



STORMSHIELD



GUIDE

**STORMSHIELD DATA SECURITY
ENTERPRISE**

STORMSHIELD DATA MAIL ÉDITION OUTLOOK

Messagerie sécurisée

Version 10.1

Dernière mise à jour du document : 29 mars 2022

Référence : sds-fr-sd_mail_outlook-guide_d_utilisation-v10



Table des matières

Préface	4
1. Introduction	5
1.1 Présentation	5
1.1.1 Généralités	5
1.1.2 Intégration au client de messagerie	5
1.1.3 Ce qui est sécurisé	6
1.2 Sécurisation de vos messages	6
1.2.1 Cryptographie à clé publique	6
1.2.2 Chiffrement	6
1.2.3 Signature électronique	6
1.2.4 Certificats	7
1.2.5 Confiance	8
1.2.6 Annuaires de confiance	8
1.2.7 Contrôle de révocation	8
1.3 Connexion sécurisée	8
2. Installation et mise en route de Stormshield Data Mail Édition Outlook	10
2.1 Configuration requise	10
2.2 Installation de Stormshield Data Mail Édition Outlook	10
2.3 Menu Stormshield Data Security	11
2.4 Connexion à Stormshield Data Security	11
2.5 Échange de certificats	13
2.6 Importer les certificats d'un e-mail signé	14
3. Émettre un message sécurisé	15
3.1 Choix des options de sécurité	15
3.2 Certificat non trouvé, en erreur ou non valide	16
3.3 Plusieurs certificats sont disponibles	17
3.4 Certificats joints	17
3.5 Certificats contenant plusieurs adresses e-mail	17
3.6 Vous n'êtes pas connecté à Stormshield Data Security ou votre session est verrouillée	18
4. Lire un message sécurisé	19
4.1 Ouverture d'un message sécurisé	19
4.2 Consultation du compte-rendu de sécurité	19
4.3 Réponse ou transfert d'un message chiffré	20
4.4 Messages sécurisés attachés en pièces jointes	20
4.5 Messages sécurisés au format OpenPGP	20
4.5.1 Importer un porte-clés OpenPGP	20
4.5.2 Lire un message sécurisé au format OpenPGP	21
4.5.3 Lire un message sécurisé au format PGP Partitionné	21
5. Fonctions avancées	22
5.1 Interaction avec Stormshield Data Connector	22
5.2 Gestion des algorithmes de signature	22
5.2.1 Signature	22
5.2.2 Chiffrement	22
5.3 Signature détachée	22
5.4 Apprentissage de chiffrement	23



- 5.5 Délégation de déchiffrement 23
- 5.6 Transchiffrement 23
 - 5.6.1 Principes du transchiffrement 23
 - 5.6.2 Transchiffrement et gestion des collaborateurs 24
 - 5.6.3 Utilisation du transchiffrement 24
 - 5.6.4 Limitations du transchiffrement 26
- 5.7 Désactivation de la sécurité 26
 - 5.7.1 Principes de la désactivation de la sécurité 26
 - 5.7.2 Désactiver la sécurité 26
 - 5.7.3 Limitations de la désactivation de la sécurité 27

Dans la documentation, Stormshield Data Security Enterprise est désigné sous la forme abrégée : SDS.



Préface

Stormshield Data Mail Édition Outlook faisant partie de Stormshield Data Security, il est possible d'utiliser le même compte utilisateur pour accéder aux différents composants de la suite installés sur votre poste et d'utiliser les clés et certificats antérieurement disponibles.

Pour plus d'informations, reportez-vous au *Guide d'installation et de mise en œuvre*.

Il existe deux versions de Stormshield Data Mail :

- Stormshield Data Mail Édition Notes,
- Stormshield Data Mail Édition Outlook, pour Microsoft Outlook 2019 et 365 Professional.



1. Introduction

Cette section décrit les caractéristiques et fonctionnalités de Stormshield Data Mail Édition Outlook.

1.1 Présentation

1.1.1 Généralités

Stormshield Data Mail est un logiciel de sécurité informatique. Il ajoute aux messages que vous échangez tous les jours sur Internet ou sur votre Intranet les services de sécurité suivants :

- **la confidentialité** du message : seul(s) le ou les destinataires pourront lire le message transmis ;
- **l'intégrité** du message, qui ne peut être modifié en cours de transfert sans que cela ne soit détecté ;
- **l'authentification de l'émetteur** : le destinataire du message est certain de l'identité de l'émetteur.

La confidentialité est assurée par le chiffrement [cryptage] du message.

L'intégrité du message et l'authentification de l'émetteur sont garanties par une signature électronique.

Stormshield Data Mail implémente la norme S/MIME V3 : vous pouvez échanger des messages sécurisés avec tout correspondant dès lors qu'il possède un logiciel de messagerie supportant la norme S/MIME V2 ou V3.

i NOTE

Si vous essayez de sécuriser un message avec les fonctions de sécurité natives de votre client de messagerie, puis avec Stormshield Data Mail, ce message doublement sécurisé ne pourra être lu par son destinataire.

1.1.2 Intégration au client de messagerie

Stormshield Data Mail ne se substitue pas à votre client de messagerie habituel : il le complète et se charge de la sécurité de vos messages.

Stormshield Data Mail utilise le mode « intégré » pour sécuriser vos messages. C'est une extension qui s'intègre dans votre client de messagerie. Elle sécurise (chiffre et/ou signe) et dé-sécurise (déchiffre) vos messages au fur et à mesure tout en les conservant sous leur forme sécurisée dans votre base de messages.

Stormshield Data Mail est disponible sous forme d'add-in pour les clients de messagerie suivants :

- Microsoft Outlook 2019 et 365 Professional
- Lotus Notes 8.x et 9.x

Stormshield Data Mail est compatible avec les serveurs de messagerie suivants :

- Microsoft Exchange Server 2010 SP1/SP2/SP3
- Microsoft Exchange Server 2013 SP1



- Microsoft Exchange Server 365
- Microsoft Exchange Server 2019

1.1.3 Ce qui est sécurisé

La norme S/Mime V3 permet de sécuriser un message, c'est-à-dire **son texte et ses pièces jointes**.

L'enveloppe du message [en-tête rfc822], qui contient notamment le nom de l'émetteur, la liste des destinataires, la date d'émission et surtout l'objet du message, n'est quant à elle pas sécurisée.

Ainsi, même si un message est sécurisé, son objet peut être lu ou modifié lors de son acheminement sur le réseau. C'est pourquoi la prudence est de mise lorsque vous écrivez ou lisez une information dans l'objet d'un message sécurisé.

1.2 Sécurisation de vos messages

1.2.1 Cryptographie à clé publique

Stormshield Data Mail met en œuvre des moyens de cryptographie dits « à clé publique ».

