRC). Ces applications sont capables de corriger les erreurs susceptibles d'affecter le chiffrement.

Si vous utilisez Apple Boot Camp, PGP Corporation vous recommande d'effectuer toutes les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X. Assurez-vous que vous avez installé PGP Whole Disk Encryption sur les partitions Mac OS X et Windows avant d'effectuer les opérations de chiffrement et de déchiffrement à partir de la partition Mac OS X.

## Calcul de la durée du chiffrement

Le chiffrement est un processus long et très consommateur en CPU. La durée du processus de chiffrement est fonction de la taille du disque. Prenez ce facteur en compte lorsque vous planifiez le chiffrement initial du disque.

Facteurs ayant une incidence sur la vitesse du chiffrement :

- taille du disque ;
- nombre de processeurs et leur vitesse ;
- nombre de processus système exécutés sur l'ordinateur ;
- nombre d'applications exécutées sur le système ;
- quantité du temps processeur requise par ces applications.

Sur un système moyen, le chiffrement d'un disque de démarrage de 80 Go nécessite environ trois heures avec PGP Desktop (lorsqu'aucune autre application n'est exécutée). Un système très rapide, en revanche, peut facilement chiffrer ce disque en moins d'une heure.

Vous pouvez, sans problème, utiliser votre système lors du chiffrement. Au cours du processus de chiffrement, vous pouvez utiliser le système, mais son fonctionnement est ralenti.

PGP Whole Disk Encryption ralentit automatiquement le processus de chiffrement si vous utilisez le système. Le processus est plus rapide si vous ne vous servez pas de l'ordinateur au cours du chiffrement initial. Le système fonctionne de nouveau normalement une fois le chiffrement terminé.

L'exécution d'autres applications au cours du chiffrement sera légèrement moins rapide jusqu'à la fin du processus.

## Réalisation d'un test pilote afin de vérifier la compatibilité du logiciel

Pour plus de sécurité, PGP Corporation conseille de tester PGP Desktop sur quelques ordinateurs afin de vérifier qu'il n'existe aucun conflit avec d'autres logiciels installés avant un déploiement sur un grand nombre d'ordinateurs.

# Création de volumes PGP Virtual Disk

La fonction relative aux volumes PGP Virtual Disk utilise une partie de l'espace de votre disque dur en tant que volume de disque virtuel chiffré. Vous pouvez créer des utilisateurs supplémentaires pour un volume, afin de permettre aux personnes de votre choix d'y accéder.

8 Dans PGP Whole Disk Encryption, sélectionnez l'élément PGP Disk, puis cliquez sur **Nouveau PGP Virtual Disk**.


9 Dans le champ **Veuillez saisir la taille souhaitée pour le volume PGP Disk**, indiquez la quantité d'espace à réserver au nouveau volume PGP Virtual Disk. Utilisez des nombres entiers, pas des nombres décimaux. Vous pouvez augmenter ou diminuer le chiffre affiché dans le champ à l'aide des flèches. Dans le menu, sélectionnez **Ko** (kilo-octets), **Mo** (méga-octets) ou **Go** (giga-octets).

10 Précisez le type d'authentification à mettre en place pour l'utilisateur principal de ce volume PGP Virtual Disk :

- Pour protéger le volume avec votre paire de clés, sélectionnez **Clé publique**.
- Pour le protéger avec une phrase secrète, sélectionnez **Utilisateur de phrase secrète**.

11 Pour afficher ou modifier les options avancées, cochez la case **Options avancées**. Les options **Chiffrer** et **Formater** s'affichent.

---

**Attention :** les paramètres **Options avancées** par défaut conviennent à la plupart des utilisateurs. Évitez de les modifier si elles ne vous sont pas familières.

---

- Dans le menu **Chiffrer**, sélectionnez l'algorithme de chiffrement à employer pour protéger le volume PGP Virtual Disk : **AES 256 (256 bits)** ou **CAST5 (128 bits)**. Pour plus d'informations sur ces algorithmes de chiffrement, reportez-vous à la section Algorithmes de chiffrement des volumes PGP Virtual Disk du *Guide de l'utilisateur de PGP Desktop pour Mac OS X*.
- Dans le menu **Formater**, choisissez le format de disque à appliquer au volume PGP Virtual Disk.

