PGP Desktop Email

Guide de démarrage rapide
Version 10.2

Présentation de PGP Desktop Email

PGP Desktop Email fait partie de la gamme PGP Desktop. Ce logiciel vous permet de réaliser les tâches suivantes :

- chiffrer, signer, déchiffrer et vérifier les messages électroniques de façon automatique et transparente, conformément aux stratégies que vous configurez.
- Utiliser une partie de l'espace de votre disque dur en tant que lecteur virtuel chiffré possédant sa propre lettre.
- Créer des archives PGP Zip chiffrées et protégées.
- Regrouper des fichiers et dossiers au sein d'un module compressé chiffré unique pouvant être ouvert sur les systèmes Windows sur lesquels PGP Desktop Email ou PGP Desktop n'est pas installé.
- Détruire définitivement des fichiers et dossiers pour qu'ils ne puissent pas être récupérés, même à l'aide d'un logiciel de récupération de fichiers.
- Supprimer en toute sécurité l'espace libre sur vos lecteurs pour empêcher la récupération des données que vous avez supprimées.

Table des matières

Vous venez d'acheter PGP Desktop Email ?

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

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

Notions de base

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

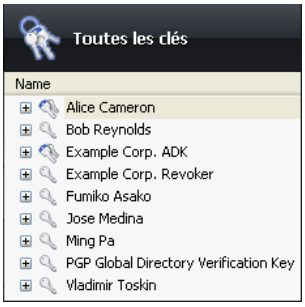
Après l'installation, PGP Desktop Email vous invite à créer une paire de clés PGP. Une paire de clés est constituée d'une clé privée et d'une clé publique.

- 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 Email 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 Desktop Email sont actives en partie ou dans leur ensemble.

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. Vous pouvez l'utiliser pour chiffrer, signer, déchiffrer et vérifier les messages électroniques de façon automatique et transparente, conformément aux stratégies que vous configurez. Cette application vous permet aussi de chiffrer vos sessions de messagerie instantanée, notamment avec les clients AIM et iChat. Les 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.

Les autres composants intégrés à PGP Desktop Email sont les suivants :

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.

Archives à auto-déchiffrement de PGP : ce type d'archive permet de regrouper des fichiers et dossiers au sein d'un module compressé chiffré pouvant être ouvert sur les systèmes Windows sur lesquels aucun logiciel PGP n'est installé. Les archives à auto-déchiffrement constituent la solution parfaite pour sécuriser l'échange de fichiers avec des tiers ne disposant pas de PGP.

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

PGP Desktop Email peut être installé sur des systèmes fonctionnant sous les versions suivantes du système d'exploitation Microsoft Windows :

- Windows XP Professionnel 32 bits (Service Pack 2 ou 3), Windows XP Professionnel 64 bits (Service Pack 2), Windows XP Édition Familiale (Service Pack 2 ou 3), Microsoft Windows XP Édition Tablet PC 2005 SP2, Windows Vista (toutes les versions 32 et 64 bits comprenant Service Pack 2), Windows 7 (toutes les versions 32 et 64 bits comprenant le Service Pack 1), Windows Server 2003 (Service Pack 1 et 2).

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.

Remarque : PGP Whole Disk Encryption (PGP WDE) n'est pas compatible avec les autres logiciels tiers pouvant contourner la protection PGP WDE sur l'enregistrement d'amorçage principal (MBR) et écrire sur ce dernier ou le modifier. Sont compris les outils de défragmentation autonomes qui contournent la protection du système de fichiers PGP WDE ou les outils de restauration système qui remplacent le MBR.

Configuration matérielle requise

- 512 Mo de RAM
- 64 Mo d'espace disque dur

Installation de PGP Desktop Email

Symantec 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 Email 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 Email

1. Localisez le programme d'installation de PGP Desktop Email 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 Email.