Chaque correspondant possède un (ou plusieurs) couple(s) de clés : une clé privée et une clé publique. La **clé privée** doit être conservée de façon confidentielle par son propriétaire. En revanche, la **clé publique** est destinée à être distribuée.

Stormshield Data Mail peut mettre en œuvre :

- un couple de clés unique pour le chiffrement et la signature ;
- deux couples de clés différents, l'un pour le chiffrement, l'autre pour la signature.

1.2.2 Chiffrement

Le chiffrement est une technique utilisant des propriétés mathématiques (cryptographie) pour transformer un message intelligible (en clair) en un message (chiffré) que seuls les destinataires désignés peuvent décoder et lire.

L'émetteur chiffre un message avec un processus mettant en œuvre la clé publique du destinataire ; ce dernier utilise un processus mettant en œuvre sa clé privée pour déchiffrer le message. Le destinataire étant le seul à posséder cette clé privée, l'émetteur est assuré que le message ne peut pas être lu par un tiers.

i NOTE

L'émetteur ne pourra chiffrer un message que s'il possède une clé de chiffrement dans son porte-clés. Un compte Stormshield Data Security ne détenant qu'une clé de signature ne pourra donc pas servir au chiffrement de messages.

1.2.3 Signature électronique

Une signature électronique est un «sceau» numérique appliqué sur le message : elle garantit l'intégrité du message et l'identité du signataire.

Le signataire signe un message au moyen de sa clé privée ; le destinataire vérifie la signature au moyen de la clé publique du signataire. Le signataire étant le seul à posséder la clé privée



ayant signé le message, le destinataire est assuré que le message a bien été émis par le signataire et qu'il n'a pas été falsifié au cours de son transfert.

i NOTE

L'émetteur ne pourra signer un message que s'il possède une clé de signature dans son portefeuille. Un compte Stormshield Data Security qui ne détient qu'une clé de chiffrement ne pourra donc pas servir à la signature de messages.

Il existe deux types de signature : les signatures opaques et les signatures détachées (en clair). Stormshield Data Mail Édition Outlook supporte ces deux types de signature pour l'émission et la réception de messages.

L'utilisation de la signature en clair permet aux destinataires de lire le message même si leur client de messagerie ne prend pas en compte le format S/MIME ou refuse d'afficher les messages avec des signatures qui ne peuvent être validées (si les certificats et les listes de révocation ne sont pas disponibles par exemple).

Cependant, une signature en clair est susceptible d'être modifiée pendant l'émission du message. En règle générale, les serveurs ne modifient pas les messages, mais des balises peuvent être ajoutées, des lignes blanches ajoutées ou enlevées. La signature du message est alors invalide.

Pour savoir comment activer la signature détachée, reportez-vous à la section [Signature détachée](#).

Lorsque le destinataire reçoit un message signé et l'ouvre dans le volet de lecture ou dans une nouvelle fenêtre, Stormshield Data Security vérifie entre autres que l'adresse e-mail de l'émetteur et l'adresse indiquée dans le certificat associé (et joint au message concerné) correspondent. Dans le cas contraire, un avertissement s'affiche dans le bandeau de sécurité du message reçu.

Si le certificat contient deux adresses e-mail séparées par un point virgule, la signature du message est considérée valide quelle que soit l'adresse utilisée par l'émetteur (parmi les adresses spécifiées dans le certificat).

Une seule erreur s'affiche dans le compte rendu de sécurité. Si plusieurs erreurs ou avertissements surviennent, seul la ou le plus critique s'affiche.

1.2.4 Certificats

Pour envoyer des messages chiffrés à des correspondants, vous devez connaître la clé publique de chiffrement de vos correspondants.

Les clés publiques sont distribuées sous forme de certificat. Un certificat est un document électronique qui associe une clé publique à son propriétaire. Stormshield Data Security supporte le format de certificat X.509 V3.

i NOTE

En cas de renouvellement de la clé de chiffrement ou de certificats, les certificats (ainsi que la clé associée) utilisés pour le chiffrement antérieur de données doivent être conservés afin de pouvoir déchiffrer ultérieurement ces données.

Pour plus d'informations sur l'export et l'import de certificats, consultez le *Guide d'installation et de mise en œuvre*.



1.2.5 Confiance

Un certificat établit un lien entre une clé publique et une identité. Vous ne pouvez utiliser un certificat que si vous faites confiance à ce lien.

En effet, si par exemple vous voulez envoyer un fichier chiffré à Alice, vous devez être certain que le certificat supposé d'Alice est effectivement bien le sien ; sinon vous prenez le risque que votre fichier soit chiffré non pas avec la véritable clé d'Alice, mais avec la clé d'un imposteur qui pourra déchiffrer votre fichier destiné à Alice.

Deux techniques permettent d'accorder sa confiance à un certificat :

- la confiance par héritage adopte le principe que si vous faites confiance à une autorité dans son rôle de certification, vous faites implicitement confiance aux certificats qu'elle délivre.
- la confiance explicite impose que vous vérifiez vous-même l'origine du certificat. Une technique usuelle consiste à en vérifier l'empreinte à partir d'une source parallèle d'information (téléphone, publication, courrier, site web, etc.).

1.2.6 Annuaire de confiance

La gestion des annuaires de confiance et des certificats est décrite dans le *Guide d'installation et de mise en œuvre*.

Stormshield Data Mail Édition Outlook permet de gérer un annuaire de confiance : vous y insérez les certificats des correspondants et des autorités auxquels vous faites confiance.

Si vous souhaitez chiffrer un message pour un ou des destinataires pour lesquels vous n'avez pas de certificat valide dans votre annuaire de confiance, l'annuaire LDAP peut être automatiquement interrogé. Pour cela, vous devez avoir déclaré un annuaire LDAP et autorisé dans le Stormshield Data Authority Manager la mise à jour automatique à partir de l'annuaire LDAP.

Pour plus d'informations sur ce paramétrage, reportez-vous à la Section [Mail] du *Guide d'administration* et à la section Paramètres de Stormshield Data Mail Édition Outlook dans le Guide du Stormshield Data Authority Manager.

1.2.7 Contrôle de révocation

Le contrôle de révocation vérifie, avant son utilisation, qu'un certificat est bien valide, c'est-à-dire qu'il n'a pas été révoqué. Les listes de révocation (CRL) sont fournies par les autorités de certification.

Stormshield Data Security assure automatiquement le téléchargement des listes de révocation à partir des points de distribution déclarés dans les certificats ou ceux configurés dans le composant Contrôleur de révocation.

L'utilisateur peut configurer les critères de téléchargement pour chaque autorité de certification. Les listes de révocation reçues sont conservées localement dans une base sécurisée.

Pour plus de détails sur les listes de révocation, reportez-vous au *Guide d'installation et de mise en œuvre*.