  **MS-DOS** : optez pour ce format si vous envisagez de partager ce volume avec un autre utilisateur de PGP Whole Disk Encryption 10.2 pour Windows.

  **Mac OS étendu** : il s'agit du format par défaut (utilisé par ailleurs dans le système de fichiers Mac OS moderne) ; il prend en charge les gros volumes PGP Virtual Disk. La taille minimale est de 4 Mo. Le format Mac OS étendu est aussi nommé HFS+.

  **Mac OS étendu (journalisé)** : optez pour ce format si la journalisation est activée sur votre système. (Avec la journalisation, une copie de tous les éléments enregistrés sur le disque est placée dans une zone privée du système de fichiers, ce qui facilite la récupération du disque en cas de besoin.)

  **Mac OS étendu (respecte la casse, journalisé)** : optez pour ce format si la journalisation avec distinction des majuscules et minuscules est activée sur votre système.

  **Mac OS standard** : ce format garantit une compatibilité ascendante avec les systèmes d'exploitation Mac OS plus anciens. La taille minimale du volume doit être de 512 Ko.

  **Système de fichiers UNIX** : optez pour ce format si vous avez l'intention de partager le volume PGP Virtual Disk avec une personne utilisant un système de fichiers UNIX. La taille minimale du volume doit être de 128 Ko.

  Pour connaître le format d'un lecteur Mac OS X existant, sélectionnez-le, puis, dans le menu Fichier, choisissez Obtenir des infos.

12 Cliquez sur **Continuer**.

13 L'étape suivante est différente selon que vous avez choisi une authentification avec clé publique ou phrase secrète.

- Dans le cas d'un accès à l'aide d'une clé publique, l'écran Sélectionnez une clé publique pour sécuriser votre PGP Disk apparaît ; il comporte les clés publiques grâce auxquelles vous pouvez vous authentifier pour accéder au volume PGP Virtual Disk que vous créez.

  Sélectionnez une clé dans la liste fournie et cliquez sur **Continuer**. Vous devez alors saisir la phrase secrète rattachée à la clé choisie (sauf si cette phrase est déjà en cache, auquel cas vous n'avez rien à faire).

  Saisissez la phrase secrète, puis cliquez sur **OK**. La boîte de dialogue Enregistrer sous s'affiche. Passez à l'étape suivante.

- Dans le cas d'un accès à l'aide d'une phrase secrète, l'écran Définir une phrase secrète principale pour votre PGP Disk apparaît.

Dans le champ **Nom**, saisissez le nom que vous souhaitez attribuer à l'utilisateur principal (ou administrateur) du volume PGP Virtual Disk.

Dans le champ **Saisissez votre phrase secrète**, tapez la phrase secrète que vous voulez utiliser. L'indicateur **Qualité de la phrase secrète** indique le niveau de sécurité de la phrase secrète saisie. Si vous souhaitez voir les caractères tapés et si vous êtes sûr que personne ne peut être témoin de la saisie, cochez la case **Afficher les frappes**.

Dans le champ **Confirmez votre phrase secrète**, saisissez à nouveau la phrase secrète à utiliser. Cliquez sur **Continuer.** La boîte de dialogue Enregistrer sous s'affiche. Passez à l'étape suivante.

14 Saisissez un nom de fichier et un emplacement pour le volume PGP Virtual Disk, puis cliquez sur **Enregistrer**.

15 Vérifiez les informations figurant dans l'écran Récapitulatif de la création de PGP Disk. Lorsque vous avez terminé, cliquez sur **Créer**.

16 L'écran Création de votre volume PGP Virtual Disk est affiché ; il indique l'état d'avancement de la création du volume. Lorsque le disque a été créé, l'écran Félicitations apparaît. Cliquez sur **Terminer**.

17 Votre nouveau volume PGP Virtual Disk est monté automatiquement, et les informations afférentes sont affichées dans une fenêtre du Finder. Le nom du disque est en outre fourni sous l'élément **PGP Disk**.

