GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

GUIDE D'ADMINISTRATION

Version 11.4.4

Dernière mise à jour du document : 10 juin 2026

Référence : sds-fr-sdse-guide_d_administration-v11.4.4

Table des matières

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

1. Avant de commencer

Ce guide contient les informations nécessaires à l'administration de la solution SDS Enterprise et à l'installation des agents SDS Enterprise dans votre environnement.

1.1 À quoi sert SDS Enterprise ?

SDS Enterprise assure la protection et la confidentialité des données stockées sur les répertoires locaux, partagés, ou dans le Cloud, en s'appuyant sur le chiffrement de bout en bout transparent et intégré aux outils de communication et collaboration. Il permet également de maîtriser l'accès aux données protégées selon les groupes et les profils des utilisateurs.

La solution SDS Enterprise comprend la console d'administration SDMC depuis laquelle vous définissez les politiques de sécurité, ainsi qu'un agent installé sur les postes de travail des utilisateurs permettant d'appliquer les politiques et fournissant les fonctionnalités suivantes :

- Le chiffrement transparent et en temps réel des fichiers, en vue d'un transfert par mail ou d'une sauvegarde sécurisée,
- Le chiffrement de fichiers stockés sur des espaces synchronisés avec les hébergeurs en ligne OneDrive, DropBox, SharePoint et Oodrive,
- Le chiffrement et la signature des courriers électroniques permettant de protéger les données qu'ils contiennent et de garantir leur provenance et l'intégrité de leur contenu,
- Le partage des dossiers chiffrés sur le réseau de l'entreprise avec des collaborateurs,
- L'effacement sécurisé et irréversible des données,
- La signature électronique de fichiers et de dossiers, permettant de garantir leur provenance et l'intégrité de leur contenu,
- Le chiffrement de disques virtuels, permettant de stocker des documents protégés. Ces disques virtuels peuvent être partagés entre collaborateurs.

La solution comprend également le composant Stormshield Data Connector, qui permet de piloter les fonctionnalités de la solution SDS Enterprise à travers un module PowerShell ou des API .NET.

La console d'administration SDMC est hébergée par les services Cloud de Stormshield. Depuis SDMC, vous pouvez :

- Créer et configurer les politiques de sécurité appliquées par les agents SDS Enterprise installés sur les postes de travail des utilisateurs,
- Déclarer les autorités de certification dont dépendent les certificats des utilisateurs,
- Déclarer les annuaires LDAP de l'entreprise afin de gérer les échanges de certificats,
- Télécharger les packages d'installation des agents SDS Enterprise.

Pour utiliser la console SDMC, commencez par créer un compte d'entreprise, puis un ou plusieurs comptes administrateur comme décrit dans la section Se connecter à SDMC.

Vous pouvez également configurer une politique de sécurité directement dans un fichier *.json* et l'intégrer au package d'installation de SDS Enterprise. Pour plus d'informations sur la configuration de ce fichier, consultez le *Guide de configuration avancée*.

1.2 Comment fonctionne SDS Enterprise ?

Prérequis
Vous devez posséder une infrastructure pour la génération des clés de chiffrement et de signature des utilisateurs de l'entreprise. Vous pouvez ensuite les diffuser auprès des utilisateurs avec le moyen de votre choix, par exemple via des cartes à puce.
Si vous souhaitez utiliser la solution d'infrastructure à clé publique de Microsoft, consultez la section Mettre en place la solution d'infrastructure à clé publique (PKI) de Microsoft.

SDS Enterprise met en œuvre des moyens cryptographiques dits “à clé publique”.

Chaque utilisateur possède au moins un couple 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.

Un couple de clés différent est nécessaire pour chaque usage :

- un couple de clés de chiffrement pour le chiffrement et le partage de documents confidentiels ou de messages électroniques,
- un couple de clés de signature pour la signature de documents et de messages.

Pour sécuriser les clés privées de vos utilisateurs, vous pouvez les stocker sur des supports cryptographiques supportant la norme PKCS#11. Dans le cadre de l'authentification Single Sign-on (SSO) des utilisateurs, vous devez stocker les clés dans le Magasin de certificats Windows.

Pour chiffrer des fichiers ou envoyer des messages chiffrés à des correspondants, l'utilisateur doit connaître la clé publique de chiffrement de ses correspondants.

Les clés publiques sont distribuées aux utilisateurs sous forme de certificats. Un certificat est un document électronique qui associe une clé publique à son propriétaire. SDS Enterprise supporte le format de certificat X.509 V3. Ces certificats sont stockés dans l'annuaire de confiance des utilisateurs, comme expliqué dans la section Comprendre la notion d'annuaire de confiance.

Les clés des utilisateurs et des autorités de certification sont de type RSA et doivent avoir une taille maximale de 4096 bits, avec un exposant public strictement supérieur à 65536. Les certificats et les listes de révocation doivent être signés avec l'algorithme d'empreinte SHA-512.

IMPORTANT
En cas de renouvellement des clés de chiffrement, veillez à conserver les anciennes clés des utilisateurs de manière sûre dans leur compte SDS Enterprise. L'utilisateur pourra ainsi toujours déchiffrer les données chiffrées avec une ancienne clé.
Pour plus d'informations, reportez-vous aux sections Déchiffrer les données d'un utilisateur avec une ancienne clé ou une clé de délégation et Déchiffrer les données d'un utilisateur avec une clé de recouvrement.

Pour plus d'informations sur la gestion des certificats, reportez-vous aux sections Gérer les certificats des autorités de certification et les certificats de recouvrement dans SDMC et Définir les paramètres de création de comptes.

1.3 Comment déployer SDS Enterprise sur votre parc ?

Vous pouvez déployer SDS Enterprise sur les postes des utilisateurs avec des solutions de télédistribution comme la solution Microsoft Endpoint Configuration Manager. Vous devez déployer sur les postes :

- le package d'installation des agents SDS Enterprise au format *.msi*. Vous pouvez le télécharger depuis la console SDMC en français et en anglais.
- le fichier de la politique de sécurité signée et le certificat correspondant. La politique est créée et paramétrée dans la console SDMC. Vous devez la télécharger depuis la console puis la faire signer par l'administrateur ayant le rôle de signataire de politique de sécurité. L'utilitaire de signature est disponible dans SDMC également.

À chaque redémarrage, l'agent SDS Enterprise vérifie si une nouvelle mise à jour de politique est disponible sur le serveur jouant le rôle de point de distribution des politiques. Si tel est le cas, il l'applique automatiquement.

Pour plus d'informations sur le déploiement des agents, reportez-vous à la section **Installer les agents SDS Enterprise sur les postes des utilisateurs et déployer les politiques de sécurité**.

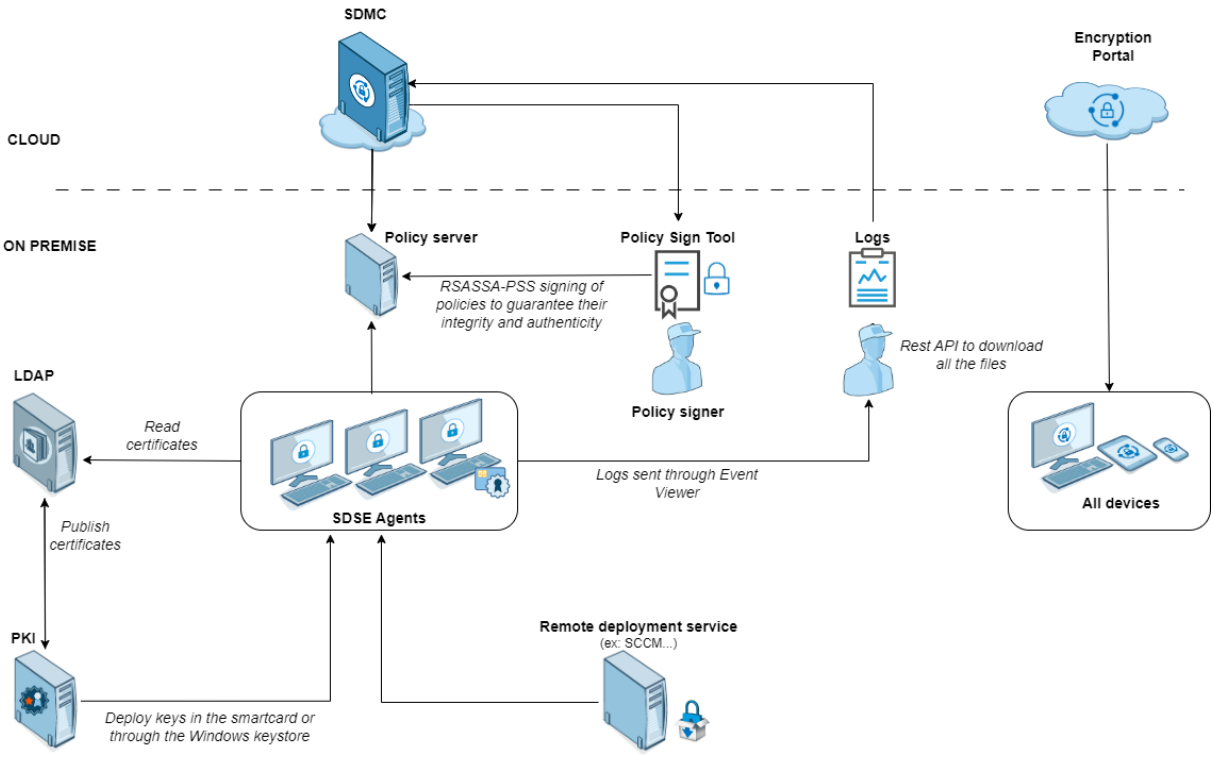
1.4 Comprendre la notion d'annuaire de confiance

SDS Enterprise permet de gérer un annuaire de confiance sur les postes des utilisateurs : vous y insérez les certificats (clés publiques) des utilisateurs et des autorités auxquels vous faites confiance.

L'annuaire de confiance peut être alimenté automatiquement par un annuaire LDAP.

Pour plus d'informations, reportez-vous aux sections **Gérer les annuaires LDAP dans SDMC** et **Configurer les annuaires d'entreprise**.

1.5 Schéma d'architecture de SDS Enterprise



2. Environnement d'utilisation

Pour utiliser SDS Enterprise dans les conditions de son évaluation Critères Communs et de sa qualification au niveau standard, il est impératif de respecter les recommandations suivantes.

2.1 Recommandations sur la veille sécurité

1. Consultez régulièrement les alertes de sécurité diffusées sur https://advisories.stormshield.eu/.
2. Appliquez systématiquement une mise à jour du logiciel si elle contient la correction d'une faille de sécurité. Ces mises à jour sont disponibles sur votre espace client MyStormshield.

2.2 Recommandations sur les clés et les certificats

1. Les clés RSA des utilisateurs et des autorités de certification doivent être d'une taille minimale de 4096 bits, avec un exposant public strictement supérieur à 65536.
2. Les certificats et les CRL doivent être signés avec l'algorithme d'empreinte SHA-512.

2.3 Recommandations sur les algorithmes

SDS Enterprise supporte l'algorithme de chiffrement AES 256 et l'algorithme de signature SHA-512.

Pour une utilisation au-delà de 2030, la taille minimale d'une clé RSA est de 3072 bits.

2.4 Recommandations sur les comptes utilisateur

1. Les comptes utilisateur doivent être protégés par l'algorithme de chiffrement AES 256 et le standard de hachage cryptographique SHA-256.
2. Les mots de passe doivent être soumis à une politique de sécurité empêchant les mots de passe faibles.
3. Des mesures organisationnelles adaptées doivent assurer l'authenticité des politiques à partir desquelles les comptes utilisateur sont créés.
4. En cas d'utilisation d'un porte-clés matériel (carte à puce ou token matériel), ce dispositif assure la protection en confidentialité et en intégrité des clés et des certificats qu'il contient.

2.5 Recommandations sur les postes de travail

1. Le poste de travail sur lequel SDS Enterprise est installé doit être sain. Il doit pour cela exister dans l'organisation une politique de sécurité du système d'information dont les exigences sont respectées sur les postes de travail. Cette politique doit notamment prévoir que les logiciels installés seront régulièrement mis à jour et que le système sera protégé contre les virus et autres logiciels espions ou malveillants (pare-feu correctement paramétré, antivirus à jour, etc).

2. La politique de sécurité doit également prévoir que les postes non équipés de SDS Enterprise n'auront pas accès aux dossiers confidentiels partagés sur un serveur, afin qu'un utilisateur ne puisse pas provoquer un déni de service en altérant ou en supprimant, par inadvertance ou par malveillance, les fichiers protégés par le produit.
3. L'accès aux fonctions d'administration du système du poste est restreint aux seuls administrateurs système.
4. Le système d'exploitation doit gérer les journaux d'événements générés par le produit en conformité avec la politique de sécurité de l'organisation. Il doit par exemple restreindre l'accès en lecture à ces journaux aux seules personnes explicitement autorisées.
5. L'utilisateur doit veiller à ce qu'un attaquant potentiel ne puisse pas observer voire accéder au poste lorsque la session SDS Enterprise est ouverte.

2.6 Recommandations sur les intervenants

1. Les administrateurs SDS Enterprise sont considérés de confiance. Ils définissent la politique de sécurité de SDS Enterprise en respectant l'état de l'art, et éventuellement créent les comptes des utilisateurs via l'application Stormshield Data Management Center.
2. L'administrateur système est également considéré de confiance. Il est en charge de l'installation et de la maintenance de l'application et du poste de travail (système d'exploitation, logiciels de protection, librairie *PKCS#11* d'interface avec une carte à puce, applications bureautiques et métier, etc). Il applique la politique de sécurité définie par les administrateurs SDS Enterprise.
3. L'utilisateur du produit doit respecter la politique de sécurité en vigueur dans son organisme.

3. Se connecter à SDMC

Pour utiliser la console d'administration SDMC, vous devez d'abord créer votre compte d'entreprise.

Lors de la création du compte, vous avez le choix entre deux modes de connexion : Mot de passe ou SAML.

Dans le premier cas, vous devez créer le premier compte d'administration pour vous connecter à SDMC. Les autres administrateurs peuvent être ensuite créés directement dans SDMC. Pour créer d'autres comptes d'administration, reportez-vous à la section Gérer les administrateurs dans SDMC.

Pour plus d'informations sur le mode de connexion SAML, reportez-vous à la section Se connecter à SDMC via un fournisseur d'identité.

À la création du compte d'entreprise, vous disposez d'une période d'évaluation de 30 jours. Vous devez ensuite importer une licence définitive. Pour plus d'informations sur la licence, reportez-vous à la section Gérer la licence.

3.1 Créer le compte d'entreprise

Le compte d'entreprise contient toutes les informations liées à votre société. Il est créé dès le début de la procédure d'enregistrement de votre société auprès de la solution SDMC.

Le compte d'entreprise est dédié à une seule société et n'est jamais partagé avec d'autres sociétés.

1. Cliquez sur l'adresse https://sds.stormshieldcs.eu/admin/#/register-my-company.
2. Complétez les informations sur votre société et vos informations de contact.
3. Cochez la case **J'accepte les Conditions générales d'utilisation** après les avoir lues.
4. Cliquez sur **Créer** pour enregistrer votre compte d'entreprise.
5. Cliquez sur le lien envoyé par e-mail pour valider la création du compte et du domaine.
6. L'activation du compte doit ensuite être validée par Stormshield. Elle vous est confirmée par e-mail.

- Si vous avez choisi le mode de connexion SAML, vous pouvez vous connecter à SDMC avec vos identifiants d'entreprise. Vous devez avoir configuré le mode de connexion via un fournisseur d'identité auparavant. Consultez la section Se connecter à SDMC via un fournisseur d'identité.
  La page de connexion à votre console d'administration SDMC reste toujours accessible à l'adresse https://sds.stormshieldcs.eu/admin. En cas d'erreur de connexion, consultez la section Résoudre les problèmes.
- Si vous avez choisi le mode de connexion Mot de passe, vous pouvez passer à l'étape suivante.

3.2 Créer le premier compte d'administration

Si vous avez choisi le mode de connexion Mot de passe, vous devez créer un compte d'administration.

1. Après la validation de l'activation de votre compte d'entreprise par Stormshield, vous recevez un e-mail vous demandant de créer un compte d'administration dans le délai indiqué. Sur cet e-mail, cliquez sur **Créer le compte d'administration**.

2. Complétez les champs. L'adresse e-mail est déjà renseignée.
3. Cliquez sur **Créer** pour enregistrer votre compte d'administration.
4. Connectez-vous à SDMC. La page de connexion à votre console d'administration SDMC reste toujours accessible à l'adresse https://sds.stormshieldcs.eu/admin.

3.3 Se connecter à SDMC via un fournisseur d'identité

Grâce au protocole SAML, SDMC peut s'appuyer sur un fournisseur d'identité (IdP) pour authentifier les administrateurs.

Pour mettre en place ce mode de connexion, vous devez :

- Mettre à disposition de SDMC un well-known indiquant l'IdP à contacter,
- Configurer l'IdP de votre choix pour qu'il fournisse à SDMC les informations attendues pour l'authentification. L'IdP doit être accessible sur Internet et vous devez posséder son certificat.

3.3.1 Mettre à disposition le well-known

Le well-known est un dossier de configuration contenant le fichier de configuration *sdmc-configuration*. Mis à disposition par un serveur, il doit être accessible en HTTPS depuis tous les réseaux. Le serveur hôte du well-known doit approuver le certificat SDMC pour que la communication entre les deux soit possible.

Le fichier *sdmc-configuration* est au format *JSON*. Il doit contenir les informations suivantes concernant l'IdP à contacter :

- *idpCertificate* : Adresse URL du certificat affecté à l'IdP,
- *idpUrl* : Adresse URL de l'IdP à contacter.

Pour être joint par SDMC, le fichier doit être accessible à l'URL suivante :

https://sdmc.[domaine-entreprise]/.well-known/sdmc-configuration

Où :

- *https* est obligatoire,
- *sdmc.* est un sous-domaine nécessaire au client pour exposer le fichier well-known,
- *[domaine-entreprise]* est remplacé par le domaine du compte d'entreprise contenu dans l'adresse e-mail de l'administrateur tentant une connexion,
- *.well-known* est le dossier contenant tous les fichiers well-known,
- *sdmc-configuration* est le fichier dédié à SDMC permettant de récupérer les informations de connexion SAML telles que l'URL de l'IdP.

Pour des raisons de performances, les informations *idpUrl* et *idpCertificate* sont conservées en cache durant 24 heures à partir de la première connexion. Les modifications du fichier *sdmc-configuration* peuvent donc ne pas être immédiatement propagées sur SDMC. Cela peut prendre jusqu'à 24 heures.

EXEMPLE

Pour le nom de domaine *example.com*, le well-known doit être accessible à l'URL https://sdmc.example.com/.well-known/sdmc-configuration et doit avoir la forme suivante :

```
{
"idpCertificate":"https://example.com/assets/certificate.pem",
```

```
    "idpUrl":"https://example.com/saml/login"
    }
```

3.3.2 Configurer le fournisseur d'identité

Configurez les paramètres suivants sur l'IdP afin qu'il envoie le format d'informations attendu à SDMC lorsqu'un administrateur tente de se connecter :

Paramètre	Type	Valeur	Statut
"email"	Chaîne de caractères	Adresse e-mail, sous la forme : http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Obligatoire
"firstName"	Chaîne de caractères	Prénom, sous la forme : http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Optionnel
"lastName"	Chaîne de caractères	Nom de famille, sous la forme : http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Optionnel

Vous devez également ajouter les URL suivantes dans la configuration de l'application IdP :

- **Entity ID** : https://sds.stormshieldcs.eu/api/internal/5/admins/saml/metadata.xml
- **Assertion Consumer Service URL** : https://sds.stormshieldcs.eu/api/internal/5/admins/saml/acs

3.3.3 Chiffrer les communications avec le certificat SDMC

Certains IdP proposent le chiffrement des communications SAML 2.0. Pour le mettre en oeuvre, ajoutez la clé publique suivante, extraite du certificat SDMC, dans la configuration de l'IdP associé au chiffrement des communications :