1.3 Connexion sécurisée

L'accès à vos clés est protégé : pour pouvoir les utiliser, vous devez vous connecter à Stormshield Data Security, processus qui consiste à vous authentifier et à vérifier que vous



êtes bien le propriétaire des clés.

Stormshield Data Security propose deux méthodes d'authentification :

- par mot de passe : vous saisissez un identifiant et un mot de passe ;
- par carte à puce ou clé USB cryptographique : vous saisissez le code secret de la carte (en anglais, "PIN" Personal Identification Number).

Stormshield Data Security supporte différents types de cartes à puces et de clés USB.

Pour plus d'informations, reportez-vous au *Guide d'installation et de mise en œuvre*.



2. Installation et mise en route de Stormshield Data Mail Édition Outlook

Cette section présente la configuration requise, l'installation et la mise en route de l'application.

Une fois installé, Stormshield Data Security se lance automatiquement au démarrage de votre système.

Pour pouvoir signer et chiffrer des messages, recevoir et vérifier du courrier sécurisé, vous devez vous connecter à Stormshield Data Security.

Pour vous connecter à Stormshield Data Security, vous devez posséder un « compte ». La procédure de création et de gestion des comptes utilisateurs est décrite dans le *Guide d'installation et de mise en œuvre* et dans le *Guide d'administration de Stormshield Data Security*.

Cette section décrit uniquement les comptes protégés par un mot de passe. Si vous disposez d'un dispositif matériel d'authentification (carte à puce, ...), reportez-vous au *Guide d'installation et de mise en œuvre* qui décrit les fonctions communes aux logiciels de la suite Stormshield Data Security.

2.1 Configuration requise

Pour connaître la configuration requise sur les systèmes d'exploitation Microsoft, reportez-vous à la section **Compatibilité** de la note de version de Stormshield Data Security 10.1.

200 Mo d'espace disque sont requis pour l'installation de tous les composants de Stormshield Data Security

La configuration matérielle requise pour le .NET Framework 4.5.2 est la suivante :

- Processeur 1 GHz minimum,
- 512 Mo de mémoire vive (RAM),
- 850 Mo d'espace disque disponible pour un système 32 bits,
- 2 Go d'espace disque disponible pour un système 64 bits.

i NOTE

Stormshield Data Security n'est pas compatible avec la fonction **Changement Rapide d'Utilisateur**.

2.2 Installation de Stormshield Data Mail Édition Outlook

Stormshield Data Mail Édition Outlook est un composant de Stormshield Data Security Enterprise.

Une clé de licence est communiquée en fonction des droits d'usage que vous avez acquis lors de la commande du produit. Cette clé de licence est demandée à l'installation.

La procédure d'installation est détaillée dans le *Guide d'installation et de mise en œuvre*.

Après l'installation de l'add-in Stormshield Data Mail Édition Outlook, la première ouverture de votre client de messagerie peut prendre plusieurs dizaines de secondes.

**i NOTE**

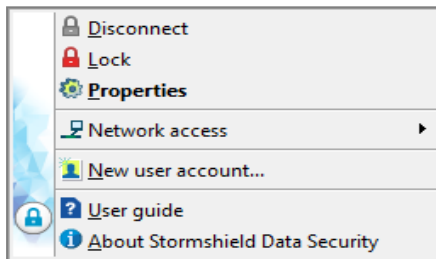
Le cumul d'autres add-ins S/MIME, tels que Microsoft MAPI S/MIME AME processor n'est pas supporté.

2.3 Menu Stormshield Data Security

Tout ce qui concerne votre connexion à Stormshield Data Security s'effectue par un clic droit sur l'icône Stormshield Data Security affichée à droite de votre barre de tâches Windows.

Cette icône est grisée tant que vous n'êtes pas connecté, rouge quand votre session est verrouillée et verte lorsque vous êtes connecté.

Un clic droit sur cette icône ouvre un menu, nommé Menu Stormshield Data Security dans la suite de ce guide.

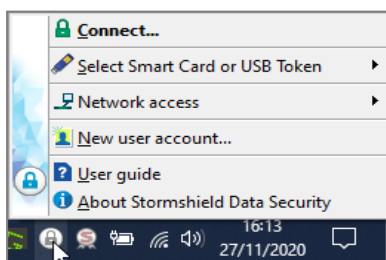


Les rubriques du menu Stormshield Data Security affichées dépendent de la façon dont ont été configurées les actions de connexion/déconnexion, verrouillage/déverrouillage, etc.

2.4 Connexion à Stormshield Data Security

L'opération de connexion permet à Stormshield Data Security de vous authentifier et de retrouver vos paramètres de configuration.

1. Pour vous connecter à Stormshield Data Security, ouvrez le menu Stormshield Data Security (clic droit sur l'icône dans la barre des tâches Windows) et choisissez **Connecter** :



2. Choisissez le **Type de compte** avec lequel vous souhaitez vous connecter.

Pour un compte mot de passe :



- a. Saisissez votre identifiant et votre mot de passe :

Stormshield Data Security - Connection

Stormshield Data Security

Type of account

Identifier:
alice smith

Enter your secret code:
●●●●●●●

Validate Cancel

- b. Cliquez sur **Valider**.
- c. Si l'identifiant ne correspond pas à un compte existant, le champ pour entrer le mot de passe et le bouton **Valider** restent grisés. Dans ce cas, créez un compte. Reportez-vous à la section **Création d'un compte** dans le *Guide d'installation*.

Pour un compte carte :

- a. Sélectionnez la carte ou le token et saisissez votre code confidentiel :

Stormshield Data Security - Connection

Stormshield Data Security

Type of account

Card No:
CGA BOB - A175FA0667FDAB41

Enter your secret code:
●●●

Validate Cancel

- b. Cliquez sur **Valider**.
- c. Si l'identifiant ne correspond pas à un compte existant, il est précédé de <NO SDS ACCOUNT>. Dans ce cas, créez un compte. Reportez-vous à la section **Création d'un compte** dans le *Guide d'installation*.

Par défaut, Stormshield Data Security pré-remplit ces champs avec les informations du dernier utilisateur à s'être connecté avec succès sur ce poste.

i NOTE

Si vous saisissez un code erroné plusieurs fois de suite (3 par défaut), votre compte se bloque.

L'image à la gauche du champ de l'identifiant utilisateur ne s'affiche qu'une fois que Stormshield Data Security reconnaît le compte.



Une fois votre connexion validée, l'icône Stormshield Data Security devient verte :  .

Vous venez d'ouvrir une session Stormshield Data Security. Tant que vous restez connecté, vous pouvez accéder aux composants installés de Stormshield Data Security (tels que Stormshield Data File, Stormshield Data Virtual Disk, Stormshield Data Shredder, Stormshield Data Mail) depuis votre bureau.