Gestion des licences

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

Démarrage de PGP Desktop Email

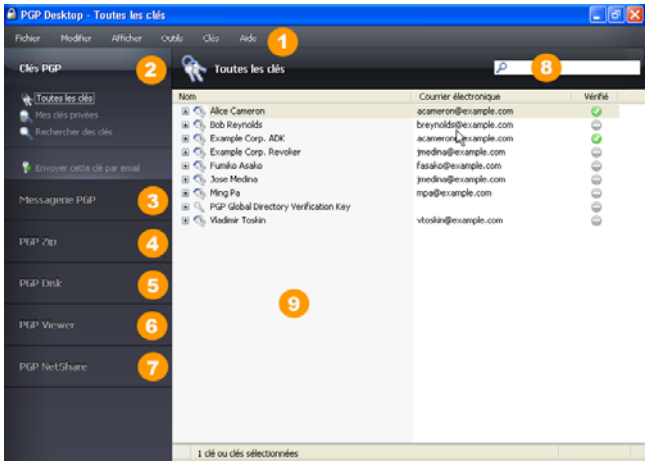
Pour démarrer PGP Desktop Email, suivez l'une des procédures ci-dessous :

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

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

Écran principal de PGP Desktop Email

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



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

1	**La barre de menus** : cette barre vous permet d'accéder aux commandes de PGP Desktop Email. Les menus qu'elle contient sont différents suivant la boîte de contrôle sélectionnée.
2	**La boîte de contrôle Clés PGP** : ce panneau vous permet de contrôler les clés PGP.
3	**La boîte de contrôle Messagerie PGP** : ce panneau vous permet de contrôler le service de messagerie PGP.
4	**La boîte 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	**La boîte de contrôle PGP Disk** : ce panneau vous permet de contrôler PGP Disk.
6	**La boîte de contrôle PGP Viewer**. Permet de déchiffrer, de vérifier et d'afficher les messages *en dehors* du flux de messagerie.
7	**La boîte de contrôle PGP NetShare** : ce panneau vous permet de contrôler PGP NetShare.
8	**La zone de travail de PGP Desktop Email** : cette zone contient des informations sur la boîte de contrôle sélectionnée, 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 Email affiche les résultats de la recherche en fonction du critère que vous avez indiqué (nom ou adresse de courrier électronique).

Vous pouvez développer chacune des boîtes de contrôle afin de visualiser les options disponibles ou les réduire dans un souci de gain d'espace (dans ce cas, seule la bannière de la boîte de contrôle est visible). Pour développer une boîte de contrôle, cliquez sur sa bannière.

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.

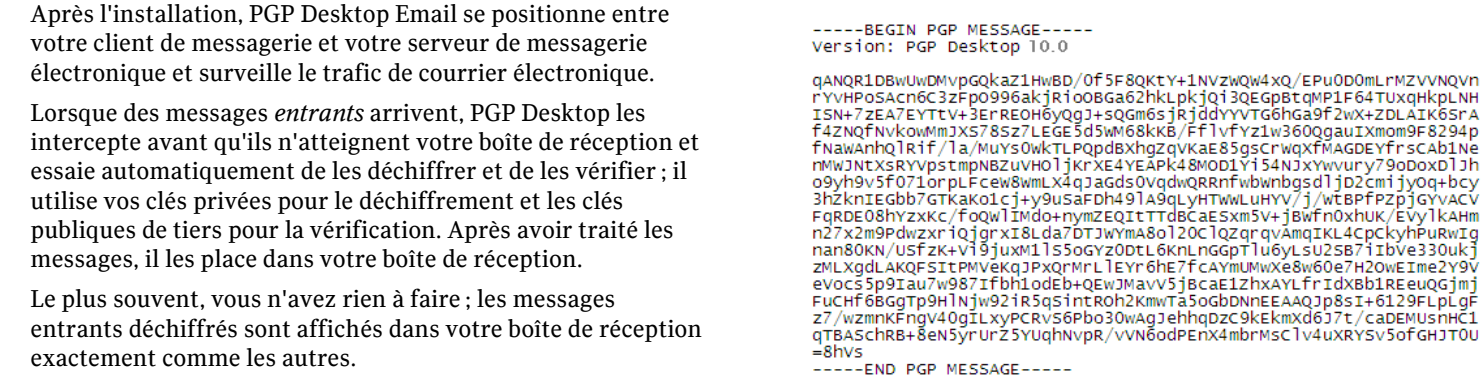
Là encore, vous n'avez rien à faire ; lorsque vous créez un message à l'aide de votre client de messagerie, puis l'envoyez, PGP Desktop Email se charge de tout.