## Création d'une archive PGP Zip

Avec les archives PGP Zip, vous pouvez regrouper différents fichiers et dossiers dans une même archive compressée et portable. Il existe trois types d'archives PGP Zip :

- **Clés des destinataires** : permet de chiffrer l'archive avec des clés publiques. Seul le détenteur des clés privées correspondantes peut ouvrir l'archive. Il s'agit du type d'archive PGP Zip le plus sécurisé. Les destinataires doivent également utiliser le logiciel PGP (pour Windows ou Mac OS X).
- **Phrase secrète** : permet de chiffrer l'archive avec une phrase secrète, qui doit être transmise aux destinataires. Les destinataires doivent également utiliser le logiciel PGP (pour Windows ou Mac OS X).
- **Signer uniquement** : permet de signer l'archive sans la chiffrer, simplement pour prouver que vous êtes bien l'expéditeur. Les destinataires doivent également utiliser le logiciel PGP (pour Windows ou Mac OS X) pour pouvoir ouvrir et vérifier l'archive.

Les types d'archive PGP Zip Phrase secrète et Signer uniquement sont décrits brièvement dans le présent document, mais de manière plus détaillée dans le *Guide de l'utilisateur de PGP Desktop*.

1 Ouvrez PGP Whole Disk Encryption et sélectionnez l'élément PGP Zip. La boîte de dialogue PGP Zip s'affiche.

2 Cliquez sur **Créer un PGP Zip**. La boîte de dialogue PGP Zip sans titre apparaît.

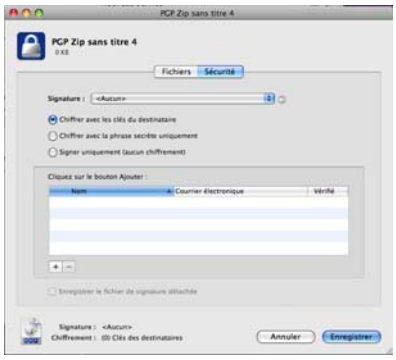
3 Sous l'onglet **Fichiers**, précisez les fichiers ou dossiers à inclure dans l'archive PGP Zip que vous créez. Procédez comme suit :

- Faites glisser les fichiers et dossiers vers la liste.
- Cliquez sur le signe « plus » situé sous la liste, puis, dans la boîte de dialogue qui s'ouvre, sélectionnez les fichiers ou dossiers à inclure dans l'archive PGP Zip. Cliquez ensuite sur **Ajouter** afin d'ajouter les fichiers ou dossiers à la liste.

Si vous ajoutez un fichier ou un dossier et vous apercevez par la suite que vous n'en avez plus besoin, sélectionnez-le dans la liste et cliquez sur le signe « moins » situé au-dessous. Le fichier ou dossier est alors supprimé de la liste.

4 Pour supprimer en toute sécurité de votre système les fichiers ou dossiers que vous placez dans l'archive PGP Zip, choisissez l'option **Décomposer les fichiers originaux**.

5 Lorsque vous avez précisé les fichiers ou dossiers à inclure dans l'archive, cliquez sur l'onglet **Sécurité**.



6 Si vous le souhaitez, spécifiez la clé privée de votre trousseau de clés à utiliser pour doter l'archive PGP Zip en cours de création d'une **signature**.

Cette clé servira à signer numériquement l'archive. Le ou les destinataires peuvent vérifier qui a envoyé l'archive en vérifiant la signature numérique avec la clé publique correspondante.

Pour consulter les propriétés de la clé de signature sélectionnée, cliquez sur l'icône de clé située à droite de

l'ID utilisateur associé à la clé. Lorsque vous avez terminé, fermez la boîte de dialogue Infos sur la clé.

7 Sélectionnez le type de chiffrement à employer :

- **Chiffrer avec les clés du destinataire** : cette option permet de chiffrer l'archive PGP Zip avec les clés publiques du ou des destinataires. Ainsi, seules ces personnes peuvent l'ouvrir.

  Si vous optez pour un chiffrement par clé publique, faites glisser les clés publiques des destinataires sur la liste, ou cliquez sur le signe « plus » et sélectionnez les clés publiques des destinataires souhaités.

- **Chiffrer avec la phrase secrète uniquement** : cette option permet de chiffrer l'archive PGP Zip à l'aide d'une phrase secrète que vous fournissez lors de l'enregistrement de l'archive. Seules les personnes qui connaissent la phrase secrète peuvent ouvrir l'archive. N'oubliez pas de communiquer cette phrase secrète aux personnes auxquelles vous voulez donner accès à l'archive.

