Guard

Manuel de l'utilisateur

Guard: Manuel de l'utilisateur

Date de publication mercredi, 23. mars 2016 Version 2.2.0

Table des matières

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 ?

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 *Utilisation de 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 Utilisation de 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 de l'en-tête.
2. Il vous sera alors demandé de renseigner un mot de passe de sécurité Guard et une adresse électronique secondaire. Saisissez ces données.

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. Dans la barre latérale, cliquez sur **Réglages de sécurité de Guard**.
   Lors de la première sélection des réglages de sécurité de Guard, la fenêtre *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
- Accès pour les destinataires externes

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 la dernière utilisation de Guard, vous avez spécifié que Guard doive se rappeler de votre mot de passe, le courriel est affiché immédiatement, en fonction de ce paramètre.
2. Saisissez le mot de passe de sécurité Guard.

   Vous pouvez définir combien de temps le mot de passe doit être mémorisé. 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 le destinataire 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**.
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.
3. Cliquez sur **Envoi sécurisé**.

   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.

3.2.3 Accès pour les destinataires externes

Vous pouvez également envoyer des courriels chiffrés à des destinataires externes qui ne sont pas des utilisateurs du collecticiel. Lorsque vous envoyez pour la première fois un courriel chiffré à un destinataire externe, cela déclenche les événements suivants :

- Un compte spécial est automatiquement mis en place pour le destinataire externe.
- Vous définissez si la notification relative au courriel chiffré envoyée au destinataire externe est automatique ou personnalisée.
- Le destinataire externe reçoit un courriel comportant la notification, ainsi qu'un mot de passe créé automatiquement.

  Suivant la configuration du collecticiel, vous pouvez transférer au destinataire un code pin à 4 chiffres permettant de sécuriser le mot de passe créé automatiquement.
- Le destinataire externe reçoit un courriel comportant un lien vers la page d'authentification au compte spécial.
- Le destinataire externe saisit dans la page d'authentification le mot de passe créé automatiquement.

  Ensuite, le destinataire externe doit modifier le mot de passe automatique. Pour pouvoir réinitialiser le compte en cas de perte du mot de passe, une question de sécurité et la réponse correspondante doivent être définies.

  Le courriel chiffré est affiché.
- Le destinataire externe peut envoyer une réponse chiffrée au courriel.

Lorsqu'un nouveau courriel chiffré est envoyé à ce destinataire externe, cela déclenche les événements suivants :

- Le destinataire externe reçoit un courriel avec un lien vers la page d'authentification pour le compte spécial.
- Sur la page d'authentification, le destinataire saisit le mot de passe qu'il/elle a configuré à réception du premier courriel chiffré.

  Si le destinataire ne se souvient plus du mot de passe, il/elle peut demander un nouveau mot de passe. Pour ce faire, il/elle doit répondre correctement à la question de sécurité.

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** dans l'*Afficheur*. Cliquez sur **Chiffrer** dans le menu.

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. Dans la fenêtre *Saisissez le mot de passe de sécurité Guard*, saisissez le mot de passe de sécurité Guard.

   Vous pouvez définir combien de temps le mot de passe doit être mémorisé. 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. Dans la fenêtre *Saisissez le mot de passe de sécurité Guard*, saisissez le mot de passe de sécurité Guard.

   Vous pouvez définir combien de temps le mot de passe doit être mémorisé. 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. Dans la fenêtre *Saisissez le mot de passe de sécurité Guard*, 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. Cliquez sur **Se déconnecter de Guard** dans le menu.

3.5 Réglages de Guard

Vous disposez des options suivantes :

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

3.5.1 Réglages de sécurité Guard

Vous disposez des options suivantes :

- modifier le mot de passe de sécurité Guard
- Si vous avez oublié votre mot de passe Guard, vous pouvez demander à ce qu'un mot de passe temporaire vous soit envoyé en réinitialisant votre mot de passe Guard.
- modifier l'adresse électronique secondaire

Pour modifier 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 de Guard**.
3. Dans le champ **Saisissez le mot de passe de sécurité Guard actuel** sous le *Mot de passe*, saisissez le mot de passe que vous aviez utilisé jusqu'à présent pour chiffrer vos données.

   Dans le champ **Saisissez le nouveau mot de passe de sécurité Guard**, saisissez le mot de passe que vous voulez utiliser pour chiffrer vos données à partir de maintenant.

   Confirmez le mot de passe dans le champ **Vérifier le nouveau mot de passe de sécurité Guard** en le saisissant à nouveau.
4. Cliquez sur **Modifier 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 de Guard**.
3. Cliquez sur **Réinitialiser le mot de passe de sécurité Guard**. Un nouveau mot de passe vous sera transmis par le biais de 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 actuel. 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 de Guard**.
3. Saisissez le mot de passe pour chiffrer vos données dans le champ **Saisissez le mot de passe de sécurité Guard actuel** sous le champ *Courriel 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 le courriel**.

3.5.2 Réglages par défaut de Guard

Les réglages par défaut 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 par défaut :

1. Cliquez sur l'icône **Menu système** à droite de la barre de menu. Cliquez sur **Réglages** dans le menu.
2. Sélectionnez l'entrée **Sécurité de Guard** dans la barre latérale. Puis, cliquez sur **Réglages PGP de Guard**.
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.

Utiliser PGP Inline par défaut pour la compatibilité

Définit si le chiffrement PGP utilise PGP Inline. 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. Sélectionnez l'entrée **Sécurité de Guard** dans la barre latérale. Cliquez sur **Réglages PGP de Guard**.

La page comporte les éléments suivants :

- Options permettant de définir les Réglages par défaut de Guard.
- Section *Vos clés*. Contient des fonctions de gestion de vos clés PGP publiques et privées.
- 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 vos clés existantes en transférant des clés locales vers le serveur ou en créant de nouvelles clés Guard
- télécharger votre clé privée
- 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 **Ajouter** +. La fenêtre d'*Ajout des clés* s'ouvre alors.
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 une 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 des clés de sécurité Guard* s'ouvre alors.

     Saisissez un mot de passe pour la nouvelle clé. Confirmez le mot de passe.

   La nouvelle clé apparaîtra sous *Votre liste de clés*.

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** .

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** +. Sélectionnez un fichier contenant une clé publique.

Index