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAu5nGaYFmaHGk6fu6+H5b
qo/JBUvbuZQlhWE7Ybocns4YIEKVSi6B9QtxasLN4BhZuh6autZmhLqQtZtxV8S4
4BkU44KXNeKPGGhD1izp2mJ8iE6Z3lhUCYRxrRebZQ2Fmu8Z/rKpUDMxwhjOskkQ
LVHWflUIT8heRQuUNqN3nqF7049Fe3rQQvI07NOokmPnwO5EpptopOCRj0b2FSGx
KdTk/RNm/QKBuirF/7w8JremeG6W+HIC6810cN/Lf88aHoL9NKm0A9eknJyzcKy3
wH0TTBF3N4n521psttg22hOZjQXMqSjkXUPHEMBq6br9Tixg53Q8rJhthS+Ahosb
qsxRkAOUiaEPmOR8Kx6AlJ6gdGJe0PAqiZTOiYKEFx1yU6kEbpnU7KkKJwsmOZVg
VQMFIVOQiv/1wRLx49ybviZqyNgFuZx4+4pGQt3ETkDQhK10s0xO7/UUMYEKu59C
YSAyJNVYVjujC2QqaP8YXcJNndEbSPH58PxFDZ8SmBa9uSzxcO2o+Zg2972dxUXW
fIZpWifdkDw6ktor9LhaqDYUw6KLmHh8phRzg49Kt7JaJUtBc9x0YgaXJ23ZfaP9
ndOaWK4loycCS4yyA6Uqupqp5oJV/pyPEAIzrYAVHHBtyxcv2uCXWFlmBZeN6RDZ
Y6tY9gfqqoatDT32PfH4Xs0CAwEAAQ==
-----END PUBLIC KEY-----
```

3.3.4 Résoudre les problèmes

L'authentification d'un administrateur de SDMC échoue et un code d'erreur s'affiche. Demandez à l'administrateur de vous fournir le code. Les erreurs peuvent être les suivantes :

4001	Le well-known n'est pas disponible.
4002	Le fournisseur d'identité n'envoie pas les bonnes informations. Vérifiez sa configuration.
4003	L'URL du certificat n'est pas accessible. Erreur interne. Transmettez le code d'erreur à Stormshield.
4004	Le well-known n'est pas configuré correctement. Vérifiez sa configuration.
4006	Erreur interne. Veuillez contacter Stormshield et transmettre le code d'erreur.

3.4 Changer de mode de connexion

Si vous souhaitez changer de mode de connexion (SAML ou Mot de passe), nous vous invitons à contacter Stormshield. Stormshield fera la modification.

4. Gérer la licence

La console d'administration SDMC est fournie par défaut avec une licence d'évaluation permettant de l'utiliser pendant 30 jours après le premier démarrage.

Au-delà de 30 jours, vous devez récupérer votre licence sur votre espace client MyStormshield et l'importer dans SDMC.

4.1 Récupérer la licence SDS Enterprise

1. Munissez-vous de votre bon de livraison Stormshield (delivery document au format PDF) et connectez-vous sur votre espace client MyStormshield.
2. Dans le menu de gauche, choisissez **SDS – General > Enregistrer un logiciel SDS**, et lisez puis acceptez les conditions d'utilisation.
3. Entrez les informations suivantes :
   - **Société cible** : Nom de la société sous lequel vous êtes enregistré chez Stormshield.
   - **Clé de licence** : Suite de caractères qui se trouve dans la colonne Numéro de série du bon de livraison (par exemple F0BBABBJ-At07vu9Y).
   - **Revendeur** : Nom de votre revendeur SDS Enterprise.
4. Cliquez sur **Enregistrer**.
5. Dans la zone **Liste des produits** sur le tableau de bord de votre espace client, cliquez sur votre numéro de série.
6. Cliquez sur **Télécharger toutes les licences** et décompressez le fichier zip reçu.

4.2 Importer la licence dans SDMC

1. Dans SDMC, sélectionnez le menu de gauche **Licence**.
2. Cliquez sur le bouton **Importer** et choisissez le fichier que vous venez de décompresser (par exemple *F0BBABBJ-At07vu9Y.licence*).

La console SDMC refuse l'import d'une licence si elle a expiré.

4.3 Consulter les informations de licence

Les informations suivantes sont disponibles dans le menu **Licence** :

- La clé de licence à utiliser pour les agents sur les postes de travail,
- Les dates de validité de la licence.

5. Gérer les administrateurs dans SDMC

Si vous avez opté pour le mode de connexion Mot de passe lors de la création du compte d'entreprise, lors de la première connexion à SDMC, vous avez créé un compte administrateur. Cet administrateur est autorisé à effectuer toutes les opérations de configuration sur la console. Il peut également inviter d'autres administrateurs à accomplir ces opérations.

Si vous avez opté pour le mode de connexion SAML, la liste des administrateurs se remplit automatiquement à chaque connexion d'un nouvel administrateur. Aucune action manuelle n'est possible.

5.1 Inviter un nouvel administrateur

Le premier administrateur créé est autorisé à partager les tâches d'administration avec d'autres personnes. Il leur envoie une invitation afin qu'elles créent leur compte d'administration. Ces administrateurs invités n'ont par défaut que les droits de création et modification de politiques de sécurité. Pour plus d'informations, reportez-vous à la section Modifier les droits d'un administrateur.

1. Sélectionnez le menu de gauche **Administrateurs**.
2. Cliquez sur **Inviter**.
3. Dans le champ **E-mail**, saisissez l'adresse e-mail de la personne que vous souhaitez inviter. L'adresse doit appartenir au même domaine que le compte d'entreprise.
4. Cliquez sur **Inviter**. Le nouvel administrateur reçoit un e-mail lui suggérant de créer son compte d'administration via un lien. Ce lien est valable 72 heures.
5. Sélectionnez le menu de gauche **Administrateurs**. L'administrateur que vous venez d'inviter s'affiche désormais dans la liste. Seule son adresse e-mail est renseignée car il reste en attente jusqu'à ce qu'il crée son compte d'administration.

5.2 Accepter une invitation à administrer

Après réception d'un e-mail vous invitant à administrer SDS Enterprise, vous avez 72 heures pour créer votre compte d'administration.

1. Ouvrez l'e-mail reçu de la part de SDS Enterprise.
2. Cliquez sur le bouton **Créer mon compte**.
3. Remplissez le formulaire avec les informations de votre compte, puis cliquez sur **Enregistrer**.
4. Vous pouvez maintenant vous connecter à la console SDMC afin d'administrer SDS Enterprise selon vos droits. Pour plus d'informations sur les droits, reportez-vous à la section Modifier les droits d'un administrateur.

Si le délai des 72 heures est dépassé ou si l'administrateur ne souhaite plus vous inviter, un message d'erreur s'affiche lorsque vous tentez d'accéder au formulaire. Veuillez contacter l'administrateur pour plus d'informations.

5.3 Gérer la liste des administrateurs

- Sélectionnez le menu de gauche **Administrateurs**. La liste des administrateurs s'affiche. Le statut de l'administrateur est affiché dans la colonne **Création** :
  - **Validation en cours** : L'administrateur a reçu l'invitation mais n'a pas encore créé son compte. Vous pouvez lui renvoyer l'e-mail en cliquant sur la ligne de l'administrateur puis sur **Renvoyer l'invitation**.
  - **Invitation expirée** : L'administrateur n'a pas créé son compte dans les 72 heures et l'invitation a expiré. Vous pouvez lui renvoyer l'e-mail en cliquant sur la ligne de l'administrateur puis sur **Renvoyer l'invitation**.
  - **Date** : L'administrateur a créé son compte et peut se connecter à SDMC.

5.4 Modifier les droits d'un administrateur

Pour modifier les droits d'un administrateur, vous devez disposer du droit **Administrateur global**.

1. Sélectionnez le menu de gauche **Administrateurs**. La liste des administrateurs s'affiche.
2. Cliquez sur l'administrateur dont vous souhaitez modifier les droits. La page des propriétés de l'administrateur s'affiche.
3. Dans l'onglet **Droits**, activez ou désactivez ces différents droits selon vos besoins :
   - **Administrateur global** permet d'inviter d'autres administrateurs, de supprimer un administrateur ou de modifier ses droits.
     Un administrateur ne peut pas modifier ce droit pour lui-même.
   - **Gérer les clés API** permet de générer des clés d'accès à l'API de SDMC afin de les fournir à des applications tierces. Il permet aussi de visualiser la liste des clés, et de les supprimer.

5.5 Supprimer un administrateur

Vous pouvez supprimer un administrateur si vous ne souhaitez plus l'autoriser à administrer SDS Enterprise. L'administrateur connecté ne peut pas se supprimer lui-même.

1. Sélectionnez le menu de gauche **Administrateurs**.
2. Dans la liste des administrateurs, cliquez sur l'icône  sur la ligne de l'administrateur à supprimer.
3. Cliquez sur **Supprimer définitivement**, puis confirmez la suppression.

6. Gérer les certificats des autorités de certification et les certificats de recouvrement dans SDMC

L'utilisation de SDS Enterprise requiert l'usage de clés pour le chiffrement et la signature. Les clés doivent être certifiées par des autorités de certification de confiance.

Prérequis
Vous devez posséder une infrastructure pour la génération des clés de chiffrement et de signature des utilisateurs de l'entreprise. Vous pouvez ensuite les diffuser auprès des utilisateurs avec le moyen de votre choix, par exemple via des cartes à puce.
Si vous souhaitez utiliser la solution d'infrastructure à clé publique de Microsoft, consultez la section Mettre en place la solution d'infrastructure à clé publique (PKI) de Microsoft.

SDMC permet de déclarer les autorités de certification qui ont émis les certificats contenant l'identité et les clés publiques de vos utilisateurs. Elles sont alors considérées comme étant de confiance.

Pour cela vous devez importer les certificats de toutes les autorités dans la bibliothèque de certificats, puis les utiliser dans vos politiques de sécurité.

SDMC permet également d'importer des certificats de recouvrement, nécessaires en cas de perte d'une clé de chiffrement d'un utilisateur. Pour plus d'informations, reportez-vous à la section Permettre le recouvrement de données.

Les certificats sont diffusés aux utilisateurs par le biais d'annuaires LDAP et ajoutés automatiquement dans leur annuaire de confiance. Pour plus d'informations, reportez-vous à la section Gérer les annuaires LDAP dans SDMC.

6.1 Comprendre l'utilisation des clés et certificats des utilisateurs

Les formats de certificats supportés sont les suivants :

- *.cer*
- *.cert*
- *.crt*
- *.der*
- *.pem*

Dans le cas où plusieurs certificats sont disponibles pour un utilisateur (que ce soit dans l'annuaire de confiance ou sur un annuaire LDAP), SDS Enterprise sélectionne automatiquement le certificat valide ayant la date de début de validité la plus récente.

En cas de changement d'adresse e-mail d'un utilisateur (mariage, prestataire qui devient salarié de l'entreprise), il est impératif de renouveler son certificat (avec publication sur l'annuaire LDAP le cas échéant) afin que l'adresse e-mail de l'utilisateur soit identique à celle indiquée sur son/ses certificat(s). Si ce n'est pas le cas, les autres utilisateurs ne pourront plus envoyer de message sécurisé ou chiffrer de fichier ou de dossier pour la personne dont l'adresse a changé.

Enfin, les clés générées par votre infrastructure doivent respecter les attributs PKCS#11 suivants :

- Clé privée :
  - CKA_DECRYPT
  - CKA_SIGN
  - CKA_SIGN_RECOVER
  - CKA_UNWRAP
- Clé publique :
  - CKA_ENCRYPT
  - CKA_VERIFY
  - CKA_VERIFY_RECOVER
  - CKA_WRAP

6.2 Importer un certificat dans SDMC

1. Sélectionnez le menu de gauche **Bibliothèque de certificats**.
2. Cliquez sur **Importer** en haut à droite.
3. Sélectionnez le fichier et le type de certificat puis importez.

La liste des certificats affiche leur nom et leur type, les politiques de sécurité dans lesquelles ils sont utilisés et leur date d'expiration.

Après avoir importé les certificats des autorités de certification que vous considérez de confiance et les certificats de recouvrement, vous pouvez les utiliser dans vos politiques de sécurité. Reportez-vous à la section Créer une politique.

6.3 Renommer, supprimer ou télécharger un certificat

- Dans le menu de gauche **Bibliothèque de certificats**, cliquez sur l'icône  d'un certificat pour choisir l'une des trois actions.

7. Gérer les annuaires LDAP dans SDMC

La bibliothèque LDAP de SDMC permet de déclarer les annuaires LDAP de votre entreprise qui contiennent les certificats de vos utilisateurs.

Les certificats au format X509 contiennent notamment des données concernant la clé publique et son détenteur. La clé publique est utilisée pour le chiffrement de données confidentielles, qui peuvent alors être transmises en toute confidentialité.

Les annuaires LDAP permettent de compléter l'annuaire de confiance SDS Enterprise des utilisateurs. Pour plus d'informations sur l'annuaire de confiance, reportez-vous à la section Gérer l'annuaire de confiance depuis l'agent SDS Enterprise.

Vous allez ensuite indiquer les annuaires LDAP à utiliser dans vos politiques de sécurité, permettant ainsi les opérations de chiffrement et de signature sur les postes des utilisateurs. Pour plus d'informations sur comment utiliser les annuaires dans vos politiques, reportez-vous à la section Configurer les annuaires d'entreprise.

7.1 Ajouter un annuaire LDAP

1. Sélectionnez le menu de gauche **Bibliothèque LDAP**.
2. Cliquez sur **Ajouter** en haut à droite.
3. Remplissez tous les champs.
   Le port standard est 389 pour les connexions LDAP et 636 pour les connexions sécurisées LDAPS.
   Nous vous recommandons d'indiquer un compte avec un accès en lecture seule sur l'annuaire car les identifiants sont stockés en clair dans les politiques de sécurité.
4. Cliquez sur **Ajouter**.

La liste des annuaires affiche leur nom, les politiques de sécurité dans lesquelles ils sont utilisés et la date de la dernière modification.

Après avoir ajouté les annuaires LDAP, vous pouvez les utiliser dans vos politiques de sécurité. Reportez-vous à la section Configurer les annuaires d'entreprise.

7.2 Modifier, dupliquer ou supprimer un annuaire LDAP

- Dans le menu de gauche **Bibliothèque LDAP**, cliquez sur l'icône  d'un annuaire pour choisir l'une des trois actions.

8. Gérer les politiques de sécurité dans SDMC

SDMC permet de créer et configurer des politiques de sécurité que vous déployez ensuite sur les postes de travail des utilisateurs.

> **NOTE**
> Les packages d'installation des agents sont fournis avec une politique de sécurité par défaut, qui s'applique si vous ne déployez pas de politique personnalisée.

Dans les politiques, vous définissez les éléments suivants :

- Les paramètres de chiffrement et signature et la gestion des comptes utilisateur, incluant la création de comptes et les paramètres de connexion, ainsi que la gestion du recouvrement des données,
- Le paramétrage des fonctionnalités,
- Le paramétrage des annuaires,
- Le paramétrage de la révocation de certificats,
- Les points de distribution pour la mise à jour des politiques.

Vous avez également la possibilité de configurer une politique directement dans un fichier *.JSON*. Pour plus d'informations, reportez-vous au *Guide de configuration avancée* de SDS Enterprise.

Après avoir configuré une politique de sécurité, vous pouvez la télécharger pour l'intégrer dans votre package d'installation de l'agent.

8.1 Créer une politique

Vous pouvez soit créer une nouvelle politique, soit dupliquer une politique existante.

8.1.1 Créer une nouvelle politique

1. Sélectionnez le menu de gauche **Politiques**.
2. Cliquez sur **Créer** en haut à droite.
3. Donnez un nom à la politique.
4. Sélectionnez un modèle de politique.
5. Cliquez sur **Créer** pour terminer. La nouvelle politique s'affiche dans la liste des politiques.
6. Cliquez sur la ligne de la politique pour la configurer. Reportez-vous aux sections suivantes pour connaître le détail des paramètres.

8.1.2 Créer une politique à partir d'une politique existante

1. Dans la liste des politiques, cliquez sur l'icône  de la politique à dupliquer.
2. Sélectionnez le menu **Dupliquer**.
3. Donnez un nom à la politique.
4. Cliquez sur **Dupliquer**. La politique dupliquée s'affiche dans la liste.
5. Cliquez sur la ligne de la politique pour la configurer. Reportez-vous aux sections suivantes pour connaître le détail des paramètres.

8.2 Importer une politique

Vous pouvez importer une politique de sécurité existante au format *.json* dans SDMC.

La politique doit avoir été précédemment téléchargée depuis SDMC. Cette procédure permet par exemple de conserver les politiques existantes en cas de suppression et de recréation d'un compte d'entreprise.

Pour importer une politique :

1. Sélectionnez le menu de gauche **Politiques**.
2. Cliquez sur **Importer** en haut à droite.
3. Sélectionnez un fichier de politique au format *JSON*.
4. Modifiez le nom par défaut de la politique si besoin puis importez.

Les annuaires LDAP et les certificats des autorités de certification indiqués dans la politique ne sont toutefois pas importés. Vous devez les sélectionner de nouveau dans les menus **Annuaires** et **Autorités** de la politique.

8.3 Configurer les comptes utilisateur

Vous avez le choix entre trois types de comptes utilisateur : Mot de passe, Carte à puce ou mode Single Sign-on (SSO).

Avec les comptes Mot de passe et Carte à puce, les utilisateurs de l'entreprise doivent se connecter à leur compte SDS Enterprise.

En mode Single Sign-on, la connexion de l'utilisateur à SDS Enterprise est transparente et se fait automatiquement lorsqu'il se connecte à sa session Windows.

Le menu **Comptes** de la politique de sécurité permet de choisir les paramètres génériques des comptes utilisateur, les paramètres pour la création des comptes, les paramètres pour le recouvrement des données chiffrées, ainsi que les paramètres d'affichage des clés dans le menu **Porte-clés** de l'agent.

Pour plus d'informations sur la création des comptes utilisateur, reportez-vous aux sections Créer et gérer les comptes SDS Enterprise sur les postes des utilisateurs et Créer un compte Single Sign-On (SSO).

8.3.1 Définir les paramètres génériques des comptes

Dans le menu **Politiques** > **Comptes** > **Paramètres**, définissez les paramètres génériques des comptes utilisateur :

Type de compte	Sélectionnez un type de compte SDS Enterprise pour les utilisateurs : Carte à puce, Mot de passe, Mot de passe et carte à puce, ou Single Sign-on (SSO). Pour plus d'informations sur l'utilisation du mode SSO, reportez-vous à la section Créer un compte Single Sign-On (SSO).
Chiffrement et signature	
Algorithme de chiffrement	Algorithme utilisé pour chiffrer les données. SDS Enterprise propose l'algorithme AES uniquement.
Algorithme de signature	Algorithme utilisé pour signer les données. Choisissez SHA-256 ou SHA-512.
Comptes Carte ou token USB	

Middleware	Le middleware permet à SDS Enterprise de communiquer avec tous types de carte à puce ou token USB. Sélectionnez le middleware à utiliser sur les postes des utilisateurs parmi la liste des middleware supportés par SDS Enterprise. Vous ne pouvez sélectionner qu'un middleware par politique. Le middleware Stormshield Data Security est sélectionné et installé par défaut. Dans le fichier de configuration *.json* de la politique de sécurité, vous pouvez spécifier manuellement plusieurs middleware à utiliser (paramètre cardMiddlewares). Pour plus d'informations, reportez-vous au *Guide de configuration avancée SDS Enterprise*. Le middleware doit être installé au préalable sur les postes des utilisateurs. Pour plus d'informations, reportez-vous à la section Configurer les middleware nécessaires aux comptes Carte ou token USB.

8.3.2 Définir les paramètres de création de comptes

Dans le menu **Politiques** > **Comptes** > **Création**, définissez les paramètres de création des comptes utilisateur. Les comptes utilisateur sont ensuite créés manuellement ou automatiquement depuis les agents SDS Enterprise. Pour plus d'informations sur la création de comptes, reportez-vous à la section Créer et gérer les comptes SDS Enterprise sur les postes des utilisateurs.

Paramètres généraux	Autorisez ou interdisez la création de comptes Carte ou token USB ou Mot de passe sur l'agent SDS Enterprise. La création de comptes Carte ou token USB peut être manuelle ou automatique. La création de compte Mot de passe est uniquement manuelle. Ces paramètres ne sont pas disponibles si vous avez choisi le type de compte SSO.
Gestion des clés	Définissez s'il s'agit de comptes avec une seule clé (chiffrement ou signature) ou un compte avec deux clés (clé de chiffrement et clé de signature). Dans le cas de la création automatique de comptes sur l'agent, sélectionnez l'autorité ou les autorités de certification dont sont issues les clés à utiliser pour créer le compte. Les autorités présentes dans la liste sont celles ayant été préalablement déclarées dans la bibliothèque de certificats. Pour plus d'informations, reportez-vous à la section Gérer les certificats des autorités de certification et les certificats de recouvrement dans SDMC.
Création de compte Mot de passe	
Force du mot de passe	Sélectionnez les critères à respecter pour définir la force du mot de passe dans le cas d'un compte Mot de passe. Ces paramètres ne sont pas disponibles si vous avez choisi le type de compte SSO.
Création manuelle de comptes mot de passe	Dans le cas de la création manuelle de comptes Mot de passe sur l'agent : Sélectionnez la provenance des clés des utilisateurs, utilisées pour le chiffrement et/ou la signature : vous pouvez autoriser l'import de clés et de leurs certificats associés sous forme de fichiers .p12, ou bien la génération locale de clés RSA au moment de la création du compte. Vous pouvez également autoriser les deux méthodes à la fois. Si vous sélectionnez **Générer localement les clés**, SDS Enterprise génère des certificats auto-certifiés. Vous devez ensuite : • Choisir la taille des clés RSA qui seront générées par SDS Enterprise à la création du compte. • Définir la durée de validité des certificats pour les clés publiques en nombre d'années **Lors d'une création de compte** ou **Lors d'un renouvellement de clé**.

8.3.3 Paramétrer la connexion de l'utilisateur

Dans le menu **Politiques** > **Comptes** > **Connexion**, définissez le comportement de la session SDS Enterprise dans les situations suivantes :

- lorsque l'utilisateur retire sa carte à puce ou son token USB, dans le cas des comptes Carte ou token USB,
- lorsque l'économiseur d'écran Windows se déclenche en cas d'inactivité,
- lorsque l'utilisateur verrouille sa session Windows.

Pour plus d'informations sur le verrouillage et la déconnexion des comptes, reportez-vous à la section *Verrouiller le compte SDS Enterprise ou se déconnecter* du *Guide d'utilisation avancée*.

À l'activation de l'économiseur d'écran	Lorsque l'économiseur d'écran Windows s'active sur le poste de l'utilisateur, par défaut la session SDS Enterprise est verrouillée. Vous pouvez également choisir de déconnecter l'utilisateur ou bien de conserver la session SDS Enterprise active. Cette dernière option n'est pas recommandée pour des raisons de sécurité. L'usage des options **Verrouiller la session SDS Enterprise** ou **Déconnecter l'utilisateur** peut avoir des effets indésirables si vous utilisez la fonctionnalité Stormshield Data Virtual Disk avec des données en cours d'utilisation au moment de l'activation de l'économiseur d'écran ou du verrouillage.
Au verrouillage de la session Windows	Lorsque l'utilisateur verrouille sa session Windows, par défaut il est déconnecté de sa session SDS Enterprise. Vous pouvez également choisir de verrouiller la session SDS Enterprise ou bien de conserver la session active.
Au retrait de la carte ou du token USB	Lorsque l'utilisateur retire sa carte à puce ou son token USB, par défaut il est déconnecté de sa session SDS Enterprise. Vous pouvez également choisir de verrouiller la session SDS Enterprise.

8.3.4 Permettre le recouvrement de données

Un compte de recouvrement permet de sécuriser l'utilisation de SDS Enterprise. Si un utilisateur quitte par exemple son entreprise sans déchiffrer la totalité de ses données, le compte de recouvrement permet de retrouver toutes les données.

Le ou les comptes de recouvrement sont créés par les administrateurs de l'infrastructure à clé publique (PKI) utilisée par l'entreprise.

Si vous utilisez la solution d'infrastructure à clé publique de Microsoft, pour savoir comment obtenir le certificat d'un compte de recouvrement, reportez-vous à la section Créer un compte de recouvrement.

SDMC permet de lister les certificats (clés publiques) de comptes de recouvrement. Cette liste est propre à chaque politique de sécurité.

Les certificats de recouvrement sont diffusés sur les postes des utilisateurs via la politique de sécurité et ainsi, tout ce que les utilisateurs chiffrent est également chiffré avec le certificat de recouvrement. Vous pourrez alors déchiffrer toutes les données au moyen de la clé privée du compte de recouvrement.

IMPORTANT
Un compte de recouvrement doit être muni d'un mot de passe suffisamment robuste et être conservé en lieu sûr.

Les certificats de recouvrement doivent avoir été préalablement ajoutés dans le menu Bibliothèque de certificats.

Dans le menu **Politiques** > **Comptes** > **Recouvrement de données**, indiquez les certificats de recouvrement que vous souhaitez utiliser pour cette politique :

1. Cliquez sur **Ajouter depuis la bibliothèque**.
2. Sélectionnez un ou plusieurs certificats.
3. Cliquez sur **Ajouter**.

Du côté de l'agent SDS Enterprise, les certificats de recouvrement peuvent être consultés dans le porte-clés de l'utilisateur. Pour plus d'informations, reportez-vous à la section Déchiffrer les données d'un utilisateur avec une clé de recouvrement.

8.3.5 Gérer le porte-clés des utilisateurs

Dans le menu **Politiques** > **Comptes** > **Porte-clés**, paramétrez l'affichage des onglets permettant de gérer les clés de chiffrement, de signature, de déchiffrement et de recouvrement dans le porte-clés des utilisateurs. Ces onglets permettent de réaliser différentes actions sur les clés : les renouveler, les exporter ou importer, etc. Pour plus d'informations, reportez-vous à la section Créer et gérer les comptes SDS Enterprise sur les postes des utilisateurs.

Pour afficher le porte-clés de l'utilisateur sur le poste de travail, rendez-vous dans les propriétés de l'agent SDS Enterprise :

1. Faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Configuration**.
4. Double-cliquez sur l'icône **Porte-clés**.

8.4 Configurer les fonctionnalités

Le menu **Fonctionnalités** de la politique de sécurité permet de configurer les grandes fonctionnalités de SDS Enterprise. La licence détermine les fonctionnalités disponibles pour les agents.

8.4.1 Configurer Stormshield Data File

Stormshield Data File permet de garantir la confidentialité des données que vos utilisateurs manipulent tous les jours grâce au chiffrement de fichiers. Il permet également d'automatiser des tâches de chiffrement et déchiffrement sur des événements définis par l'utilisateur.

Pour plus d'informations, reportez-vous à la section *Sécuriser des fichiers* du *Guide d'utilisation avancée SDS Enterprise*.

Configurer le chiffrement de fichiers

- Rendez-vous dans le menu **Politiques** > **Fonctionnalités** > **File**, et activez les paramètres de votre choix.

Propriétés	Le format de chiffrement par défaut est le format *.sdsx*. Ce format permet à l'utilisateur de modifier un document chiffré de façon transparente sans avoir à le déchiffrer puis à le rechiffrer ensuite, comme c'est le cas avec l'ancien format *.sbox*.

Conversion des fichiers .sbox au format .sdsx	Ces options fonctionnent avec le format de chiffrement *.sdsx*. Si vous souhaitez que les fichiers de vos utilisateurs à l'ancien format *.sbox* soient remplacés par des fichiers au format *.sdsx*, activez l'option **Forcer la conversion des fichiers .sbox au format .sdsx**. Lorsqu'un utilisateur ouvre un fichier chiffré portant l'extension *.sbox*, celui-ci est alors automatiquement converti au format *.sdsx* et l'utilisateur n'a pas besoin de le rechiffrer après ouverture. Le nouveau fichier est protégé pour les mêmes destinataires que le fichier d'origine. Vous pouvez indiquer un chemin pour déplacer les anciens fichiers *.sbox* après la conversion. Sinon, ils restent à leur emplacement original. La conversion ne fonctionne que sur un seul fichier *.sbox* à la fois. Si cette option est désactivée, deux menus contextuels permettent d'**Ouvrir** ou de **Retirer la protection** d'un fichier *.sbox*. Si l'option est activée, un seul menu permet d'**Ouvrir** le fichier. Si l'utilisateur sélectionne plusieurs fichiers dont au moins un fichier *.sbox*, seul le menu **Ouvrir** est visible.
Chiffrement et déchiffrement	Sélectionnez les éléments pour lesquels vous souhaitez autoriser le chiffrement et le déchiffrement.
Chiffrement multiple	• Si l'utilisateur a besoin de chiffrer fréquemment un nombre important de fichiers, décochez **Confirmer le chiffrement de chaque fichier**. • Vous pouvez décider de chiffrer ou pas les fichiers cachés.
Chiffrements spéciaux	• Lorsque vous autorisez le chiffrement de fichiers pour un destinataire, vous utilisez sa clé publique et le destinataire utilise sa clé privée pour déchiffrer. • Les fichiers auto-déchiffrables peuvent être partagés avec des destinataires ne disposant pas de Stormshield Data File ni de Security BOX SmartFILE. • Les fichiers SmartFILE peuvent être partagés avec des destinataires ne disposant que de Security BOX SmartFILE. Pour plus d'informations, reportez-vous à la section *Créer un fichier compatible Security BOX SmartFILE* du *Guide d'utilisation avancée SDS Enterprise*.
Chiffrement de fichiers en lecture seule	Vous avez le choix entre plusieurs options en cas de tentative de chiffrement de fichiers en lecture seule.
Chiffrement et déchiffrement manuels des listes	Consultez la section ci-dessous pour utiliser les listes.
Chiffrement Windows du répertoire temporaire de déchiffrement	Par défaut, le chiffrement Windows est activé sur le répertoire temporaire de déchiffrement des fichiers *.sdsx* (répertoire C:\Users\[user]\AppData\LocalLow\Stormshield\Stormshield Data Security\Decrypted). Vous pouvez le désactiver.

Pour des informations sur une utilisation avancée de la fonctionnalité File sur l'agent SDS Enterprise, reportez-vous à la section Stormshield Data File.

Utiliser les listes

Les listes de chiffrement et déchiffrement permettent l'automatisation du chiffrement et du déchiffrement des fichiers pour un fonctionnement plus simple et sans erreur. Il est également

possible de créer une liste de fichiers afin d'empêcher leur chiffrement.

Utiliser les listes de chiffrement et déchiffrement

Les fichiers inclus dans les listes de chiffrement et déchiffrement sont automatiquement chiffrés ou déchiffrés à des moments prédéfinis. Ainsi, vous pouvez décider de chiffrer automatiquement au verrouillage de la session, à la déconnexion de l'utilisateur de son compte SDS Enterprise ou à intervalles fixés (par exemple toutes les 15 minutes) en tâche de fond.

- Indiquez les chemins des fichiers ou dossiers à chiffrer ou déchiffrer. Vous pouvez importer ou exporter la liste au format *JSON*.

EXEMPLE DE FICHIER .JSON

