PGP Desktop pour Windows

Guide de démarrage rapide
Version 10.0

Présentation de PGP Desktop?

PGP Desktop garantit une sécurité complète pour les ordinateurs de bureau et les portables, permettant ainsi aux entreprises, aux groupes de travail et aux individus de protéger leurs informations sensibles sans modifier leur infrastructure informatique ni interrompre leur processus en cours. Cette solution primée facile à utiliser chiffre les messages électroniques, les fichiers, les volumes virtuels et les disques entiers grâce à une application bureautique unique.

La famille d'applications PGP Desktop se combine en plusieurs offres groupées.

- **PGP Desktop Professional** comprend PGP Desktop Email et PGP Whole Disk Encryption
- **PGP Desktop Storage** comprend PGP Whole Disk Encryption et PGP NetShare
- **PGP Desktop Corporate** comprend PGP Desktop Email, PGP Whole Disk Encryption et PGP NetShare

PGP Desktop Email

Grâce à PGP Desktop Email, vous pouvez chiffrer, signer, déchiffrer et vérifier les messages électroniques de façon automatique et transparente conformément à des stratégies qui ont été définies pour vous par des administrateurs ou des stratégies que vous configurez si vous ne vous trouvez pas dans un environnement géré par PGP Universal Server.

PGP NetShare

PGP NetShare permet à des utilisateurs autorisés de partager des fichiers protégés dans un espace commun, tel qu'un serveur de fichiers, un dossier partagé ou un lecteur amovible USB.

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 Desktop 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 Desktop ?

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

- Ce *guide de démarrage rapide* vous explique comment installer PGP Desktop et commencer à l'utiliser.
- Vous trouverez des informations plus détaillées sur PGP Desktop 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 Desktop vous donne accès à un ensemble donné de fonctionnalités PGP Desktop. Certaines fonctionnalités spéciales de PGP Desktop 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 Desktop, consultez le manuel *Guide de l'administrateur de PGP Universal Server*.

Notions de base

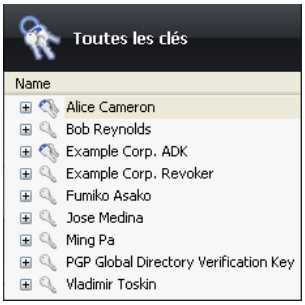
PGP Desktop chiffre, signe, déchiffre et vérifie vos messages à l'aide de clés.

Après l'installation, PGP Desktop 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 Desktop utilise des licences pour octroyer l'accès aux fonctionnalités incluses dans le logiciel. Selon le type de licence dont vous disposez, une partie ou l'intégralité des applications de la gamme PGP Desktop est active.

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

PGP Desktop Email fait partie de la gamme PGP Desktop. Cette application vous permet de chiffrer, signer, déchiffrer et vérifier les messages électroniques de façon automatique et transparente, conformément aux stratégies que vous configurez. Elle vous permet également de chiffrer vos sessions de messagerie instantanée, notamment avec les clients AIM et iChat. Les deux utilisateurs discutant par messagerie instantanée doivent tous deux avoir activé PGP Desktop Email.

La **Visionneuse PGP** fait également partie de la gamme PGP Desktop. Elle vous permet de déchiffrer, de vérifier et d'afficher les messages électroniques en dehors du flux de messagerie. Elle permet également de déchiffrer et d'afficher le contenu des anciens messages IMAP/SMTP/POP hérités.

PGP NetShare fait également partie de la gamme PGP Desktop. Grâce à PGP NetShare, vous pouvez autoriser des utilisateurs à partager des fichiers protégés dans un espace commun, tel qu'un serveur de fichiers d'entreprise, un dossier partagé ou un support amovible de type lecteur USB. Les fichiers chiffrés résidant dans le dossier partagé continuent à apparaître comme des fichiers d'applications normaux aux utilisateurs autorisés ; tout autre utilisateur disposant d'un accès physique aux fichiers peut les afficher mais pas les utiliser.

PGP Whole Disk Encryption (PGP WDE) fait partie de la gamme d'applications PGP Desktop. Vous pouvez avoir recours à cette application 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 de chiffrement complet du disque 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, sans la phrase secrète appropriée, aucun pirate ne pourra accéder à vos données.

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 requise

- Microsoft Windows 2000 (Service Pack 4),

  Remarque : les systèmes d'exploitation ci-dessus sont pris en charge uniquement lorsque tous les correctifs logiciels et de sécurité les plus récents fournis par Microsoft ont été appliqués.

  PGP Whole Disk Encryption (WDE) est pris en charge sur toutes les versions client ci-dessus, ainsi que sur les versions de Windows Server suivantes :

  - Windows Server 2003 SP 2 (éditions 32 et 64 bits)
  - Windows Server 2008 SP 1 et 2 (éditions 32 et 64 bits)
  - Windows Server 2008 R2 (éditions 32 et 64 bits)

  Pour plus d'informations sur la configuration système requise et sur les meilleures pratiques relatives à l'utilisation de PGP WDE sur les systèmes Windows Server, consultez l'*article 1737 de la base de connaissances de PGP* (http://support.pgp.com/?faq=1737).
- 512 Mo de RAM
- 64 Mo d'espace disque dur

Installation de PGP Desktop

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

Remarque : si vous utilisez PGP Desktop au sein d'un environnement géré par un PGP Universal Server, des fonctions et/ou paramètres peuvent être prédéfinis dans le programme d'installation.

➢ Pour installer PGP Desktop

1. Localisez le programme d'installation de PGP Desktop que vous avez téléchargé.

   Celui-ci peut vous avoir été fourni par votre administrateur PGP par le biais de l'outil Déploiement SMS de Microsoft.
2. Double-cliquez sur ce programme.
3. Suivez les instructions affichées à l'écran.
4. Redémarrez votre système lorsque vous y êtes invité.
5. Lorsque votre système redémarre, suivez les instructions à l'écran pour la configuration de PGP Desktop.

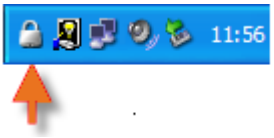
Gestion des licences

Pour connaître les fonctionnalités prises en charge par votre licence, ouvrez PGP Desktop et sélectionnez **Aide > Licence**. Les fonctionnalités prises en charge sont signalées par une coche.

Démarrage de PGP Desktop

Pour démarrer PGP Desktop, suivez l'une des procédures ci-dessous :

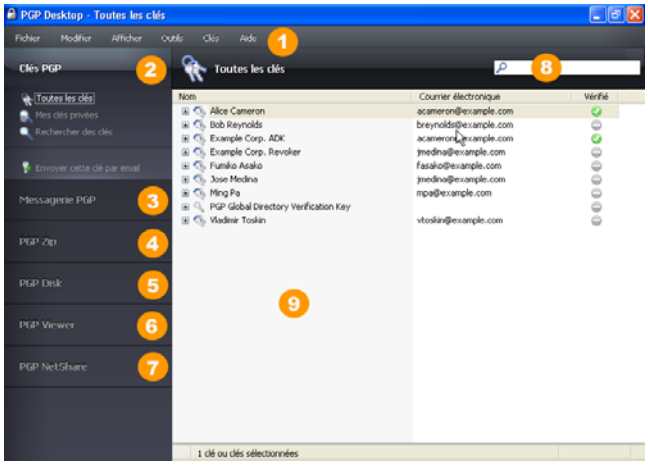
- Double-cliquez sur l'icône de la zone de notification PGP.