  Saisissez-la dans le champ **Phrase secrète**, puis retapez-la dans le champ **Confirmer**. Pour que la phrase secrète s'affiche à mesure que vous saisissez les caractères, sélectionnez **Afficher les frappes**.

- **Signer uniquement (aucun chiffrement)** : cette option permet de créer une archive PGP Zip non chiffrée. Néanmoins, étant donné que vous ne chiffrez pas l'archive, vous devez spécifier une clé de signature dans le champ **Signature**.

8 Si votre archive PGP Zip ne contient qu'un seul fichier et que vous signiez le fichier, mais ne le chiffriez pas, vous devez créer un fichier de signature détachée ; pour cela, cochez la case **Enregistrer le fichier de signature détachée**.

Si vous souhaitez créer ce type de fichier, vous ne pouvez inclure dans l'archive qu'*un seul* fichier, vous devez choisir une clé de signature et vous pouvez pas chiffrer l'archive.

9 Cliquez sur **Enregistrer**.

10 Indiquez un nom de fichier et un emplacement pour l'archive PGP Zip, puis cliquez sur **Enregistrer**. Si vous avez indiqué une clé de signature dans le champ **Signature**, vous êtes invité à saisir la phrase secrète associée (si celle-ci n'est pas en cache).

11 Saisissez la phrase secrète, puis cliquez sur **OK**. L'archive PGP Zip est créée à l'emplacement indiqué.

# Décomposition de fichiers à l'aide de PGP Shred

La fonctionnalité PGP Shredder détruit totalement les fichiers et dossiers, de sorte que même un logiciel de récupération de fichiers élaboré n'est pas en mesure de les récupérer. Lorsque l'icône de PGP Shredder et la Corbeille (sur les systèmes Windows et Mac OS X) apparaissent toutes deux sur votre bureau, seul PGP Shredder écrase immédiatement les fichiers indiqués de sorte qu'ils ne soient pas récupérables.

Pour décomposer des fichiers, utilisez l'un des éléments suivants :

- l'icône PGP Shredder ;
- la barre d'outils de PGP ;
- l'option de ment Décomposer dans PGP Whole Disk Encryption ;
- le Finder.

## Décomposition de fichiers à l'aide de l'icône de PGP Shredder

**Pour décomposer un fichier ou un dossier à l'aide de l'icône de PGP Shredder**

1 Recherchez le fichier ou le dossier à supprimer en toute sécurité.

2 Faites glisser son icône sur celle de PGP Shredder. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.

3 Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

**Conseil :** Créez un alias de l'icône de PGP Shredder sur votre bureau, ainsi vous n'aurez pas besoin de rechercher l'icône de PGP Shredder dans le dossier /Applications pour décomposer les fichiers. Déplacez ensuite l'alias sur le Bureau (ou Dock).

## Décomposition de fichiers à l'aide de l'icône Décomposer les fichiers dans la barre d'outils PGP Whole Disk Encryption

**Pour décomposer un fichier ou un dossier à l'aide de la barre d'outils PGP Whole Disk Encryption**

1 Cliquez sur l'icône **Décomposer les fichiers** dans la barre d'outils.

2 Recherchez le fichier ou le dossier à décomposer, puis cliquez sur **Décomposer**. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.

3 Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

## Décomposition de fichiers à l'aide de la fonction Décomposer du menu Fichier

**Pour décomposer un fichier ou un dossier à l'aide de la fonction Décomposer**

1. Sélectionnez **Fichier > Décomposer.**
2. Accédez au fichier ou au dossier à décomposer, puis cliquez sur **Décomposer**. Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.
3. Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

## Décomposition de fichier dans le Finder

**Pour décomposer un fichier ou un dossier dans le Finder**

1. Dans le Finder, recherchez le fichier ou le dossier à décomposer.
2. Maintenez la touche Ctrl enfoncée et cliquez sur le fichier ou le dossier (ou cliquez avec le bouton droit sur le fichier ou le dossier si votre souris possède deux boutons), puis sélectionnez **PGP > Décomposer.** Une boîte de dialogue de confirmation s'affiche et vous invite à confirmer que vous voulez décomposer (par suppression sécurisée) les fichiers ou les dossiers indiqués.
3. Cliquez sur **OK**. Le fichier ou le dossier est supprimé de votre système en toute sécurité.