```
{
"askForConfirmation":false,
"path":"C:\\Users\\john\\Documents\\Files","recursive":true
},
{
"askForConfirmation":false,
"path":"C:\\Users\\john\\Documents\\Images","recursive":false
}
```

Les listes de chiffrement et déchiffrement peuvent également être utilisées pour lancer le chiffrement ou déchiffrement groupé de tout ou partie de liste.

La récursivité du chiffrement ou déchiffrement des listes de fichiers permet de l'étendre aux sous-dossiers. Elle est appelée par l'option **Inclure les sous-dossiers** et peut prendre deux valeurs (oui/non). Elle s'applique de diverses façons :

- En tant que mode, elle s'applique à tous les items et peut être activée et répétée dans plusieurs écrans.
- En tant que propriété de dossier, elle définit si seulement le dossier indiqué sera chiffré ou déchiffré ou si ses sous-dossiers le seront aussi.
- En tant que propriété de fichier, elle définit si seulement le fichier indiqué sera chiffré ou déchiffré ou si les fichiers de même nom, mais situés dans d'autres dossiers, le seront aussi.
- En tant que propriété d'un ensemble de fichiers définie par une expression qui utilise des jokers (* et ?), elle définit si seulement l'ensemble de fichiers sera chiffré ou déchiffré ou si les fichiers de même nom, mais situés dans d'autres dossiers, le seront aussi.

Utiliser les listes d'exclusion

Pour des raisons de sécurité, il peut être important d'empêcher le chiffrement de certains fichiers pour éviter qu'ils ne soient chiffrés par erreur. Vous pouvez créer une liste d'exclusion, qui va contenir la liste des fichiers ne devant pas être chiffrés.

- Indiquez les chemins des fichiers ou dossiers à exclure du chiffrement. Vous pouvez importer ou exporter la liste au format *JSON*.

Les principes de récursivité expliqués à la section Utiliser les listes de chiffrement et déchiffrement s'appliquent aux listes d'exclusion.

Pour éviter le chiffrement du dossier système (C:\WINDOWS\ par défaut) et du dossier d'installation de Stormshield Data File (C:\Program Files\Arkoon\Security BOX\ par défaut), il est recommandé d'indiquer ces dossiers dans la liste d'exclusion.

De plus, veuillez prendre connaissance des règles suivantes :

1. Si un fichier ou dossier appartient aux deux listes (chiffrement et exclusion), celle des fichiers exclus est prioritaire sur la première.
2. Quand plusieurs règles d'exclusion s'appliquent à un fichier (par exemple l'une s'appliquant à c:\tmp et l'autre à c:\tmp\folder1), la plus restrictive s'applique : si l'une nécessite une confirmation et l'autre exclut immédiatement, le fichier sera exclu sans confirmation.
3. Les règles d'exclusion sont en vigueur entre la vérification de l'attribut “caché” des fichiers et celle de l'attribut “en lecture seule”. En d'autres termes, si les règles sont les suivantes :

a. les fichiers cachés ne doivent pas être chiffrés,

b. une demande de confirmation est nécessaire pour les fichiers en lecture seule.

Alors un fichier pour lequel ces deux règles s'appliquent ne sera pas chiffré sans une demande de confirmation.

8.4.2 Configurer Stormshield Data Team

INFORMATION
Stormshield ne proposera plus d’évolutions fonctionnelles de la fonctionnalité Stormshield Data Team à partir de janvier 2025. La fonctionnalité passera en mode maintenance à partir de cette date.

Stormshield Data Team permet de chiffrer automatiquement des fichiers là où ils se trouvent, en temps réel et de façon transparente. Le chiffrement est défini par des règles de sécurité sur des dossiers, partagés ou non, et ces règles mentionnent les collaborateurs autorisés à lire et modifier les fichiers stockés dans les dossiers.

Pour plus d'informations, reportez-vous à la section *Sécuriser automatiquement le contenu d'un dossier* du *Guide d'utilisation avancée SDS Enterprise*.

Pour configurer le chiffrement automatique de dossiers :

- Rendez-vous dans le menu **Politiques** > **Fonctionnalités** > **Team**, et activez les paramètres de votre choix.

Propriétés	Choisissez les actions possibles en cas de changements concernant les collaborateurs sélectionnés dans les règles de sécurité ou en cas de problème avec la liste de révocation des certificats des utilisateurs. La première option permet d'interdire l'accès aux fichiers à un collaborateur qui a été supprimé d'une règle. Les deux options suivantes permettent de maintenir l'accès aux fichiers aux collaborateurs concernés.
Affichage des collaborateurs	Lorsqu'un dossier est sécurisé par une règle : • soit tous les utilisateurs peuvent afficher la règle, qu'ils soient collaborateurs au sein de la règle ou non, • soit seuls les collaborateurs de la règle peuvent afficher la règle.

Permissions	Ces quatre options correspondent aux menus disponibles dans le menu contextuel SDS Enterprise lorsque l'utilisateur fait un clic droit sur un dossier. • Si l'option **Autoriser le chiffrement selon les règles définies** est activée, le menu contextuel **Sécuriser selon les règles définies** s'affiche pour l'utilisateur et permet de chiffrer un dossier en le partageant à d'autres utilisateurs. • Si l'option **Autoriser la sauvegarde et la restauration** est activée, les menus contextuels **Avancé > Sauvegarder** et **Avancé > Restaurer** s'affichent pour l'utilisateur. • Si l'option **Autoriser le chiffrement** est activée, le menu contextuel **Sécuriser le dossier** s'affiche pour l'utilisateur et permet de chiffrer un dossier sans le partager à d'autres utilisateurs. • Si l'option **Autoriser la suppression est activée**, le menu contextuel **Avancé** > **Supprimer** s'affiche pour l'utilisateur. Pour des informations détaillées sur ces menus, reportez-vous à la section *Sécuriser automatiquement le contenu d'un dossier* du *Guide d'utilisation avancée SDS Enterprise*.
Accès aux fichiers chiffrés	Définissez les règles d'accès aux fichiers chiffrés dans un dossier dans le cas où le certificat d'un utilisateur est révoqué ou présente un problème, ou dans le cas où la liste de révocation des certificats n'est plus accessible.
Indication des dates lorsque les fichiers sont chiffrés ou déchiffrés	Sélectionnez ces options si vous souhaitez que les dates de modification, de dernier accès et de création soient modifiées à chaque fois qu'un fichier est chiffré ou déchiffré.
Paramètres avancés	Les paramètres avancés permettent de modifier certains comportements par défaut de Stormshield Data Team : • par défaut, la fenêtre de compte-rendu se ferme après le chiffrement. • par défaut, la fenêtre de progression du chiffrement ne s'affiche pas. • par défaut, l'ouverture de fichiers chiffrés dans un dossier non sécurisé est autorisée. Attention, selon l'application utilisée, si vous ouvrez un fichier chiffré dans un dossier non sécurisé, un fichier temporaire en clair peut être créé dans ce dossier. Quand vous enregistrez et fermez le fichier, le fichier temporaire en clair remplace le fichier chiffré original. De plus, même si vous n'enregistrez pas le fichier, le fichier temporaire en clair qui a été supprimé reste sur votre ordinateur et peut être récupéré à l'aide d'outils spécialisés. • par défaut, un fichier ou dossier chiffré est déchiffré s'il est copié ou déplacé vers un dossier non sécurisé. Quelle que soit l'option sélectionnée ici, le menu contextuel de l'agent **Sauvegarder** permet toujours de copier un fichier chiffré ou un dossier sécurisé tout en gardant le chiffrement. Pour plus d'informations sur ce menu, reportez-vous à la section *Sauvegarder un fichier chiffré* du *Guide d'utilisation avancée SDS Enterprise*. Vous pouvez également spécifier une liste de dossiers sur lesquels un utilisateur ne pourra pas créer de règle de sécurité Team pour sécuriser automatiquement le dossier. Entrez des chemins de dossiers. Si vous entrez une valeur qui est déjà présente dans la liste, vous ne pourrez pas l'ajouter. La liste est récursive, elle inclut automatiquement les sous-dossiers.

Pour des informations sur une utilisation avancée de la fonctionnalité Team sur l'agent SDS Enterprise, reportez-vous à la section Stormshield Data Team.

8.4.3 Configurer Stormshield Data Disk

Stormshield Data Disk permet de créer des volumes virtuels chiffrés sur lesquels les utilisateurs peuvent stocker des données confidentielles de manière sécurisée. Le propriétaire du disque peut autoriser des collaborateurs à accéder à son disque chiffré.

Pour plus d'informations, reportez-vous à la section *Créer des volumes virtuels sécurisés* du *Guide d'utilisation avancée SDS Enterprise*.

Pour configurer la création de volumes virtuels chiffrés :

- Rendez-vous dans le menu **Politiques** > **Fonctionnalités** > **Disk**, et activez les paramètres de votre choix.

Monter les volumes en tant que disques non amovibles	Selon votre infrastructure, choisissez de monter les volumes en tant que disques virtuels ou amovibles.
Taille maximale autorisée	Spécifiez la taille maximale que peut occuper le volume en Mo. Vous devez saisir une taille supérieure à 1Mo.
Système de fichiers	Choisissez le type de système de fichiers : NTFS, FAT32 ou FAT.
Nom des volumes	Conservez le nom du volume par défaut qui s'affiche dans l'explorateur Windows des utilisateurs ou bien personnalisez le nom.
Actions rapides	Si vous autorisez la création rapide de volumes, la méthode employée permet de créer le volume Disk plus rapidement. Cependant cette méthode n'est pas recommandée pour la création d'un volume sur un partage réseau. Le formatage rapide de volumes réduit le temps de formatage mais n'efface pas complètement les données du disque, tout comme la fonctionnalité Windows de formatage rapide.

Création automatique de volumes	• Sélectionnez **Créer automatiquement un volume** si vous souhaitez qu'un volume soit créé à la première connexion de l'utilisateur à SDS Enterprise. Vous pouvez choisir d'afficher un rapport à la fin de la création. • Saisissez le chemin complet du fichier lié au volume virtuel et dans lequel seront stockées les données confidentielles de l'utilisateur. Il s'agit d'un fichier avec l'extension *.vbox*. Vous pouvez utiliser des variables d'environnement Windows dans le chemin du fichier (e.g., %PATH%), les valeurs CSIDL Windows, ainsi que les mots-clés SDS Enterprise suivants entre <> : <*UserId*> : Identifiant SDS Enterprise de l'utilisateur, <*RootPath1*> : Dossier principal des comptes utilisateurs, spécifié dans la politique, <*RootPath2*> : Dossier de secours des comptes utilisateurs, spécifié dans la politique. <*COMMON_APPDATA*> : Dossier contenant les données d'applications de tous les utilisateurs, C:\Program Data. <*COMMON_DOCUMENTS*> : Dossier contenant les fichiers communs à tous les utilisateurs, C:\Users\Public\Documents. <*DESKTOP*> : Dossier contenant les fichiers sur le bureau, C:\Users\username\Desktop. <*LOCAL_APPDATA*> : Dossier contenant les données des applications locales, C:\Users\username\AppData\Local. <*MYDOCUMENTS*> : Dossier contenant les documents de l'utilisateur, C:\Users\username\Documents. <*PROFILE*> : Dossier du profil de l'utilisateur, C:\Users\username. <*USERNAME*> : Nom d'utilisateur Windows. • Spécifiez la taille du volume créé automatiquement. Par défaut, elle équivaut à 10% de l'espace disponible sur le poste de travail de l'utilisateur. • Activez ou non le montage automatique du volume à la connexion de l'utilisateur à SDS Enterprise. • Choisissez la **Lettre du lecteur** associée au volume (par défaut la lettre Z:).

Pour des informations sur une utilisation avancée de la fonctionnalité Disk sur l'agent SDS Enterprise, reportez-vous à la section Stormshield Data Virtual Disk.

8.4.4 Configurer Stormshield Data Mail

Stormshield Data Mail permet de chiffrer et signer des messages électroniques afin de garantir leur confidentialité, leur intégrité et l'identité de l'émetteur. Stormshield Data Mail fonctionne grâce à une extension qui s'intègre dans le client de messagerie Outlook des utilisateurs.

Pour plus d'informations, reportez-vous à la section *Sécuriser des messages électroniques* du *Guide d'utilisation avancée SDS Enterprise*.

Connaître les concepts liés à la sécurisation des messages

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

Chaque correspondant possède un ou plusieurs couples 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** (certificat) 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.

Pour plus d'informations sur les couples de clés, reportez-vous à la section Définir les paramètres de création de comptes.

Niveau de sécurité

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.

Chiffrement

L'émetteur chiffre un message avec la clé publique du destinataire ; ce dernier utilise 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.

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

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.

NOTE
L'émetteur ne pourra signer un message que s'il possède une clé de signature dans son porte-clés. Un compte SDS Enterprise 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 (i.e. en clair). Stormshield Data Mail 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. Par exemple si les certificats et les listes de révocation ne sont pas disponibles.

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.

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

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.

Annuaires de confiance

Stormshield Data Mail 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 la mise à jour automatique à partir de l'annuaire LDAP. Pour plus d'informations, reportez-vous à la section Configurer les annuaires d'entreprise.

Configurer le chiffrement et la signature des messages électroniques

Pour configurer le chiffrement et la signature de messages :

- Rendez-vous dans le menu **Politiques** > **Fonctionnalités** > **Mail**, et activez les paramètres de votre choix.

Propriétés	Sélectionnez le type de signature opaque ou claire (détachée) pour l'émission et la réception des messages. Veuillez vous reporter à la section Signature électronique pour plus d'informations. Si vous choisissez d'activer la signature ou le chiffrement par défaut pour tous les messages, l'utilisateur pourra toujours les désactiver sur un message.
Chiffrement PGP	Si vous souhaitez autoriser le chiffrement et déchiffrement de messages au format PGP, vous devez spécifier un ou plusieurs serveurs WKD (Web Key Directories) à consulter. Reportez-vous à la ligne suivante du tableau.
Serveur WKD	Dans le menu **Annuaires** de la politique, vous pouvez indiquer les serveurs WKD à consulter pour le chiffrement au format PGP. Ces annuaires de clés publiques permettent à Stormshield Data Mail de récupérer les clés publiques PGP des destinataires de messages chiffrés. Pour plus d'informations, reportez-vous à la section Configurer les annuaires d'entreprise.
Mise à jour d'annuaire	**A l'envoi de messages chiffrés** : Pour mettre à jour l'annuaire de confiance à l'envoi de messages chiffrés, vous devez avoir déclaré un annuaire LDAP. Pour plus d'informations, reportez-vous à la section Configurer les annuaires d'entreprise. **A réception d'un message signé** : Un utilisateur peut transmettre son certificat de chiffrement (sa clé publique) à un collaborateur en lui envoyant un message signé. Vous pouvez autoriser ou non le destinataire à importer manuellement le certificat dans son annuaire de confiance pour le mettre à jour, et vous pouvez autoriser ou non la mise à jour automatique de l'annuaire. Si vous autorisez ces actions uniquement pour les autorités connues, cela signifie que le certificat de chiffrement de l'utilisateur sera importé seulement s'il est issu d'une autorité dont le certificat est déjà présent dans l'annuaire de confiance du destinataire.

Chiffrement et signature automatiques avec Microsoft Purview	Si votre société utilise le système d'étiquettes de confidentialité proposé par Microsoft Purview Information Protection, vous pouvez déclarer ces étiquettes dans votre politique SDS Enterprise et y associer une action automatique de l'agent (en anglais, sensitivity labels). Lorsque l'utilisateur appliquera une étiquette à un message, l'agent vérifiera sa présence dans la politique et déclenchera l'action de sécurisation correspondante : chiffrement seul du message, signature seule du message ou la combinaison des deux actions. Pour utiliser des étiquettes de confidentialité dans la politique, vous devez connaître leurs noms tels que définis par votre société dans la configuration de Microsoft Purview Information Protection. Pour chaque étiquette : 1. Indiquez le nom (correspondant au champ "Name" et non pas "Display name" de la configuration de l'étiquette dans le produit Microsoft Purview Information Protection). 2. Sélectionnez l'action ou les actions que l'agent doit déclencher automatiquement lorsque l'étiquette est utilisée sur un message. Le format de chiffrement PGP n'est pas supporté par cette fonctionnalité. **NOTE** La fonctionnalité des étiquettes de confidentialité fonctionne uniquement avec Office365. Pour plus d'informations, reportez-vous à la documentation de Microsoft.

Pour des informations sur une utilisation avancée de la fonctionnalité Mail sur l'agent SDS Enterprise, reportez-vous à la section Stormshield Data Mail.

8.4.5 Configurer Stormshield Data Sign

Stormshield Data Sign permet de signer électroniquement des documents et de garantir l'authenticité des signataires et l'intégrité du contenu d'un fichier.

Pour plus d'informations, reportez-vous à la section *Signer des documents* du *Guide d'utilisation avancée SDS Enterprise*.

Pour configurer la signature de documents :

- Rendez-vous dans le menu **Politiques** > **Fonctionnalités** > **Sign**, et activez les paramètres de votre choix.

Propriétés	Sélectionnez l'extension de fichier qui sera utilisée pour identifier le nouveau fichier après sa signature. Le nom du fichier source est conservé et seule l'extension diffère. Les extensions possibles sont Stormshield Data sign (**.p7f**) ou S/MIME (**.p7m**). Il est recommandé de sélectionner l'extension **.p7f** afin d'éviter tout conflit avec d'autres outils utilisant des fichiers de type .p7m. Lorsque vous choisissez l'extension .p7f : • Le pictogramme  est ajouté en bas à droite de l'icône d'origine du fichier, visible dans l'Explorateur Windows. • Le fichier ne peut pas être lu par une personne utilisant un autre outil de signature électronique. Utilisez le format .p7m pour expédier vers et faire valider par des correspondants qui n'utilisent pas Stormshield Data Sign, mais utilisent un autre logiciel conforme à la norme RFC 2630.

Types de signature	Choisissez les types de signatures que vous souhaitez autoriser. Pour plus d'informations, reportez-vous à la section Signer des documents du Guide d'utilisation avancée de SDS Enterprise.
Gestion du contenu actif	Autorisez ou non la signature de documents contenant des macros ou des champs dynamiques. En effet, le contenu ou la structure d'un tel document peut être modifié après signature, ce qui peut entraîner des problèmes d'intégrité.
Processus de signature	Imposez ou non à l'utilisateur de toujours afficher le document avant de le signer.
Détection de contenu actif dans les fichiers PDF	Informez ou non l'utilisateur de la présence de macros dans le contenu d'un document PDF.
Détection de contenu actif dans les fichiers Microsoft Word	Informez ou non l'utilisateur de la présence de macros et de champs dynamiques dans le contenu d'un document Microsoft Word.

8.4.6 Configurer Stormshield Data Shredder

Stormshield Data Shredder garantit un effacement irréversible des données que l'utilisateur souhaite supprimer. Il permet d'empêcher une tierce personne de récupérer à son insu une information que l'utilisateur pensait avoir supprimée.

Pour plus d'informations, reportez-vous à la section *Supprimer définitivement des fichiers* du *Guide d'utilisation avancée SDS Enterprise*.

Pour configurer la suppression définitive de documents :

- Rendez-vous dans le menu **Politiques** > **Fonctionnalités** > **Shredder**, et activez les paramètres de votre choix.

Broyage	Autorisez ou non le broyage de fichiers et/ou de dossiers.
Glisser-déplacer	Autorisez ou non l'utilisation du glisser-déposer de fichiers et dossiers sur l'icône Stormshield Data Shredder du bureau Windows.
Divers	• Autorisez ou non l'utilisateur à interrompre une opération de broyage. Si l'interruption est autorisée, l'utilisateur peut cliquer sur le bouton **Arrêter**. • Autorisez ou non l'utilisation de Stormshield Data Shredder pour vider la corbeille de manière sécurisée. Si l'option est activée, le menu contextuel **Vidage sécurisé de la corbeille** s'affiche sur l'icône du Shredder.
Demande de confirmation	Dans le cas où la demande de broyage concerne plusieurs fichiers, choisissez le type de confirmation que vous souhaitez : • **Confirmer une fois pour tous les fichiers** : La confirmation du broyage est globale. • **Confirmer pour chaque fichier** : La confirmation du broyage est unitaire. Lors de l'opération, l'utilisateur peut néanmoins décocher la case **Demandez une confirmation pour chaque élément** afin d'éviter les demandes de confirmation pour les fichiers suivants.
Accès à Stormshield Data Shredder dans Windows	Choisissez ou non d'ajouter un raccourci Stormshield Data Shredder sur le bureau Windows. Le raccourci permet d'effacer les fichiers par glisser-déposer sur l'icône du bureau.

Paramètres avancés	Vous avez le choix entre plusieurs options en cas de tentative de broyage de fichiers en lecture seule. Vous pouvez également personnaliser le mode d'effacement sécurisé des fichiers en choisissant le nombre d'octets permettant de remplacer le contenu des fichiers à effacer, en trois passes successives. Vous devez entrer des valeurs hexadécimales de deux caractères, séparées par des points-virgules. La valeur par défaut est de 00;FF;55. Elle correspond à la valeur 0,255,85 dans le fichier *.json* d'une politique de sécurité. Pour plus d'informations sur le fichier au format *.json*, reportez-vous à la section *Stormshield Data Shredder* du *Guide de configuration avancée*.

8.4.7 Configurer Stormshield Data Share

Stormshield Data Share permet aux utilisateurs de chiffrer automatiquement des documents stockés sur des espaces collaboratifs synchronisés avec les hébergeurs en ligne DropBox, OneDrive, OneDrive for Business, SharePoint et Oodrive. Cette fonctionnalité est dépendante de la fonctionnalité Stormshield Data File et ne peut pas fonctionner sans cette dernière.

Pour plus d'informations, reportez-vous à la section *Protéger des documents sur des espaces collaboratifs synchronisés* du *Guide d'utilisation avancée SDS Enterprise*.

Pour activer la protection automatique :

1. Dans le menu **Politiques** > **Fonctionnalités** > **Share**, sélectionnez le ou les types d'espaces synchronisés pour lesquels vous souhaitez activer la protection automatique.
2. Dans le menu **Avancé**, choisissez de protéger tout le contenu de l'espace collaboratif, ou une sélection de dossiers. Pour la deuxième option, sélectionnez **Protéger uniquement les dossiers ci-dessous**, et ajoutez le nom ou le chemin relatif d'un ou plusieurs dossiers (e.g *Data\Project* pour protéger uniquement le sous-dossier *Project*).
3. L'utilisateur peut également créer des règles de protection automatique sur des dossiers depuis son poste de travail. Dans ce cas, par défaut, il peut choisir de partager ou non la règle avec les autres utilisateurs ayant accès au dossier concerné. Dans la section **Gestion des règles de protection partagées**, vous pouvez forcer le partage des règles, au contraire l'interdire ou bien laisser le comportement par défaut. Sur le poste de l'utilisateur, la case **Partager la règle de protection** sera alors grisée dans les deux premiers cas (cochée ou non cochée selon l'option sélectionnée) dans la fenêtre de choix des correspondants, au moment de la création de la règle de protection. Pour plus d'informations sur la création et le partage des règles de protection, reportez-vous au *Guide d'utilisation avancée*, section *Protéger automatiquement des dossiers d'espaces collaboratifs synchronisés* .

Stormshield Data Team ne sécurise pas les dossiers des espaces collaboratifs. Il est donc recommandé de configurer la fonctionnalité Team afin que ses menus ne s'affichent pas lors du clic droit sur un dossier synchronisé.

Pour exclure les dossiers synchronisés du périmètre de Team :

- Configurez le paramètre `excludedFolders` dans le fichier *.json* de la politique de sécurité. Pour plus d'informations, reportez-vous à la section *Stormshield Data Team* du *Guide de configuration avancée*.

ASTUCE
Vous pouvez ajouter une clé de registre pour qu'une icône SDS Enterprise personnalisée remplace l'icône de dossier Windows par défaut et permette d'identifier facilement les dossiers d'espaces collaboratifs synchronisés protégés par une règle de protection automatique. Pour

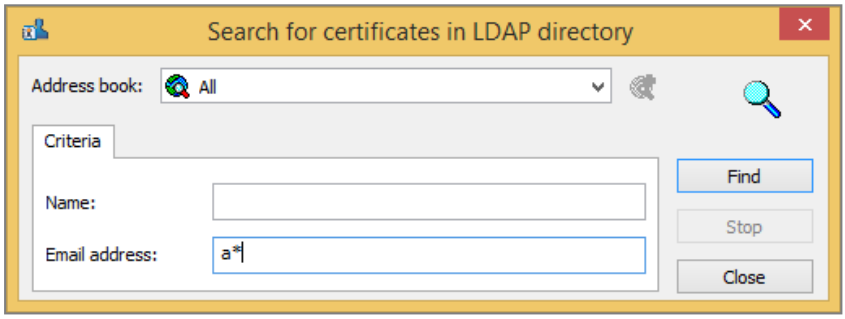
plus d'informations, reportez-vous à la section Configurer les paramètres avancés dans la base de registre du *Guide de configuration avancée*.

8.5 Configurer les annuaires d'entreprise

Dans une politique de sécurité, vous pouvez indiquer les annuaires LDAP à utiliser pour fournir les certificats des utilisateurs et paramétrer les critères de recherche de certificats dans l'annuaire.

Les annuaires doivent avoir été préalablement ajoutés dans le menu Bibliothèque LDAP.

Depuis son annuaire de confiance, l'utilisateur peut faire une recherche manuelle de certificats provenant des annuaires LDAP sélectionnés dans la politique :



La configuration de l'annuaire de confiance et des annuaires LDAP associés peut être consultée en lecture seule depuis l'agent SDS Enterprise.

Pour plus d'informations, reportez-vous à la section Gérer l'annuaire de confiance depuis l'agent SDS Enterprise.

SDMC permet également d'indiquer des adresses de serveurs WKD pour le chiffrement des messages au format PGP.

8.5.1 Ajouter des annuaires LDAP depuis la bibliothèque

Pour ajouter un annuaire LDAP :

1. Rendez-vous dans le menu **Politique** > **Annuaires** > **LDAP**.
2. Si vous souhaitez que la recherche de certificats dans l'annuaire soit automatiquement suffixée ou préfixée par le caractère "*", activez les deux premières options. Cela est transparent pour l'utilisateur.
3. Cliquez sur **Ajouter depuis la bibliothèque** dans la section **Annuaires LDAP/LDAPS**.
4. Sélectionnez un ou plusieurs annuaires.
5. Si besoin, réordonnez les annuaires avec un cliquer-glisser.

8.5.2 Paramétrer la mise à jour automatique de l'annuaire

A chaque fois que l'annuaire LDAP de l'entreprise est mis à jour, SDMC permet de mettre automatiquement à jour l'annuaire local de confiance pour refléter les modifications.

Les options de la section **Mise à jour de l'annuaire de confiance** dans le menu **Politique** > **Annuaires** > **LDAP** vous permettent de paramétrer finement cette mise à jour automatique.

Activation et exécution	• **Mettre à jour l'annuaire automatiquement** : si cette option est désactivée, les options des sections **Activation et exécution** et **Mise à jour des certificats à partir d'un annuaire LDAP** sont grisées. • **Fréquence de la mise à jour** : indiquez une valeur entre 0 et 24. • **Démarrer la mise à jour de l'annuaire lorsque l'utilisateur se connecte à son compte SDS** : activez cette option pour mettre à jour l'annuaire à chaque connexion de l'utilisateur, quelle que soit la fréquence de mise à jour définie au-dessus.
Mise à jour des certificats à partir d'un annuaire LDAP	Activez ces options pour mettre à jour les états des certificats dans l'annuaire local.
Suppression des certificats expirés/révoqués/retirés de l'annuaire LDAP	Si vous ne souhaitez pas supprimer de l'annuaire local tous les certificats expirés, révoqués ou retirés de l'annuaire LDAP, vous pouvez sélectionner les autorités de certification émettrices pour filtrer les certificats à supprimer.

8.5.3 Ajouter des serveurs WKD pour le chiffrement des messages au format PGP

Pour permettre aux utilisateurs d'envoyer et de recevoir des messages chiffrés au format PGP avec la fonctionnalité Stormshield Data Mail, vous devez :

- Activer le chiffrement/déchiffrement des messages en PGP dans le menu **Fonctionnalités** > Mail de la politique.
- Ajouter l'adresse d'un ou plusieurs serveurs WKD (Web Key Directories) à consulter dans le menu **Annuaires** > **PGP**. Ces annuaires de clés publiques permettent à Stormshield Data Mail de récupérer les clés publiques PGP des destinataires de messages chiffrés.

Pour ajouter des serveurs WKD :

- Dans l'onglet **PGP** du menu **Annuaires**, indiquez les adresses URL des serveurs WKD en respectant l'un des deux formats suivants et en les adaptant avec les noms de domaines ou sous-domaines des serveurs :
  - **https://openpgpkey.**sous-domaines-optionnels.domaine.toplevel**/.well-known/openpgpkey/<d>/hu/<k>?**parametres_get=optionnels
  - **https://**sous-domaines-optionnels.domaine.toplevel**/.well-known/openpgpkey/hu/<k>?**parametres_get=optionnels
    Les parties en gras des URL doivent être conservées telles quelles.

SDS Enterprise communique avec les serveurs WKD en HTTPS. Tous les ordinateurs hébergeant Stormshield Data Mail doivent donc disposer du certificat de l'autorité ayant émis le certificat SSL du serveur WKD.

8.6 Ajouter des autorités de certification et configurer le contrôle de révocation des certificats

SDMC permet d'ajouter les certificats de vos autorités de certification dans vos politiques de sécurité, afin que l'agent SDS Enterprise puisse contrôler la chaîne de parenté des certificats des utilisateurs.

Il permet également de mettre en place le contrôle de révocation qui constitue le seul moyen de signaler que le certificat d'un utilisateur ne doit plus être utilisé. Par exemple, si son titulaire ne fait plus partie d'un groupe, s'il suspecte que sa clé a été compromise ou s'il en a obtenu une autre.

Il s'opère au moyen de listes de révocation de certificats (CRL) ou au moyen du protocole OCSP dans le cas où une adresse URL d'un répondeur OCSP est indiquée dans le certificat.

Ces données sont gérées par l'administrateur de l'infrastructure à clés publiques (PKI) utilisée par l'entreprise.

SDMC permet de lister des points de distribution de CRL personnalisés pour chaque autorité de certification émettrice des certificats de vos utilisateurs. Cette liste est propre à chaque politique de sécurité.

Les agents SDS Enterprise téléchargent les CRL sur les points de distribution indiqués pour permettre le contrôle de la validité des certificats des utilisateurs.

8.6.1 Comprendre le contrôle de révocation

Le contrôle d'un certificat porte sur trois aspects :

- contrôle des données propres du certificat : format, dates de validité, signature, extension…
- contrôle de la chaîne de parenté. Il faut être capable d'établir une chaîne complète de certificats jusqu'à un certificat d'autorité de confiance. Chaque certificat de cette chaîne subit le même niveau de contrôle que le certificat à contrôler initialement. Lorsqu'un certificat d'une chaîne ne peut être validé, une autre chaîne est vérifiée (tant qu'une chaîne valide n'a pas été trouvée).
- contrôle de la révocation. Ce contrôle est effectué en vérifiant que le certificat soit bien absent de la CRL émise par son autorité de délivrance (ou par un tiers ayant délégation pour la produire). Les CRL étant elles-mêmes signées avec des certificats, le mécanisme de contrôle de certificats s'applique également aux certificats mis en œuvre au niveau des CRL.

8.6.2 Comprendre les listes de révocation

Le mécanisme de vérification d'une CRL est décrit dans les normes définissant les certificats et les CRL (norme X.509, RFC 3280 et RFC 5280).

Il existe deux façons pour les agents SDS Enterprise d'obtenir les CRL à télécharger en local pour vérifier les certificats :

- à partir du point de distribution de CRL défini dans les paramètres des certificats des autorités,
- à partir des points de distribution de CRL personnalisés indiqués pour chaque autorité, dans la politique de sécurité dans SDMC.

Vous pouvez limiter la validité des CRL à un nombre de jours paramétrable.

8.6.3 Ajouter des certificats d'autorité de certification

Lorsque vous ajoutez des certificats d'autorité de certification dans SDMC, ils sont consultables dans l'onglet **Autorité** de l'annuaire de confiance sur les postes des utilisateurs. Ils permettent à l'agent SDS Enterprise de garantir que les certificats des utilisateurs sont issus d'autorités de confiance et de vérifier la validité des certificats.

Pour ajouter un certificat :

1. Dans le menu **Politique** > **Autorités**, cliquez sur **Ajouter depuis la bibliothèque** à gauche du panneau.
2. Sélectionnez un ou plusieurs certificats parmi ceux qui ont été ajoutés préalablement dans le menu Bibliothèque de certificats.

Les certificats des autorités de certification contiennent dans leurs paramètres les points de distribution des listes de révocation de certificats (CRL). Si vous souhaitez indiquer des points de distribution de CRL personnalisés pour chaque autorité, consultez la section suivante.

8.6.4 Paramétrer le contrôle de révocation dans une politique

Pour personnaliser les points de distribution des CRL de chaque autorité de certification, rendez-vous dans le menu **Politique** > **Autorités**. Vous pouvez indiquer autant de points de distribution que nécessaire. Pour télécharger les CRL, l'agent SDS Enterprise consulte ces points de distribution en plus de celui indiqué dans le certificat de chaque autorité.

1. Indiquez une période de validité des CRL. Il s'agit de la durée à l'issue de laquelle l'agent SDS Enterprise télécharge de nouveau les CRL en local pour garantir d'avoir toujours les données à jour.
2. Sélectionnez une autorité de certification à gauche du panneau.
3. À droite du panneau, indiquez un ou plusieurs points de distribution de CRL pour chaque autorité sélectionnée. Le point de distribution peut être accessible par le biais des protocoles suivants :
   - http:// ou https://
   - LDAP:// ou LDAPS://
   - file:///
4. Si besoin, réordonnez les points de distribution avec un cliquer-glisser.

Depuis son compte SDS Enterprise, l'utilisateur peut consulter la liste des autorités de certification et des points de distribution des CRL. Pour plus d'informations, reportez-vous à la section Consulter les autorités de certification depuis l'agent SDS Enterprise.

8.7 Configurer les points de distribution de politiques

Dans le menu **Politiques** > **Diffusion**, indiquez un ou plusieurs points de distribution pour chaque politique de sécurité. Ceux-ci contiennent les fichiers de mise à jour des politiques.

Au démarrage du poste de travail, l'agent Stormshield Data Security Enterprise vérifie la liste des points de distribution dans l'ordre que vous avez déterminé. Il applique la première politique valide qu'il rencontre : elle doit être accessible, signée et plus récente que sa politique courante.

Pour configurer les points de distribution :

1. Dans le champ **Chemin complet du fichier de la politique**, saisissez le chemin complet du fichier de la politique *.jwt* de votre choix. Le chemin doit commencer par l'un des préfixes suivants :

Préfixe	Exemples
http://	http://mycompany.example.com/folder/policy.jwt
https://	https://mycompany.example.com/folder/policy.jwt
file:	file://myserver/sharing/folder/policy.jwt file:///c:/folder/policy.jwt

2. Cliquez sur le bouton + pour ajouter le chemin à la liste. Le bouton est désactivé si le chemin existe déjà ou si le préfixe est incorrect.
3. Répétez l'opération pour chaque point de distribution à déclarer.
4. Utilisez le glisser-déposer pour réordonner les points de distribution à votre convenance. Les agents SDS Enterprise analyseront les points de distribution dans l'ordre de la liste.

Une fois les points de distribution déclarés, vous devez mettre à disposition les fichiers de mise à jour de politiques, afin qu'ils soient déployés sur les agents SDS Enterprise. Pour plus d'informations, reportez-vous à la section Mettre à jour la politique de sécurité sur les agents SDS Enterprise.

9. Installer les agents SDS Enterprise sur les postes des utilisateurs et déployer les politiques de sécurité

Les agents SDS Enterprise permettent d'appliquer les politiques de sécurité définies dans SDMC et d'utiliser les fonctionnalités du produit sur les postes des utilisateurs.

Pour installer les agents SDS Enterprise sur les postes de travail, vous devez suivre les étapes suivantes :

1. Télécharger les politiques,
2. Signer les politiques avec l'utilitaire de signature fourni par Stormshield,
3. Télécharger le package d'installation des agents SDS Enterprise,
4. Déployer les agents SDS Enterprise sur les postes des utilisateurs,
5. Déployer le fichier de la politique de sécurité signée et le certificat correspondant sur les postes des utilisateurs.

9.1 Connaître les prérequis système pour l'agent SDS Enterprise

SDS Enterprise est une solution pour postes de travail sous Microsoft Windows 64 bits.

Pour connaître les versions de Microsoft Windows compatibles, reportez-vous au *Cycle de vie produits*.

Si vous choisissez le mode silencieux de déploiement du package d'installation de l'agent, l'installation préalable du package VSTO Runtime 4.0 Office 2010 est requise pour la fonctionnalité Stormshield Data Mail. Le package VSTO est disponible sur votre espace client MyStormshield (menu **Téléchargements** > **Stormshield Data Security** > **Enterprise** > **Tools**).

NOTE
L'installation de l'agent en étant authentifié sous Windows avec un compte utilisateur est impossible pour un utilisateur du domaine si l'UAC (User Account Control) est activée car l'élévation de privilège ne fonctionne pas.

IMPORTANT
L'agent SDS Enterprise n'est pas compatible avec la fonction **Changement Rapide d'Utilisateur**.

9.2 Télécharger et signer une politique de sécurité

Les packages d'installation des agents sont fournis avec une politique de sécurité par défaut. Vous pouvez ensuite ajouter votre propre politique de sécurité.

Avant de déployer une politique de sécurité personnalisée, vous devez la télécharger pour pouvoir la faire signer par un compte signataire, afin de garantir son authenticité et son intégrité.

Stormshield fournit un utilitaire de signature pour signer vos politiques.

La signature se base sur la norme JWT. L'algorithme utilisé par défaut est le RSASSA-PSS SHA256 (PS256), mais vous pouvez le paramétrer.

L'utilitaire de signature permet de signer plusieurs politiques à la fois si nécessaire.

En cas de changement de signataire de la politique, reportez-vous à la section Modifier le signataire d'une politique de sécurité.

9.2.1 Connaître les prérequis

Pour signer une politique de sécurité, vous avez besoin :

- D'un fichier au format *.p12* contenant une clé privée de signature. Nous vous recommandons de protéger le fichier par un mot de passe robuste. Pour savoir comment créer un compte signataire de politique de sécurité si vous utilisez la solution d'infrastructure à clé publique de Microsoft, reportez-vous à la section Créer un compte signataire des politiques de sécurité SDS Enterprise.
- De télécharger l'utilitaire de signature *SDSPolicySignCLI.exe* depuis le menu **Téléchargements** de SDMC.

9.2.2 Télécharger la politique de sécurité (format *.JSON*)

1. Sélectionnez le menu de gauche **Politiques**,
2. Dans la liste des politiques, cliquez sur l'icône  de la politique à télécharger.
3. Cliquez sur **Télécharger**.

9.2.3 Signer la politique

1. Exécutez l'outil *SDSPolicySignCLI.exe* en ligne de commande. Pour afficher la liste des paramètres, tapez `--help` :

`-k` ou `--key`	Paramètre obligatoire. Indique le chemin, relatif au répertoire courant ou absolu, du fichier *.p12* permettant la signature.
`-p` ou `--password`	Mot de passe protégeant le fichier *.p12*. Si le fichier est protégé par mot de passe et que vous n'entrez pas le paramètre manuellement, le mot de passe est automatiquement demandé (méthode recommandée).
`-f` ou `--file`	Paramètre obligatoire. Indique le chemin, relatif au répertoire courant ou absolu, du fichier *.json* de la politique à signer. Vous pouvez indiquer plusieurs fichiers en les séparant par des virgules ou par des espaces.
`-a` ou `--algo`	Indique l'algorithme à utiliser pour signer la politique. Les valeurs possibles sont `PS256` et `RS256`. Par défaut, si le paramètre n'est pas renseigné, l'algorithme `PS256` est utilisé. Choisissez l'algorithme RS256 pour signer une politique pour des agents dont la version est inférieure à 11.1.
`--help`	Affiche l'aide.
`--version`	Affiche la version de l'utilitaire.

2. Lors de la signature, un sous-dossier portant le nom de la politique est créé au même emplacement que le fichier de la politique. Il contient le fichier signé *policy.jwt*. Récupérez ce fichier pour l'intégrer au package d'installation des agents, comme indiqué dans la section suivante.

EXEMPLE