- Cliquez sur cette icône avec le bouton droit et sélectionnez **Ouvrir PGP Desktop**.
- Dans le menu **Démarrer**, sélectionnez **Programmes > PGP > PGP Desktop**.

Écran principal de PGP Desktop

La fenêtre de l'application PGP Desktop constitue votre principale interface avec le produit.



L'écran principal de PGP Desktop comporte les éléments suivants :

1	**La barre de menus** : cette barre vous permet d'accéder aux commandes de PGP Desktop. Les menus qu'elle contient sont différents suivant le panneau de contrôle sélectionné.
2	**Le panneau de contrôle Clés PGP** : ce panneau vous permet de contrôler les clés PGP.

3	**Le panneau de contrôle Messagerie PGP** : ce panneau vous permet de contrôler le service de messagerie PGP.
4	**Le panneau de contrôle PGP Zip** : ce panneau vous permet de contrôler PGP Zip, ainsi que l'assistant de PGP Zip, grâce auquel vous pouvez créer des archives PGP Zip.
5	**Le panneau de contrôle PGP Disk** : ce panneau vous permet de contrôler PGP Disk.
6	**Le panneau de contrôle Visionneuse PGP**. Permet de déchiffrer, de vérifier et d'afficher les messages *en dehors* du flux de messagerie.
7	**Le panneau de contrôle PGP NetShare** : ce panneau vous permet de contrôler PGP NetShare.
8	**La zone de travail de PGP Desktop** : cette zone contient des informations sur le panneau de contrôle sélectionné, ainsi que sur les actions que vous pouvez lui appliquer.
9	**La zone de recherche de clés PGP** : cette zone sert à rechercher des clés spécifiques dans votre trousseau de clés. Au fur et à mesure de votre saisie, PGP Desktop affiche les résultats de la recherche en fonction du critère que vous avez indiqué (nom ou adresse de courrier électronique).

Vous pouvez développer chacun des panneaux de contrôle afin de visualiser les options disponibles ou les réduire dans un souci de gain d'espace (dans ce cas, seul le bandeau du panneau de contrôle est visible). Pour développer un panneau de contrôle, cliquez sur son bandeau.

Utilisation de PGP Desktop Email

PGP Desktop Email chiffre et signe les messages sortants, et déchiffre et vérifie les messages entrants, tout cela de manière totalement automatique et transparente. Continuez à envoyer et recevoir votre courrier électronique comme à l'accoutumée ; PGP Desktop Email s'occupe du reste.

Envoi de courriers électroniques chiffrés

Après l'installation, PGP Desktop Email se positionne entre votre client de messagerie et votre serveur de messagerie électronique et surveille le trafic de courrier électronique.

Lorsque des messages *entrants* arrivent, PGP Desktop les intercepte avant qu'ils n'atteignent votre boîte de réception et essaie automatiquement de les déchiffrer et de les vérifier ; il utilise vos clés privées pour le déchiffrement et les clés publiques de tiers pour la vérification. Après avoir traité les messages, il les place dans votre boîte de réception.

Le plus souvent, vous n'avez rien à faire ; les messages entrants déchiffrés sont affichés dans votre boîte de réception exactement comme les autres.

Lorsque vous envoyez du courrier électronique, PGP Desktop Email intercepte ces messages *sortants* lors de leur transfert vers votre serveur de messagerie électronique et essaie automatiquement de les chiffrer et de les signer, conformément aux stratégies configurées.

Là encore, vous n'avez rien à faire ; lorsque vous créez un message à l'aide de votre client de messagerie, puis l'envoyez, PGP Desktop Email se charge de tout.

Pour savoir en détail comment PGP Desktop Email gère vos messages entrants et sortants en toute transparence, reportez-vous aux sections ci-après.

Messages entrants

PGP Desktop Email gère les messages entrants en fonction de leur contenu :

- **Message ni chiffré ni signé** : si un message n'est ni chiffré ni signé, PGP Desktop Email se contente de le transférer vers votre client de messagerie. Vous pouvez lire le message tel qu'il se présente ; PGP Desktop Email ne le traite donc d'aucune manière.
- **Message chiffré mais non signé** : si un message est chiffré, PGP Desktop Email tente de le déchiffrer pour vous permettre de le lire. Il commence par rechercher dans votre trousseau de clés la clé privée capable de déchiffrer le message. S'il la trouve, PGP Desktop Email l'utilise pour l'opération de déchiffrement, puis transmet le message à votre client de messagerie. Dans le cas contraire, il transmet le message au client de messagerie sans le déchiffrer. Celui-ci est alors semblable à l'illustration ci-dessous.

```
-----BEGIN PGP MESSAGE-----
Version: PGP Desktop 10.0

qANQR1DBwUwDMvpGQkaZ1HwBD/0f5F8QKtY+1NVzwQW4xQ/EPuODOmLrMZVVNQVn
rYvHPoSAcn6C3zFpO996akjRioOBGa62hkLpkjQi3QEGpBtqMP1F64TUxqHkpLNH
ISN+7zEA7EYTtV+3ErREOH6yQgJ+sQGm6sjRjddYYvTG6hGa9f2wX+ZDLAIK6SrA
f4ZNQfNvkowMmJXS78Sz7LEGE5d5wM68kKB/FflvfYz1w360QgauIXmom9F8294p
fNaWAnhQlRif/la/MuYs0WkTLPQpdBXhgZqVKaE85gsCrWqXfMAGDEYfrsCAb1Ne
nMWJNtXsRYVpstmpNBZuVHOljKrXE4YEAPk48MOD1Yi54NJxYwvury79oDoxDlJh
o9yh9v5f071orpLFcew8wmLX4qJaGds0VqdwQRRnfwbwnbgsdljD2cmijyOq+bcy
3hZknIEGbb7GTKaKo1cj+y9u5aFDh49lA9qLyHTWwLuHYV/j/wtBPfPZpjGYvACV
FqRDE08hYzxKc/foQwlIMdo+nymZEQItTTdBCaESxm5V+jBwfn0xhUK/EVylkAHm
n27x2m9PdwzxriQjgrxI8Lda7DTJWYmA8ol2OClQZqrqvAmqIKL4CpckyhPuRwIg
nan80KN/USfzK+Vi9juxM1lS5oGYzODtL6KnLnGGpTlu6yLsU2SB7iIbVe33Oukj
zMLXgdLAKQFSItPMVeKqJPxQrMrLlEYr6hE7fcAYmUMwXe8w60e7H2OwEIme2Y9V
eVocs5p9Iau7w987Ifbh1odEb+QEwJMavV5jBcaE1ZhxAYLfrIdXBb1REeuQGjmj
FuCHf6BGgTp9HlNjw92iR5qSintROh2KmwTa5oGbDNnEEAAQJp8sI+6129FLpLgF
z7/wzmnKFngV4OgILxyPCRvS6Pbo3OwAgJehhqDzC9kEkmXd6J7t/caDEMUsnHC1
qTBAScHRB+8eN5yrUrZ5YUqhNvpR/vVN6odPEnX4mbrMsClv4uXRYSv5ofGHJT0U
=8hVs
-----END PGP MESSAGE-----
```

- **Message signé mais non chiffré** : si un message est signé, PGP Desktop Email tente de vérifier la signature. Il recherche la clé publique appropriée aux emplacements suivants, en respectant l'ordre indiqué : votre trousseau de clés par défaut, le serveur de clés de keys.domain (« domain » correspond au domaine de l'expéditeur du message), le serveur PGP Global Directory (keyserver.pgp.com) et enfin tout autre serveur de clés configuré. Si PGP Desktop Email trouve la clé publique qui convient, il tente de vérifier la signature, puis de transférer le message vers votre client de messagerie. Dans le cas contraire, il transfère le message au client de messagerie sans le vérifier.
- **Chiffré et signé** : si un message est à la fois chiffré et signé, PGP Desktop Email commence par rechercher la clé privée qui permettra de le déchiffrer, puis la clé publique à utiliser pour le vérifier.