2.5 Échange de certificats

Émettre un message chiffré nécessite que l'émetteur connaisse la clé publique du destinataire, laquelle est contenue dans son certificat.

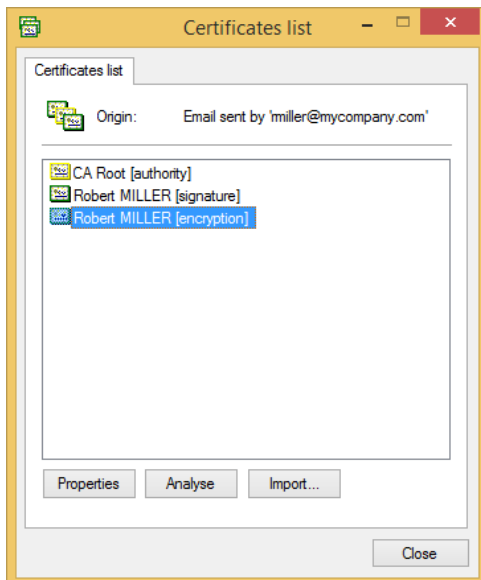
Il existe plusieurs moyens pour s'échanger des certificats :

- mettre en œuvre un annuaire LDAP ;
- s'échanger son certificat par envoi de message ;
- consulter et gérer son annuaire de confiance.

La procédure d'installation est détaillée dans le *Guide d'installation et de mise en œuvre*.

Pour l'échange de certificat par envoi de message, suivez la procédure ci-dessous :

1. Si votre correspondant vous a transmis son certificat en signant un mail, dans le bandeau inférieur cliquez sur le lien **Compte-rendu de sécurité** lors de l'ouverture d'un mail sécurisé. Pour plus d'informations sur le compte-rendu de sécurité, reportez-vous à la section [Consultation du compte-rendu de sécurité](#).
2. Dans la fenêtre du compte-rendu, cliquez sur le lien **Certificat joints** dans le coin supérieur droit pour débiter la procédure d'intégration des certificats dans votre annuaire.
3. Double-cliquez sur un certificat pour voir ses propriétés.
4. Sélectionnez un ou plusieurs certificats à importer.



Cliquez sur **Importer**.

5. Cliquez sur **Suivant** et vérifiez le récapitulatif. Cliquez sur **Terminer**.



2.6 Importer les certificats d'un e-mail signé

Lorsque vous recevez un e-mail signé dont les certificats sont absents de votre annuaire de confiance, Stormshield Data Security vous propose de les importer en fonction des paramètres définis par votre administrateur.

Pour importer les certificats à réception d'un e-mail signé :

1. Dans le bandeau inférieur Stormshield Data Security, cliquez sur **Importer les certificats**.
2. Les certificats sont importés et votre annuaire de confiance est mis à jour. Le lien n'est donc plus affiché dans le bandeau inférieur.

En cas d'erreur, consultez le [compte-rendu de sécurité](#).



3. Émettre un message sécurisé

Cette section vous explique comment émettre un message sécurisé.

3.1 Choix des options de sécurité

Ce paragraphe suppose que vous êtes déjà connecté à Stormshield Data Security au moment d'émettre votre message. Si ce n'est pas le cas, reportez-vous à la section [Vous n'êtes pas connecté à Stormshield Data Security ou votre session est verrouillée](#).

IMPORTANT

Le format RTF n'est pas supporté par Stormshield Data Mail Édition Outlook car il ne permet pas d'assurer une interopérabilité fiable avec le mécanisme de sécurisation de Stormshield Data Security. Utiliser le format RTF présente un risque de perte d'informations.



Par conséquent, il est recommandé d'utiliser le format HTML pour la rédaction de votre message sécurisé, car ce format ne présente pas de souci d'interopérabilité.

Pour émettre un message :

1. Écrivez le message comme vous le faites d'habitude avec votre client de messagerie.

NOTE

Si vous sauvegardez votre message avant de l'envoyer, c'est-à-dire si vous l'enregistrez comme "brouillon", votre message n'est pas sécurisé : il ne l'est qu'à l'envoi.

2. Vous pouvez choisir de signer et/ou chiffrer votre message. Pour cela, dans la zone **Sécurité** de l'onglet *Message*, cliquez sur l'icône  pour signer le message et/ou sur l'icône  pour chiffrer le message.
3. Le bandeau inférieur Stormshield Data Security apparaît dans la fenêtre du message et indique les options de sécurité sélectionnées.

Cliquez sur le lien **Modifier...** pour :

- choisir le format d'émission des messages sécurisés, S/MIME ou PGP. Ce choix n'est offert que si le format PGP a été configuré dans SDS. Pour plus d'informations, reportez-vous au *Guide d'administration SDS*.
 - consulter et modifier si besoin les algorithmes de signature disponibles. Pour plus de détails sur les algorithmes, consultez la section [Gestion des algorithmes de signature et chiffrement](#).
 - activer la signature détachée. Pour plus d'informations, reportez-vous à la section [Signature électronique](#).
 - activer l'apprentissage de chiffrement. Pour plus d'informations, reportez-vous à la section [Apprentissage de chiffrement](#).
 - masquer la fenêtre qui demande de confirmer l'émission d'un message au format PGP.
4. Cliquez sur **Envoyer**.

Le message émis est placé dans le dossier approprié (**Éléments envoyés** par défaut) sécurisé avec les options de sécurité sélectionnées. Si vous avez choisi le chiffrement, le message est automatiquement chiffré avec votre clé publique. Il sera déchiffré quand vous l'ouvrirez. Reportez-vous à la section [Ouverture d'un message sécurisé](#).

**i NOTE**


L'édition d'un message sécurisé directement dans la boîte d'envoi n'est pas supportée.

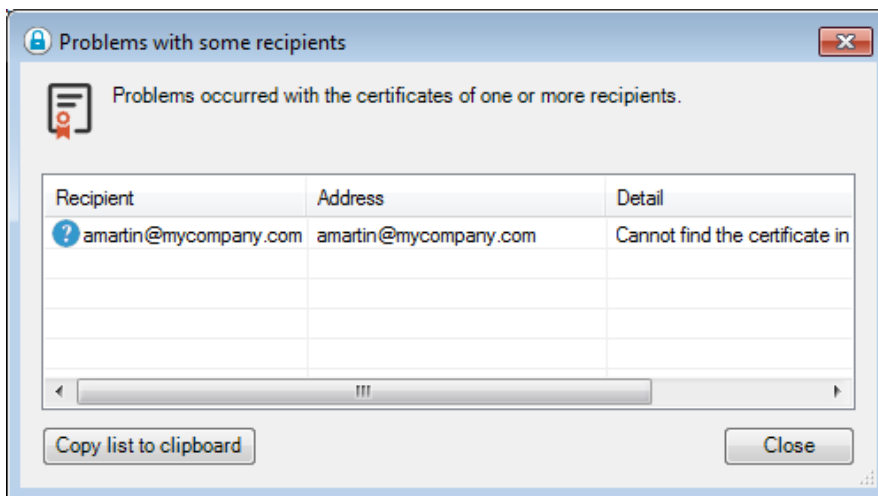
3.2 Certificat non trouvé, en erreur ou non valide