```
C:\Myfolder\SDSPolicySignCLI.exe --key C:\Keys\MyPrivateKey.p12 --file
C:\Policies\Policy1.json C:\Policies\Policy2.json --algo RS256
```

Remplacez les noms des dossiers et fichiers par vos propres noms. Dans cet exemple, les deux politiques sont signées respectivement dans les fichiers *C:\Policies\Policy1\policy.jwt* et *C:\Policies\Policy2\policy.jwt* en utilisant l'algorithme RS256.

9.3 Déployer le package d'installation des agents SDS Enterprise et une politique de sécurité personnalisée sur les postes des utilisateurs

Pour déployer le package d'installation des agents SDS Enterprise sur les postes des utilisateurs, vous pouvez choisir entre une installation interactive et une installation silencieuse. Vous pouvez également choisir les fonctionnalités à déployer.

Après le déploiement des agents, vous devrez déployer le fichier de la politique de sécurité personnalisée signée et le certificat signataire correspondant sur les postes des utilisateurs, dans les dossiers indiqués ci-dessous, afin que les agents SDS Enterprise appliquent votre politique de sécurité.

Le déploiement de l'agent SDS Enterprise nécessite d'être administrateur de la machine.

NOTE

Avant d'installer la fonctionnalité Stormshield Data Mail, veuillez vous assurer que votre parc utilise une version de Windows compatible avec SDS Enterprise. Pour plus d'informations sur les compatibilités, reportez-vous au *Cycle de vie produits*.

9.3.1 Télécharger le package d'installation des agents SDS Enterprise depuis SDMC

1. Sélectionnez le menu de gauche **Téléchargements**.
2. Dans la partie supérieure, sélectionnez le package *.msi* ou *.exe* dans la langue de votre choix :
   - *.exe* : Package autonome permettant d'installer la solution et ses prérequis en mode interactif. Le package contient une politique de sécurité par défaut, utilisée si vous ne déployez pas votre propre politique de sécurité.
   - *.msi* : Package permettant d'installer la solution en mode silencieux. Le package contient une politique de sécurité par défaut, utilisée si vous ne déployez pas votre propre politique de sécurité.
3. Téléchargez le package puis consultez la section suivante pour le déployer.

Les liens de cette page de téléchargement pointent vers l'espace client MyStormshield. Par défaut, ils téléchargent la dernière version disponible de l'agent. Si vous souhaitez télécharger une version précédente, vous devez vous rendre directement sur votre espace MyStormshield.

9.3.2 Déployer le package d'installation

Deux modes de déploiement du package sont disponibles :

- Le mode interactif : mode autonome utilisant le package *.exe*. Il suffit de cliquer sur le package *.exe* personnalisé pour lancer l'installation.
  Après avoir saisi la clé de licence, et avoir accepté le contrat de licence, la procédure d'installation propose l'installation de toutes les fonctionnalités du produit autorisées par la clé de licence.
- Le mode silencieux : il s'agit de l'installation sans interaction avec l'utilisateur. Ce mode utilise le package *.msi*. Veuillez consulter les prérequis avant l'installation. Il est ensuite possible d'installer le package *.msi* en tant qu'administrateur par les commandes traditionnelles de Windows Installer. Si l'installation n'est pas faite avec les droits d'administrateur, le produit ne s'installe pas (erreur 1925).

Pour déployer le package *.msi* en mode silencieux, vous pouvez utiliser l'outil d'édition de package Windows Installer *msiexec* ou bien l'outil Microsoft Endpoint Configuration Manager.

Pour utiliser l'outil *msiexec*, suivez la procédure suivante :

1. Ouvrez une fenêtre de ligne commande en tant qu'administrateur,
2. Entrez la commande suivante :
   ```
   msiexec /qn /i "<chemin>Stormshield Data Security 11.4.4"
   LICENCENUM=<numéro de licence>
   ```
   `<numéro de licence>` est composé de 16 caractères attachés.
3. La procédure installe alors toutes les fonctionnalités autorisées par la licence. Grâce à la propriété `REMOVE`, (reportez-vous à la section Choisir les fonctionnalités à installer ci-dessous), vous pouvez limiter les fonctionnalités installées.
   Une fois l'installation terminée, SDS Enterprise démarre automatiquement chaque fois que vous démarrez Windows.

Les variantes possibles de la commande sont :

- `/qn` : installation sans aucun écran,
- `/qn+` : installation avec un écran final de confirmation,
- `/qb` : installation avec un écran comportant une barre d'avancement et une durée estimée restante,
- `/qb+` : installation avec un écran comportant une barre d'avancement et une durée estimée restante, ainsi qu'un écran final de confirmation.

> **NOTE**
> Le commutateur `/norestart` n'est pas supporté. Pour empêcher le redémarrage de la machine, il faut créer un *.mst* avec les options ad hoc.

9.3.3 Déployer un fichier de politique de sécurité personnalisée signée et le certificat signataire correspondant

Après le déploiement de l'agent SDS Enterprise sur les postes des utilisateurs via le package *.exe* ou le package *.msi*, vous pouvez déployer les fichiers suivants sur les postes afin que les agents appliquent votre propre politique de sécurité :

- Le fichier de la politique signée *policy.jwt*,
- Le certificat (clé publique) permettant de vérifier la signature de la politique. Il doit se nommer *admin_policy.cer*.

Pour déployer ces fichiers dans les dossiers attendus :

1. Placez le fichier de la politique signée *policy.jwt* dans le sous-dossier *%programdata%\Stormshield\Stormshield Data Security* ou remplacez-le s'il existe déjà.
2. Placez le certificat *admin_policy.cer* dans le dossier *C:\Programmes\Arkoon\Security BOX*, ou remplacez-le s'il existe déjà.

9.3.4 Choisir les fonctionnalités à installer

Vous pouvez utiliser la propriété `REMOVE` pour limiter les fonctionnalités installées par l'utilisateur, même si la clé de licence en autorise d'autres.

L'application de cette propriété permet par exemple d'avoir différents profils d'installation tout en ayant une seule clé de licence et un seul package d'installation.

Voici la liste des valeurs possibles :

Code	Fonctionnalité supprimée
SBoxFile	Stormshield Data File
SBoxShare	Stormshield Data Share (la fonctionnalité Share est une sous-fonctionnalité de Stormshield Data File. Elle est donc automatiquement supprimée si Stormshield Data File est supprimé)
SBoxDisk	Stormshield Data Virtual Disk
SBoxShredder	Stormshield Data Shredder (la fonctionnalité Shredder requiert l'installation de Stormshield Data File pour fonctionner)
SBoxMailOutlookAddIn	Stormshield Data Mail
SBoxTeam	Stormshield Data Team
SBoxExtCarte	Stormshield Data Extension Carte
SBoxSign	Stormshield Data Sign
SBoxConnector	Stormshield Data Connector

Dans la définition de la valeur de la propriété `REMOVE`, les différentes fonctionnalités dont l'installation est interdite doivent être séparées par une virgule et il ne doit pas y avoir d'espace.

Par exemple, pour installer le package *.msi* en supprimant les fonctionnalités Stormshield Data File et Stormshield Data Virtual Disk :

1. Ouvrez une fenêtre de ligne de commande en tant qu'administrateur,
2. Entrez la commande suivante :

