



Guard

Manuel de l'utilisateur



Guard: Manuel de l'utilisateur

Date de publication mardi, 12. juillet 2016 Version 2.4.2

Copyright © 2016-2016 OX Software GmbH, Ce document est la propriété intellectuelle de OX Software GmbH

Ce document peut être copié en totalité ou en partie, à condition que chaque copie contienne cette note de copyright. Les informations contenues dans cet ouvrage ont été compilées avec le soin le plus extrême. Néanmoins, des affirmations erronées ne peuvent être exclues d'emblée. OX Software GmbH, les auteurs et les traducteurs ne peuvent être tenus responsables des erreurs éventuelles ni de leurs conséquences. Les noms des logiciels et des matériels utilisés dans cet ouvrage peuvent être des marques de commerce déposées ; ils sont cités sans garantie de libre usage. OX Software GmbH se conforme généralement aux conventions typographiques des fabricants. La reproduction de noms de marques, de dénominations sociales, de logos, etc. dans ce livre (même sans annotation particulière) ne permet pas de supposer que de tels noms puissent être considérés comme libres (au sens des réglementations sur les marques de commerce et les noms de marque).

Table des matières

| | |
|---|-----------|
| 1 À propos de cette documentation | 5 |
| 2 À quoi sert Guard ? | 7 |
| 3 Utiliser Guard | 9 |
| 3.1 Configuration de <i>Guard</i> | 10 |
| 3.2 Chiffrer les conversations par courriel | 11 |
| 3.2.1 Lire des courriels chiffrés | 11 |
| 3.2.2 Envoyer des courriels chiffrés | 11 |
| 3.2.3 Comment un destinataire externe peut-il lire un courriel chiffrée ? | 12 |
| 3.3 Chiffrer des fichiers | 13 |
| 3.3.1 Chiffrer des fichiers | 13 |
| 3.3.2 Créer de nouveaux fichiers chiffrés | 13 |
| 3.3.3 Ouvrir des fichiers chiffrés | 13 |
| 3.3.4 Télécharger des fichiers chiffrés | 14 |
| 3.3.5 Déchiffrer des fichiers | 14 |
| 3.4 Se déconnecter de Guard | 15 |
| 3.5 Réglages de Guard | 16 |
| 3.5.1 Réglages de sécurité Guard | 16 |
| 3.5.2 Réglages de chiffrement PGP | 17 |
| 3.5.3 Gérer les clés | 18 |
| Index | 21 |

1 À propos de cette documentation

Les informations qui suivent vous aideront à tirer le meilleur profit de la documentation.

- [À qui s'adresse cette documentation ?](#)
- [Que contient cette documentation ?](#)
- [Plus d'aide](#)

À qui s'adresse cette documentation ?

Cette documentation s'adresse aux utilisateurs souhaitant utiliser le chiffrement pour protéger leur communication par courrier électronique et leurs fichiers contre des accès non autorisés.

Que contient cette documentation ?

Cette documentation inclut les informations suivantes :

- Dans [À quoi sert Guard ?](#), vous trouverez une brève description de Guard.
- Dans [Utiliser Guard](#) vous trouverez des instructions pour l'utilisation de Guard.

Cette documentation décrit l'utilisation du collecticiel dans le cadre d'une installation et d'une configuration classique. La version installée et la configuration de votre collecticiel peut différer de la description faite ici.

Plus d'aide

Une documentation complète du collecticiel peut être trouvée dans le guide utilisateur de Collecticiel.

2 À quoi sert Guard ?

Guard est un composant de sécurité du collecticiel, qui permet de chiffrer les courriels et fichiers.

- Chiffrez vos communications par courriel avec d'autres utilisateurs ou des participants externes.
- Chiffrez des fichiers individuels. Partagez les données chiffrées avec d'autres utilisateurs.
- Utilisez les options de sécurité pour définir le niveau de chiffrement.
- Les données chiffrées sont protégées par mot de passe. Utilisez la fonction de réinitialisation du mot de passe pour vous protéger en cas de mot de passe perdu.