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.



- **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 Email 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 du notificateur correspondante apparaît dans le coin inférieur droit de l'écran. Elle comprend les éléments suivants :

- l'objet de l'alerte ;
- le nom du destinataire ;
- les clés trouvées pour ce dernier ;
- l'état du message.

Pour afficher de plus amples informations sur le message envoyé, cliquez sur **Plus**. D'autres éléments deviennent disponibles :

- les opérations que PGP Desktop Email Email a effectuées sur le message ;
- le nom du signataire du message.

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

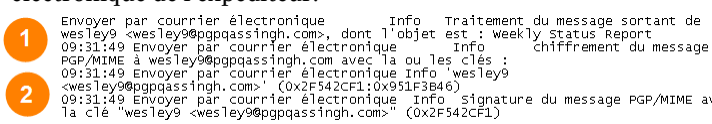
Remarque : dans un environnement géré par PGP Universal Server, votre administrateur peut avoir défini certains paramètres de notification (par exemple, si les notifications doivent s'afficher ou l'emplacement du notificateur). Dans ce cas, il est possible que vous ne voyiez aucun message de notification.

Journal de PGP

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

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

1. Une mention indiquant 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

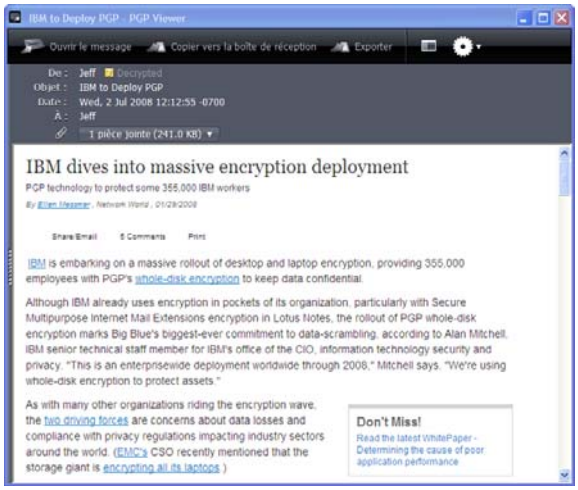
Utilisez la Visionneuse PGP pour ouvrir (déchiffrer, vérifier et afficher) les fichiers de messages chiffrés des types suivants :

- ***.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

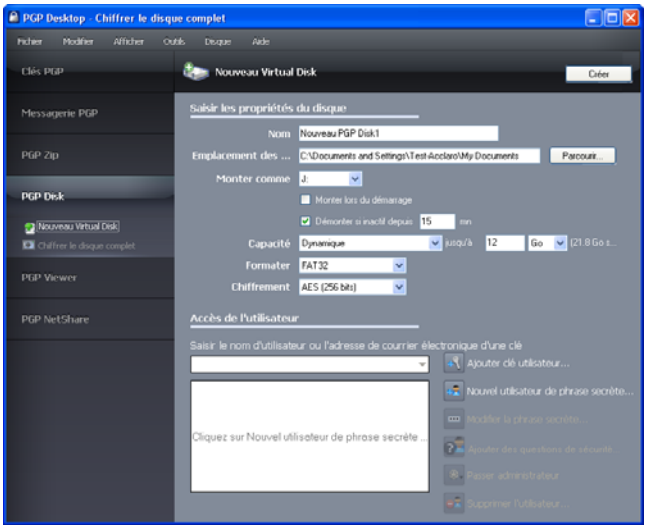
Visionneuse PGP. Ainsi, vous pourrez obtenir davantage d'informations concernant le message.

- **Préférences** : cette option permet d'ouvrir la boîte de dialogue des préférences de la Visionneuse PGP.

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 Email, 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 Email.
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**.

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