```
msiexec /i "<chemin>\ Stormshield Data Security 11.4.4"
LICENCENUM=<SBOXLICENCENUM> REMOVE=SBoxFile,SBoxDisk
```

9.4 Mettre à jour la politique de sécurité sur les agents SDS Enterprise

Après le déploiement initial d'une politique personnalisée sur les agents, vous pouvez la mettre à jour de façon automatique sur votre parc en la déposant sur un serveur qui fait office de point de distribution.

Vous devez au préalable déclarer des points de distribution dans les politiques. Pour plus d'informations, reportez-vous à la section Configurer les points de distribution de politiques.

1. Téléchargez le fichier *.json* de la politique que vous avez mise à jour. Pour plus d'informations, reportez-vous à la section Télécharger une politique de sécurité.
2. Signez le fichier. Pour plus d'informations, reportez-vous à la section Télécharger et signer une politique de sécurité.
3. Copiez le fichier sur les points de distribution que vous avez déclarés pour cette politique.

Au prochain démarrage de l'agent, celui-ci vérifiera si une nouvelle mise à jour est disponible, et si tel est le cas, il l'appliquera automatiquement.

Si aucun point de distribution n'est déclaré, la mise à jour manuelle de la politique est également possible en remplaçant le fichier de la politique localement.

9.5 Modifier le signataire d'une politique de sécurité

Les politiques de sécurité sont signées par un signataire de politique, avant d'être déployées sur les postes des utilisateurs avec le certificat du signataire. Ceci permet de garantir l'authenticité et l'intégrité d'une politique.

Pour en savoir plus, reportez-vous à la section Télécharger et signer une politique de sécurité.

Veuillez suivre la procédure suivante si vous souhaitez modifier le signataire d'une politique, par exemple en cas de compromission de la clé de signature du signataire ou en cas de départ de l'entreprise du signataire.

Les conditions suivantes sont requises :

- Vous devez avoir configuré un point de distribution de la politique de sécurité. Pour plus d'informations, reportez-vous à la section Configurer les points de distribution de politiques.
- Vous avez besoin d'un fichier *.p7b* qui contient le certificat de l'ancien signataire et le certificat du nouveau signataire. Pour plus d'informations, reportez-vous à la section ci-dessous Autoriser la signature d'une politique par plusieurs signataires.

Si vous utilisez la solution d'infrastructure à clé publique de Microsoft, pour savoir comment obtenir le certificat d'un compte signataire de politique de sécurité, reportez-vous à la section Créer un compte signataire des politiques de sécurité SDS Enterprise.

9.5.1 Autoriser la signature d'une politique par plusieurs signataires

Le temps de la transition entre deux signataires, vous devez installer sur les postes des utilisateurs un fichier *.p7b* qui contient le certificat de l'ancien signataire et le certificat du nouveau signataire. Vous devez réaliser cette opération avant de redéployer la politique signée par le nouveau signataire. Ainsi, l'agent SDS Enterprise considère les deux certificats comme étant des signataires valides de la politique.

1. Générez un fichier *admin_policy.p7b* contenant les deux certificats concernés. Vous pouvez par exemple utiliser la fonction d'export du Gestionnaire de certificats Windows.
2. Sur les postes des utilisateurs, installez le fichier *admin_policy.p7b* dans le dossier d'installation *C:\Programmes\Arkoon\Security BOX*.

Le fichier *.p7b* supplante l'éventuel certificat de signataire *.cer* déjà présent dans le même dossier.

9.5.2 Déployer la politique signée par le nouveau signataire

Après avoir installé le fichier *admin_policy.p7b* sur les postes des utilisateurs, suivez les étapes ci-dessous pour déployer la politique :

1. Placez le certificat *admin_policy.cer* du nouveau signataire dans le dossier d'installation *C:\Programmes\Arkoon\Security BOX* des utilisateurs, au même emplacement que le fichier *.p7b* et que le certificat de l'ancien signataire. L'ancien certificat est écrasé par le nouveau.
2. Suivez la procédure de mise à jour de politique via un point de distribution comme décrit dans la section Mettre à jour la politique de sécurité sur les agents SDS Enterprise.
3. Indiquez aux utilisateurs qu'ils doivent accepter le changement de signataire de politique dans le message d'avertissement qui s'affiche lors de leur reconnexion à leur compte SDS Enterprise.
4. Lorsque tous les utilisateurs ont accepté le nouveau signataire, supprimez le fichier *.p7b* du dossier d'installation de SDS Enterprise afin que l'ancien signataire ne soit plus considéré comme valide.

Tant que l'utilisateur n'accepte pas le changement de signataire de politique, le message d'avertissement s'affiche à chaque nouvelle connexion à son compte SDS Enterprise et la connexion lui est refusée.

Dans le cas du type de compte SSO, si l'utilisateur refuse le changement du signataire de politique, il n'est alors pas connecté automatiquement à son compte SDS Enterprise lorsqu'il ouvre sa session Windows. Pour continuer à utiliser SDS Enterprise, l'utilisateur doit fermer puis rouvrir sa session Windows, et accepter le changement de signataire. Pour plus d'informations sur le compte SSO, reportez-vous à la section Créer un compte Single Sign-On (SSO).

9.5.3 Consulter le certificat du signataire de politique sur l'agent

Depuis les propriétés de l'agent SDS Enterprise sur les postes des utilisateurs, vous pouvez consulter le certificat du signataire de politique :

1. Faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Dans l'onglet **Configuration**, double-cliquez sur l'icône **Porte-clés**.
4. Affichez l'onglet **Signataire de politique**. En cas de changement de signataire, l'onglet est automatiquement mis à jour lorsque l'utilisateur accepte le changement dans le message d'avertissement qui s'affiche lorsqu'il se connecte à son compte SDS Enterprise.
5. Cliquez sur **Détails** pour afficher toutes les informations du certificat.

10. Créer et gérer les comptes SDS Enterprise sur les postes des utilisateurs

Une fois les agents déployés sur les postes de travail des utilisateurs, les utilisateurs ont besoin d'un compte SDS Enterprise pour pouvoir utiliser les fonctionnalités du produit.

Selon les types de compte définis dans la politique, la création est manuelle ou automatique :

- compte Mot de passe : création manuelle
- compte Carte ou token USB : création manuelle ou automatique
- compte Single Sign-on (SSO) : création automatique avec authentification transparente

Quel que soit le type de compte, vous devez avoir autorisé au préalable la création de comptes dans la politique de sécurité. Pour plus d'informations, reportez-vous à la section **Configurer les comptes utilisateur**.

La création d'un compte peut impliquer la création d'une ou plusieurs clés qui seront utilisées pour la sécurisation des volumes et des messages, et l'auto-certification de ces clés pour un usage immédiat.

Lorsque l'utilisateur dispose d'un compte SDS Enterprise, il est prêt à utiliser le produit. Pour savoir comment utiliser SDS Enterprise, reportez-vous au *Guide d'utilisation avancée SDS Enterprise*.

10.1 Configurer les middleware nécessaires aux comptes Carte ou token USB

Pour communiquer avec une carte à puce ou un token USB, SDS Enterprise requiert la présence d'un middleware sur les postes des utilisateurs.

SDS Enterprise permet d'utiliser toute carte ou token USB dès lors que son constructeur fournit un module cryptographique PKCS#11 (interface standard) compatible.

SDS Enterprise fournit par défaut le middleware Stormshield Data Security, mais vous pouvez en utiliser d'autres en les spécifiant dans la politique de sécurité.

Dans ce cas, vous devez installer manuellement les middleware sur les postes des utilisateurs.

Pour les cartes ou tokens dont le fabricant a publié ses minidrivers auprès de Microsoft, vous pouvez utiliser le middleware Stormshield Data Security afin de bénéficier d'un fonctionnement Plug-and-Play.

De plus, pour faire fonctionner le type de compte Carte ou token USB pour vos utilisateurs, vous devez au préalable installer l'extension pour carte sur les postes de travail, comme indiqué dans les sections ci-dessous.

Le Configurateur de l'extension pour carte permet de consulter le middleware utilisé par SDS Enterprise pour communiquer avec la carte ou le token USB. Le middleware utilisé est inscrit en base de registre. Si besoin, l'extension permet également de sélectionner un autre middleware que vous avez spécifié dans la politique de sécurité.

L'installation de l'extension est également requise pour le fonctionnement des comptes Single Sign-on (SSO). Le middleware Stormshield Data Security est utilisé pour ce type de compte. Pour plus d'informations sur les comptes SSO, reportez-vous à la section **Créer un compte Single Sign-On (SSO)**.

10.1.1 Spécifier une liste de middleware dans la politique de sécurité

La politique de sécurité liste les middleware que SDS Enterprise peut utiliser sur les postes des utilisateurs pour communiquer avec les cartes ou tokens USB.

Si vous configurez la politique de sécurité via SDMC, reportez-vous à la section Définir les paramètres génériques des comptes. Par défaut, le middleware Stormshield Data Security est sélectionné. Vous ne pouvez sélectionner qu'un seul middleware via SDMC.

Depuis le fichier de configuration *.json* de la politique, vous pouvez spécifier manuellement plusieurs middleware à utiliser (paramètre cardMiddlewares). Pour plus d'informations, reportez-vous au *Guide de configuration avancée SDS Enterprise*.

Lorsque la politique de sécurité est déployée et prise en compte par les postes des utilisateurs, le middleware à utiliser est inscrit dans la base de registre. Si plusieurs middleware sont spécifiés dans la politique, SDS Enterprise prend en compte, par ordre d'apparition, le premier middleware de la liste qui est fonctionnel sur le poste. C'est-à-dire qu'il doit être disponible et s'exécuter sans erreur.

Les informations de configuration du middleware utilisé sont inscrites dans les clés de registre suivantes :

- **HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel\Components\Pkix**
  - `Pkcs11CardDll` : chemin vers la DLL du middleware,
  - `Pkcs11CardLabel` : nom du middleware.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\NewUserWizardGP1** et **NewUserWizardGP2**
  - `eCKA_[ATTRIBUTE]` : valeurs correspondant à des paramètres contrôlant l'utilisation de divers attributs PKCS#11 lors de la communication avec les cartes à puce/tokens USB.

A chaque démarrage de SDS Enterprise, la base de registre lui indique ainsi le middleware à utiliser. Nous vous déconseillons de modifier manuellement ces valeurs.

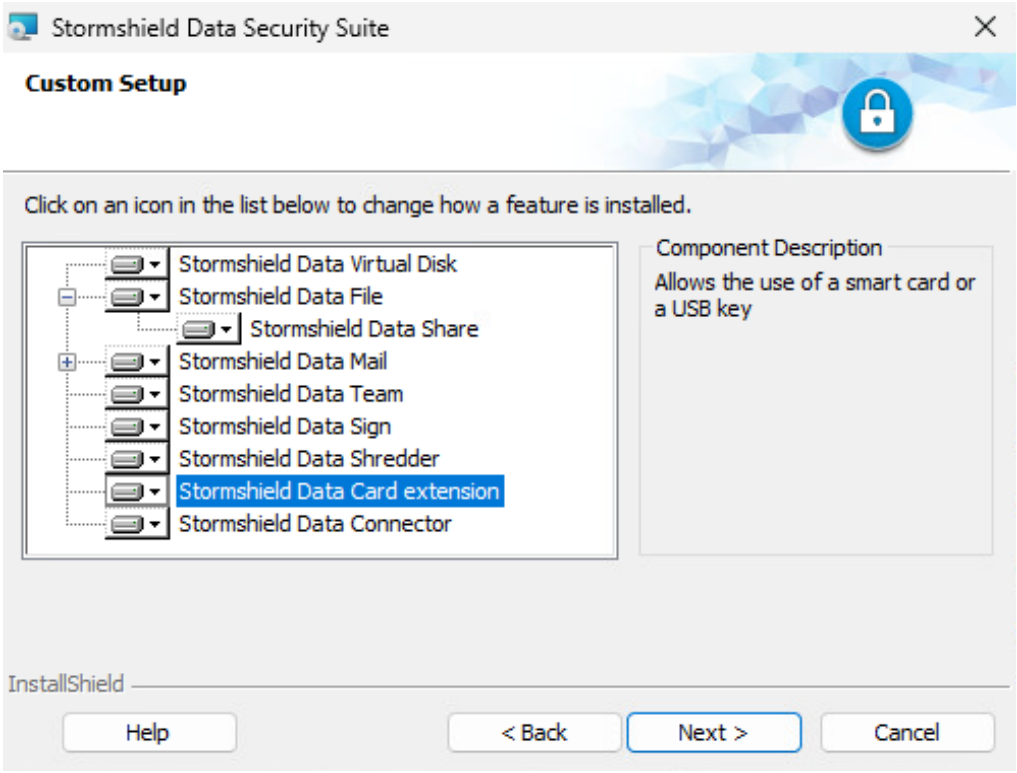
Vous pouvez sélectionner un autre middleware à utiliser à tout moment depuis le poste d'un utilisateur. Les valeurs en base de registre sont alors mises à jour automatiquement. Pour plus d'informations, reportez-vous à la section Configurer l'extension pour carte.

10.1.2 Installer l'extension pour carte

L'extension SDS Enterprise pour carte et token USB ou compte Single Sign-on peut être installée sur les postes des utilisateurs en même temps que les autres fonctionnalités. Pour plus d'informations, reportez-vous à la section Déployer le package d'installation des agents SDS Enterprise et une politique de sécurité personnalisée sur les postes des utilisateurs.

Pour une installation ultérieure, suivez la procédure ci-dessous :

1. Ouvrez le menu **Démarrer** de la barre de tâches du poste utilisateur.
2. Ouvrez le **Panneau de configuration** et choisissez la fonctionnalité **Ajout/Suppression de programmes**.
3. Sélectionnez dans la liste la ligne correspondant à SDS Enterprise.
4. Cliquez sur **Changer**. Vous entrez en mode **Maintenance**.
5. Choisissez l'option **Modifier** puis passez les différents écrans.



6. Sélectionnez la fonctionnalité **Stormshield Data Card extension**.
7. Terminez la procédure d'installation.

10.1.3 Configurer l'extension pour carte

Pour ouvrir le Configurateur de l'extension pour carte :

- Cliquez sur le menu **Démarrer** > **Stormshield Data Security Suite** > **Configurateur de l'extension carte**.

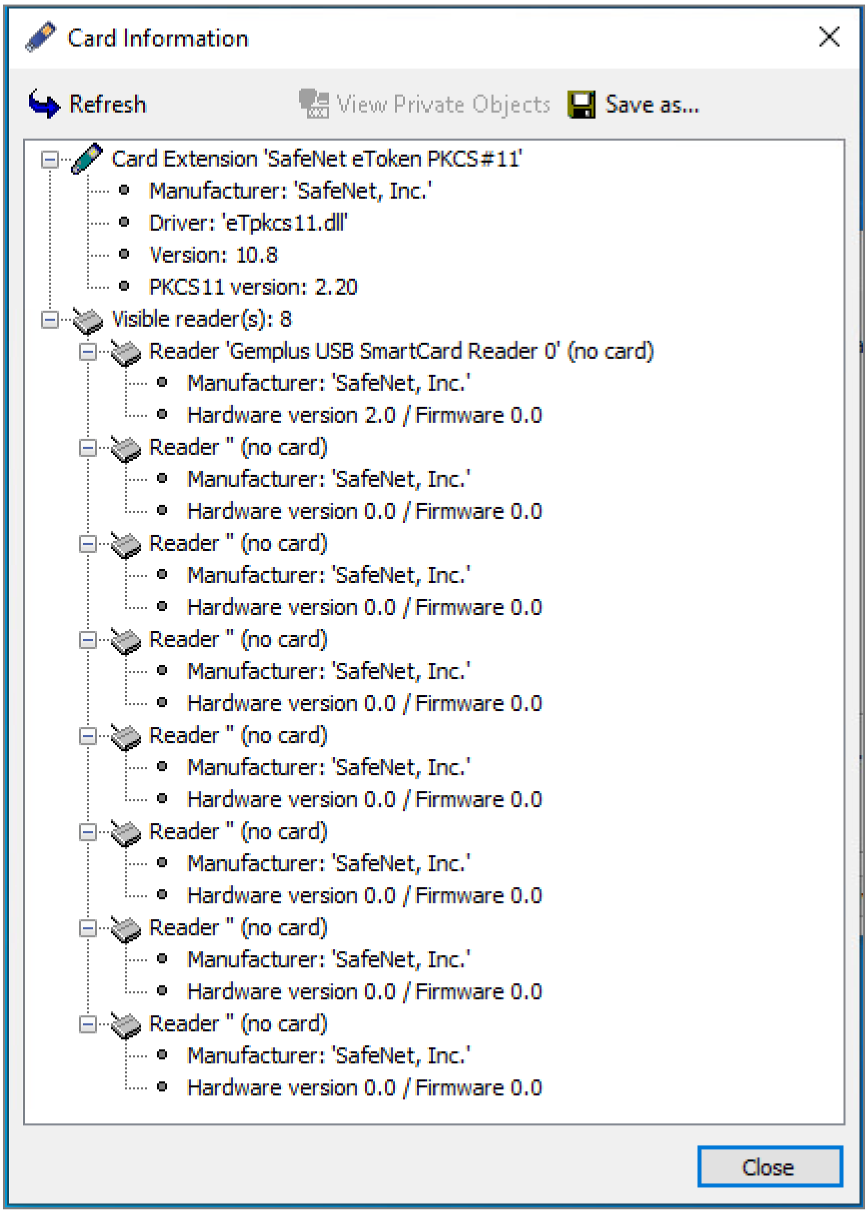
Le menu **Type de carte ou de clé USB** affiche le middleware utilisé par SDS Enterprise sur le poste de travail, comme défini par la politique de sécurité.

Vous pouvez sélectionner un autre middleware. La liste déroulante présente tous ceux spécifiés dans la politique de sécurité, dans leur ordre d'apparition dans la politique. Dans ce cas, la configuration de middleware est modifiée dans la base de registre et un redémarrage de SDS Enterprise est requis.

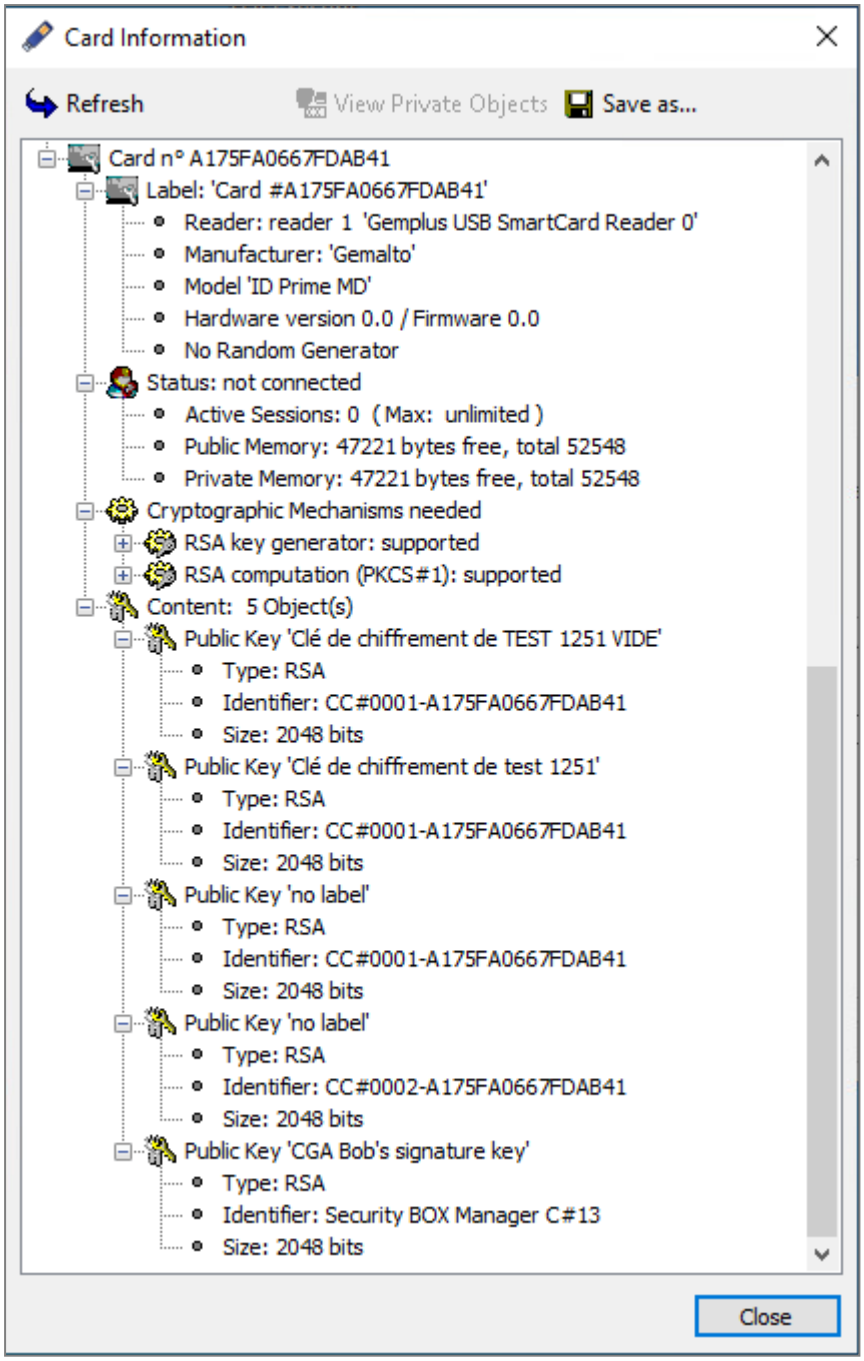
Si le nouveau middleware sélectionné est indisponible, une erreur s'affiche.

- Cliquez sur **Informations** pour analyser les problèmes d'accès aux cartes ou tokens. Le menu permet de tester le module d'interface *PKCS#11* : le nombre de lecteurs visibles est indiqué. Si la DLL *PKCS#11* n'est pas accessible, un message d'erreur le signale ; vérifiez alors le nom et le chemin de la DLL ainsi que la présence des éléments prérequis à cette DLL (notamment d'autres DLL).

L'écran suivant montre que l'extension carte est présente et configurée pour des cartes Gemalto. Il n'y a cependant pas de token USB effectivement présent.



L'écran suivant montre qu'un token USB est inséré et présente les caractéristiques du token USB ainsi que les objets publics (notamment les clés publiques et les certificats).



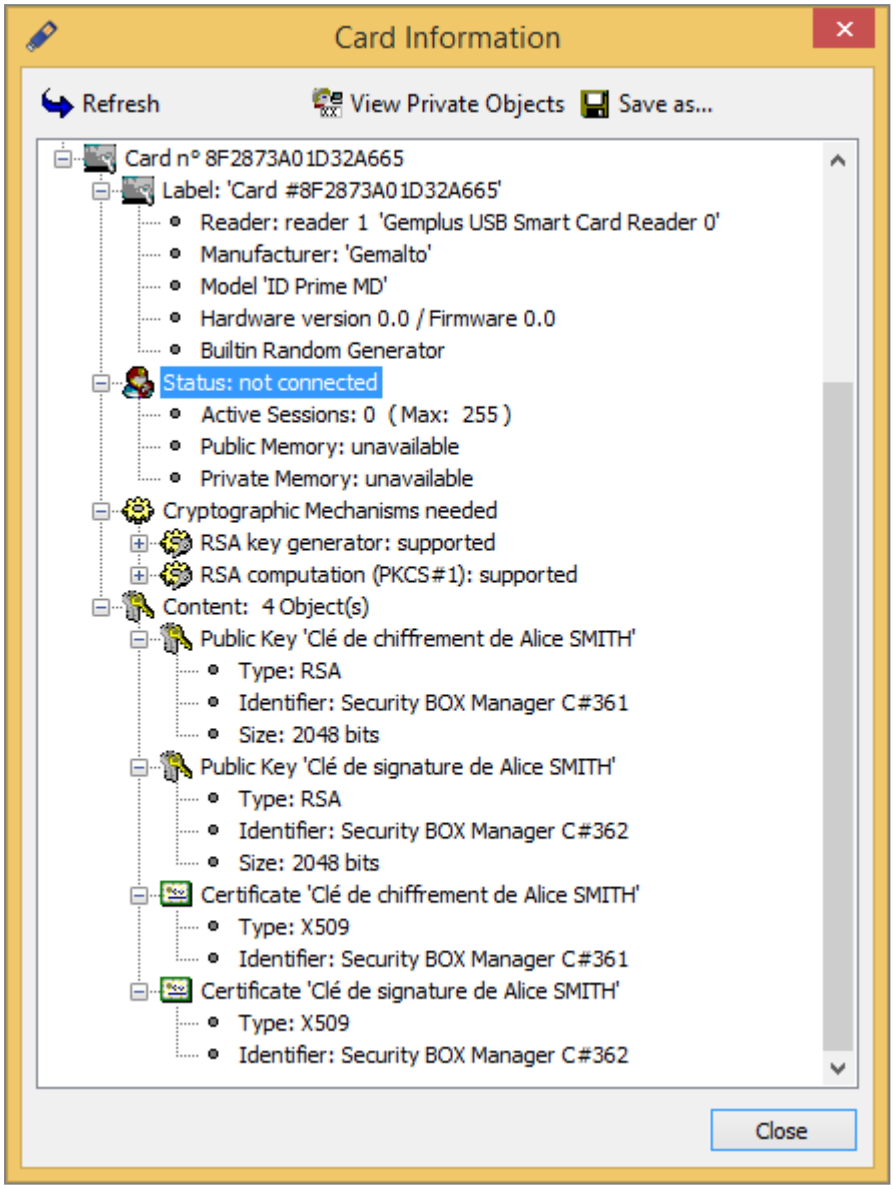
Vous pouvez également sélectionner un autre middleware depuis le menu SDS Enterprise :

- Faites un clic droit sur l'icône SDS Enterprise depuis la barre des tâches Windows, puis sélectionnez le menu **Choisir un type de carte ou de clé USB**. Le menu n'est visible que lorsque aucun utilisateur n'est connecté. À la différence du Configurateur de l'extension pour carte, ce menu affiche seulement les middleware installés sur le poste et fonctionnels.

10.1.4 Consulter les objets privés

Vous pouvez consulter les objets privés (essentiellement les clés privées) depuis le **Configurateur de l'extension carte** :

1. Cliquez sur **Information**.
2. Sélectionnez la ligne **Statut : non connecté** dans l'écran d'information.



3. Cliquez sur **Voir les objets privés**. Ce bouton n'est pas actif tant que la ligne précédente n'a pas été sélectionnée.
4. Saisissez le code PIN.

Le bouton **Enregistrer** permet d'enregistrer le contenu de la fenêtre dans un fichier texte.

10.2 Créer un compte Carte ou token USB

Pour créer un compte Carte ou token USB, activez la création automatique de compte dans SDMC afin que la création soit transparente pour l'utilisateur au premier branchement de sa carte ou clé. Vous pouvez également créer un compte manuellement depuis l'agent sur le poste de travail.

Dans les deux cas, la fonctionnalité Stormshield Data Extension Carte doit être installée sur les postes de travail des utilisateurs, avec les autres fonctionnalités de l'agent SDS Enterprise. Pour plus d'informations, reportez-vous aux sections Déployer le package d'installation des agents

SDS Enterprise et une politique de sécurité personnalisée sur les postes des utilisateurs et Configurer les middleware nécessaires aux comptes Carte ou token USB.

Avec une carte ou un token USB :

- Vos clés et certificats sont stockés sur la carte,
- Les calculs mettant en œuvre vos clés privées sont effectués par la carte (signature, déchiffrement).

Lors de la création d'un compte associé à une carte, celle-ci doit déjà contenir les clés privées et les certificats associés.

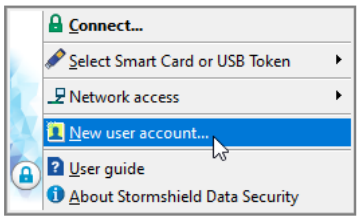
10.2.1 Créer un compte automatiquement

Pour faciliter le déploiement des comptes Carte ou token USB, et minimiser les actions de l'utilisateur, SDS Enterprise peut créer automatiquement le compte d'un utilisateur lors de la première introduction de la carte ou du token. Pour cela, vous devez avoir auparavant installé et configuré le middleware nécessaire et activé la fonctionnalité dans SDMC. Pour sélectionner le middleware à utiliser et activer la création automatique de compte, reportez-vous aux sections Définir les paramètres génériques des comptes et Définir les paramètres de création de comptes.

L'utilisateur introduit ensuite simplement sa carte à puce ou son token USB. SDS Enterprise détecte automatiquement qu'il n'y a pas de compte existant associé et propose d'en créer un. Pour effectuer cette opération, l'utilisateur n'a qu'à saisir le code confidentiel de la carte ou du token et le compte SDS Enterprise est ainsi créé.

10.2.2 Créer un compte manuellement

1. Sur le poste de l'utilisateur, insérez la carte ou le token USB.
2. Faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
3. Sélectionnez **Nouvel utilisateur**.



4. Sélectionnez **Compte avec carte à puce physique ou virtuelle**.
5. Cliquez sur **Créer un compte**.
6. Sélectionnez la carte ou le token USB que vous souhaitez utiliser.
7. Saisissez le code confidentiel de la carte ou du token USB. SDS Enterprise se connecte à la carte ou au token USB et affiche leur contenu (clés et certificats).
8. Validez les écrans suivants. Si la carte ou le token USB contiennent plusieurs clés utilisables, choisissez la clé souhaitée.
9. Vérifiez le récapitulatif du compte.
10. Cliquez sur **Terminer**.

Le compte SDS Enterprise créé en utilisant une carte à puce/token USB est identifié par le numéro de série de la carte/token USB.

10.2.3 Utiliser les clés de la carte ou du token USB

Indépendamment des clés courantes de l'utilisateur, il est possible de placer dans la carte ou token d'autres clés de chiffrement.

Ces clés de chiffrement sont automatiquement utilisées par SDS Enterprise pour déchiffrer des documents (messages/fichiers) lorsque la clé courante ne peut pas y parvenir.

Ces clés peuvent avoir plusieurs provenances :

- Anciennes clés de chiffrement de l'utilisateur. Il est possible de placer dans la carte des clés obsolètes (avec les certificats associés) afin de permettre à l'utilisateur de déchiffrer des fichiers chiffrés avec d'anciennes clés (cela sert notamment pour les fichiers archivés),
- Clés externes. Par exemple, des clés d'anciens collaborateurs dont on veut pouvoir récupérer les informations (fichiers/messages).

Selon les fonctionnalités SDS Enterprise, les clés de la carte ne sont pas identifiées de la même façon. Pour certaines fonctionnalités, les clés sont identifiées à partir de leur attribut PKCS#11 CKA_ID (il faut donc que la clé garde toujours la même valeur de CKA_ID) tandis que pour d'autres fonctionnalités, l'identification est faite à partir des informations du certificat (émetteur et numéro de série).

Il est donc recommandé que les clés stockées dans les cartes le soient toujours avec le même attribut PKCS#11 CKA_ID et que tous les certificats associés soient également présents.

10.3 Créer un compte Mot de passe manuellement

À la création d'un compte Mot de passe SDS Enterprise, deux méthodes sont possibles pour attribuer des clés de chiffrement et signature à l'utilisateur :

- La génération des clés de chiffrement et/ou signature par SDS Enterprise localement,
- L'import de clés préalablement sauvegardées dans un fichier au format *PKCS#12*, extensions *P12* ou *PFX*.

Les méthodes de gestion des clés ainsi que le type de clés disponibles dépendent du paramétrage de la politique de sécurité dans SDMC.

Si vous créez un compte à deux clés, vous pouvez utiliser l'une ou l'autre des deux méthodes pour la création de chaque clé.

10.3.1 Choisir de générer les clés

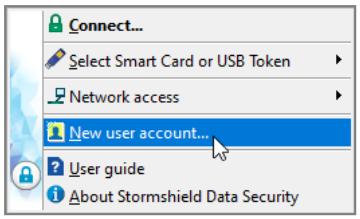
Les clés générées serviront par exemple à la sécurisation des fichiers et messages électroniques. Elles sont auto-certifiées pour être immédiatement utilisables par SDS Enterprise. Cependant, elles ne seront pas automatiquement considérées comme étant de confiance par les correspondants mais elles pourront être ultérieurement certifiées par une autorité de confiance.

Si vous utilisez deux clés distinctes, l'une pour le chiffrement et l'autre pour la signature, exécutez deux fois la procédure ci-dessous. Elle décrit la création d'une clé de chiffrement.

Pour générer une clé :

1. Sur le poste de l'utilisateur, faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.

2. Sélectionnez **Nouvel utilisateur**.



3. Sélectionnez **Compte avec mot de passe**.
4. Cliquez sur **Créer un compte**.
5. Entrez l'identifiant et le mot de passe de votre choix. Ils seront demandés pour se connecter à SDS Enterprise.
6. Cliquez sur **Suivant**.
7. Choisissez **Générer votre clé de chiffrement** et sélectionnez le type de clé.
8. Cliquez sur **Suivant**.
9. Sur la fenêtre suivante, générez la clé à partir de nombres aléatoires en bougeant la souris ou en tapant sur le clavier.
   Une fois la capture terminée, cliquez sur **Suivant**.
10. Saisissez les informations constituant l'identité de l'utilisateur, telle qu'elle sera indiquée dans le certificat auto-certifié.
11. Cliquez sur **Suivant**.
12. Choisissez un mot de passe de secours qui sera demandé en cas d'oubli du mot de passe principal ou si l'utilisateur bloque son compte en saisissant consécutivement trop de codes erronés. Pour plus d'informations, reportez-vous à la section Débloquer un compte Mot de passe.
    Cliquez sur **Suivant**.
13. Vérifiez le récapitulatif du compte.
14. Cliquez sur **Terminer**.

SDS Enterprise génère les clés et crée le compte.

Le compte comporte un certificat personnel auto-certifié. Ce certificat, produit par l'utilisateur, peut éveiller la méfiance de certains correspondants qui n'accordent leur confiance qu'aux certificats délivrés par une autorité reconnue. Nous vous recommandons d'utiliser des clés certifiées provenant d'une PKI (*Public Key Infrastructure*). Si vous souhaitez utiliser la solution de PKI de Microsoft, consultez la section Mettre en place la solution d'infrastructure à clé publique (PKI) de Microsoft.

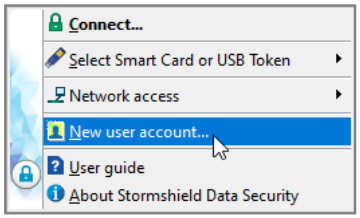
10.3.2 Choisir d'importer les clés

Cette section explique comment créer un compte en récupérant des clés et des certificats sauvegardés dans un fichier au format *PKCS#12* (extensions *P12* ou *PFX*).

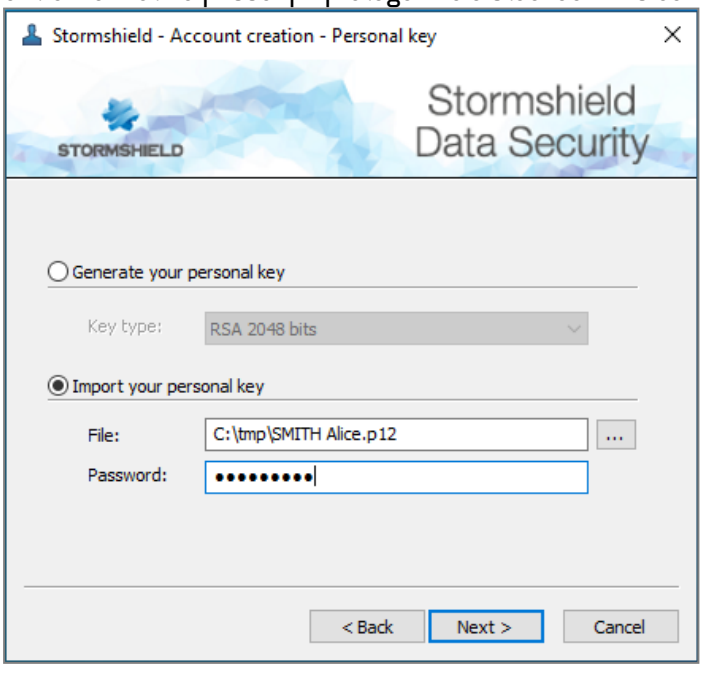
Cette fonction offre la possibilité d'utiliser une clé (et son certificat associé) générée par le passé ou encore d'utiliser une clé générée de façon centralisée par une PKI. Enfin, cette fonction permet de sauvegarder des clés privées qui peuvent être utilisées pour des opérations de recouvrement.

Les actions décrites ci-dessous s'appliquent à la fois à la clé de chiffrement et à la clé de signature.

1. Sur le poste de l'utilisateur, faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Sélectionnez **Nouvel utilisateur**.



3. Sélectionnez **Compte avec mot de passe**.
4. Cliquez sur **Créer un compte**.
5. Entrez l'identifiant et le mot de passe de votre choix. Ils seront demandés pour se connecter à SDS Enterprise.
6. Cliquez sur **Suivant**.
7. Choisissez **Importer votre clé de chiffrement** et :
   - sélectionnez le fichier au format *PKCS#12* portant l'extension *P12* ou *PFX*,
   - entrez le mot de passe qui protège la clé stockée dans ce fichier.



8. Cliquez sur **Suivant**.
   Si le fichier comporte plusieurs clés ou certificats, sélectionnez la clé à importer et cochez le certificat associé à cette clé.
9. Cliquez sur **Suivant**.
10. Choisissez un mot de passe de secours qui sera demandé en cas d'oubli du mot de passe principal ou si l'utilisateur bloque son compte en saisissant consécutivement trop de codes erronés (par défaut trois codes erronés). Pour plus d'informations, reportez-vous à la section Débloquer un compte utilisateur.
    Cliquez sur **Suivant**.
11. Vérifiez le récapitulatif du compte.
12. Cliquez sur **Terminer**.

SDS Enterprise importe la clé et crée le compte.

10.4 Créer un compte Single Sign-On (SSO)

SDS Enterprise permet aux utilisateurs de se connecter automatiquement et de façon transparente à SDS Enterprise grâce au mode SSO qui associe le compte SDS Enterprise à leur compte utilisateur Windows. SDS Enterprise utilise alors les clés de chiffrement et de signature stockées dans le Magasin de certificats Windows.

Si vous souhaitez utiliser la solution d'infrastructure à clé publique de Microsoft pour générer les clés de chiffrement et de signature des utilisateurs, consultez la section Mettre en place la solution d'infrastructure à clé publique (PKI) de Microsoft.

La politique de sécurité permet de paramétrer l'utilisation du type de compte SSO. Les comptes des utilisateurs sont alors créés automatiquement sur leur poste. Vous pouvez paramétrer la politique de sécurité dans l'interface web SDMC ou en mode avancé directement dans le fichier *.json* de la politique.

Ce tableau décrit les différentes étapes pour déployer SDS Enterprise en mode SSO. Cliquez sur un lien pour ouvrir la procédure correspondante dans ce guide.

Étapes	Description
1	Se conformer aux prérequis
2	Paramétrer la politique de sécurité en mode SSO : • En mode standard via l'interface web SDMC, • En mode avancé via le fichier .json de la politique.
3	Télécharger et signer une politique de sécurité
4	Déployer le package d'installation des agents SDS Enterprise et une politique de sécurité personnalisée sur les postes des utilisateurs
5	Utiliser les comptes SSO

10.4.1 Prérequis

- La fonctionnalité Stormshield Data Extension Carte doit être installée sur les postes de travail des utilisateurs, avec les autres fonctionnalités de l'agent SDS Enterprise. Pour plus d'informations, reportez-vous aux sections Déployer le package d'installation des agents SDS Enterprise et une politique de sécurité personnalisée sur les postes des utilisateurs et Configurer les middleware nécessaires aux comptes Carte ou token USB.
- Les certificats des clés de chiffrement et de signature des utilisateurs doivent avoir été stockés au préalable sur les postes de travail dans le magasin de certificats **Personnel** via le Gestionnaire de certificats Windows.
  Ces certificats doivent avoir été émis par les autorités de certification déclarées dans la politique de sécurité, lors du paramétrage des comptes SSO, comme indiqué dans les deux sections suivantes.
- Les utilisateurs doivent disposer d'une clé privée pour chacun de leurs certificats stockés dans les magasins de certificats Windows.
- Deux certificats doivent avoir été ajoutés au préalable dans la Bibliothèque de certificats de SDMC :
  - Le certificat de l'autorité certification qui a émis les certificats des utilisateurs,
  - Le certificat du compte de recouvrement.

  Pour plus d'informations, reportez-vous à la section Ajouter des certificats d'autorité de certification.
- Votre annuaire LDAP doit avoir été ajouté au préalable dans la Bibliothèque LDAP de SDMC. Pour plus d'informations, reportez-vous à la section Gérer les annuaires LDAP dans SDMC.

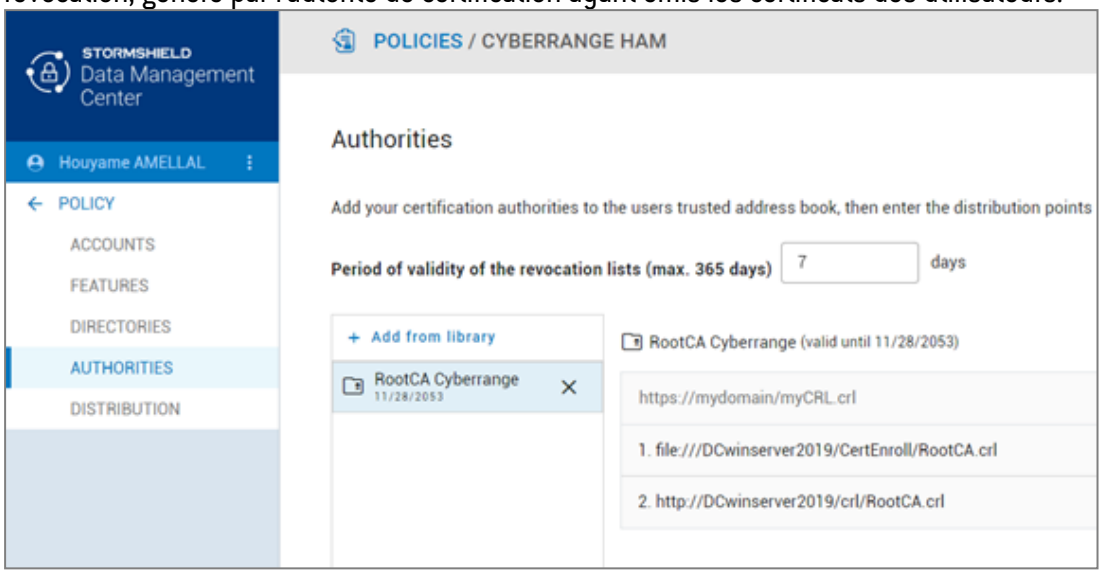
10.4.2 Paramétrer les comptes SSO dans SDMC

Pour paramétrer le type de compte SSO et faire en sorte que les comptes SDS Enterprise des utilisateurs soient associés à leur compte utilisateur Windows, paramétrez les options suivantes dans SDMC :

1. Allez dans le menu **Comptes** de la politique de sécurité concernée.
2. Dans l'onglet **Paramètres**, sélectionnez :
   - **Type de compte** : Single Sign-on (SSO),
   - **Compte carte ou token USB** : Middleware Stormshield Data Security.

   Pour plus d'informations, reportez-vous à la section Définir les paramètres génériques des comptes.
3. Dans l'onglet **Création**, sélectionnez :
   Gestion des clés : Compte avec deux clés (clé de chiffrement et clé de signature).
   Filtrer les autorités lors de la création automatique : Autorités de certification ayant émis les clés de chiffrement et signature des utilisateurs.
   Pour plus d'informations, reportez-vous à la section Définir les paramètres de création de comptes.
4. Dans l'onglet **Recouvrement de données**, ajoutez le certificat du compte de recouvrement.
5. Dans le menu **Politiques > Fonctionnalités**, conservez le paramétrage par défaut ou configurez les différentes fonctionnalités selon vos besoins.
   Pour plus d'informations, reportez-vous à la section Configurer les fonctionnalités.

6. Dans le menu **Politiques** > **Autorités**, ajoutez le chemin vers le fichier **.crl* de la liste de révocation, généré par l'autorité de certification ayant émis les certificats des utilisateurs.



7. Dans le menu **Politiques** > **Diffusion**, ajoutez le chemin vers le point de distribution du fichier *Policy.jwt*. Ce fichier correspond au format de votre politique de sécurité après signature par le compte signataire de politique.
   Pour plus d'informations, reportez-vous à la section Configurer les points de distribution de politiques.
8. Lorsque la politique de sécurité est prête, déployez-la sur les postes des utilisateurs comme indiqué à la section Installer les agents SDS Enterprise sur les postes des utilisateurs et déployer les politiques de sécurité ou à la section Mettre à jour la politique de sécurité sur les agents SDS Enterprise.

Consultez ensuite la section Utiliser le compte SSO.

10.4.3 Mode avancé - Paramétrer les comptes SSO dans le fichier *.json*

Pour paramétrer manuellement le type de compte SSO directement dans le fichier *.json* d'une politique de sécurité, vous devez compléter les champs suivants :

1. Indiquez le type SSO dans le paramètre "AccountMode" :