3 Utiliser Guard

Apprenez à travailler avec l'application *Guard*.

- [appliquer](#) les réglages basiques
- chiffrer les [communications par courriel](#)
- chiffrer les [fichiers](#)
- [appliquer](#) les réglages de sécurité

3.1 Configuration de *Guard*

Avant de pouvoir utiliser *Guard*, vous devez effectuer quelques réglages élémentaires.

- Avant toute chose, vous devez saisir un mot de passe de sécurité Guard qui servira à chiffrer les données et accéder aux données chiffrées.
- Saisissez une adresse électronique secondaire qui servira si vous oubliez votre mot de passe Guard. Si cette situation se présente, utilisez la fonctionnalité de réinitialisation du mot de passe Guard. Un nouveau mot de passe vous sera alors envoyé. Pour des raisons de sécurité, il est fortement recommandé de fournir une adresse électronique secondaire pour ce cas de figure. Sinon, le nouveau mot de passe est envoyé à votre compte de courriel principal.

Deux options sont disponibles pour effectuer les réglages de base :

- Définir les réglages de base **après** avoir commencé à utiliser la fonction de chiffrement.
- Définir les réglages de base dans la page des réglages du collecticiel **avant** de faire appel à la fonction de chiffrement.

Pour définir les réglages de base après avoir lancé la fonction de chiffrement :

1. Activez la fonction de chiffrement lorsque vous rédigez un courriel, chiffrez un fichier ou transférez un nouveau fichier en cliquant sur l'icône **Chiffrer**  à proximité du nom du dossier dans l'arborescence des dossiers.
2. Il vous sera successivement demandé de saisir un mot de passe de sécurité Guard et une adresse électronique secondaire. Renseignez ces informations.

Pour définir les réglages de base avant de lancer la fonction de chiffrement :

1. Cliquez sur l'icône **Menu système**  à droite de la barre de menu. Dans le menu, choisissez l'élément **Réglages**.
2. Cliquez sur **Sécurité Guard** dans la barre latérale.
Lorsque vous ouvrez pour la première fois les réglages de sécurité Guard, la fenêtre intitulée *Créer des clés de sécurité Guard* s'ouvre.
3. Dans le champ **Mot de passe**, saisissez le mot de passe à utiliser pour chiffrer vos données.
Confirmez le mot de passe dans le champ **Vérification** en le saisissant à nouveau.
4. Dans le champ **Saisissez une adresse de courriel secondaire**, saisissez l'adresse de courriel à utiliser pour recevoir un mot de passe temporaire permettant de réinitialiser votre mot de passe de sécurité Guard.
5. Cliquez sur **Ok**.

3.2 Chiffrer les conversations par courriel

Les options suivantes sont disponibles :

- Lire des courriels chiffrés
- Envoyer des courriels chiffrés
- Comment un destinataire externe peut-il lire un courriel chiffré ?

3.2.1 Lire des courriels chiffrés

Afin de pouvoir lire un courriel chiffré, le mot de passe de sécurité Guard est au minimum nécessaire. L'expéditeur du courriel chiffré peut protéger son message avec un mot de passe complémentaire.

Comment lire un courriel chiffré :

1. Sélectionnez un courriel comportant l'icône *Chiffré* . Dans la vue détaillée apparaît la notification *Courriel sécurisé. Veuillez saisir votre mot de passe de sécurité Guard.*

Remarque : Si, lors de votre dernière utilisation de Guard, vous avez demandé à mémoriser le mot de passe de sécurité Guard, le courriel est immédiatement affiché conformément aux réglages.

2. Saisissez le mot de passe de sécurité Guard.

Vous pouvez définir la durée de mémorisation du mot de passe par l'application Guard. Pour cela, activez l'option Rester connecté à **Guard**. Choisissez une durée dans la liste.