Messages sortants

PGP Desktop Email gère vos messages électroniques sortants en fonction des stratégies, qui sont des suites d'instructions configurées pour parer à toute situation.

Stratégies par défaut

PGP Desktop Email inclut quatre stratégies par défaut :

- **Demandes administrateur de liste de publipostage** : les demandes administratives de listes de publipostage sont envoyées en clair, c'est-à-dire ni chiffrées, ni signées.
- **Envois de listes de publipostage** : les envois de listes de publipostage sont transférés signés, à des fins d'authentification, mais pas chiffrés.
- **Demander le chiffrement : confidentiel [PGP]** : tout message marqué comme confidentiel dans votre client de messagerie ou contenant le texte « [PGP] » en objet doit être chiffré à l'aide de la clé publique valide du destinataire, sans quoi il ne sera pas envoyé. Cette stratégie représente un moyen de gérer facilement les messages qui *doivent* être envoyés sous forme chiffrée ou ne seront pas envoyés du tout.
- **Chiffrement opportuniste** : indique que tout message pour lequel aucune clé de chiffrement n'a pu être trouvée doit être envoyé en clair (sans chiffrement). Placer cette stratégie en dernier dans la liste des stratégies permet de vous assurer que le message sera effectivement envoyé (sauf si vous le marquez comme étant confidentiel), même si c'est en clair, y compris si la clé de chiffrement du destinataire est introuvable.

Création de stratégies

PGP Desktop Email offre la possibilité de créer et d'utiliser d'autres stratégies que les quatre stratégies par défaut. Vous pouvez créer des stratégies sur la base d'un large choix de critères. Si vous utilisez PGP Desktop Email dans un environnement géré par un PGP Universal Server, vos stratégies de messagerie ainsi que d'autres paramètres peuvent être contrôlés par l'administrateur PGP de l'entreprise.

Pour obtenir des informations exhaustives à propos de la création et de la mise en œuvre des stratégies de messagerie, reportez-vous au manuel *Guide de l'utilisateur de PGP Desktop*.

Mon message a-t-il été chiffré ?

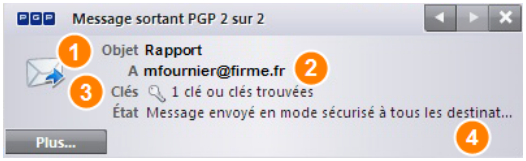
Dans la mesure où PGP Desktop Email agit de façon automatique et transparente, vous pouvez parfois être amené à vous demander si vos messages sont vraiment envoyés sous forme chiffrée. C'est probablement le cas, mais vous pouvez vous en assurer.

Alertes du Notificateur

Les alertes du Notificateur PGP Desktop vous signalent les événements liés à votre système de messagerie et vous permettent de les contrôler.

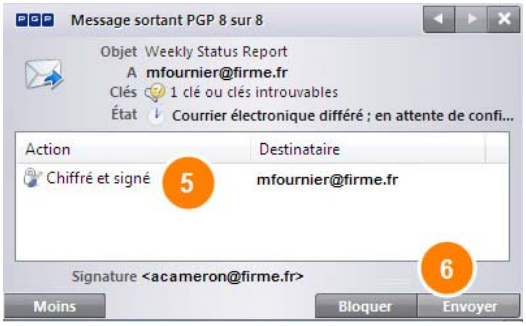
Par exemple, lorsque vous envoyez un message chiffré, l'alerte de Notificateur correspondante apparaît dans le coin inférieur droit de l'écran. Elle comporte les éléments suivants :

1. L'objet de l'alerte.
2. Le nom du destinataire.
3. Les clés trouvées pour ce dernier.
4. L'état du message.



Si vous souhaitez davantage d'informations concernant le message envoyé, cliquez sur **Plus.** D'autres éléments deviennent disponibles :

5. Les opérations que PGP Desktop Email a effectuées sur le message.
6. Le nom du signataire du message.



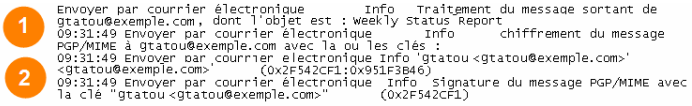
Pour plus d'informations sur les notifications, consultez le manuel *Guide de l'utilisateur de PGP Desktop*.

Journal de PGP

Le journal de PGP répertorie diverses mesures prises par PGP Desktop dans le but de sécuriser votre messagerie.

Par exemple, le message pour lequel les alertes de Notificateur ci-dessus sont affichées a généré dans le journal de PGP une entrée comprenant les éléments suivants :

1. l'indication qu'un message sortant a été envoyé, accompagnée du nom de l'expéditeur et de l'objet du message.
2. L'heure du chiffrement, l'adresse de courrier électronique utilisée pour le chiffrement et l'adresse de courrier électronique de l'expéditeur.



Utilisation de la Visionneuse PGP

En temps normal, PGP Desktop joue le rôle d'intermédiaire entre votre client de messagerie (Mozilla Thunderbird, par exemple) et votre serveur de messagerie électronique, chiffrant et signant les messages sortants, d'une part, et

déchiffrant et vérifiant les messages entrants, d'autre part. Il se trouve alors dans ce que l'on appelle le « flux de messagerie ».

La Visionneuse PGP vous permet de déchiffrer, de vérifier et d'afficher les messages *en dehors* du flux de messagerie.

Ouverture d'un message ou d'un fichier chiffré

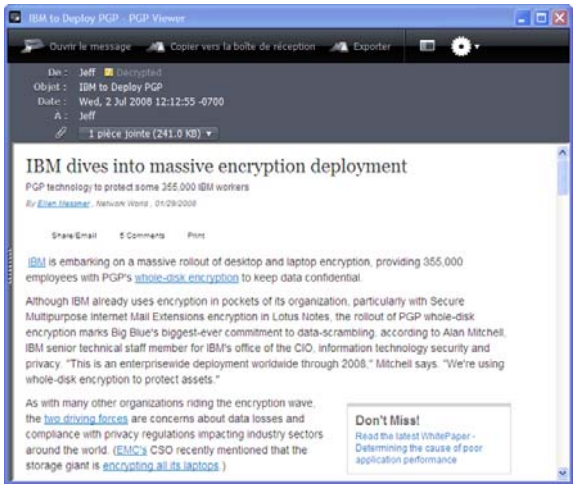
Utilisez la Visionneuse PGP pour ouvrir (déchiffrer, vérifier et afficher) les fichiers de messages chiffrés des types suivants :

- ***.pgp** : créé par une application PGP.
- ***.eml** : créé par Outlook Express ou Thunderbird.
- ***.emlx** : créé par le programme Mail.app d'Apple sur les systèmes Mac OS X.
- ***.msg** : créé par Microsoft Outlook.