Si vous chiffrez votre message, Stormshield Data Mail Édition Outlook recherche dans votre annuaire de confiance et éventuellement dans votre (vos) annuaire(s) LDAP le certificat de chaque destinataire. Il vérifie aussi que chaque certificat est valide, permet le chiffrement, ne présente aucune extension critique non supportée (s'il en comporte une, la règle oblige à rejeter le certificat). Dans le cas où l'un des destinataires est de type groupe de contacts Outlook ou groupe de distribution Exchange, Stormshield Data Mail Édition Outlook se charge de rechercher l'ensemble des certificats correspondant aux destinataires faisant partie de cette liste (et éventuellement de ses sous-listes).


i NOTE


Il n'est pas possible de rechercher les certificats des destinataires lors de l'envoi d'un message à un groupe de distribution dynamique. En effet, contrairement aux groupes de distribution habituels qui contiennent un ensemble défini de membres, la liste des membres de ces groupes de distribution dynamiques est calculée chaque fois qu'un message leur est envoyé.

Si lors de l'envoi, au moins un certificat est absent ou introuvable, Stormshield Data Mail Édition Outlook indique les destinataires incriminés par un signe .



Vous devez résoudre le(s) problème(s) de certificat(s) avant de pouvoir envoyer votre message. S'ils sont absents de votre annuaire, vous devez les importer au préalable. Si les destinataires font partie d'un groupe de contacts, il vous est possible de retirer le(s) destinataire(s) dont le certificat pose problème.

Stormshield Data Mail Édition Outlook indique les certificats en avertissement (certificat auto-certifié, liste de révocation périmée, etc...) par un signe . Si, lors de l'envoi, tous les certificats sont en avertissement, il est possible de poursuivre quand même l'envoi avec le bouton Continuer ou de résoudre les problèmes soulevés par les certificats après annulation de l'envoi.

Si, lors de l'envoi, au moins un certificat est en erreur (périmé, révoqué, etc...), Stormshield Data Mail Édition Outlook indique les certificats incriminés par un signe . Vous devez résoudre le(s) problème(s) de certificat(s) avant de pouvoir envoyer votre message.



Dans tous les cas, il est possible de copier la liste des certificats dans le presse-papier à l'aide du bouton **Copier la liste dans le presse-papier**. Ainsi, vous pourrez conserver cette liste afin de résoudre le(s) problème(s) ultérieurement.

! IMPORTANT

En cas de changement d'adresse e-mail d'un collaborateur de l'entreprise (mariage, prestataire qui devient salarié de l'entreprise), il est impératif de renouveler le certificat utilisateur (avec republication sur l'annuaire LDAP le cas échéant) afin que l'adresse e-mail du collaborateur soit identique à celle indiquée sur son/ses certificat(s). Si ce n'est pas le cas, le collaborateur ne pourra plus envoyer de message sécurisé.

3.3 Plusieurs certificats sont disponibles

Dans le cas où plusieurs certificats sont disponibles pour un destinataire (que ce soit dans votre annuaire de confiance ou sur votre (vos) annuaire(s) LDAP), Stormshield Data Security sélectionne automatiquement le certificat valide ayant la date de début de validité la plus récente.

3.4 Certificats joints

En signant votre message, Stormshield Data Mail Édition Outlook facilite les échanges de certificats avec vos destinataires en joignant automatiquement à vos mails sécurisés vos certificats (signature et/ou chiffrement) ainsi que toute leur parenté. Pour plus d'informations, reportez-vous à la section [Échange de certificats](#).

i NOTE

Les certificats auto-signés ne sont pas joints aux messages signés.

3.5 Certificats contenant plusieurs adresses e-mail

Stormshield Data Mail Édition Outlook supporte le chiffrement de messages pour des destinataires possédant plusieurs adresses e-mails dans leurs certificats.

Si les certificats sont situés dans votre annuaire de confiance Stormshield Data Security, aucune modification de configuration n'est nécessaire.

Si les certificats sont absents de votre annuaire de confiance mais sont présents sur votre (vos) annuaire(s) LDAP, une modification de configuration de votre (vos) annuaire(s) LDAP est nécessaire.



Veillez noter qu'il n'est pas possible d'envoyer un message chiffré à un destinataire sur son adresse secondaire indiquée dans le SDAM si cette dernière n'est pas présente dans son certificat.

Pour plus d'information concernant les modifications à effectuer dans l'annuaire LDAP, reportez-vous à la section *Paramétrage LDAP : certificats comportant plusieurs adresses e-mail* du *Guide d'administration Stormshield Data Security*.



3.6 Vous n'êtes pas connecté à Stormshield Data Security ou votre session est verrouillée

Si vous sélectionnez une option de sécurisation (signer et/ou chiffrer) alors que vous n'êtes pas connecté à Stormshield Data Security ou que votre session est verrouillée, une fenêtre vous invite à vous connecter ou à déverrouiller votre session.

Si vous cliquez sur **Annuler**, la sécurisation est conservée. Si vous ne souhaitez plus sécuriser de message, désactivez explicitement la sécurisation en cliquant sur l'icône  et/ou sur l'icône .



4. Lire un message sécurisé

Cette section vous explique comment lire un message sécurisé.

4.1 Ouverture d'un message sécurisé

Vous recevez et lisez vos messages comme vous avez l'habitude de le faire avec votre client de messagerie : Stormshield Data Mail Édition Outlook se charge de déchiffrer au moment où vous l'ouvrez tout message ayant été chiffré par son émetteur. Si le message comporte une signature (avec ou sans chiffrement), Stormshield Data Mail Édition Outlook la vérifie et signale les éventuelles anomalies détectées.

Si vous n'êtes pas connecté à Stormshield Data Security, une fenêtre vous invite à vous connecter pour pouvoir lire le message ou vérifier la signature.

i NOTE

Un fichier `.msg` chiffré et/ou signé ne peut être ouvert depuis l'Explorateur Windows. Reportez-vous à l'article à ce sujet dans la [Base de connaissance](#) Stormshield (anglais uniquement).

! IMPORTANT

Il est interdit de modifier un message sécurisé reçu avec le menu Outlook **Actions > Modifier le message** car cette opération pourrait désactiver la sécurité du message.