3. Cliquez sur **OK**. Le contenu apparaît en texte pur.

Si le courriel comporte des pièces jointes, des fonctions permettant d'exploiter les versions chiffrées ou déchiffrées des pièces jointes sont affichées.

Remarque : vous pouvez uniquement répondre ou transmettre lorsque vous utilisez un courriel chiffré.

3.2.2 Envoyer des courriels chiffrés

Les options suivantes sont disponibles :

- Envoyer un courriel chiffré. Seuls vous et les destinataires pouvez lire le contenu du courriel.
Avertissement : lorsque vous envoyez un courriel chiffré, le brouillon sera supprimé du dossier *Brouillons* à l'envoi.
- Envoyer un courriel avec signature. La signature garantit que le destinataire peut identifier si le contenu du courriel a été modifié lors du transport.
- Envoyer un courriel chiffré avec signature.

Pour envoyer un courriel chiffré :

1. Rédigez un courriel dans l'app *Courriel* comme à l'accoutumée.
Dans la page *Rédiger un nouveau courriel*, cliquez sur l'icône **Chiffrer**  en haut à droite.
Vous pouvez aussi cliquer sur **Sécurité** sous le sujet. Cochez l'option **Chiffrer**.
Les icônes à côté des destinataires indiquent si le message peut être chiffré pour un destinataire donné. En passant le curseur sur une icône, une description sera affichée.
2. Pour afficher des options supplémentaires, cliquez sur **Sécurité**. Vous pouvez utiliser les fonctionnalités suivantes.
Pour, de surcroît, signer le courriel, cochez **Signer**.
Si le client de courriel du destinataire ne prend pas en charge PGP mais que le message doit rester lisible, cochez **Utiliser PGP dans le corps**. Si vous utilisez ce réglage, vous ne pouvez pas envoyer de courriels au format HTML.
Pour permettre au destinataire du courriel d'envoyer une réponse chiffrée, celui-ci doit détenir votre clé publique. Vous pouvez envoyer votre clé publique en tant que pièce jointe. Pour cela, activez l'option **Joindre ma clé**.
3. Cliquez sur **Envoi chiffré**.
Lors de l'envoi à des destinataires externes, une fenêtre est affichée vous permettant d'envoyer des [remarques pour l'ouverture de courriel chiffré \[12\]](#) aux destinataires externes.
Lors de l'envoi initial d'un courriel chiffré à un destinataire externe, celui-ci reçoit votre clé publique en pièce jointe.

3.2.3 Comment un destinataire externe peut-il lire un courriel chiffré ?

Vous pouvez également envoyer des courriels chiffrés à des destinataires externes n'étant pas référencés comme utilisateurs du collecticiel. Lors de l'ajout d'un destinataire externe, Guard vérifie si une clé publique est disponible pour ce destinataire. En fonction de cela, Guard utilise différentes procédures pour envoyer le message chiffré.

- S'il existe une clé publique pour le destinataire :
 - Le message est envoyé chiffré avec cette clé. Le destinataire peut lire le message avec sa clé privée.
 - Pour permettre au destinataire de vous répondre de manière chiffrée, votre clé publique est envoyée en pièce jointe. La pièce jointe est nommée « public.asc ». Le destinataire peut alors importer cette clé dans son client de messagerie.
- S'il n'existe pas de clé publique pour le destinataire :
 - Si le destinataire externe possède déjà un compte invité, il reçoit un courriel avec un lien vers la page d'authentification à son compte invité. Une fois connecté, il peut lire le message chiffré depuis la page de l'invité. Il peut alors envoyer une réponse chiffrée depuis cette page.
 - S'il n'existe pas de compte invité, un compte sera créé pour l'occasion. Le destinataire externe reçoit un courriel lui indiquant la marche à suivre et un mot de passe créé automatiquement. Ce destinataire reçoit un courriel complémentaire contenant un lien vers la page de l'invité. Sur cette page, le destinataire peut se connecter avec le mot de passe créé automatiquement. Il peut alors définir son propre mot de passe.
 - En fonction de la configuration du collecticiel, les courriels électroniques des comptes invités sont supprimés après un certain nombre de jours. Pour rendre ces courriels disponibles, le courriel contenant un lien vers la page de l'invité contient en pièce jointe le courriel chiffré. La pièce jointe est nommée « encrypted.asc ». Cette pièce jointe peut être envoyée et lue sur la page de l'invité.