Lorsque la Visionneuse PGP ouvre un message chiffré, elle n'écrase pas le texte chiffré. Le message d'origine reste intact.

➢ Pour déchiffrer, vérifier et afficher un message chiffré issu d'un fichier

1. Ouvrez la Visionneuse PGP. Pour cela, cliquez sur l'icône PGP dans la zone de notification et sélectionnez Visionneuse PGP ou, si vous vous trouvez déjà dans PGP Desktop, cliquez sur le panneau de contrôle Visionneuse PGP.
2. Cliquez sur **Ouvrir le fichier dans la Visionneuse PGP**, ou ouvrez le menu **Visionneuse** et sélectionnez **Ouvrir le fichier dans la Visionneuse PGP**. La boîte de dialogue **Ouvrir le fichier du message** s'affiche.
3. Dans celle-ci, accédez au fichier à ouvrir, sélectionnez-le et cliquez sur **Ouvrir**. La Visionneuse PGP déchiffre, vérifie et affiche le message dans une fenêtre séparée.



Conseil : vous pouvez faire glisser le fichier à ouvrir vers la partie de la fenêtre de la Visionneuse PGP qui présente l'intitulé : **Faites glisser les messages ou les fichiers ici**. La Visionneuse PGP ouvre le fichier, le déchiffre et le vérifie, puis affiche le message.

4. Pour ouvrir un autre message, cliquez sur **Ouvrir le message** dans la barre d'outils, accédez au fichier voulu, sélectionnez-le, puis cliquez sur **Ouvrir**. La Visionneuse PGP déchiffre, vérifie et affiche le message. Un volet présentant tous les messages ouverts apparaît sur la gauche de l'écran Visionneuse PGP.
5. Pour ouvrir ce volet ou le fermer s'il est ouvert, cliquez sur le bouton Volet dans la barre d'outils.

Copie de messages électroniques dans votre boîte de réception

Utilisez la Visionneuse PGP pour copier, dans la boîte de réception de votre client de messagerie, des versions en texte brut des messages déchiffrés.

➢ Pour copier un message dans la boîte de réception de votre client de messagerie

1. Lorsque le message est affiché dans la fenêtre de la Visionneuse PGP, cliquez sur **Copier vers la boîte de réception**. La boîte de dialogue de confirmation Copier vers la boîte de réception contient le nom du client de messagerie vers lequel le message va être copié. Pour modifier ce paramètre, reportez-vous aux préférences de la Visionneuse PGP.
2. Cliquez sur **OK** pour continuer. Si vous copiez un message vers le client de messagerie Mozilla Thunderbird pour la première fois, une boîte de dialogue vous informant que vous devez installer un module complémentaire s'affiche.

   Si vous décidez d'installer ce module, cliquez sur **Oui** et suivez les instructions à l'écran ; dans le cas contraire, cliquez sur **Non**. Vous devez utiliser Thunderbird version 2.0 ou ultérieure pour pouvoir installer le module complémentaire.
3. La Visionneuse PGP ouvre votre client de messagerie et copie une version en texte brut du message dans la boîte de réception.

Exportation de messages électroniques

Pour exporter un message déchiffré vers un fichier, utilisez la Visionneuse PGP.

➢ Pour exporter un message depuis la Visionneuse PGP vers un fichier

1. Lorsque le message est affiché dans la fenêtre de la Visionneuse PGP, cliquez sur **Exporter**. La boîte de dialogue Exporter le fichier du message apparaît.
2. Indiquez dans celle-ci l'emplacement, le nom et le format souhaités pour le fichier, puis cliquez sur **Enregistrer**. La Visionneuse PGP enregistre le fichier à l'emplacement choisi.

Indication d'options supplémentaires

Pour spécifier plusieurs fonctionnalités de la Visionneuse PGP, dans la barre d'outils de cette dernière (située à l'extrême

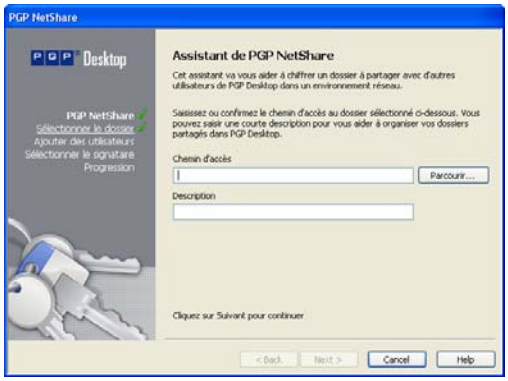
droite), cliquez sur le bouton Outils :

- **Codage du texte** : cette option permet de préciser le format de codage du texte pour le message affiché dans la Visionneuse PGP.
- **Afficher les images distantes** : cette option permet d'afficher les ressources externes (images, feuilles de style CSS, contenu iframe, etc.) pour le message présenté dans la Visionneuse. Vous pouvez configurer la Visionneuse de sorte qu'elle affiche automatiquement les ressources externes dans les préférences.
- **Afficher la source du message** : cette option permet de visualiser la source du message affiché dans la Visionneuse PGP. Ainsi, vous pourrez obtenir davantage d'informations concernant le message.
- **Préférences** : cette option permet d'ouvrir la boîte de dialogue des préférences de la Visionneuse PGP.

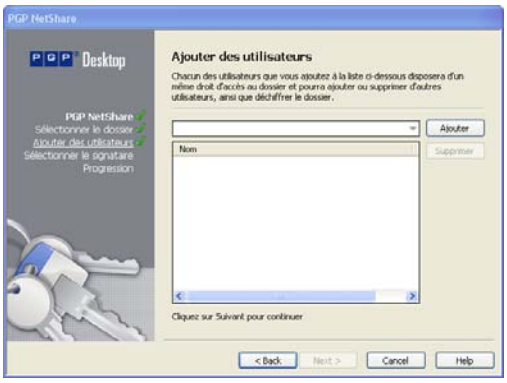
Utilisation de PGP NetShare

La fonctionnalité PGP NetShare permet aux utilisateurs autorisés de partager des fichiers protégés. Vous devez d'abord créer un dossier protégé, puis indiquer les utilisateurs que vous souhaitez autoriser à utiliser ces fichiers.

1. Cliquez sur **Ajouter un dossier** dans le panneau de contrôle PGP NetShare. L'écran Sélectionner le dossier s'affiche.



2. Cliquez sur **Parcourir**, puis sélectionnez le dossier que vous souhaitez protéger.
3. Dans le champ **Description**, saisissez la description du dossier protégé que vous créez ou ne tapez rien pour utiliser le nom par défaut.
4. Cliquez sur **Suivant.** L'écran Ajouter des utilisateurs s'affiche.