4.2 Consultation du compte-rendu de sécurité

A l'ouverture d'un message sécurisé, vous pouvez consulter le compte-rendu de sécurité en cliquant sur le lien dans le bandeau inférieur Stormshield Data Security.

Une icône est visible à côté du lien **Compte-rendu de sécurité** pour signaler une erreur ou un avertissement consultables dans le compte-rendu. En cas d'erreur, le bandeau de sécurité apparaît en rouge.

Le compte-rendu de sécurité indique le détail des algorithmes employés pour le chiffrement et la signature du message.

Si le message est signé, le compte-rendu comprend également :

- l'identité de l'émetteur signataire du message ;
- un indicateur de confiance à accorder au certificat de l'émetteur dans le bandeau supérieur de la fenêtre du compte-rendu qui indique :
 - le résultat de la vérification cryptographique de la signature. La signature est alors considérée comme correcte ou incorrecte.
 - le résultat des contrôles effectués sur le certificat de l'émetteur : Stormshield Data Mail Édition Outlook vérifie que le certificat est valide, qu'il est autorisé à signer et qu'il ne présente aucune extension critique non supportée. S'il en comporte une, la règle de sécurité l'oblige à rejeter le certificat.

i NOTE

La vérification de la signature de messages signés au format PGP (donc non S/MIME) n'est pas



supportée par Stormshield Data Mail Édition Outlook. Un message indiquant que la signature n'a pas pu être vérifiée sera affiché dans le bandeau de sécurité pour les messages de ce type.

4.3 Réponse ou transfert d'un message chiffré

Lorsque vous répondez à un ou plusieurs destinataires d'un message chiffré, l'option de chiffrement est automatiquement sélectionnée dans votre message de réponse.

Ce mécanisme s'applique également lors du transfert des messages chiffrés.

4.4 Messages sécurisés attachés en pièces jointes

Pour lire un message sécurisé qui se trouve en pièce jointe d'un autre message (sécurisé ou non), glissez-déposez le dans un des dossiers de votre boîte de réception.

i NOTE

Lorsque des messages comportant des pièces jointes sont réceptionnés, Outlook indique la taille de ces pièces jointes. Dans le cas de messages chiffrés, Outlook indique systématiquement "0 octet".

4.5 Messages sécurisés au format OpenPGP

Les messages sécurisés par un client de messagerie supportant le protocole OpenPGP (format PGP/MIME) peuvent être déchiffrés par Stormshield Data Mail Édition Outlook. Il faut au préalable avoir importé les clés de déchiffrement au format OpenPGP dans votre porte-clés.

Reportez-vous à la section *Clés de déchiffrement OpenPGP* du *Guide d'installation et de mise en œuvre* de Stormshield Data Security.

4.5.1 Importer un porte-clés OpenPGP

1. Ouvrez le menu **Stormshield Data Security**.
2. Choisissez **Propriétés**.
3. Cliquez sur l'onglet *Configuration*.
4. Choisissez l'icône **Porte-clés**.
5. Sélectionnez l'onglet *Porte-clés OpenPGP*.
6. Cliquez sur **Opérations** puis **Importer un porte-clés**.
7. Sélectionnez un fichier au format OpenPGP (*.pgp*, *.pgpou*, *.asc*). Le fichier peut contenir plusieurs clés.
8. Saisissez le mot de passe protégeant le fichier.

Pour supprimer ou remplacer le porte-clés, sélectionnez les menus **Supprimer le porte-clés** ou **Remplacer le porte-clés** dans le menu **Opérations**.

Le remplacement du porte-clés écrase le porte-clés déjà présent.



4.5.2 Lire un message sécurisé au format OpenPGP

Vous recevez et lisez vos messages comme vous avez l'habitude de le faire avec votre client de messagerie : Stormshield Data Mail Édition Outlook se charge de déchiffrer au moment où vous l'ouvrez tout message ayant été chiffré par son émetteur.

Si vous n'êtes pas connecté à Stormshield Data Security, une fenêtre vous invite à vous connecter pour pouvoir lire le message.

La sécurité d'un message chiffré et signé ou seulement signé au format OpenPGP ne peut pas être désactivée.

i NOTE

La vérification de la signature de messages signés au format PGP n'est pas supportée par Stormshield Data Mail Édition Outlook. Un message indiquant que la signature n'a pas pu être vérifiée sera affiché dans le bandeau de sécurité pour les messages de ce type.

4.5.3 Lire un message sécurisé au format PGP Partitionné

Le format PGP Partitionné est le prédécesseur du format PGP/MIME. Les deux formats s'appuient sur les mêmes mécanismes de sécurité et le format de porte-clés est donc le même.

La lecture d'un message sécurisé au format PGP Partitionné s'effectue de la même façon que la lecture d'un message au format PGP/MIME.



5. Fonctions avancées

Cette section traite des fonctions avancées de Stormshield Data Mail Édition Outlook et s'adresse aux utilisateurs avertis.

5.1 Interaction avec Stormshield Data Connector

Si le module Stormshield Data Connector est installé sur la machine, vous pouvez envoyer des messages chiffrés et/ou signés depuis un script PowerShell ou un programme .NET.

Pour plus d'informations, consultez le Guide d'utilisation du module Stormshield Data Connector.

5.2 Gestion des algorithmes de signature

Les algorithmes de signature Stormshield Data Mail Édition Outlook par défaut peuvent être modifiés lors de la rédaction d'un nouveau message. Cliquez sur le lien **Modifier** en bas à droite du bandeau de sécurité inférieur Stormshield Data Security dans la fenêtre de rédaction du message.

5.2.1 Signature

Dans la liste déroulante **Algorithme d'empreinte**, choisissez l'algorithme à utiliser lors de la signature du message parmi SHA-512 (sélectionné par défaut) et SHA-256.

Si vous possédez l'outil d'administration Stormshield Data Authority Manager, vous pouvez modifier l'algorithme présélectionné par défaut.

5.2.2 Chiffrement

Dans la liste déroulante **Algorithme/Longueur**, choisissez l'algorithme à utiliser lors du chiffrement du message parmi AES 256 (sélectionné par défaut) et Triple DES 192.

Si vous possédez l'outil d'administration Stormshield Data Authority Manager, vous pouvez modifier l'algorithme présélectionné par défaut.

Un message chiffré peut être déchiffré avec n'importe quel client de messagerie possédant Stormshield Data Mail Édition Outlook, quel que soit l'algorithme employé. En revanche, si votre destinataire utilise un client de messagerie ne gérant pas nativement l'algorithme AES 256 et dépourvu de Stormshield Data Mail Édition Outlook, il est possible qu'il ne puisse pas déchiffrer votre message.

5.3 Signature détachée

Pour activer la signature détachée, cliquez sur le lien **Modifier** en bas à droite du bandeau de sécurité Stormshield Data Security dans la fenêtre de rédaction du message.