3.3 Chiffrer des fichiers

Les options suivantes sont disponibles :

- [Chiffrer des fichiers](#)
- [Créer de nouveaux fichiers chiffrés](#)
- [Ouvrir des fichiers chiffrés](#)
- [Télécharger des fichiers chiffrés](#)
- [Déchiffrer des fichiers](#)

3.3.1 Chiffrer des fichiers

Lors du chiffrement d'un fichier, seule la dernière version de ce fichier sera chiffrée. Les autres versions seront supprimées.

Pour chiffrer un fichier :

Avertissement : lors du chiffrement d'un fichier, toutes les versions de ce fichier seront supprimées, exceptée la version actuelle. Si vous avez besoin de conserver une ancienne version, veuillez l'enregistrer avant chiffrement.

1. Sélectionnez un ou plusieurs fichiers dans l'app *Fichiers*. Cliquez sur l'icône **Actions**  dans la barre d'outils. Cliquez ensuite sur **Chiffrer** dans le menu.

Vous pouvez également utiliser l'icône **Actions**  à droite de la barre de catégories. Dans le menu, cliquez sur **Chiffrer**.

2. Si le fichier comporte plusieurs versions, la fenêtre *Chiffrer des fichiers* sera affichée. Confirmez votre souhait de chiffrer le fichier et de supprimer toutes les anciennes versions en cliquant sur **OK**.
Si le fichier ne comporte qu'une seule version, il est chiffré sans autre demande de confirmation.

3.3.2 Créer de nouveaux fichiers chiffrés

Vous pouvez créer un nouveau fichier chiffré en transférant un fichier local vers le serveur avec chiffrement.

Pour créer un nouveau fichier chiffré :

1. Dans l'app *Fichiers*, sélectionnez un dossier dans l'arborescence des dossiers.

Remarque : ouvrez un dossier dans lequel vous avez le droit de créer des objets.

2. Cliquez sur **Nouveau** dans la barre d'outils. Cliquez sur **Ajouter et chiffrer un fichier local**.

3. Sélectionnez un ou plusieurs fichiers dans la fenêtre *Envoi de fichiers*.

Cliquez sur **Ouvrir**. La zone d'affichage affiche l'état actuel du transfert.

Afin d'annuler l'action, cliquez sur **Détails du fichier** en bas à droite de la zone d'affichage. Cliquez sur **Annuler** après le nom du fichier dans la fenêtre *Progression de l'envoi*.

Conseil : vous pouvez aussi créer un nouveau fichier en faisant glisser un fichier depuis le bureau de votre système d'exploitation local vers la fenêtre de l'app *Fichiers* et en le déposant dans la partie supérieure.

3.3.3 Ouvrir des fichiers chiffrés

Vous pouvez ouvrir et lire un fichier chiffré. Le fichier reste chiffré sur le serveur.

Pour ouvrir un fichier chiffré :

1. Dans l'app *Fichiers*, sélectionnez un fichier chiffré dans la zone d'affichage. Cliquez sur l'icône **Afficher**  dans la barre d'outils.
2. La fenêtre intitulée *Saisissez le mot de passe de sécurité Guard* s'ouvre alors. Saisissez le mot de passe de sécurité Guard.
Vous pouvez définir combien de temps le mot de passe doit être mémorisé par Guard. Pour cela, activez l'option **Mémoriser le mot de passe**. Choisissez une durée dans la liste.
Cliquez sur **Ok**.