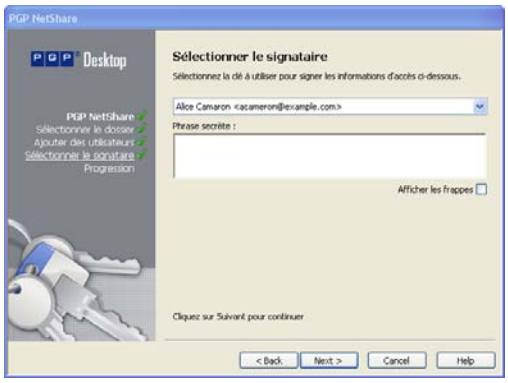
5. Pour spécifier les utilisateurs des fichiers dans le dossier protégé, cliquez sur la flèche vers le bas, sélectionnez un utilisateur, puis cliquez sur **Ajouter.** N'oubliez pas de vous ajouter si vous souhaitez accéder aux fichiers du dossier protégé.

   PGP NetShare n'informe pas les utilisateurs qu'ils peuvent accéder aux fichiers protégés ; cette tâche incombe au créateur d'un dossier protégé.
6. Pour attribuer un rôle à chaque utilisateur, cliquez avec le bouton droit sur son nom et sélectionnez le rôle souhaité :

   - **Administrateur** : créez un seul administrateur par dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture, permet d'ajouter et de supprimer des utilisateurs, d'attribuer des rôles à d'autres utilisateurs et de promouvoir un autre utilisateur au rôle d'administrateur.
   - **Administrateur du groupe** : créez autant d'administrateurs du groupe que nécessaire pour chaque dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture, permet d'ajouter et de supprimer des utilisateurs, ainsi que d'attribuer des rôles à d'autres utilisateurs.
   - **Utilisateur** : créez autant d'utilisateurs que nécessaire pour chaque dossier protégé PGP NetShare. Ce rôle dispose de droits complets en lecture/écriture pour le dossier.

   Vous pouvez modifier le rôle d'un utilisateur à tout moment après la création du dossier protégé. Cliquez sur le dossier protégé dans PGP Desktop, puis cliquez avec le bouton droit sur le nom de l'utilisateur afin de modifier le rôle.

7. Cliquez sur **Suivant.** L'écran Sélectionner le signataire s'affiche.



8. Parmi les clés privées du trousseau local, sélectionnez-en une et saisissez la phrase secrète appropriée (si la phrase secrète n'est pas mise en cache). Cette clé servira à sécuriser les informations de configuration de PGP NetShare pour le dossier protégé et les fichiers qu'il contient.
9. Cliquez sur **Suivant.** L'écran Progression s'affiche. Les fichiers du dossier protégé spécifié sont chiffrés et les utilisateurs spécifiés sont autorisés à les utiliser. Si certains fichiers ont été ignorés (des fichiers système, par exemple), ils sont répertoriés ici.
10. Cliquez sur **Terminer.**

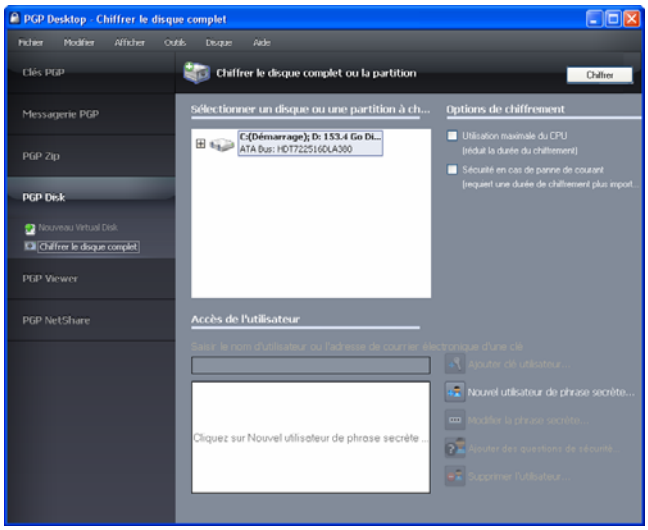
Chiffrement d'un lecteur à l'aide de PGP WDE

La fonctionnalité PGP WDE verrouille l'intégralité du contenu de votre système ou d'un lecteur externe ou USB Flash de votre choix.

L'algorithme de chiffrement employé par PGP WDE est AES256. L'algorithme de hachage est SHA-1. Les lecteurs avec systèmes de fichiers FAT16, FAT32 et NTFS sont pris en charge. Aucune limite de taille (minimale ou maximale) ne s'applique. Tout lecteur compatible avec le système d'exploitation (ou votre BIOS matériel pour le lecteur de démarrage) doit pouvoir fonctionner avec PGP WDE.

Attention : PGP Corporation vous recommande vivement de sauvegarder vos données avant de chiffrer votre disque.

1. Dans le panneau de contrôle PGP Disk, cliquez sur **Chiffrer le disque complet**.



2. Sélectionnez le disque ou la partition à chiffrer.
3. Pour que votre disque soit protégé dans les plus brefs délais, sélectionnez l'option **Utilisation maximale du CPU**. Le chiffrement est alors réalisé avant toute autre opération prévue sur votre système.
4. Si vous craignez une coupure d'alimentation du système au cours du processus, activez l'option **Sécurité en cas de panne de courant**.

   Lorsque cette option est sélectionnée, si le chiffrement est brusquement interrompu, il reprend en toute sécurité. **Cette option peut toutefois augmenter la durée du chiffrement initial.**
5. Pour ajouter des utilisateurs qui s'authentifieront à l'aide du chiffrement par clé publique pour accéder au disque entièrement chiffré, cliquez sur **Ajouter clé utilisateur**.

   Si vous chiffrez un lecteur fixe, vous pouvez seulement utiliser une paire de clés PGP sur un jeton USB Aladdin eToken. En revanche, si vous chiffrez une partition ou un lecteur amovible, vous pouvez employer n'importe quelle paire de clés du système.
6. Pour ajouter des utilisateurs qui s'authentifieront à l'aide d'une phrase secrète, y compris si vous souhaitez utiliser un dispositif USB Flash pour une authentification à deux facteurs, cliquez sur **Nouvel utilisateur de phrase secrète**. Suivez les instructions affichées dans les boîtes de dialogue de l'assistant PGP Disk.

   Si vous chiffrez votre lecteur de démarrage, vous avez la possibilité d'employer votre phrase secrète d'ouverture de session Windows ; ainsi, vous ne devrez saisir vos informations d'identification qu'une seule fois au démarrage.
7. Cliquez sur **Chiffrer**.

Remarque : pour chiffrer des données stockées sur disquette ou sur CD-RW, utilisez des volumes PGP Virtual Disk, pas PGP WDE.

Vous pouvez avoir recours à la fonctionnalité PGP WDE sur un système à double amorçage, dans la mesure où celle-ci est installée et prend en charge le système d'exploitation de démarrage (tel que Windows XP, Windows 2000 ou Windows Vista). Le double amorçage avec un autre système d'exploitation (tel que Linux) est possible, mais seule la partition Windows peut être chiffrée. Le deuxième système d'exploitation doit se trouver sur une autre partition non chiffrée.

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

Meilleures pratiques avec PGP WDE

PGP Corporation recommande d'appliquer les meilleures pratiques suivantes lors de la préparation au chiffrement du disque avec PGP WDE. Veuillez les respecter pour que vos données demeurent protégées pendant et après le chiffrement.