```
"accountPolicy": {
        "parameters": {
                "accountMode": "SSO"
        }
}
```

2. Indiquez le nombre de clés dans le paramètre "accountKeyMode" ("dualKey", "singleKeyEncryption" ou "singleKeySignature") :

```
"accountPolicy": {
        "creation": {
                "accountKeyMode": "dualKey"
        }
}
```

3. Indiquez l'identifiant du certificat de l'autorité ayant émis les clés à utiliser pour créer les comptes dans les paramètres "encryptionKeyAuthorityId" et "signatureKeyAuthorityId" :

```
"accountPolicy": {
        "creation": {
                "automatic": {

"encryptionKeyAuthorityId": "0123456789ab-cdef-0123-4567-
89abcdef",
"signatureKeyAuthorityId": "0123456789ab-cdef-0123-4567-89abcdef"
                }

       }
}
```

4. Indiquez les données des certificats mentionnés à l'étape 3 dans le paramètre "certificateData" au format "base 64" :

```
"certificateData": [
        {
           "id": "0123456789ab-cdef-0123-4567-89abcdef",
           "data": "LS0tLS1CRUdJTiBDR [...] GSUNBVEUtLS0tLQ0K"
        }
]
```

5. Lorsque la politique de sécurité est prête, déployez la sur les postes des utilisateurs comme indiqué à la section Installer les agents SDS Enterprise sur les postes des utilisateurs et déployer les politiques de sécurité ou à la section Mettre à jour la politique de sécurité sur les agents SDS Enterprise.

Pour configurer la politique de sécurité au format *.json*, consultez le *Guide de configuration avancée* de SDS Enterprise.

Consultez ensuite la section Utiliser le compte SSO.

10.4.4 Utiliser le compte SSO

Une fois la politique déployée sur les postes, le compte SDS Enterprise SSO des utilisateurs est automatiquement créé lors de leur prochaine connexion à leur compte Windows. Ils peuvent alors utiliser SDS Enterprise sans passer par sa fenêtre de connexion.

Pour spécifier un emplacement pour les fichiers du compte SDS Enterprise sur le poste de l'utilisateur, utilisez les paramètres "primaryUserPath" et "secondaryUserPath" dans le fichier de configuration *.json*. Les fichiers sont stockés dans un sous-dossier nommé avec le nom de l'utilisateur courant de la session Windows. Ce sous-dossier se trouve lui-même dans un sous-dossier "SSO" du chemin spécifié par les paramètres "primaryUserPath" et "secondaryUserPath".

Pour configurer le fichier *.json*, reportez-vous au *Guide de configuration avancée* de SDS Enterprise.

La connexion et la déconnexion du compte SDS Enterprise sont automatiques à chaque ouverture et fermeture de la session Windows de l'utilisateur. Il en est de même pour le verrouillage et déverrouillage du compte.

En cas de changement du signataire de la politique de sécurité, reportez-vous à la section Modifier le signataire d'une politique de sécurité.

Les particularités suivantes s'appliquent au type de compte SSO :

- Les menus de connexion et verrouillage restent visibles en cliquant sur l'icône SDS Enterprise  de la barre des tâches Windows, mais ils sont grisés.
- L'utilisateur peut cependant choisir dans les propriétés de son compte SDS Enterprise> **Paramètres de connexion** > onglet **Écran de veille** de verrouiller la session SDS Enterprise lors du déclenchement de l'écran de veille Windows ou sur verrouillage de la session Windows, et de ne pas déverrouiller au réveil ou à la reprise. Dans ce cas, il peut utiliser le menu **Déverrouiller** en cliquant sur l'icône SDS Enterprise  de la barre des tâches.
- Dans le porte-clés de l'utilisateur, accessible depuis l'icône SDS Enterprise  de la barre des tâches Windows, le bouton **Opérations** n'est pas visible dans les onglets **Chiffrement** et **Signature**.

10.5 Renouveler les clés et certificats

Lorsque des clés de chiffrement ou signature, ou bien des certificats, sont perdus ou compromis ou encore expirés, veuillez suivre les procédures suivantes pour les renouveler selon le type de compte de vos utilisateurs.

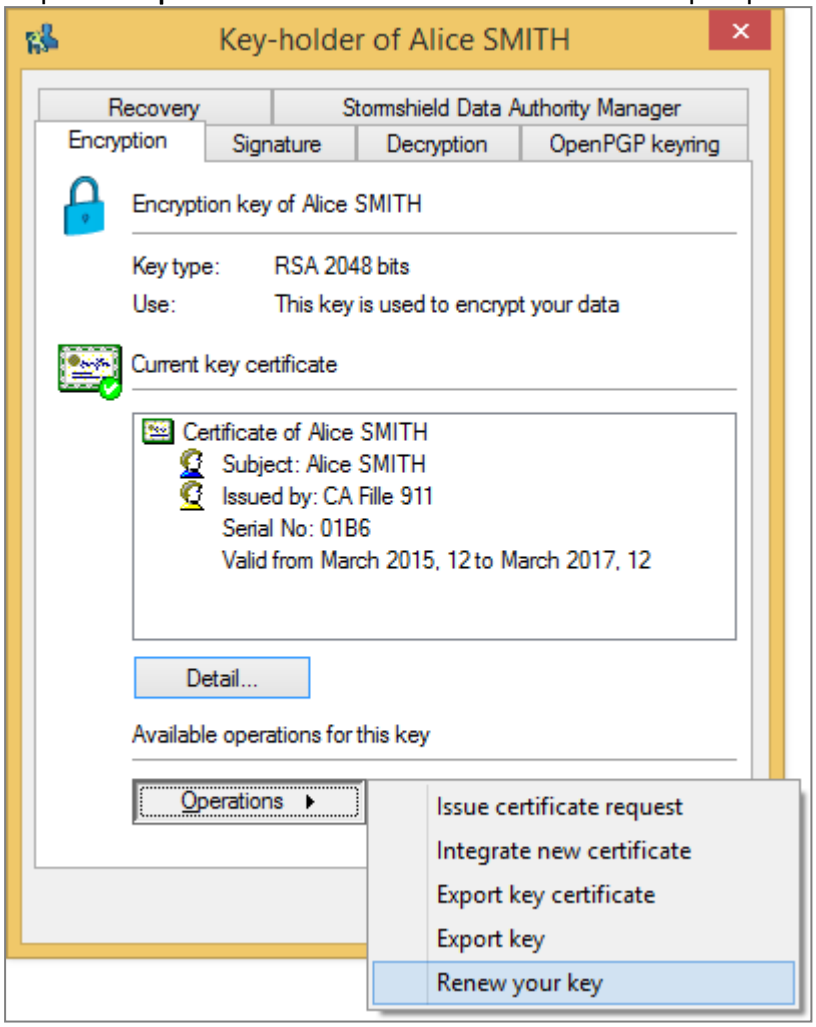
10.5.1 Comptes Mot de passe

Vous pouvez renouveler les clés d'un utilisateur de compte Mot de passe afin de changer ses clés de chiffrement ou de signature.

Pour renouveler les clés depuis le poste d'un utilisateur :

1. Faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Configuration**.
4. Double-cliquez sur l'icône **Porte-clés**.
   - Si l'utilisateur possède deux clés, choisissez l'onglet **Clé de chiffrement** ou **Clé de signature**.
   - Si l'utilisateur ne possède qu'une seule clé, choisissez l'onglet **Clé personnelle**.

5. Cliquez sur **Opérations** et choisissez **Renouveler votre clé** puis passez l'écran d'introduction.



6. Indiquez comment créer la clé de chiffrement :
   - Pour créer une nouvelle clé, choisissez l'option **Générer votre clé** et sélectionnez le type et la longueur de la clé. Reportez-vous à la section Créer un compte Mot de passe manuellement pour la suite de la procédure.
   - Pour importer une clé existante, choisissez **Importer votre clé**. Reportez-vous à la section Créer un compte Mot de passe manuellement pour la suite de la procédure.
7. Cliquez sur **Terminer**.

SDS Enterprise génère ou importe la clé personnelle et déplace l'ancienne clé en tant que clé de déchiffrement afin que l'utilisateur puisse déchiffrer ses anciens documents. Elle est visible dans l'onglet **Déchiffrement** du porte-clés de l'utilisateur.Les clés de signature ne sont pas gardées.

Pour plus d'informations, reportez-vous à la section Déchiffrer les données d'un utilisateur avec une ancienne clé ou une clé de délégation.

10.5.2 Comptes Carte ou token USB

Pour renouveler des certificats ou clés sur les cartes à puce et tokens USB, veuillez prendre en compte les informations suivantes.

Renouveler les certificats

En cas de renouvellement de certificats sur la carte ou sur le token USB, les nouveaux certificats sont pris en compte lors de la prochaine connexion de l'utilisateur à SDS Enterprise.

Lorsqu'un nouveau certificat est ajouté, il faut que l'objet certificat créé ait bien le même attribut *PKCS#11* CKA_ID que l'ancien.

L'ancien certificat ne doit pas être supprimé tant que le nouveau n'a pas été pris en compte correctement par SDS Enterprise. Il est possible de vérifier que le nouveau certificat a bien été pris en compte dans le porte-clés de l'agent SDS Enterprise.

Renouveler les clés

En cas de renouvellement de clés (avec le certificat associé) sur la carte ou sur le token USB, les nouvelles clés sont prises en compte lorsque les certificats des anciennes clés expirent.

Dans le cas de compte avec plusieurs clés (une de chiffrement et une de signature), le choix des nouvelles clés s'effectue en fonction des usages des certificats associés.

Vous pouvez vérifier que les nouvelles clés ont bien été prises en compte dans le porte-clés de l'agent SDS Enterprise.

IMPORTANT
Veillez à bien conserver l'ancienne clé de chiffrement, même après prise en compte de la nouvelle clé par SDS Enterprise.

L'ancienne clé devient automatiquement une clé de déchiffrement et permet de toujours déchiffrer les anciens documents de l'utilisateur. Elle est visible dans l'onglet **Déchiffrement** du porte-clés de l'utilisateur.

Il n'est pas nécessaire de garder l'ancienne clé de signature.

Pour plus d'informations, reportez-vous à la section Déchiffrer les données d'un utilisateur avec une ancienne clé ou une clé de délégation.

10.5.3 Comptes Single Sign-on (SSO)

En mode SSO, les clés de chiffrement et de signature ainsi que les certificats peuvent être stockés dans le Magasin de certificats Windows de l'utilisateur. Dans ce cas, veuillez prendre en compte les informations suivantes.

Renouveler les clés

Si vous avez besoin de renouveler les clés d'un utilisateur dans le Magasin de certificats Windows, suivez les étapes suivantes :

1. Le mécanisme de gestion des clés étant similaire pour les comptes Carte et pour les comptes SSO, commencez par activer le renouvellement automatique des clés dans le fichier de configuration *.json* de la politique. Pour cela, indiquez la valeur "confirm" ou "silent" pour le paramètre enableAutomaticRenewFromCard dans la section *accountPolicy* du fichier. Pour plus d'informations, reportez-vous à la section Compte du *Guide de configuration avancée de SDS Enterprise*.
2. Après la modification du fichier *.json* de l'utilisateur, celui-ci doit redémarrer son ordinateur pour s'assurer de la bonne prise en compte de la modification.

3. Par précaution, si vous renouvelez une clé de chiffrement, sauvegardez en lieu sûr la clé privée de l'utilisateur afin qu'il puisse continuer à déchiffrer ses anciennes données en cas de problème au cours de la procédure de renouvellement. La sauvegarde n'est pas nécessaire pour le renouvellement d'une clé de signature.
4. Via le Gestionnaire de certificats Windows, dans le magasin personnel de l'utilisateur, faites un clic droit sur le certificat correspondant à la clé à renouveler puis sélectionnez le menu **Toutes les tâches** > **Demander un certificat avec une nouvelle clé**.
   Une nouvelle clé et son certificat sont générés et affichés dans le Gestionnaire de certificats.

IMPORTANT
Veillez bien à demander un nouveau certificat avec une nouvelle clé et pas un renouvellement de certificat. En effet, la clé précédente serait écrasée par la nouvelle. Or, dans le cas du chiffrement, l'ancienne clé doit rester présente dans le Magasin de certificats afin que l'utilisateur puisse toujours déchiffrer ses anciennes données. **Ne supprimez donc jamais les anciennes clés de chiffrement.**

L'agent SDS Enterprise prend alors en compte la nouvelle clé, lorsque le certificat de l'ancienne clé expire.

À l'issue de cette opération, l'ancienne clé de chiffrement est automatiquement ajoutée dans l'onglet **Déchiffrement** du porte-clés de l'utilisateur, en tant que clé de déchiffrement. Même si la clé est visible dans le porte-clés, elle reste stockée dans le Magasin de certificats Windows de l'utilisateur. Il est donc important de la conserver dans le Magasin.

Pour plus d'informations sur la clé de déchiffrement, reportez-vous à la section Déchiffrer les données d'un utilisateur avec une ancienne clé ou une clé de délégation.

Après le renouvellement d'une clé, si vous avez indiqué la valeur "confirm" pour le paramètre enableAutomaticRenewFromCard dans le fichier *.json* de la politique, l'utilisateur devra confirmer le renouvellement de la clé dans la fenêtre qui s'ouvrira lors de sa prochaine connexion à son compte SDS Enterprise.

Deux fenêtres de confirmation différentes s'affichent si la clé de chiffrement et la clé de signature ont été renouvelées.

Vous pouvez vérifier que les nouvelles clés ont bien été prises en compte dans le porte-clés de l'agent SDS Enterprise.

Renouveler les certificats

Si vous avez besoin de renouveler le certificat d'un utilisateur (sans changer de clé), vous devez effectuer le renouvellement via le Gestionnaire de certificats Windows afin qu'il reste associé à la même clé de chiffrement ou de signature :

- Dans le magasin personnel de l'utilisateur, faites un clic droit sur le certificat à renouveler puis sélectionnez le menu **Toutes les tâches** > **Opérations avancées** > **Renouveler ce certificat avec la même clé**.

Au prochain démarrage de SDS Enterprise, le nouveau certificat est alors pris en compte automatiquement dans le porte-clés de l'utilisateur.

10.6 Débloquer un compte Mot de passe

Si l'utilisateur a oublié son mot de passe, ou si le compte est bloqué parce qu'il a saisi trop de mots de passe erronés, il est possible de débloquer son compte.

10.6.1 Utiliser le mot de passe de secours

1. Dans la fenêtre de connexion, sélectionnez **Déverrouiller** pour démarrer l'outil de déverrouillage puis cliquez sur **Suivant**.
2. Sélectionnez **Vous connaissez le mot de passe de secours**.
3. Saisissez le mot de passe de secours saisi lors de la création du compte puis cliquez sur **Suivant**.

> **IMPORTANT**
> En cas de blocage du mot de passe de secours, il n'est plus possible de débloquer le compte.

4. Saisissez un nouveau mot de passe en respectant les critères affichés puis confirmez-le.
5. Cliquez sur **Terminer**.

Le compte est à nouveau opérationnel avec le nouveau mot de passe.

10.6.2 Utiliser la sauvegarde du compte utilisateur

A chaque connexion réussie, SDS Enterprise effectue une sauvegarde (*.bak*) des fichiers keystore (*.usr*), annuaire (*.usd*) et base de révocation (*.bcrl*) composant le compte de l'utilisateur.

Si le compte de l'utilisateur est bloqué ou s'il est corrompu, vous pouvez restaurer le compte à partir de sa dernière sauvegarde.

Pour cela, dans le dossier contenant le compte de l'utilisateur (paramétré dans la politique de sécurité) :

1. Renommez les trois fichiers *.usr*, *.usd*, *.brcl*,
2. Faites une copie de sauvegarde des trois fichiers *.usr.bak*, *.usd.bak*, *.brcl.bak*,
3. Supprimez l'extension *.bak* des trois fichiers *.usr.bak*, *.usd.bak*, *.brcl.bak*.

L'utilisateur est ainsi remis dans l'état de sa dernière connexion réussie.

10.7 Exporter un compte SDS Enterprise

Vous pouvez exporter un compte utilisateur dans un fichier Windows Installer qui contiendra toutes les informations et les fichiers du compte.

Une fois le compte exporté sur ce fichier Windows Installer, vous pourrez le conserver pour le sauvegarder, ou le transporter sur un autre poste utilisant SDS Enterprise pour y installer le compte utilisateur.

Pour exporter le compte :

1. Sur le poste de l'utilisateur, faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Assistants**.
4. Cliquez sur **Exporter votre compte**.
5. Passez l'écran d'introduction.
6. Cliquez sur l'icône **Parcourir** pour déterminer le répertoire dans lequel exporter le compte et saisissez le nom du fichier à créer
7. Cliquez sur **Suivant**.
8. Vérifiez le récapitulatif puis cliquez sur **Terminer**.
   SDS Enterprise crée alors le fichier *.usi* à l'endroit indiqué et affiche un compte rendu.

10.8 Exporter une clé de sécurité

Vous pouvez exporter dans un fichier une clé de sécurité (clé publique et clé privée), avec son certificat et son éventuelle parenté.

Pour un compte à deux clés, vous pouvez exporter les clés individuellement.

En sauvegardant ce fichier, vous pourrez :

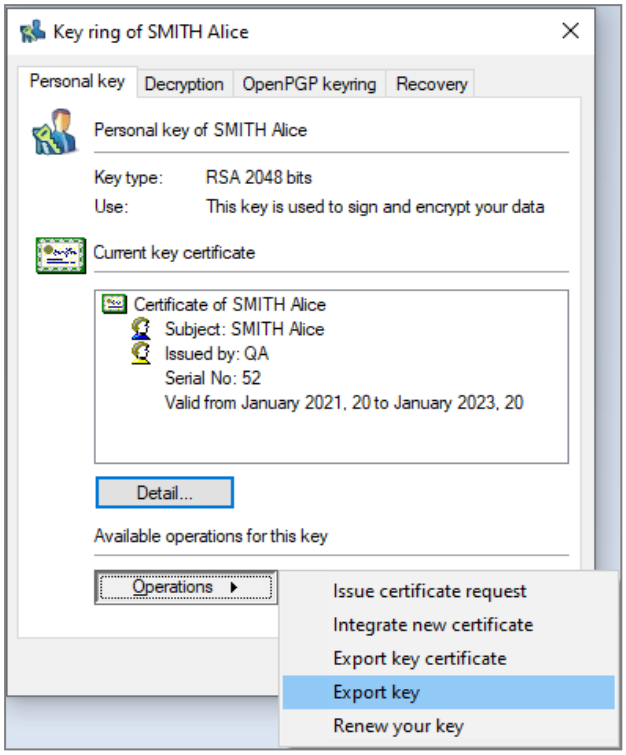
- Recréer un nouveau compte à partir de la clé actuelle,
- Utiliser cette clé dans toute application capable d'importer une clé de sécurité.

Cela sera utile pour les clés de déchiffrement dans les cas de déchiffrement par délégation (reportez-vous à la section Déchiffrer les données d'un utilisateur avec une ancienne clé ou une clé de délégation). Cela peut être utilisé également pour déchiffrer les documents antérieurement chiffrés avec cette clé.

Le fichier contenant la clé est généré au format *PKCS#12* (extensions *.p12* ou *.pfx*). Si l'utilisateur possède deux clés, chacune sera exportée dans un fichier séparé.

Pour exporter une clé :

1. Sur le poste de l'utilisateur, faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Configuration**.
4. Double-cliquez sur l'icône **Porte-clés**.
   - Si l'utilisateur possède deux clés, choisissez l'onglet **Clé de chiffrement** ou **Clé de signature**.
   - Si l'utilisateur ne possède qu'une seule clé, choisissez l'onglet **Clé personnelle**.
5. Cliquez sur **Opérations** et choisissez **Exporter votre clé** puis passez l'écran d'introduction.



6. Cochez l'une des deux options suivantes. Vous pouvez cochez les deux options.

- L'option **Fournir la parenté de votre certificat** pour associer à la clé le certificat de/des autorités qui ont certifié la clé.
  Seuls les certificats dans l'annuaire de confiance sont affichés. Aucune recherche n'est faite sur l'annuaire LDAP.
- L'option **Fournir les anciens certificats de votre clé** si l'utilisateur a effectué un ou plusieurs renouvellements de certificats mais qu'il souhaite pouvoir déchiffrer des documents chiffrés avec d'anciens certificats.
  Passez ensuite à l'écran suivant.

7. Saisissez le nom du fichier à créer et passez à l'écran suivant.
   Le bouton **Enregistrer sous** permet de modifier le nom du fichier, mais les clés ne sont pas exportées.
8. Saisissez le mot de passe de protection du fichier qui va permettre de chiffrer la clé dans le fichier généré.

> **NOTE**
> Le mot de passe saisi doit faire au moins huit caractères de long et contenir soit un chiffre, soit un signe de ponctuation. Si ce n'est pas le cas, l'exportation est refusée.

9. Passez à l'écran suivant, vérifiez le récapitulatif, puis cliquez sur **Terminer**.
   La clé a été exportée dans le fichier indiqué.

10.9 Déchiffrer les données d'un utilisateur avec une ancienne clé ou une clé de délégation

Avec les clés de déchiffrement, SDS Enterprise permet de déchiffrer des fichiers et messages de manière transparente alors qu'ils sont chiffrés avec une clé différente de la clé de chiffrement courante de l'utilisateur.

SDS Enterprise gère deux types de clés de déchiffrement :

- Les anciennes clés personnelles. Si l'utilisateur effectue le renouvellement de sa clé de chiffrement (ou de la clé personnelle), son ancienne clé est automatiquement déplacée dans les clés de déchiffrement qu'il possède déjà,
- Les clés de délégation. Il s'agit des clés de chiffrement que des collaborateurs peuvent confier à un utilisateur afin de lui permettre de déchiffrer des fichiers ou messages chiffrés à leur attention.

10.9.1 Mettre en place une délégation de déchiffrement

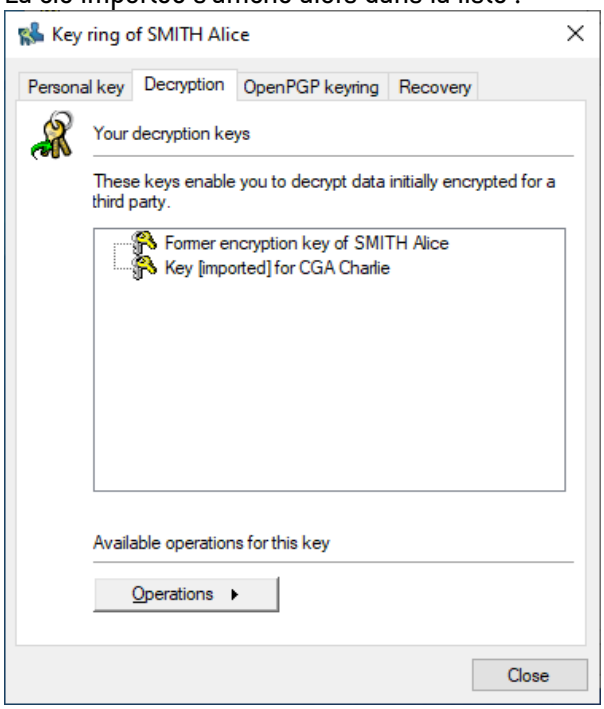
La délégation de déchiffrement consiste à permettre à un utilisateur A de déchiffrer les messages ou fichiers chiffrés pour un utilisateur B en son absence. Il faut pour cela confier à l'utilisateur A la clé de chiffrement de l'utilisateur B.

Muni de la clé de chiffrement, l'utilisateur A ne pourra que déchiffrer les messages. Afin d'être certain qu'il ne puisse signer à la place de l'utilisateur B, nous recommandons d'utiliser des clés de chiffrement et de signature séparées.

Pour mettre en place la délégation, l'utilisateur B doit exporter sa clé de chiffrement depuis son compte SDS Enterprise, puis l'utilisateur A doit l'importer dans son compte SDS Enterprise en suivant les étapes suivantes :

1. L'utilisateur B se connecte à son compte SDS Enterprise depuis l'icône  dans la barre des tâches.
2. Il double-clique sur **Porte-clés**.
3. Dans l'onglet **Chiffrement**, il sélectionne le menu **Opérations** > **Exporter votre clé**.
4. L'utilisateur B transmet le fichier exporté à l'utilisateur A.
5. L'utilisateur A se connecte à son compte SDS Enterprise.