3.3.4 Télécharger des fichiers chiffrés

Vous pouvez télécharger un fichier chiffré pour le lire ou le modifier localement. Le fichier reste chiffré sur le serveur.

Pour télécharger un fichier chiffré :

1. Dans l'app *Fichiers*, sélectionnez un fichier chiffré dans la zone d'affichage. Cliquez sur l'icône **Afficher**  dans la barre d'outils.
Remarque : si, au lieu de cela, vous cliquez sur **Télécharger** dans la nouvelle fenêtre, le fichier téléchargé reste chiffré.
2. La fenêtre intitulée *Saisissez le mot de passe de sécurité Guard* s'ouvre alors. Saisissez le mot de passe de sécurité Guard.
Vous pouvez définir combien de temps le mot de passe doit être mémorisé par Guard. Pour cela, activez l'option **Mémoriser le mot de passe**. Choisissez une durée dans la liste.
Cliquez sur **Ok**.
3. Cliquez sur l'icône **Actions**  dans l'afficheur. Cliquez sur **Télécharger déchiffré**.

3.3.5 Déchiffrer des fichiers

Vous pouvez lever le chiffrement d'un fichier en le déchiffrant.

Pour déchiffrer un fichier :

1. Dans l'app *Fichiers*, cliquez sur un fichier chiffré dans la zone d'affichage. Cliquez sur l'icône **Actions**  dans la barre d'outils. Cliquez sur **Supprimer le chiffrement** dans le menu.
2. La fenêtre intitulée *Saisissez le mot de passe de sécurité Guard* s'ouvre alors. Saisissez le mot de passe de sécurité Guard.
Vous pouvez définir combien de temps le mot de passe Guard doit rester valide. Pour cela, activez l'option **Mémoriser le mot de passe**. Choisissez une durée dans la liste.
Cliquez sur **Ok**.

3.4 Se déconnecter de Guard

Vous pouvez vous déconnecter de Guard sans fermer le collecticiel. Pour ouvrir ultérieurement un courriel, fichier ou dossier chiffré, vous devrez à nouveau saisir le mot de passe Guard.

Remarque : Cette fonction n'est disponible que si vous activez l'option **Mémoriser le mot de passe** lorsque vous avez ouvert un courriel ou fichier chiffré.

Pour vous déconnecter de Guard:

1. Cliquez sur l'icône **menu Système**  à droite de la barre de menus.
2. Dans le menu, cliquez sur **Se déconnecter de Guard**.

3.5 Réglages de Guard

Vous disposez des options suivantes :

- Pour gérer votre mot de passe de sécurité Guard, passez par les [Réglages de sécurité Guard](#).
- Pour changer les réglages par défaut pour l'envoi de courriels sécurisés, utilisez les [Réglages de chiffrement PGP](#).
- Vous pouvez [gérer vos clés PGP](#).

3.5.1 Réglages de sécurité Guard

Vous disposez des options suivantes :

- [Changer](#) le mot de passe de sécurité Guard
- Si vous avez perdu votre mot de passe de sécurité Guard, vous pouvez demander un mot de passe Guard temporaire en [réinitialisant](#) le mot de passe de sécurité Guard.
- [modifier](#) l'adresse électronique secondaire

Pour changer le mot de passe de sécurité Guard

1. Cliquez sur l'icône **menu Système**  à droite de la barre de menu. Cliquez sur l'élément **Réglages**.
2. Dans la barre latérale, cliquez sur Sécurité **Guard**.
3. Dans le champ **Saisissez votre mot de passe Guard actuel** figurant sous *Mot de passe*, saisissez le mot de passe que vous avez utilisé jusqu'à présent pour chiffrer vos données.
Dans le champ **Saisissez votre nouveau mot de passe Guard**, saisissez le mot de passe que vous souhaitez dorénavant utiliser pour chiffrer vos données.
Confirmez le mot de passe en le saisissant à nouveau dans le champ **Vérifiez votre nouveau mot de passe Guard**.
4. Cliquez sur **Changer le mot de passe de sécurité Guard**.