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

1. **Déterminer si le disque concerné est pris en charge :** la fonction PGP WDE protège les disques des ordinateurs de bureau et portables (dans leur intégralité ou seulement quelques partitions), les disques externes et les disques USB Flash. Elle ne prend *pas* en charge les CD-RW/DVD-RW ni les serveurs. 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*.
2. **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.
3. **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. Pour plus d'informations, reportez-vous à la section *Vérification du bon fonctionnement du disque avant le chiffrement* (page 9).
4. **Créer un disque de récupération :** bien qu'il soit très peu probable qu'un enregistrement d'amorçage principal soit endommagé sur un disque ou une partition de démarrage bénéficiant d'une protection via PGP Whole Disk Encryption, cela reste une éventualité. Avant de chiffrer un disque ou une partition de démarrage à l'aide de PGP Whole Disk Encryption, créez un disque de récupération. Pour obtenir des instructions sur la création de ce type de disque, reportez-vous à la section *Création d'un CD de récupération (page 10)*.
5. **S'assurer de disposer d'un accès à l'alimentation secteur** pendant tout le processus de chiffrement : reportez-vous à la section *Alimentation continue pendant le chiffrement* (page 10).
6. **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. Pour connaître la liste des logiciels qui posent des problèmes de compatibilité avec PGP WDE, consultez la section *Réalisation d'un test pilote afin de vérifier la compatibilité du logiciel* (page 10).
7. **Effectuer une récupération de disque sur des disques déchiffrés :** Si vous devez procéder à des opérations de récupération sur un disque protégé à l'aide de PGP Whole Disk Encryption (WDE), PGP Corporation vous recommande, lorsque cela est possible, de commencer par déchiffrer ce disque. Pour cela, dans PGP Desktop, cliquez sur **Disque > Déchiffrer**, soit en utilisant le disque de récupération PGP WDE que vous avez préparé, soit en connectant le disque dur de votre ordinateur à un autre système avec un câble USB et en réalisant le déchiffrement à l'aide du logiciel PGP Desktop installé sur ce dernier. Une fois le disque déchiffré, vous pouvez effectuer la récupération.
8. **Installation sur un système Windows Server**. Si vous installez PGP WDE sur un système Windows Server, consultez l'*article 1737 de la base de connaissances de PGP* (http://support.pgp.com/?faq=1737) pour plus d'informations sur les meilleures pratiques.

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 ou une partition avec 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.

- Avant d'utiliser PGP WDE, exécutez 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). L'utilitaire de vérification du disque de Microsoft Windows (chkdsk.exe) ne permet pas de détecter ces erreurs sur le disque dur cible. Faites plutôt appel à un logiciel tel que SpinRite ou Norton Disk Doctor™. Ces applications sont capables de corriger les erreurs susceptibles d'affecter le chiffrement.
- Il est vivement conseillé de défragmenter les disques

présentant une fragmentation importante avant de les chiffrer.

Remarque : si vous utilisez PGP Desktop dans un environnement géré par un PGP Universal Server, les secteurs défectueux identifiés lors du chiffrement sont consignés sur ce serveur et le processus se poursuit.

Création d'un CD de récupération

Dans la procédure ci-après, le logiciel Roxio est utilisé à titre d'exemple. Les opérations que vous devrez effectuer peuvent être légèrement différentes.

1. Vérifiez que PGP Desktop et Roxio Easy Media Creator ou Roxio Easy CD Creator (ou tout autre logiciel permettant de créer un CD à partir d'une image ISO) sont installés sur votre système.
2. Ouvrez Roxio Easy Media Creator ou Roxio Easy CD Creator et créez un projet de disque de données.
3. Sélectionnez **Fichier > Graver un fichier image disque**.
4. Dans le menu **Fichiers de type**, sélectionnez **Fichiers image disque (ISO)**.
5. Accédez au répertoire PGP. Le répertoire par défaut est `C:\Program Files\PGP Corporation\PGP Desktop\`.
6. Sélectionnez `bootg.iso` et cliquez sur **Ouvrir**.
7. Insérez un CD enregistrable vierge dans le lecteur de CD.
8. Dans l'écran Configuration de la gravure, cliquez sur **Commencer la gravure**.
9. Lorsque la gravure est terminée, cliquez sur **OK**.
10. Retirez le CD de récupération du lecteur et étiquetez-le.

Attention : les disques de récupération PGP WDE sont uniquement compatibles avec la version de PGP Desktop utilisée pour les créer. Par exemple, si vous tentez d'utiliser un disque de récupération 9.0.x pour déchiffrer un disque protégé à l'aide du logiciel PGP WDE 9.7, le disque PGP WDE 9.7 sera inutilisable.

Alimentation continue pendant le chiffrement

Dans la mesure où le chiffrement est un processus très consommateur d'UC, il ne peut être lancé sur un ordinateur portable alimenté par batterie. L'ordinateur *doit* impérativement être branché au secteur. Si un ordinateur portable passe sur l'alimentation par batterie au cours du processus de chiffrement initial (ou lors d'un déchiffrement ou d'un nouveau chiffrement), PGP WDE interrompt l'opération. Celle-ci reprend lorsque l'ordinateur est rebranché sur l'alimentation secteur.

Quel que soit le type d'ordinateur utilisé, il est impératif que son alimentation ne soit pas coupée et que le système ne soit pas arrêté subitement au cours du processus de chiffrement, à moins que vous ayez activé l'option Sécurité en cas de panne de courant.

Ne retirez pas le câble d'alimentation avant la fin du chiffrement. Si néanmoins vous redoutez une coupure d'alimentation ou si vous ne disposez pas d'onduleur, activez l'option Sécurité en cas de panne de courant, en suivant les instructions qui figurent dans le *Guide de l'utilisateur de PGP Desktop*.

Attention : il en est de même pour les disques amovibles, tels que les périphériques USB. À moins d'avoir activé l'option **Sécurité en cas de panne de courant**, vous risquez d'endommager le périphérique en le retirant au cours du processus.

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

Certains logiciels de protection des disques sont incompatibles avec PGP WDE et peuvent causer de graves problèmes, tels que la perte de données. Consultez les problèmes d'interopérabilité connus répertoriés ci-après, ainsi que les Notes de publication de PGP Desktop contenant les mises à jour apportées à cette liste.

Incompatibilités logicielles :

- Faronics Deep Freeze (toutes éditions confondues).
- Utimaco Safeguard Easy 3.x.
- Produit de suivi et de sécurisation de portable CompuTrace d'Absolute Software. PGP Whole Disk Encryption est compatible uniquement avec la configuration BIOS de CompuTrace. Il ne peut pas être utilisé si CompuTrace fonctionne en mode MBR.
- Produits de chiffrement de disque dur de GuardianEdge Technologies : Encryption Anywhere Hard Disk et Encryption Plus Hard Disk, anciennement connus sous le nom de PC Guardian.