Pour plus d'informations sur la signature détachée, reportez-vous à la section [Signature électronique](#).

Si vous possédez l'outil d'administration Stormshield Data Authority Manager, vous pouvez activer cette option par défaut.



5.4 Apprentissage de chiffrement

L'apprentissage de chiffrement est un mécanisme qui détecte les habitudes de l'utilisateur en matière de chiffrement de message.

Dès lors que l'apprentissage est activé, lorsque l'utilisateur rédige un message à destination d'une personne en particulier, Stormshield Data Security estime la fréquence d'envoi de messages sécurisés vers ce destinataire.

Si depuis que la journalisation est activée (avec une limite maximum de 90 jours), trois messages chiffrés au moins ont été envoyés à ce destinataire, tout nouveau message vers ce destinataire est désormais automatiquement chiffré.

L'utilisateur peut toujours désactiver manuellement le chiffrement. Dans ce cas, l'automatisation est temporairement désactivée pour le message en cours de rédaction. L'utilisateur devra alors activer manuellement le chiffrement s'il désire de nouveau l'activer.

- Pour activer l'apprentissage, cliquez sur le lien **Modifier** en bas à droite du bandeau de sécurité Stormshield Data Security dans la fenêtre de rédaction du message.

L'apprentissage peut être réinitialisé dans les options de sécurité.

5.5 Délégation de déchiffrement

La délégation de déchiffrement consiste à permettre à une autre personne (par exemple votre secrétaire) de déchiffrer vos messages en votre absence. Il faut pour cela lui confier votre clé personnelle (si vous ne possédez qu'une seule bi-clé de signature et de chiffrement) ou votre bi-clé de chiffrement (si vous possédez deux bi-clés différentes pour les fonctions de signature et de chiffrement).

Il faut bien noter qu'avec la clé que vous allez lui confier, la personne ne pourra que déchiffrer vos messages : elle ne pourra pas signer en votre nom.

La technique consiste à effectuer un export de la clé utilisée pour le chiffrement, à partir de votre compte de sécurité, pour permettre un import sur la machine et dans le compte de sécurité de la personne à qui vous la confiez.

Pour exporter votre clé de sécurité ou l'importer dans un compte comme clé de déchiffrement, reportez-vous au *Guide d'installation et de mise en œuvre*.

5.6 Transchiffrement

5.6.1 Principes du transchiffrement

Le transchiffrement est une opération qui permet de mettre à jour le niveau de protection des messages sécurisés (messages au format S/MIME ou messages en clair contenant une pièce jointe chiffrée avec le composant Stormshield Data Mail Édition Outlook) en re-chiffrant avec une nouvelle clé les messages sécurisés avec une ancienne clé de chiffrement et en utilisant l'algorithme de chiffrement configuré par défaut dans le compte utilisateur.

L'ancienne clé de chiffrement peut devenir obsolète pour les raisons suivantes :

- La clé de chiffrement a été renouvelée.
- Le compte utilisateur a été mis à jour et la clé de chiffrement est devenue inutilisable (passage d'un compte mot de passe à un compte carte, révocation de clé, clé provenant d'un autre système de chiffrement).



- La clé de chiffrement a été transmise par un tiers (par exemple lors d'une passation de pouvoir dans le cadre d'un changement de poste).

Pour transchiffrer un message sécurisé, l'ancienne clé de chiffrement est nécessaire afin de le déchiffrer au préalable. Elle doit donc être présente dans le porte-clés en tant que clé de déchiffrement.

Une fois transchiffré, le message est alors déchiffrable uniquement avec la nouvelle clé.

Un message ou une pièce jointe est transchiffré dans son format d'origine : s'il est au format .sbox, il reste au format .sbox après transchiffrement.

i NOTE

Une clé de délégation ne peut pas être utilisée pour transchiffrer car elle donne uniquement le droit de lire des messages sécurisés.

5.6.2 Transchiffrement et gestion des collaborateurs

Le comportement du processus de transchiffrement vis-à-vis des collaborateurs est le suivant dans ces deux cas :

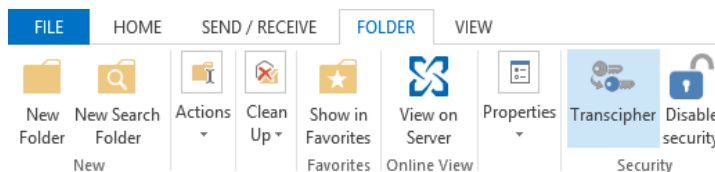
- Lorsqu'un message sécurisé au format S/MIME reçu par plusieurs destinataires est transchiffré, il est alors sécurisé uniquement pour l'utilisateur courant. Les collaborateurs ne sont pas impactés car seule la copie personnelle locale du message est transchiffrée.
- Lorsqu'un message en clair avec une pièce jointe sécurisée .SBOX est transchiffré, seul le niveau de sécurité de la pièce jointe est mis à jour. Si cette pièce jointe est transférée aux collaborateurs déclarés dans le fichier .SBOX original et si leurs certificats sont toujours valides, ceux-ci pourront toujours accéder à la pièce jointe.

Les comptes de recouvrement associés aux comptes utilisateurs sont quant à eux toujours intégrés aux messages transchiffrés.

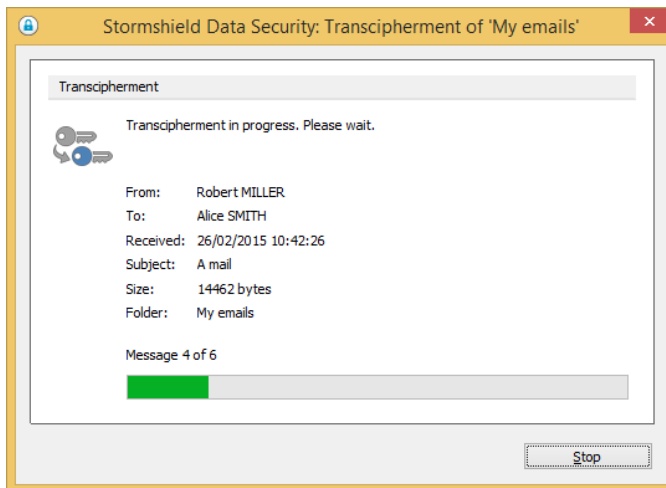
5.6.3 Utilisation du transchiffrement

Le transchiffrement est une opération qui s'effectue sur un dossier et l'ensemble de ses sous-dossiers.