Pour réinitialiser le mot de passe de sécurité Guard :

1. Cliquez sur l'icône **Menu système**  à droite de la barre de menu. Dans le menu, choisissez **Réglages**.
2. Dans la barre latérale, cliquez sur Sécurité **Guard**.
3. Cliquez sur **Réinitialiser le mot de passe de sécurité Guard**. Un nouveau mot de passe vous sera envoyé à votre adresse électronique secondaire.
Si vous n'avez pas saisi d'adresse de courriel secondaire, le nouveau mot de passe vous sera envoyé à votre adresse de courriel principale.
4. Ce nouveau mot de passe est maintenant votre mot de passe de sécurité Guard courant. Vous devriez immédiatement [modifier](#) ce mot de passe.

Pour modifier votre adresse électronique secondaire permettant de réinitialiser le mot de passe de chiffrement :

1. Cliquez sur l'icône **Menu système**  à droite de la barre de menu. Choisissez l'élément **Réglages** dans le menu.
2. Dans la barre latérale, cliquez sur Sécurité **Guard**.
3. Saisissez le mot de passe servant à chiffrer vos données dans le champ **Saisissez votre mot de passe de sécurité Guard actuel** figurant sous *Adresse électronique secondaire*
Dans le champ **Saisissez une adresse de courriel secondaire**, saisissez l'adresse de courriel à utiliser pour recevoir un mot de passe temporaire permettant de réinitialiser votre mot de passe de sécurité Guard.
Cliquez sur **Modifier l'adresse électronique**.

3.5.2 Réglages de chiffrement PGP

Les réglages de chiffrement PGP définissent les réglages pré-existants disponibles lorsque vous rédigez des courriels. Lorsque vous rédigez un nouveau courriel, les réglages par défaut peuvent être ajustés avant l'envoi de ce courriel.

Pour modifier les réglages de chiffrement PGP :

1. Cliquez sur l'icône **Menu système**  à droite de la barre de menu. Cliquez sur **Réglages** dans le menu.
2. Choisissez l'élément Sécurité **Guard** dans la barre latérale. Cliquez sur **Réglages avancés**.
3. Modifiez les réglages sous *Réglages de chiffrement PGP*.

Les réglages suivants sont disponibles :

Définir le chiffrement comme option par défaut à la rédaction d'un nouveau message

Définit si un nouveau courriel est par défaut chiffré avec PGP.

Signer par défaut les courriels sortants

Définit si un nouveau courriel est par défaut chiffré avec PGP.

Activer les fonctionnalités PGP avancées

Indique quelles fonctionnalités PGP sont affichées (par exemple la gestion des clés).

Utiliser par défaut PGP dans le corps pour la compatibilité

Pour afficher ce réglage, cochez la case **Activer les réglages PGP avancés**.

Définit si le chiffrement PGP utilise PGP dans le corps. Ces réglages ne sont à utiliser que si le client de courrier du destinataire ne prend pas en charge PGP et que le message doit néanmoins rester lisible. Si vous utilisez ce réglage, vous ne pouvez pas envoyer de courriels au format HTML.

3.5.3 Gérer les clés

Pour envoyer ou recevoir des messages chiffrés, ces fonctions de gestion des clés ne sont généralement pas nécessaires. Elles peuvent toutefois être utilisées pour les besoins suivants :

- Vous souhaitez utiliser vos clés PGP Guard dans d'autres clients de courriel, par exemple un client local.
- Vous possédez des clés PGP provenant d'autres applications PGP. Vous souhaitez utiliser ces clés dans Guard.
- Vous avez la clé publique d'un partenaire externe. Pour pouvoir lire des messages chiffrés provenant de ce partenaire externe sans avoir à consulter un serveur de clés, vous souhaitez importer dans Guard la clé publique de ce partenaire.
- Vous souhaitez mettre votre clé publique à disposition d'un destinataire pour que celui-ci puisse lire vos messages chiffrés sans avoir à consulter un serveur de clés.