6. Il double-clique sur **Porte-clés**.
7. Dans l'onglet **Déchiffrement**, il sélectionne le menu **Opérations** > **Importer une clé**.
8. Il renseigne le nom du fichier contenant la clé à importer et le mot de passe.
   SDS Enterprise affiche la liste des certificats présents dans le fichier, c'est-à-dire le certificat associé à la clé contenue dans le fichier, avec éventuellement sa parenté.
9. Pour visualiser un certificat de la liste, l'utilisateur peut cliquer dessus.
10. L'utilisateur A coche les certificats parents s'il souhaite les importer dans son annuaire de confiance puis il passe à l'écran suivant.
11. Il sélectionne le type de clé à importer (délégation ou ancienne clé), puis passe à l'écran suivant.

12. Il clique sur **Terminer** et vérifie le résultat de l'opération.
La clé importée s'affiche alors dans la liste :



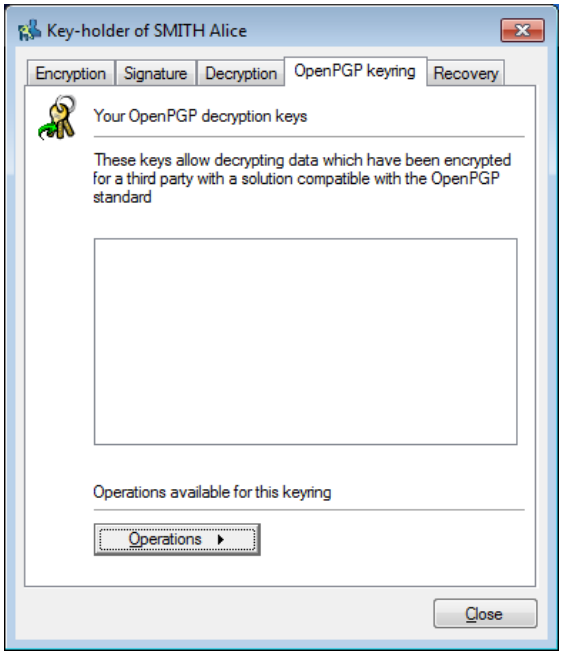
13. Dans la liste, l'utilisateur peut faire un clic droit sur la clé pour la renommer, afficher ses propriétés ou la supprimer quand la délégation n'est plus nécessaire par exemple.

NOTE
Les clés de chiffrement ainsi importées dans un compte ne peuvent pas être exportées. La personne qui a reçu la délégation ne peut donc pas la transmettre à son tour.

10.9.2 Déchiffrer des messages au format OpenPGP

SDS Enterprise gère également les clés de déchiffrement de messages au format OpenPGP. Ces clés sont utilisées par la fonctionnalité Stormshield Data Mail pour lire des messages sécurisés par les applications PGP, GnuPGP ou toute application compatible avec le format OpenPGP.

Lorsque Stormshield Data Mail est installé sur la machine, l'onglet **Porte-clés OpenPGP** dans les propriétés du compte de l'utilisateur permet de gérer ces clés.



Pour importer un porte-clés OpenPGP :

1. Sur le poste de l'utilisateur, faites un clic droit sur l'icône SDS Enterprise depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Configuration**.
4. Double-cliquez sur 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 (*.gpg*, *.pgp*ou *.asc*). Le fichier peut contenir plusieurs clés.
8. Saisissez le mot de passe protégeant le fichier.

10.10 Déchiffrer les données d'un utilisateur avec une clé de recouvrement

La clé de recouvrement permet de sécuriser l'utilisation d'un logiciel de chiffrement fort. Si un utilisateur perd son compte et n'a pas sauvegardé sa clé de chiffrement, la clé de recouvrement, si elle a été définie, permet de déchiffrer toutes les données de l'utilisateur. Par exemple, si un collaborateur quitte une société sans déchiffrer la totalité de ses données, celles-ci pourront être retrouvées en clair.

ATTENTION
La clé de recouvrement peut provenir d'un autre compte SDS Enterprise duquel on aura exporté le certificat public de chiffrement. En raison de l'usage qui peut être fait de la clé de recouvrement, il est primordial de bien protéger le compte de recouvrement.

10.10.1 Consulter les certificats de recouvrement

Pour consulter sur l'agent SDS Enterprise les certificats de recouvrement utilisés pour toute opération de chiffrement :

1. Sur le poste de l'utilisateur, depuis la barre des tâches Windows, faites un clic droit sur l'icône SDS Enterprise  .
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Configuration**.
4. Double-cliquez sur l'icône **Porte-clés**.
5. Sélectionnez l'onglet **Recouvrement**. Les certificats présents dans la liste proviennent de la politique de sécurité. Pour plus d'informations, reportez-vous à la section Permettre le recouvrement de données.

10.10.2 Utiliser une clé de recouvrement pour déchiffrer des données

Vous pouvez utiliser des clés de recouvrement provenant d'un compte SDS Enterprise ou d'une source extérieure.

- Si la clé de recouvrement est issue d'un compte SDS Enterprise, utilisez ce compte pour déchiffrer les données.
- Si la clé de recouvrement provient d'une autre source, exportez de cette autre source la clé privée (et son certificat) au format *PKCS#12* (*.P12*).
  Créez ensuite un compte SDS Enterprise en utilisant ce fichier *.P12* et son mot de passe associé, puis utilisez ce compte SDS Enterprise pour déchiffrer les données. Pour plus d'informations sur la création du compte, reportez-vous à la section Choisir d'importer les clés.
  Vous pouvez créer un compte avec seulement la fonction de déchiffrement.

Vous devriez être en mesure de déchiffrer toutes les données de l'utilisateur, chiffrées par lui-même, ou par ses collaborateurs à son intention si ceux-ci utilisent la même clé de recouvrement. Néanmoins, il vous sera impossible de déchiffrer les données provenant de l'extérieur (par exemple les e-mails reçus) car elles n'ont pas été chiffrées avec la clé de recouvrement.

11. Gérer l'annuaire de confiance depuis l'agent SDS Enterprise

L'annuaire de confiance permet de conserver et d'utiliser les certificats des utilisateurs (et autorités). Cet annuaire est protégé, il ne peut être modifié que par l'utilisateur lui-même. Il est dit de « confiance » c'est-à-dire que tous les certificats qui y sont intégrés sont considérés comme valides par SDS Enterprise.

SDS Enterprise permet d'importer dans l'annuaire de confiance des certificats d'utilisateurs provenant d'un annuaire LDAP. Pour déclarer un annuaire LDAP dans une politique de sécurité, consultez la section Configurer les annuaires d'entreprise.

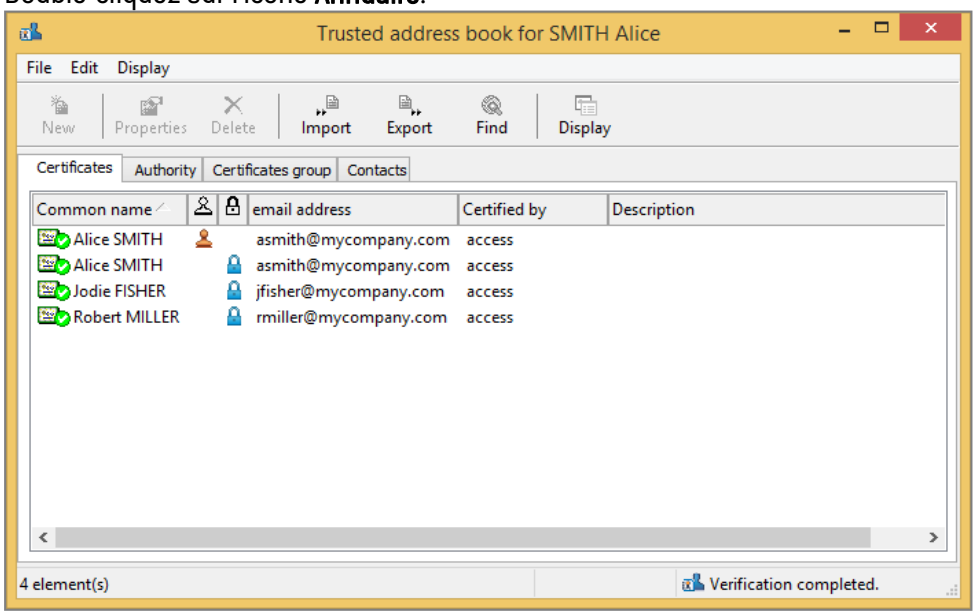
11.1 Consulter l'annuaire de confiance et gérer les certificats depuis l'agent SDS Enterprise

Le menu **Annuaire** de l'agent SDS Enterprise permet de consulter le contenu de l'annuaire de confiance de l'utilisateur, d'importer ou exporter des certificats. Il permet également de consulter la configuration des annuaires LDAP liés à l'annuaire de confiance.

11.1.1 Consulter l'annuaire de confiance

Pour consulter l'annuaire de confiance depuis le poste d'un utilisateur :

1. Faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet **Configuration**.
4. Double-cliquez sur l'icône **Annuaire**.



L'onglet *Certificat* affiche les certificats personnels des utilisateurs, c'est-à-dire les certificats qui ne sont pas des certificats d'autorité.

L'onglet *Autorité* affiche les certificats d'autorité, c'est-à-dire les certificats avec l'extension X.509 émis par une autorité reconnue (voir la note dessous).

L'onglet *Groupes de certificats* affiche les certificats qui regroupent plusieurs certificats en un seul. Par exemple, le chiffrement se fait pour plusieurs personnes avec un seul certificat.

L'onglet *Contacts* permet de créer des raccourcis vers des certificats hébergés dans un annuaire LDAP.

La validité d'un certificat est indiquée par l'icône située à gauche de sa ligne. Les différentes icônes possibles sont indiquées dans le tableau suivant.

	valide	périmé ou non encore valide	contrôlé en erreur
certificat utilisateur			
certificat d'autorité			

Pour un certificat qui n'est pas un certificat d'autorité, deux colonnes indiquent si ce certificat est autorisé à signer et/ou à chiffrer :

-  : le certificat est autorisé à chiffrer,
-  : le certificat est autorisé à signer.

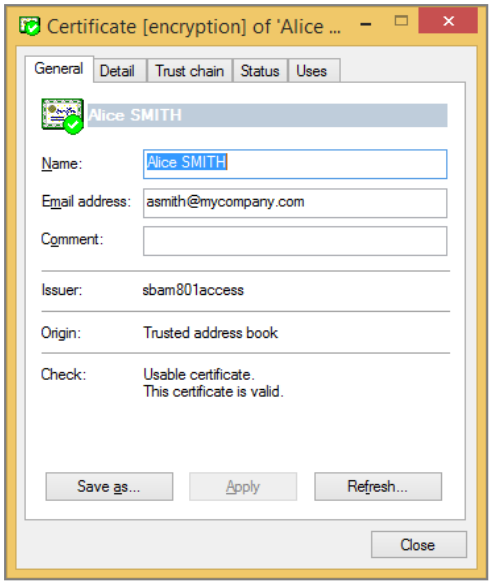
Pour modifier l'affichage des certificats, cliquez sur le bouton **Affichage** ou ouvrez le menu **Affichage>Présentation**.

NOTE

- Un certificat X.509 v3 est un certificat d'autorité s'il possède une extension particulière ("BasicConstraint"). Cette extension peut comporter la longueur maximale d'une chaîne de certification issue de ce certificat.
- Certaines autorités utilisent des certificats racines X.509 v1, version qui ne supporte pas l'extension précitée. SDS Enterprise considère tout certificat X.509 v1 auto-certifié comme un certificat d'autorité. Ces certificats peuvent être utilisés par les différentes fonctionnalités de SDS Enterprise pour signer et chiffrer. Il n'y a pas moyen de connaître les usages et le fait que ce sont explicitement des certificats d'autorité. Il est cependant recommandé de ne pas utiliser de certificats de ce type.
- SDS Enterprise ne prend pas en compte les certificats X.509 version 2.

11.1.2 Afficher un certificat

Pour afficher un certificat, double-cliquez dessus ou sélectionnez-le dans la liste et cliquez sur **Propriétés**.



L'onglet **Général** affiche un résumé du contenu du certificat :

- Le nom usuel et l'adresse e-mail du titulaire,
- Un commentaire que vous renseignez librement (celui-ci ne fait pas partie du certificat),
- Le nom usuel de l'autorité de certification,
- La provenance du certificat (annuaire de confiance, annuaire LDAP, e-mail),
- L'état après vérification ; un message d'erreur s'affiche, si besoin.

De cet onglet, vous pouvez aussi exporter le certificat, en cliquant **Enregistrer sous**.

L'onglet **Détail** affiche la totalité du contenu du certificat.

Des informations complémentaires sur les différents champs peuvent être obtenues en consultant la norme X.509 V3 ou la RFC3280.

En cas d'erreur ou d'avertissement, le message d'explication est répété dans cette fenêtre immédiatement après la première ligne.

L'onglet **Parenté** reconstitue et affiche la chaîne de certification et indique le résultat des contrôles effectués sur cette chaîne.

> **NOTE**
> Les certificats participant à la chaîne de parenté sont uniquement recherchés dans l'annuaire de confiance. Aucune recherche LDAP n'est effectuée pour rechercher cette chaîne.

En cliquant sur un des certificats de la chaîne, il est possible d'en visualiser le contenu.

11.1.3 Importer des certificats

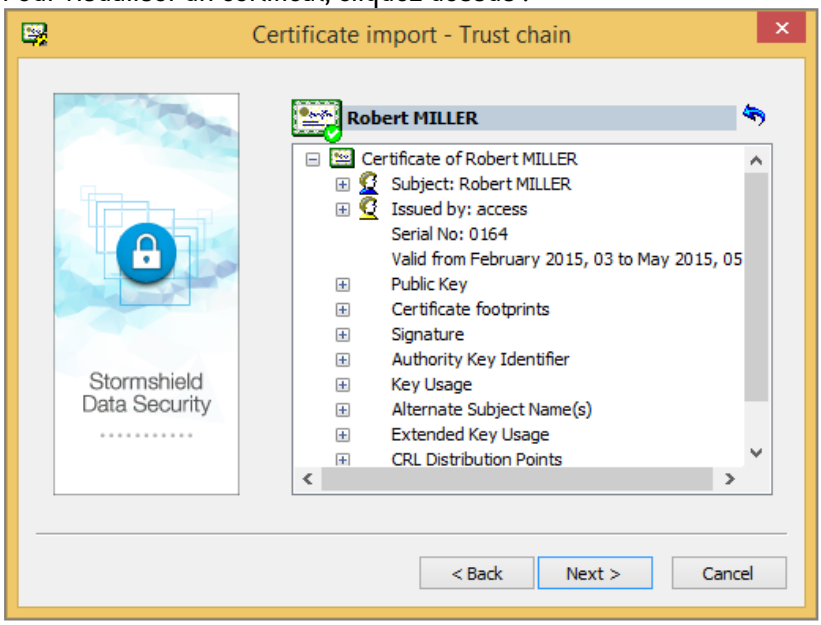
Vous pouvez importer dans l'annuaire de confiance :

- Des certificats seuls, chaque certificat étant stocké dans un fichier au format binaire (extension *.cer*) ou base 64 (extension *.crt*),
- Des listes de certificats, chaque liste provenant d'un fichier au format PKCS#7 (extension *.p7b* ou *.p7c*),
- Une sauvegarde complète de l'annuaire (extension *.p7z*),
- Des certificats provenant d'un annuaire LDAP.

Importer des certificats depuis le poste de travail

Pour importer des certificats, vous pouvez utiliser l'assistant ou les glisser-déposer.

1. Pour cela, dans la fenêtre principale de l'annuaire de confiance, cliquez sur le bouton **Importer** ou glissez-déposez un certificat ou une liste de certificats depuis le Bureau ou un dossier de l'Explorateur Windows.
2. Saisissez le nom du fichier contenant le ou les certificats à importer et passez à l'écran suivant. SDS Enterprise affiche tous les certificats qu'il contient.
3. Pour visualiser un certificat, cliquez dessus :



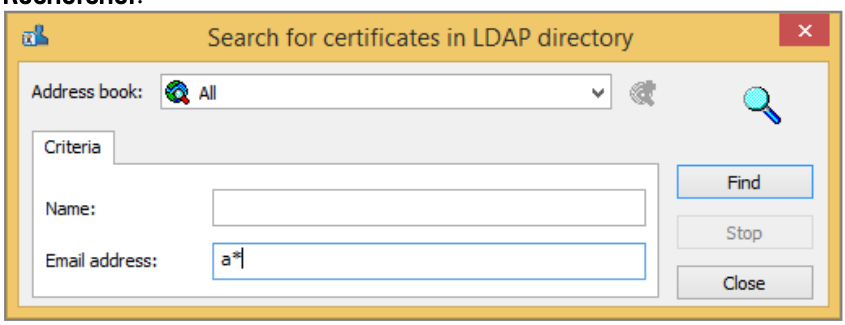
Les fichiers sont vérifiés pendant l'import. Le résultat est indiqué avec un signe de validation vert, jaune, ou rouge, sur l'icône du certificat. Quel que soit le statut valide ou non valide, le certificat est importé.

4. Pour revenir à la liste des certificats, cliquez sur le bouton .
5. Pour vérifier qu'un certificat est bien celui d'un utilisateur, contactez-le et vérifiez l'empreinte affichée.
6. Pour importer un ou plusieurs certificats de la liste, cochez-les et cliquez sur **Suivant** pour vérifier le récapitulatif, puis cliquez sur **Terminer**.

Importer un certificat publié à partir d'un annuaire LDAP

SDS Enterprise permet d'importer dans l'annuaire de confiance le certificat d'un correspondant publié à partir un annuaire LDAP :

1. Pour cela, dans la fenêtre principale de l'annuaire de confiance, cliquez sur le bouton **Rechercher**.



2. Renseignez l'adresse du serveur LDAP à interroger et les critères de recherche : nom et/ou adresse e-mail. Vous pouvez inclure dans vos critères des caractères génériques tels que "*" ou "?" si l'annuaire interrogé les accepte.
3. Cliquez sur **Rechercher** pour lancer la recherche ; la fenêtre affiche le résultat de la recherche. SDS Enterprise n'affiche dans cette fenêtre que les certificats, c'est-à-dire les certificats présents dans l'annuaire, valides (par rapport à leur période de validité) et utilisables pour le chiffrement et/ou la signature électronique.
4. Pour afficher le détail d'un certificat, sélectionnez-le et cliquez sur **Aperçu**.
5. Pour importer dans l'annuaire un ou plusieurs certificats, sélectionnez-les et cliquez sur **Importer**.

Le ou les annuaires LDAP disponibles dans cette fenêtre ont été au préalable déclarés dans la politique de sécurité dans SDMC. Pour plus d'informations, reportez-vous à la section Configurer les annuaires d'entreprise.

11.1.4 Exporter des certificats ou l'annuaire de confiance

Si un utilisateur détient dans son annuaire de confiance des certificats que certains de ses correspondants ne possèdent pas, il peut les leur fournir en exportant ces certificats.

Pour les exporter, il est possible d'utiliser l'assistant ou le glisser-déposer.

Pour exporter des groupes de certificats, reportez-vous à la section Exporter un groupe de certificats.

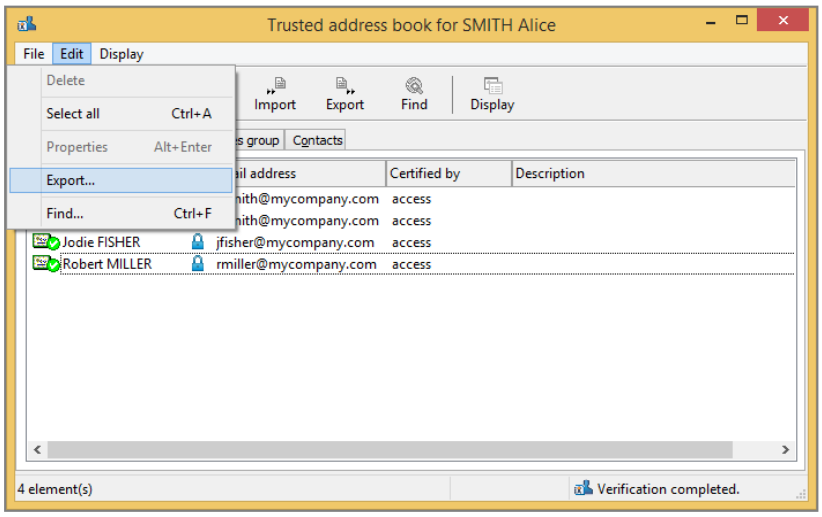
Vous pouvez également exporter la totalité d'un annuaire de confiance dans un fichier propre à SDS Enterprise, portant l'extension *.p7z*.

Ce fichier contiendra l'ensemble des certificats de l'annuaire, leurs personnalisations éventuelles, les groupes de certificats ainsi que les certificats des contacts.

Exporter par l'assistant

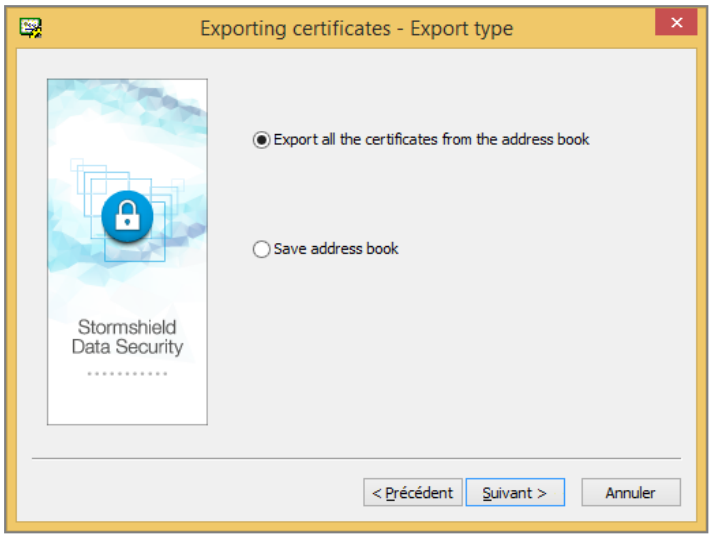
Pour exporter un ou plusieurs certificats d'un annuaire de confiance :

1. Sélectionnez-les dans l'annuaire.
2. Cliquez sur le bouton **Exporter** ou choisissez le menu **Édition > Exporter**.



Passez l'écran d'introduction.

3. Sélectionnez le type d'export.



L'intitulé de la première option diffère en fonction des éléments que vous avez sélectionnés dans l'annuaire :

- **Exporter tous les certificats de l'annuaire** : ce choix est proposé lorsqu'aucun certificat n'a été sélectionné dans l'annuaire. Dans ce cas tous les certificats seront exportés dans un fichier de type *.p7b* ou *.p7c*.
- **Exporter les certificats sélectionnés** : ce choix est proposé lorsque plusieurs certificats ou groupes ont été sélectionnés dans l'annuaire. Dans ce cas seuls les certificats sélectionnés seront exportés dans un fichier de type *.p7b* ou *.p7c*.
- **Exporter le certificat sélectionné** : ce choix est proposé lorsque vous n'avez sélectionné qu'un seul certificat dans l'annuaire. Dans ce cas le certificat sélectionné sera exporté dans un fichier de type *.cer* ou *.crt*.

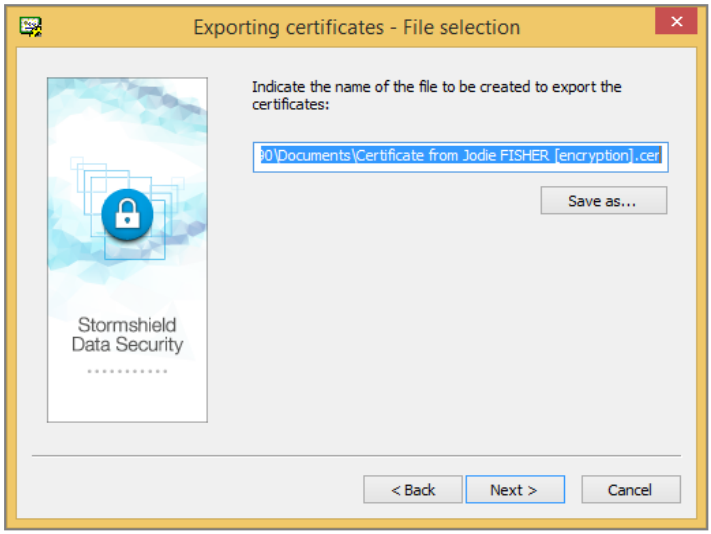
L'option **Sauvegarder l'annuaire** propose dans tous les cas de sauvegarder tous les certificats de l'annuaire avec les informations personnalisées qui leur sont associées.

4. Si vous avez sélectionné la première option de la fenêtre **Type d'export** et dans ce cas seulement, la fenêtre **Options** s'ouvre et propose d'ajouter des éléments supplémentaires au fichier d'export :
   - **Inclure la parenté** : permet d'exporter la parenté du certificat. Dans ce cas, les certificats d'autorités qui sont partagés ne sont pas dupliqués.
   - **Inclure les groupes et les contacts**: permet d'inclure dans le fichier d'export les groupes et les certificats des contacts. Pour plus d'informations sur l'export de groupes, reportez-vous à la section Exporter un groupe de certificats.

   Cette dernière case est cochée par défaut lorsque des groupes ont été sélectionnés dans l'annuaire. Elle est également grisée pour éviter de la décocher au risque de générer un fichier d'export vide.

> **NOTE**
> Si vous cochez cette option alors qu'aucun groupe n'est sélectionné dans l'annuaire, tous les groupes seront exportés.

5. Indiquez un nom et un emplacement pour le fichier d'export. L'assistant propose un nom par défaut, adapté au type d'export à effectuer. Sinon, entrez les informations directement dans la zone d'édition ou en utilisant le bouton **Enregistrer sous**.



> **NOTE**
> L'assistant corrige automatiquement l'extension du fichier si elle ne correspond pas au type de fichier d'export qui va être généré.

6. Un récapitulatif vous permet de vérifier les informations avant de commencer l'export.
7. Les certificats que vous avez sélectionnés ont été exportés dans le fichier indiqué. Vous pouvez maintenant envoyer le fichier en utilisant un e-mail, une clé USB, un fichier partagé, etc., ou bien l'utiliser pour restaurer le contenu d'un annuaire si le fichier exporté porte l'extension *.p7z*.

Exporter par glisser-déposer

Il est possible d'exporter des certificats en effectuant un glisser-déposer à partir de l'annuaire de confiance.

1. Sélectionnez un ou plusieurs certificats dans l'annuaire de confiance.
2. Faites un glisser-déposer vers le Bureau, vers un dossier dans l'Explorateur Windows ou vers une autre application Windows susceptible de recevoir un fichier.

Si un seul certificat est exporté, le fichier résultant s'appelle *<CommonName>.cer*. Il n'est pas possible de choisir un autre nom ou un autre format. Il n'y a pas de distinction entre les certificats de signature et de chiffrement au niveau du nom.

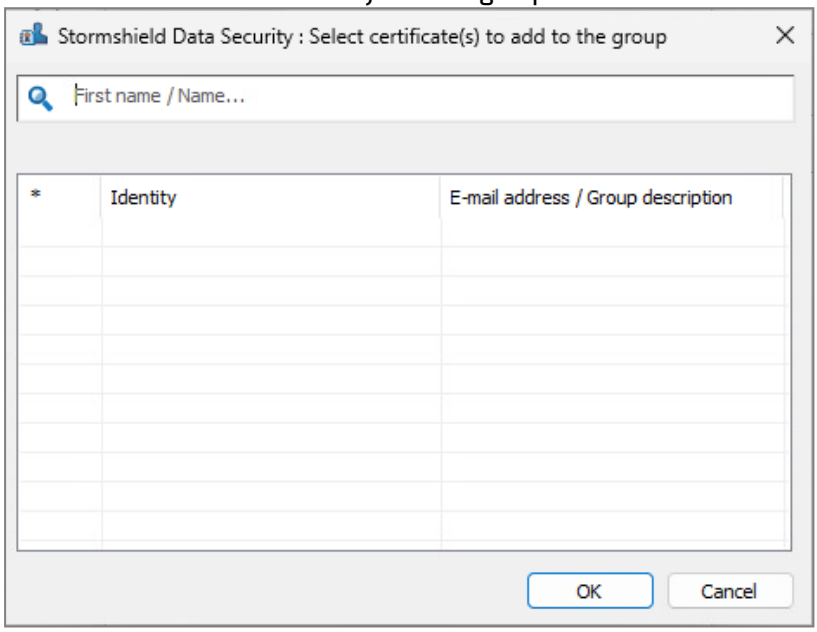
Si plusieurs certificats sont exportés, le fichier résultant s'appelle *Certificate List.p7b*. Il n'est pas possible de choisir un autre nom ou un autre format.

11.1.5 Créer un groupe de certificats

Créer un groupe de certificats simplifie le chiffrement de fichiers à destination de groupes de destinataires fixes. Au lieu de sélectionner chaque destinataire, vous sélectionnez un groupe prédéterminé. Dans ce cas, le ou les documents sont chiffrés pour chaque destinataire ayant un certificat valide.

Seuls les groupes sauvegardés dans l'annuaire de confiance sont acceptés par SDS Enterprise. Vous ne pouvez pas importer ou utiliser de groupes provenant d'annuaires LDAP.

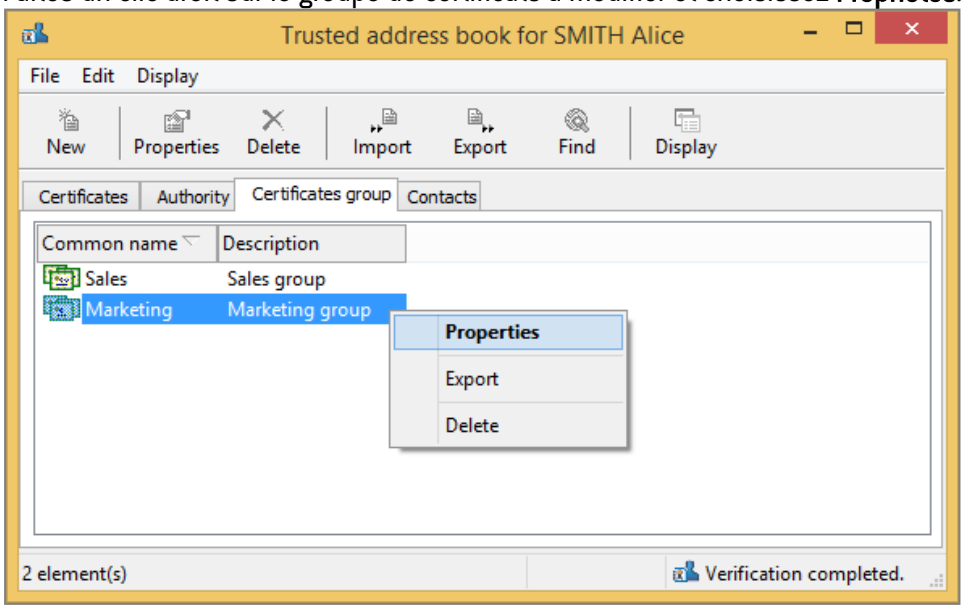
1. Pour créer un groupe de certificats, choisissez l'onglet **Groupes de certificats** dans l'annuaire de confiance.
2. Faites un clic droit dans la fenêtre et choisissez **Nouveau**.
3. Entrez les informations sur le groupe et cliquez sur **Ajouter** pour ajouter des certificats.
4. Recherchez les utilisateurs à ajouter au groupe.



5. Cliquez sur **OK** lorsque vous avez fini.
6. Cliquez sur **OK** pour fermer la fenêtre du groupe.

11.1.6 Modifier un groupe de certificats

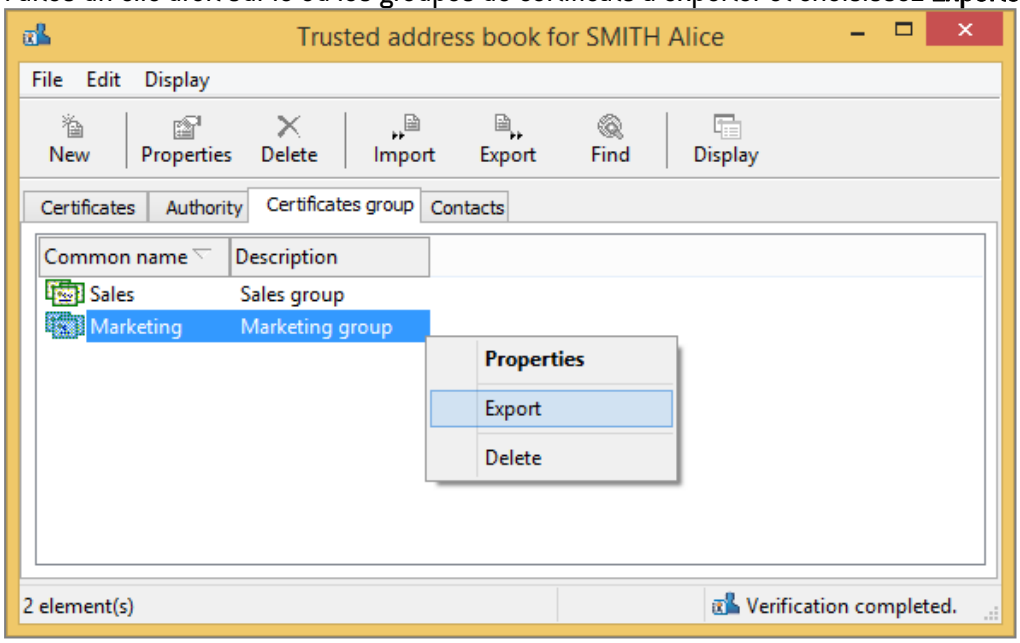
1. Choisissez l'onglet **Groupes de certificats** dans l'annuaire de confiance.
2. Faites un clic droit sur le groupe de certificats à modifier et choisissez **Propriétés**.



3. Ajoutez ou retirez les certificats.
   Vous pouvez aussi modifier le nom du groupe et la description.
4. Cliquez **OK** pour confirmer vos modifications.

11.1.7 Exporter un groupe de certificats