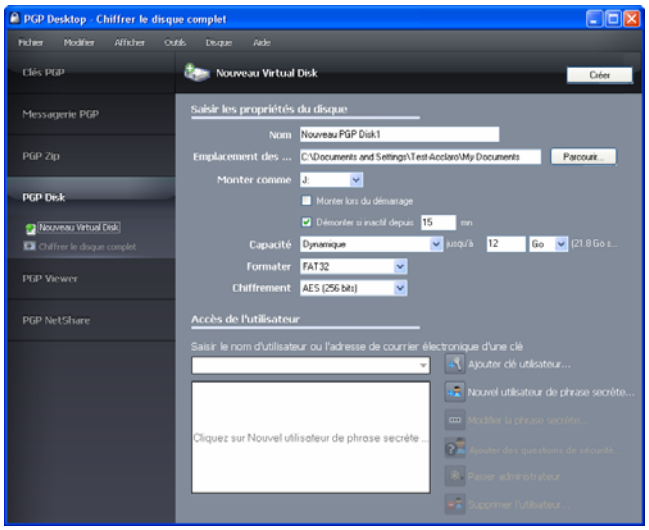
Les programmes suivants peuvent être installés sur le même système que PGP Desktop, mais bloqueront la fonctionnalité PGP Whole Disk Encryption :

- Safeboot Solo
- SecureStar SCPP

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 lecteur virtuel chiffré possédant sa propre lettre. Vous pouvez créer des utilisateurs supplémentaires pour un volume, afin de permettre aux personnes de votre choix d'y accéder.

1. Dans le panneau de contrôle PGP Disk, cliquez sur **Nouveau Virtual Disk**.



2. Dans le champ **Nom**, saisissez un nom pour le volume.
3. Dans le champ **Emplacement des fichiers de disque**, indiquez l'emplacement des fichiers du disque.
4. Pour préciser vos préférences de montage, procédez comme suit :
   - Sélectionnez la lettre correspondant au volume auquel vous voulez appliquer l'opération **Monter comme**.
   - Sélectionnez **Monter lors du démarrage** pour que votre nouveau volume soit automatiquement monté au démarrage.
   - Pour qu'il soit démonté de façon automatique lorsqu'il est resté inactif durant le délai indiqué, activez l'option **Démonter si inactif depuis x min**.
5. Dans **Capacité**, sélectionnez **Dynamique (redimensionnable)** si vous souhaitez que la taille du volume augmente à mesure que vous ajoutez des fichiers ou **Taille fixe** si vous préférez conserver toujours la même taille.
6. Indiquez un **format** de système de fichiers pour le volume.
7. Indiquez un algorithme de **chiffrement**.
8. Cliquez sur **Ajouter clé utilisateur** afin d'ajouter des utilisateurs qui ont recours au chiffrement par clé publique pour s'authentifier ou sur **Nouvel utilisateur de phrase secrète** afin d'ajouter des utilisateurs qui ont recours à une phrase secrète.
9. Cliquez sur **Créer**.

Vous pouvez contrôler les utilisateurs existants d'un volume PGP Virtual Disk par le biais de la section **Accès de l'utilisateur** :

1. Pour ajouter des utilisateurs qui s'authentifieront à l'aide du chiffrement par clé publique, cliquez sur **Ajouter clé utilisateur**.
2. Pour ajouter des utilisateurs qui s'authentifieront à l'aide d'une phrase secrète, cliquez sur **Nouvel utilisateur de phrase secrète**.
3. Sélectionnez un utilisateur de phrase secrète, puis cliquez sur **Modifier la phrase secrète** pour modifier cette dernière.
4. Choisissez un utilisateur et cliquez sur **Passer administrateur** pour lui octroyer des droits d'administrateur.
5. Choisissez un utilisateur, puis cliquez sur **Supprimer** pour le supprimer.

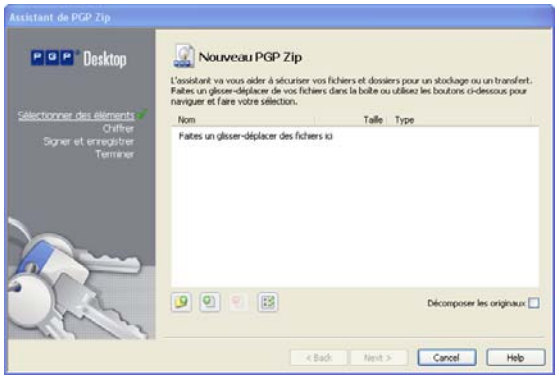
Création d'une archive PGP Zip

Avec les archives PGP Zip, vous pouvez regrouper différents fichiers et dossiers dans une même archive compressée et portable. Il existe quatre 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).
- **Archive à auto-déchiffrement de PGP** : permet de chiffrer l'archive avec une phrase secrète. Les destinataires peuvent ouvrir cette dernière même s'ils n'ont pas installé le logiciel PGP, mais leur ordinateur doit être doté du système d'exploitation Microsoft Windows. Ils doivent en outre avoir reçu la phrase secrète.
- **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. Dans le panneau de contrôle PGP Zip, cliquez sur **Nouveau PGP Zip**.



2. Faites glisser les fichiers/dossiers à inclure dans l'archive ou utilisez les boutons pour les sélectionner.
3. Pour que ces fichiers/dossiers soient décomposés lors de la création de l'archive, sélectionnez l'option **Envoyer les fichiers originaux vers PGP Shredder**.
4. Cliquez sur **Suivant**.
5. Choisissez le type d'archive PGP Zip souhaité :
   - **Clés des destinataires ;**
   - **Phrase secrète ;**
   - **Archive à auto-déchiffrement de PGP**
   - **Signer uniquement.**
6. Cliquez sur **Suivant**.

Les types d'archive **Phrase secrète** et **Signer uniquement** sont décrits en détail dans le *Guide de l'utilisateur de PGP Desktop*.

Reportez-vous à la section correspondant au type d'archive choisi dans les pages suivantes.

Clés des destinataires

L'écran Ajouter des clés utilisateur apparaît.

1. Cliquez sur **Ajouter** et, dans l'écran Sélection d'utilisateurs, choisissez les clés publiques des personnes que vous souhaitez autoriser à ouvrir l'archive. Si vous voulez pouvoir l'ouvrir vous-même, pensez à inclure votre propre clé publique.
2. Cliquez sur **Suivant**.
3. Choisissez sur le système local la clé privée qui servira à signer l'archive.
4. Indiquez un nom et un emplacement pour l'archive. Le nom par défaut est le nom du premier fichier ou dossier de l'archive ; quant à l'emplacement par défaut, il s'agit du répertoire dans lequel se trouvent les fichiers/dossiers qui la composent.
5. Cliquez sur **Suivant**. L'archive PGP Zip est créée. L'écran Terminé présente des informations sur la nouvelle archive.
6. Cliquez sur **Terminer**.

Remarque : les types d'archive PGP Zip Phrase secrète et Clés des destinataires sont très semblables, la seule différence étant que dans un cas, une phrase secrète est employée pour protéger l'archive, alors que dans l'autre, il s'agit d'une clé.

Remarque : de même, les types d'archive PGP Zip Signer uniquement et Clés des destinataires sont très proches, mais avec Signer uniquement, vous ne sélectionnez pas de clés publiques, étant donné que l'archive est seulement signée, pas chiffrée.

Archive à auto-déchiffrement de PGP

L'écran Créer une phrase secrète apparaît.

1. Saisissez une phrase secrète pour l'archive à auto-déchiffrement PGP Zip et confirmez-la.
2. Cliquez sur **Suivant**.
3. Choisissez sur le système local la clé privée qui servira à signer l'archive.
4. Indiquez un nom et un emplacement pour l'archive. Le nom par défaut est le nom du premier fichier ou dossier de l'archive ; quant à l'emplacement par défaut, il s'agit du répertoire dans lequel se trouvent les fichiers/dossiers qui la composent.
5. Cliquez sur **Suivant**. L'archive à auto-déchiffrement de PGP est créée.
6. Cliquez sur **Terminer**.