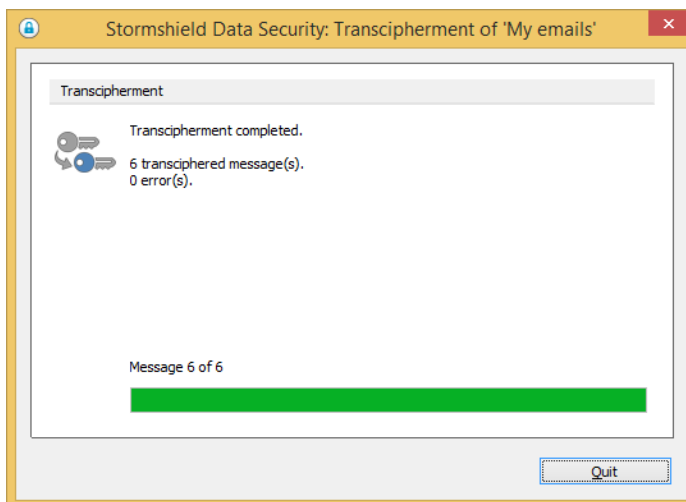
1. Sélectionnez le dossier à transchiffrer.
2. Effectuez un clic droit sur le dossier pour faire apparaître le menu contextuel et sélectionnez **Transchiffrer** ou bien cliquez sur **Transchiffrer** depuis l'onglet *Dossier* du ruban principal.



3. Dans la fenêtre de transchiffrement, cliquez sur **Transchiffrer**. Au cours du traitement, des informations sont affichées pour suivre le bon déroulement des opérations.



4. A la fin du processus, un rapport affiche le nombre de messages transchiffrés et le nombre d'erreurs rencontrées. En cas d'erreur, cliquez sur le bouton **Voir le compte-rendu**.



Le compte-rendu détaille le type d'erreur pour chaque message concerné :

- L'utilisateur ne possède pas de clé de chiffrement valide.
- L'utilisateur ne possède qu'une clé de délégation.
- Le traitement du message a provoqué une erreur.
- Le module Stormshield Data File n'est pas installé (dans le cas où le message contient une pièce jointe sécurisée *.SBOX*).

Le fichier de compte-rendu est intitulé *SBoxTransciphermentReport-<utilisateur>-<horodatage>.txt* et se trouve dans le dossier temporaire de l'utilisateur. Ce fichier est conservé dans ce dossier.

IMPORTANT

L'accès aux clés privées de l'utilisateur pendant le transchiffrement nécessite d'être connecté au compte Stormshield Data Security.

La fenêtre de progression empêche toute interaction avec Microsoft Outlook pendant la durée du processus. Si malgré cela, le transchiffrement est interrompu, il faut le relancer manuellement.



5.6.4 Limitations du transchiffrement

Certaines configurations de messages transchiffrés ne sont pas prises en charge par le processus de transchiffrement :

- Une pièce jointe *.SBOX* contenue dans un message sécurisé S/MIME n'est pas transchiffrée.
- Un message sécurisé transmis en tant que pièce jointe *.MSG* dans un message en clair n'est pas transchiffré.

Le transchiffrement des messages chiffrés à l'aide du protocole OpenPGP n'est pas possible.

5.7 Désactivation de la sécurité

5.7.1 Principes de la désactivation de la sécurité

Par défaut, les messages sécurisés reçus sont conservés sécurisés dans la base de messages du client de messagerie.

Il peut arriver que vous ne souhaitiez pas conserver la sécurité d'un message sécurisé, par exemple si vous voulez le déposer dans un dossier public.

Lors de la désactivation de la sécurité, les messages chiffrés et/ou signés seront stockés en clair, sans chiffrement ni signature.

NOTE

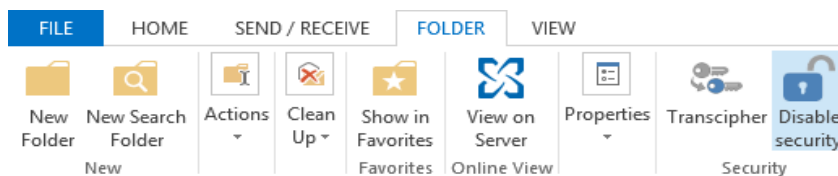
Une clé de délégation ne peut pas être utilisée pour désactiver la sécurité.

5.7.2 Désactiver la sécurité

La désactivation de la sécurité est une opération qui peut s'effectuer sur un dossier et l'ensemble de ses sous-dossiers ou sur une sélection de messages électroniques.

Pour désactiver la sécurité d'un dossier :

1. Sélectionnez le dossier.
2. Effectuez un clic droit sur le dossier pour faire apparaître le menu contextuel et sélectionnez **Désactiver la sécurité** ou bien cliquez sur **Désactiver la sécurité** depuis l'onglet *Dossier* du ruban principal.



3. Dans la fenêtre de désactivation de la sécurité, cliquez sur **Désactiver la sécurité**. Au cours du traitement, des informations sont affichées pour suivre le bon déroulement des opérations.
4. A la fin du processus, un rapport affiche le nombre de messages désécurisés et le nombre d'erreurs rencontrées. En cas d'erreur, cliquez sur le bouton **Voir le compte-rendu**.

Pour désactiver la sécurité d'une sélection de messages :



1. Sélectionnez un ou plusieurs messages.
2. Effectuez un clic droit sur la sélection pour faire apparaître le menu contextuel et sélectionnez **Désactiver la sécurité** ou bien cliquez sur **Désactiver la sécurité** depuis l'onglet *Accueil* du ruban principal.
3. Le reste de la procédure est identique à la désactivation de la sécurité d'un dossier.

Le compte-rendu détaille le type d'erreur pour chaque message concerné :

- L'utilisateur ne possède pas de clé de chiffrement valide.
- L'utilisateur ne possède qu'une clé de délégation.
- Le traitement du message a provoqué une erreur.

Le fichier de compte-rendu est intitulé *SBoxDeleteSecurityReport-<horodatage>.txt* et se trouve dans le dossier temporaire de l'utilisateur. Ce fichier est conservé dans ce dossier.

Généralement les messages erronés sont des messages chiffrés qui utilisent une clé inconnue (par exemple, une ancienne clé, qui n'a pas été importée comme clé de déchiffrement dans votre compte).

i NOTE

L'accès aux clés privées de l'utilisateur pendant la désactivation de la sécurité nécessite d'être connecté au compte Stormshield Data Security.

La fenêtre de progression empêche toute interaction avec Microsoft Outlook pendant la durée du processus. Si malgré cela, la désactivation de la sécurité est interrompue, il faut la relancer manuellement.

5.7.3 Limitations de la désactivation de la sécurité

Certaines configurations de messages ne sont pas prises en charge par le processus de désactivation de la sécurité :

- Un message sécurisé transmis en tant que pièce jointe *.msg* d'un message en clair ou d'un message sécurisé ne peut pas être désécurisé.
- Un message chiffré et signé ou seulement signé au format OpenPGP ne peut pas être désécurisé.



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2022. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.