Pour ouvrir la page de gestion de vos clés :

1. Cliquez sur l'icône **Menu système**  à droite de la barre de menu. Cliquez sur **Réglages** dans le menu.
2. Choisissez l'élément **Sécurité Guard** dans la barre latérale. Cliquez sur **Réglages avancés**. Cliquez sur **Activer les fonctionnalités PGP avancées**.

La page comporte les éléments suivants :

- Options permettant d'ajuster les [Réglages par défaut de Guard](#)
- Section *Vos clés*. Contient des fonctions de gestion de vos clés PGP publiques et privées. Vos clés existantes sont affichées sous *Votre liste de clés*. La liste de clés contient deux clés :
 - Une clé principale. Entre autres choses, cette clé est utilisée pour signer vos courriels.
 - Une sous-clé. Cette clé est utilisée pour chiffrer et déchiffrer des courriels et fichiers. L'existence d'une clé principale et d'une sous-clé fait partie des fonctionnalités de la technologie de chiffrement PGP. Chaque clé principale et sous-clé contiennent aussi bien une clé publique qu'une clé privée. En fonction du besoin, Guard utilise automatiquement la clé requise.
- Section *Clés publiques*. Affiche les clés publiques partagées par vous-même ou d'autres utilisateurs. Si la clé publique d'un utilisateur apparaît dans cette liste, vous pouvez supposer que cet utilisateur est en mesure de déchiffrer les courriels que vous lui envoyez chiffrés.

Les fonctions suivantes sont disponibles :

- [télécharger](#) votre clé publique
- [envoyer votre clé publique par courriel](#)
- [ajouter de nouvelles clés](#) à votre trousseau existant en téléchargeant des clés locales ou en créant de nouvelles clés Guard
- [passer une clé comme clé actuelle](#)
- [afficher les détails](#) d'une clé
- [supprimer](#) une clé
- [télécharger](#) votre clé privée
- [ajouter un compte de courrier électronique supplémentaire](#) à une clé
- [transférer](#) sur le serveur la clé publique d'un partenaire externe

Pour télécharger votre clé publique :

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur **Télécharger la clé publique PGP** sous *Vos clés*.

Pour envoyer votre clé publique par courriel :

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur **Envoyer votre clé publique par courriel** sous *Vos clés*.

Pour ajouter une nouvelle clé à vos clés :

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur l'icône **Modifier +** à côté de *Votre liste de clés* sous *Vos clés*. La fenêtre *Ajouter une clé* s'ouvre.
3. Les options suivantes s'offrent à vous :
 - Pour ajouter une clé privée, cliquez sur **Télécharger une clé privée**. Sélectionnez un fichier contenant une clé privée. La fenêtre *Télécharger une clé privée* s'ouvre alors.
Pour transférer la nouvelle clé, saisissez votre mot de passe de sécurité Guard. Saisissez un nouveau mot de passe pour la nouvelle clé.
 - Pour ajouter une clé publique, cliquez sur **Télécharger une clé publique seulement**. Sélectionnez un fichier contenant une clé publique.
 - Pour créer une nouvelle paire de clés, cliquez sur **Créer de nouvelles clés**. La fenêtre *Créer de nouvelles clés de sécurité Guard* s'ouvre alors.
Saisissez un mot de passe pour la nouvelle clé. Confirmez le mot de passe.
La nouvelle clé consiste en une clé principale et une sous-clé correspondante.
La nouvelle clé sera ajoutée en haut de votre liste de clés. La nouvelle clé devient donc la clé courante.

Comment passer une clé en clé actuelle :

Vous pouvez utiliser cette fonction si votre liste de clés contient plus d'une clé principale et d'une sous-clé. À partir de maintenant, la clé actuelle sera utilisée pour le chiffrement.