# Support technique

Le support technique Symantec possède des centres de support dans le monde entier. Le rôle principal du support technique est de répondre aux demandes spécifiques concernant les caractéristiques et les fonctionnalités des produits. Le groupe de support technique crée également du contenu pour notre base de connaissances en ligne. Le groupe de support technique travaille en collaboration avec les autres domaines fonctionnels de Symantec afin de répondre à vos questions en temps utile. Par exemple, le groupe de support technique collabore avec les services d'ingénierie produit et Symantec Security Response pour fournir des services d'alerte et des mises à jour des définitions de virus.

Les offres de support de Symantec incluent ce qui suit :

- Une gamme d'options de support qui vous offre une flexibilité de sélection de la prestation de service adéquate en fonction de la taille de votre entreprise
- Support téléphonique et/ou en ligne offrant des délais de réponse rapides et des informations de dernière minute
- Assurance de mise à niveau offrant une protection au moyen de la mise à niveau des logiciels
- Support global souscrit en fonction des heures ouvrables régionales ou 24 heures sur 24, 7 jours sur 7
- Service Premium incluant des services de gestion de compte

Pour plus d'informations à propos des offres de support Symantec, vous pouvez visiter notre site Web à l'adresse suivante :

www.symantec.com/business/support/

Tous les services de support seront fournis selon votre contrat de support et la politique de support technique d'entreprise en vigueur.

## Prise de contact avec le support technique

Les clients possédant un contrat de support en cours peuvent accéder aux informations de support technique à l'adresse suivante :

www.symantec.com/business/support/

Avant de contacter le support technique, vérifiez que votre système est conforme à la configuration requise indiquée dans la documentation de votre produit. Vous devez également vous trouver devant l'ordinateur sur lequel le problème s'est produit, au cas où il serait nécessaire de répliquer le problème.

Lorsque vous contactez le support technique, veuillez avoir les informations suivantes à portée de main :

- Niveau de version du produit
- Informations sur le matériel
- Mémoire disponible, espace sur le disque et informations sur la carte réseau
- Système d'exploitation
- Version et niveau de correctif
- Topologie du réseau
- Informations sur le routeur, la passerelle et l'adresse IP
- Description du problème :
  - Messages d'erreur et fichiers journaux
  - Dépannage effectué avant d'avoir contacté Symantec
  - Modifications récentes de la configuration logicielle et modifications du réseau

## Gestion des licences et enregistrement

Si votre produit Symantec requiert un enregistrement ou une clé de licence, rendez-vous sur notre page Web de support technique à l'adresse suivante :

www.symantec.com/business/support/

## Service client

Les coordonnées du service client sont disponibles à l'adresse suivante :

www.symantec.com/business/support/

Le service client est à votre disposition pour des questions non techniques, telles que les types de problèmes suivants :

- Questions concernant la gestion des licences ou la sérialisation de produit
- Mises à jour d'enregistrements de produit, telles que les changements d'adresse ou de nom
- Informations générales sur le produit (fonctionnalités, langues disponibles, distributeurs locaux)
- Dernières informations concernant les mises à jour et les mises à niveau de produits
- Informations sur l'assurance de mise à niveau et les contrats de support
- Informations à propos des programmes d'achat de Symantec
- Conseils sur les options de support technique de Symantec
- Questions de pré-vente non techniques
- Problèmes liés aux CD-ROM ou aux manuels

## Ressources de contrat de support

Si vous souhaitez contacter Symantec concernant un contrat de support existant, veuillez contacter l'équipe d'administration de contrat de support pour votre région, tel que suit :

| | |
|---|---|
| Asie-Pacifique et Japon | customercare_apac@symantec.com |
| Europe, Moyen-Orient, Afrique | semea@symantec.com |
| Amérique du Nord, Amérique latine | supportsolutions@symantec.com |

# Copyright et marques

Copyright (c) 2012 Symantec Corporation. Tous droits réservés. Symantec, le logo Symantec, PGP Corporation, Pretty Good Privacy, et le logo PGP Corporation sont des marques commerciales ou déposées de Symantec Corporation ou de ses sociétés affiliées aux États-Unis et dans d'autres pays. Les autres noms peuvent être des appellations commerciales de leurs détenteurs respectifs.