Décomposition de fichiers à l'aide de PGP Shred

La fonctionnalité PGP Shredder détruit totalement les fichiers et dossiers, et même un logiciel de récupération de fichiers élaboré n'est pas en mesure de les récupérer. Les icônes PGP Shredder et de la Corbeille Windows figurent toutes deux sur le bureau, mais seule la première permet de supprimer immédiatement et irrémédiablement les fichiers que vous indiquez.

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

- l'icône PGP Shredder ;
- la barre d'outils de PGP ;
- le menu contextuel de PGP.

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

➢ Pour décomposer des fichiers à l'aide de l'icône PGP Shredder

1. Sur le bureau Windows, faites glisser les fichiers et dossiers à décomposer dans PGP Shredder. Une boîte de dialogue apparaît ; vous êtes invité à confirmer la décomposition des éléments.
2. Cliquez sur **Oui**. Les fichiers et dossiers indiqués sont alors décomposés.

Décomposition de fichiers à l'aide de la barre d'outils de PGP

➢ Pour décomposer des fichiers à l'aide de la barre d'outils de PGP

1. Dans la fenêtre principale de l'application PGP Desktop, sélectionnez **Outils > Décomposer les fichiers**. La boîte de dialogue Ouvrir s'affiche.
2. Sélectionnez les fichiers de votre système à décomposer,

puis cliquez sur **Ouvrir.** 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 **Oui** . Les fichiers sont supprimés de votre système de façon sécurisée.

Décomposition de fichiers à l'aide du menu contextuel de PGP

➢ Pour décomposer des fichiers par le biais de l'Explorateur Windows

1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur les fichiers/dossiers à 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.
2. Cliquez sur **Oui** . Les fichiers sont supprimés de votre système de façon sécurisée.

Remarque : si vous n'utilisez la fonctionnalité PGP Shredder que rarement, vous pouvez supprimer l'icône correspondante du bureau par l'intermédiaire des options PGP. Pour ce faire, sélectionnez **Outils > Options**, cliquez sur l'onglet Disque, désactivez l'option **Placer l'icône de PGP Shredder sur le bureau** , puis cliquez sur **OK**.

Remarque : vous pouvez recourir aux options PGP pour contrôler le nombre de passes lors de la décomposition (plus il est important, plus le processus est sécurisé, mais aussi long), définir si les fichiers présents dans la Corbeille Windows doivent être décomposés lorsque vous videz cette dernière et configurer l'affichage de la boîte de dialogue d'avertissement pendant la décomposition.

Décomposition de l'espace libre

La fonctionnalité de décomposition de l'espace libre par PGP décompose totalement l'espace libre sur vos lecteurs, rendant les données supprimées irrécupérables. N'oubliez pas que la mention « espace libre » est impropre. En réalité, cette fonctionnalité remplace les sections du disque dur que Windows considère vierges ; cet espace peut effectivement être vide ou bien contenir des fichiers que Windows croyait supprimés.

Lorsque vous placez des fichiers dans la Corbeille, puis que vous videz celle-ci, les fichiers ne sont pas réellement supprimés ; Windows fait simplement comme si aucun élément n'était présent et remplace les fichiers. Toutefois, tant que les fichiers ne sont pas remplacés, ils peuvent être facilement récupérés par un pirate. La fonctionnalité de décomposition de l'espace libre par PGP écrase cet « espace libre », de sorte qu'il devient impossible de les récupérer même avec un logiciel de récupération de disque.

➢ Pour décomposer de l'espace libre sur vos disques

1. Ouvrez PGP Desktop.
2. Sélectionnez **Outils > Décomposer de l'espace libre par PGP**.
3. Lisez les informations figurant dans l'écran d'introduction, puis cliquez sur **Suivant**.
4. Dans l'écran Collecte des informations en cours, dans le champ **Décomposer le lecteur**, choisissez le disque ou le volume que vous voulez décomposer et le nombre de passes que PGP doit effectuer pour décomposer de l'espace libre.

   Le nombre de passes recommandé est :

   - 3 passes pour un usage personnel ;
   - 10 passes pour un usage commercial ;
   - 18 passes pour un usage militaire ;
   - 26 passes pour une sécurité maximale.
5. Activez ou désactivez l'option **Décomposer les structures de données internes NTFS** (disponible sur certains systèmes seulement) et cliquez sur **Suivant**.

   Cette option permet de décomposer les petits fichiers (taille inférieure à 1 Ko) des structures de données internes qui ne le seraient pas en temps normal.
6. Dans l'écran Effectuer une décomposition, cliquez sur **Démarrer la décomposition**.

   Remarque : pour programmer une décomposition ultérieure de l'espace libre, cliquez sur **Planification**. Le planificateur de tâches de Windows doit être installé sur votre système.

   La durée de l'opération de décomposition dépend du nombre de passes indiqué, de la vitesse du processeur, du nombre d'applications en cours d'exécution, etc.
7. Lorsque l'opération prend fin, cliquez sur **Suivant**.
8. Dans l'écran Fin, cliquez sur **Terminer**.

Assistance

Coordonnées

Prise de contact avec le support technique

- Pour connaître les différentes options de support offertes par PGP et savoir comment contacter le support technique, accédez à la *page d'accueil du support de PGP Corporation* (https://support.pgp.com).
- Pour consulter la base de connaissances du support PGP ou entrer en relation avec le support technique, accédez au *portail du support PGP* (https://support.pgp.com). **Remarque : il vous est possible de consulter certaines parties de la base de connaissances du support PGP même si vous ne bénéficiez pas d'un contrat de**

support technique, mais vous devez avoir souscrit à ce type de contrat pour pouvoir faire appel au support technique.

- Pour accéder aux forums de support PGP, visitez le *support de PGP* (http://forum.pgp.com). Vous pourrez alors participer aux forums de communautés d'utilisateurs hébergés par PGP Corporation.

Prise de contact avec le service clientèle

- Pour obtenir de l'aide à propos des commandes, des téléchargements et de la gestion des licences, consultez le *service clientèle de PGP Corporation* (https://pgp.custhelp.com/app/cshome).

Prise de contact avec les autres services

- Pour contacter d'autres personnes de PGP Corporation, consultez la *page des contacts PGP* (http://www.pgp.com/about_pgp_corporation/contact/index.html).
- Pour des informations générales sur PGP Corporation, visitez le *site Web de PGP* (http://www.pgp.com).

Documentation disponible

Avant l'installation, vous pouvez consulter la documentation complète relative au produit sur le *portail du support de PGP Corporation* (https://support.pgp.com).

Sauf indication contraire, l'aide en ligne est installée et accessible à partir de PGP Desktop. Des notes de publication sont également disponibles ; elles présentent les informations de dernière minute qui n'ont pas pu être incluses dans la documentation du produit. Les guides de l'utilisateur et les guides de démarrage rapide, fournis sous la forme de fichiers PDF, sont disponibles sur le *portail du support de PGP Corporation* (https://support.pgp.com).

Une fois que PGP Desktop est commercialisé, des informations complémentaires sont intégrées à la base de connaissances en ligne disponible sur la *base de connaissances du support de PGP* (https://support.pgp.com/?faq=589).

Copyright et marques