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Sous *Votre liste de clés*, cliquez sur la case à cocher à côté d'une clé sous l'**Actuelle**. Lors du passage d'une clé principale comme clé actuelle, la sous-clé correspondante sera également marquée comme actuelle, et vice versa.

Comment afficher les détails d'une clé :

Vous pouvez obtenir les détails des clés. Les détails d'une clé sont particulièrement utiles aux utilisateurs ayant des connaissances PGP.

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur l'icône **Détails**  à droite de la barre de catégories. La fenêtre *Détails d'une clé* s'ouvre. Pour afficher les signatures d'une clé, cliquez sur **Signatures**.

Pour supprimer une clé :

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur l'icône **Supprimer**  à droite de la barre de catégories. La fenêtre *Supprimer une clé privée* s'ouvre.
3. Vous avez les options suivantes :
 - Pour révoquer une clé privée, cliquez sur **Révoquer**.
Saisissez le mot de passe de la clé privée. Si cela est nécessaire, sélectionnez la raison de la révocation.
Cliquez sur **Révoquer**.
 - Afin de supprimer une clé privée, cliquez sur **Supprimer**.
Saisissez le mot de passe de la clé privée.
Cliquez sur le bouton **Supprimer**.
Lors de la suppression de la clé principale, la sous-clé est également supprimée.

Pour télécharger votre clé privée :

Attention : Télécharger une clé privée sur votre ordinateur local peut présenter un risque de sécurité. Assurez-vous que personne ne peut avoir accès à votre clé privée.

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur l'icône **Télécharger**  à droite de la barre de catégories.

Pour ajouter un compte de courrier électronique supplémentaire à une clé :

Lors de l'ajout d'identifiants d'utilisateurs supplémentaires à une clé, vous pouvez utiliser cette clé pour plusieurs comptes de courriers électroniques.

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur l'icône **Modifier**  à droite de la barre de catégories. La fenêtre *Ajouter un identifiant utilisateur* s'ouvre.
3. Saisissez un nom pour l'identifiant utilisateur. Saisissez l'adresse électronique que vous souhaitez coupler à cette clé.
Saisissez votre mot de passe pour cette clé.
Cliquez sur **Ok**.

Pour transférer vers le serveur la clé publique d'un partenaire externe :

1. Dans les réglages, [ouvrez](#) la page de gestion des clés.
2. Cliquez sur l'icône **Ajouter**  à droite de la barre de catégories. Sélectionnez un fichier contenant une clé publique.

Index

C

Chiffrer

- conversation par courriel, 11
- créer de nouveaux fichiers chiffrés, 13
- Fichiers, 13

Chiffrer des fichiers, 13

Chiffrer les conversations par courriel, 11

Courriels chiffrés

- accès pour les destinataires externes, 12
- bloquer, 11
- envoyer, 11
- lecture, 11

Créer de nouveaux fichiers chiffrés, 13

D

Déchiffrer des fichiers, 14

Documentation, 5

F

Fichiers chiffrés

- déchiffrer, 14
- Ouvrir, 13
- télécharger, 14

G

Guard, 7, 9

- configuration, 10
- gérer les clés, 18
- Réglages, 16
- Réglages de chiffrement PGP, 17
- réglages de sécurité, 16
- se déconnecter, 15

M

Modifier le mot de passe, 16

O

Ouvrir des fichiers chiffrés, 13

R

Réglages de Guard

- changer le mot de passe, 16
- Réinitialiser le mot de passe, 16

Réglages PGP Guard Guard

- Activer les fonctionnalités PGP avancées, 17
- Définir le chiffrement comme option par défaut à la rédaction d'un nouveau message, 17
- Signer par défaut les courriels sortants, 17
- Utiliser par défaut PGP dans le corps pour la compatibilité, 17

Réinitialiser le mot de passe, 16

S

Se déconnecter

- Modifier le mot de passe, 15

T

Télécharger des fichiers chiffrés, 14