1. Faites un clic droit sur le ou les groupes de certificats à exporter et choisissez **Exporter**.



   Il est possible de sélectionner plusieurs groupes avant de demander l'export. Dans ce cas, tous les certificats présents dans les groupes seront placés dans le fichier d'export (avec suppression des éventuels doublons).

2. Les étapes suivantes sont les mêmes que pour l'export des certificats. Référez-vous à la section Exporter des certificats ou l'annuaire de confiance.

11.1.8 Supprimer un groupe de certificats

1. Sélectionnez-le dans la liste de groupes de l'annuaire de confiance.
2. Effectuez un clic droit sur le groupe à supprimer et cliquez sur le bouton **Supprimer**.

Pour sélectionner plusieurs groupes, utilisez les touches habituelles de Windows (MAJ et CTRL).

Pour supprimer tous les groupes, effectuez un clic droit sans sélectionner un seul groupe et cliquez sur **Sélectionner tout** puis cliquez sur **Supprimer**.

11.2 Échanger des certificats à l'aide de Stormshield Data Mail

Les échanges de certificats entre utilisateurs sont assez rares dans la pratique. Les annuaires LDAP sont en général utilisés pour le partage des certificats entre les correspondants. Les échanges manuels ne sont donc utilisés que pour des échanges ponctuels entre correspondants d'entreprises différentes ou pour des tests.

La procédure d'échange de certificats est différente si vous avez la fonctionnalité Stormshield Data Mail. Si vous n'avez pas Stormshield Data Mail, vous devez utilisez les procédures d'export et d'import décrites à la section Consulter l'annuaire de confiance et gérer les certificats depuis l'agent SDS Enterprise, puis expédier votre fichier de certificats par un moyen approprié.

En signant un message, Stormshield Data Mail facilite les échanges de certificats en joignant automatiquement aux messages sécurisés les certificats de signature et de chiffrement ainsi que toute leur parenté.

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

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

1. Dans Microsoft Outlook, si un correspondant a transmis son certificat en signant un message avec SDS Enterprise, 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. Pour plus d'informations, reportez-vous à la section *Sécuriser des messages électroniques* du *Guide d'utilisation avancée SDS Enterprise*.

11.3 Travailler hors connexion

SDS Enterprise vérifie la connexion physique au réseau local d'entreprise.

Lorsque l'utilisateur est connecté à son réseau (travail en ligne), chaque fois qu'il recherche un certificat sur son annuaire LDAP, le ou les certificats trouvés sont enregistrés dans un fichier temporaire local (cache).

Lorsqu'il est déconnecté de son réseau (travail hors connexion), SDS Enterprise détecte la déconnexion : les recherches de certificats sont alors redirigées vers le cache local qui a été alimenté lors de sa connexion.

Ce mécanisme permet de chiffrer des fichiers et mails adressés à des collaborateurs même lorsque l'utilisateur n'est pas connecté à son réseau d'entreprise : il faut simplement avoir préalablement utilisé au moins une fois le certificat de chaque collaborateur.

Il en est de même des listes de révocation : elles sont téléchargées en ligne, enregistrées dans un fichier local consultable quand l'utilisateur travaille hors connexion.

SDS Enterprise permet de forcer le fonctionnement en mode hors connexion, par exemple si le réseau local rencontre des problèmes. Pour cela :

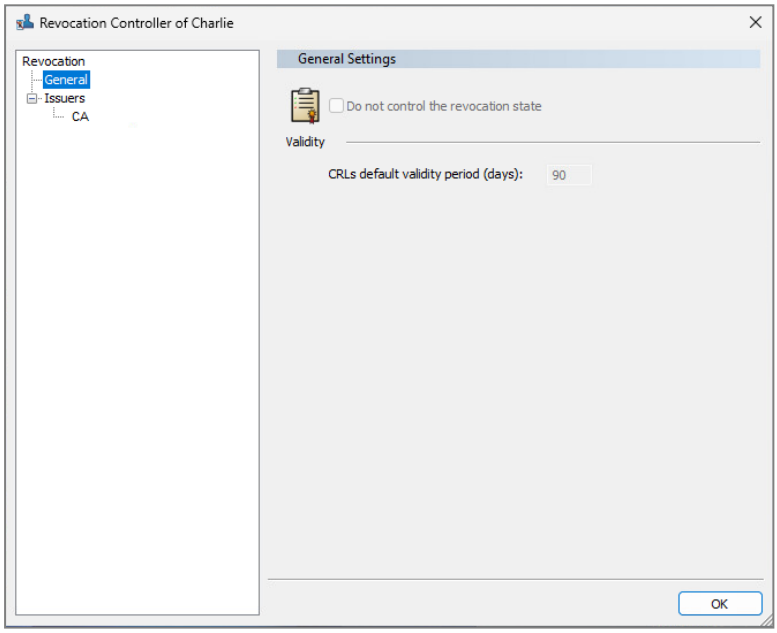
1. Effectuez un clic-droit sur l'icône de SDS Enterprise dans la barre des tâches.
2. Sélectionnez **Accès réseau > Travailler hors connexion**.
3. Désélectionnez **Accès réseau > Rétablir la connexion automatiquement**.
4. En sélectionnant à nouveau **Rétablir la connexion automatiquement**, SDS Enterprise détecte automatiquement la connexion au réseau d'entreprise et repasse automatiquement en fonctionnement en ligne.

12. Consulter les autorités de certification depuis l'agent SDS Enterprise

Depuis l'agent SDS Enterprise, le contrôleur de révocation permet de consulter les autorités de certification émettrices des certificats des utilisateurs, ainsi que les points de distribution des listes de révocation (CRL) pour chaque autorité.

Pour afficher le contrôleur de révocation sur les postes des utilisateurs :

1. Faites un clic droit sur l'icône SDS Enterprise depuis la barre des tâches Windows.
2. Sélectionnez **Propriétés**.
3. Dans l'onglet **Configuration**, double-cliquez sur l'icône **Révocation**.



Le contrôleur de révocation est en lecture seule. Pour configurer la révocation des certificats des utilisateurs, vous devez spécifier des autorités de certification dans les politiques de sécurité, ainsi que les points de distribution des CRL associés. Pour plus d'informations, reportez-vous à la section Ajouter des autorités de certification et configurer le contrôle de révocation des certificats.

12.1 Télécharger une CRL

- Pour télécharger une CRL depuis le contrôleur de révocation, effectuez un clic-droit sur le nom de l'autorité dans la liste **Émetteurs**, puis **Télécharger** .

NOTE
Le téléchargement manuel est à réserver à des cas particuliers notamment pour des utilisateurs itinérants qui n'ont que très rarement accès au réseau de l'entreprise.

12.2 Supprimer une autorité

Il est possible de supprimer une autorité du contrôleur de révocation.

- Sélectionnez l'autorité dans la liste **Émetteurs** et cliquez sur **Supprimer**.

Cette action n'a aucun effet sur les performances du produit et sert uniquement à nettoyer la liste des autorités prises en compte.

13. Configurer et utiliser les fonctionnalités avancées de l'agent

Cette section regroupe un ensemble d'informations techniques (astuces, limites, précaution à prendre) sur les fonctionnalités de l'agent.

13.1 Stormshield Data Virtual Disk

13.1.1 Effectuer un recouvrement de volume

Effectuer un recouvrement avec le fichier container

Le support physique d'un volume sécurisé est un fichier container portant l'extension *.vbox*, qui contient :

- les éléments cryptographiques nécessaires au montage du volume : la clé symétrique de chiffrement du volume est protégée avec la clé publique de chacun des utilisateurs autorisés et avec chaque clé de recouvrement,
- le contenu proprement dit du volume : fichiers stockés dans le volume et système de fichier.

Les éléments cryptographiques sont systématiquement sauvegardés dans un "fichier de secours" portant l'extension *.vboxsave* à la création du volume, puis à chaque modification de la liste des utilisateurs.

Le recouvrement d'un volume Stormshield Data Virtual Disk est identique au changement de propriétaire décrit dans le *Guide d'utilisation* du produit. Simplement, l'utilisateur effectuant la demande de changement de propriétaire n'est pas le propriétaire initial mais l'utilisateur dont le certificat de chiffrement a été défini comme certificat de recouvrement.

Le recouvrement consiste donc à définir un nouvel utilisateur comme étant le propriétaire du volume. Ce nouveau propriétaire peut ensuite faire toutes les opérations qu'il souhaite.

Effectuer un recouvrement sans le fichier container

Cependant, par rapport au changement simple de propriétaire, il est possible d'effectuer un recouvrement sans disposer du fichier container mais uniquement avec le volume VBOXSAVE.

Cette procédure est notamment utile pour effectuer des recouvrements à distance. L'utilisateur disposant du fichier container n'a pas besoin de le transmettre dans sa totalité pour que le recouvrement soit effectué et ne transmet que le fichier *.vboxsave*.

Pour cela, il faut que l'utilisateur désirant un recouvrement transmette le fichier *.vboxsave* à l'administrateur chargé du recouvrement. Celui-ci procède comme pour un changement de propriétaire puis retourne le fichier *.vboxsave* à l'utilisateur ayant effectué la demande. Celui-ci n'a plus qu'à mettre à jour le fichier *.vboxsave* et continuer la procédure de changement de propriétaire comme si c'était lui qui avait mis à jour le fichier *.vboxsave*.

13.1.2 Démonter un volume en force

Il n'est pas conseillé de démonter un volume Stormshield Data Virtual Disk "en force", c'est-à-dire quand il y a des fichiers ouverts dessus. Si une telle opération s'avère cependant nécessaire, il est fortement recommandé de vérifier le volume en utilisant l'outil Windows de

vérification de disque lors de son prochain montage, avant toute utilisation.

13.1.3 Dupliquer un volume

Si un volume sécurisé est dupliqué en copiant le fichier container *.vbox*, les deux exemplaires résultant ne peuvent pas être montés simultanément sur un même poste.

De façon générale, il n'est pas recommandé de dupliquer des volumes par copie du fichier container *.vbox* ; cela ne doit être utilisé que pour des sauvegardes.

13.1.4 Utiliser un volume dans un contexte multi-sessions Windows

Pour faciliter son intégration au sein de Microsoft Windows, un volume Stormshield Data Virtual Disk se comporte comme un volume de stockage standard.

Par conséquent, un volume chiffré monté dans une session Windows est accessible depuis les autres sessions Windows ouvertes en parallèle sur le poste de travail.

Afin d'éviter ceci, l'utilisateur doit définir le verrouillage de son compte SDS Enterprise lors du verrouillage de sa session Windows.

Le verrouillage a pour effet de démonter les volumes chiffrés montés dans la session. Cependant le démontage forcé peut avoir des conséquences sur les fichiers ouverts sur ce volume. L'utilisateur doit veiller à enregistrer ses modifications avant tout verrouillage de session.

Sur une version serveur de Windows, un utilisateur distant ne voit pas les volumes Stormshield Data Virtual Disk montés par les autres utilisateurs distants connectés au même serveur. Il est néanmoins conseillé d'appliquer le verrouillage automatique car les volumes disques sont simplement masqués. Les données qu'ils contiennent sont donc potentiellement accessibles.

13.1.5 Connaître les limitations de Stormshield Data Virtual Disk

- La taille maximale d'un volume Stormshield Data Virtual Disk est 2048 Go (2 To).
- Un volume de plus de 2 Go ne peut pas être formaté en FAT16 (limitation de FAT16).
- Un volume de moins de 2.5 Mo ne peut pas être formaté NTFS (limitation de NTFS).
- Il peut arriver que l'icône d'un volume Stormshield Data Virtual Disk dans l'explorateur soit incorrecte (soit une icône de disque normal, soit une icône de document).

13.2 Stormshield Data File

Si des permissions (au sens NTFS) sont définies sur un fichier, elles sont perdues après chiffrement ou déchiffrement par Stormshield Data File.

Si les permissions de Windows doivent être mises en œuvre sur des fichiers confidentiels sécurisés par Stormshield Data File, il faut définir ces permissions au niveau des dossiers contenant ces fichiers, et non sur les fichiers eux-mêmes.

13.3 Stormshield Data Mail

13.3.1 Informations sur le format RTF

Le format RTF n'est pas supporté par Stormshield Data Mail car il ne permet pas d'assurer une interopérabilité fiable avec le mécanisme de sécurisation de SDS Enterprise. 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 permet l'interopérabilité.

13.3.2 Utiliser le 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 Stormshield Data File) 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'accès aux clés privées de l'utilisateur pendant le transchiffrement nécessite d'être connecté à SDS Enterprise.

Il est donc recommandé de désactiver les options de déconnexion automatique et de verrouillage de session sur écran de veille lorsque le nombre de messages à transchiffrer est important, la durée de traitement étant proportionnelle au nombre de messages à traiter.

Un message sécurisé ne sera pas transchiffré si la clé courante de chiffrement de l'utilisateur est celle qui a servi à chiffrer originellement le message.

De même, un message qui a déjà été transchiffré par la clé courante ne sera pas transchiffré à nouveau, tant que la clé courante de l'utilisateur n'est pas mise à jour.

13.3.3 Paramétrer l'annuaire LDAP pour les certificats comportant plusieurs adresses e-mail

Si un destinataire possédant plusieurs adresses e-mail dans son certificat est absent de l'annuaire de confiance SDS Enterprise mais est présent sur l'annuaire LDAP, une boîte de dialogue indiquant que "le certificat n'a pas été trouvé dans votre annuaire de confiance" peut s'ouvrir à l'envoi d'un message chiffré vers ce destinataire.

Dans cette situation spécifique, vous pouvez paramétrer l'annuaire LDAP pour faire en sorte de retrouver le certificat à l'envoi du message chiffré.

Pour cela, vérifiez que l'attribut « proxyAddresses » de l'utilisateur dans l'annuaire LDAP contient bien toutes les adresses e-mail secondaires de l'utilisateur.

Dans cet attribut, chaque adresse e-mail secondaire doit être précédée de « smtp: », alors que l'adresse principale est précédée de « SMTP: ».

Cet attribut peut être mis à jour via des serveurs de messagerie d'entreprise de type Exchange.

13.3.4 Vérifier la cohérence des adresses e-mail

Lors de l'envoi de message, le meilleur certificat disponible pour chaque destinataire est recherché. Si ce certificat provient de l'annuaire LDAP, une vérification de cohérence est effectuée entre l'adresse e-mail du destinataire et celle contenue dans ce certificat. En cas de différence, le certificat est rejeté, et l'envoi du message peut être annulé.

Si vous utilisez des alias internes pour les adresses des utilisateurs, ce mécanisme peut devenir inopportun.

- Pour désactiver ce mécanisme de vérification de cohérence des adresses e-mail sur un poste utilisateur, positionnez la valeur **DWORD CheckLDAPCertificateEmailAddress** à 0 dans la clé de registre HKLM\SOFTWARE\Arkoon\Security BOX Enterprise\Mail.

NOTE
La vérification de cohérence d'adresses e-mail a été implémentée pour des raisons de sécurité. Il est donc recommandé de ne pas la désactiver si ce n'est pas absolument nécessaire.

13.4 Stormshield Data Team

INFORMATION
Stormshield ne proposera plus d'évolutions fonctionnelles de la fonctionnalité Stormshield Data Team à partir de janvier 2025. La fonctionnalité passera en mode maintenance à partir de cette date.

13.4.1 Restriction en environnement DFS

- Une racine DFS ne peut pas être chiffrée.
- Les comptes SDS Enterprise ne doivent pas être hébergés sur un partage DFS.

13.4.2 Gérer le dossier temporaire utilisateur (%TEMP%)

Il ne faut pas indiquer plusieurs collaborateurs sur une règle affectant le dossier temporaire du profil Windows. Ce dossier est utilisé par les applications pour stocker des fichiers temporaires propres à l'utilisateur.

Si cette règle n'est pas respectée, des blocages peuvent se produire.

13.4.3 Gérer le dossier temporaire du système

Ce dossier est utilisé par les processus système, les services par exemple, pour stocker des fichiers temporaires et il est partagé avec les autres utilisateurs du système.

Ce dossier peut être par exemple **C:\windows\temp**. La localisation exacte dépend de l'installation du système d'exploitation.

Ce dossier ne doit pas être chiffré avec Stormshield Data Team.

13.4.4 Déplacer les dossiers disponibles hors connexion

Il est possible via l'utilitaire *cachemov.exe* de déplacer le dossier système - *<%WINDIR%>\CSC* - qui contient les fichiers disponibles hors connexion.

La prise en charge de cet environnement particulier nécessite de modifier la configuration des postes de travail via la base de registre. Pour plus d'informations, reportez-vous à la section *Déplacer les dossiers disponibles hors connexion* du *Guide de configuration avancée*.

13.4.5 Maintenir les performances du poste de travail

L'utilisation de Stormshield Data Team peut provoquer un ralentissement du fonctionnement des postes de travail des utilisateurs. Afin de conserver les performances habituelles, vous pouvez modifier la configuration des postes de travail via la base de registre. Pour plus d'informations, reportez-vous à la section *Maintenir les performances du poste de travail* du *Guide de configuration avancée*.

13.4.6 Déplacer un dossier intra-volume

Le déplacement de dossier intra-volume est interdit lorsque les dossiers source et destination n'ont pas la même sécurité.

Si l'opération est effectuée dans l'explorateur Windows, celui-ci remplace l'opération de déplacement par l'enchaînement `Copie + Suppression de la source`. Dans ce cas, le dossier "déplacé" se verra appliquer la sécurité du dossier destination.

13.4.7 Interdire d'accéder à un fichier chiffré si le certificat est révoqué

Stormshield Data Team permet l'interdiction d'accéder à un fichier chiffré à un utilisateur dont le certificat de la clé de chiffrement est révoqué.

Dans ce cas :

- toute opération sur les fichiers sécurisés par Stormshield Data Team (ouverture, création, renommage, déplacement et suppression) est refusée.

Ces opérations échouent même si le fichier est chiffré avec une ancienne clé de chiffrement de l'utilisateur.

- toute opération sur les règles Team est impossible. Les interfaces utilisateurs sont grisées et permettent uniquement la consultation des paramètres des règles.

Stormshield Data Team utilise la configuration du contrôleur de révocation définie au niveau du compte de l'utilisateur. Veillez en particulier :

- à ne pas autoriser l'utilisateur à désactiver le contrôle de révocation,
- à configurer correctement la règle de téléchargement des listes de révocation.

13.4.8 Modifier les dates de derniers accès

Certaines solutions, comme les solutions d'archivage, se basent sur les dates de derniers accès de fichiers pour effectuer leurs traitements. Toutefois, lorsque Stormshield Data Team est installé sur un poste, la date de dernier accès d'un fichier est modifiée lors d'un parcours de répertoire.

Vous pouvez maîtriser la restauration des dates de dernier accès sur les fichiers et supprimer ainsi la modification de la date de dernier accès des ouvertures de fichiers par Stormshield Data Team. Pour cela, modifiez la configuration des postes de travail via la base de registre. Pour plus d'informations, reportez-vous à la section *Modifier les dates de dernier accès* du *Guide de configuration avancée*.

13.4.9 Utiliser le cache en réseau

Lors d'une utilisation du cache en réseau, les fichiers et répertoires mais également les règles, peuvent être changés hors du contrôle du système de fichiers local de l'utilisateur. Si une modification est effectuée par un utilisateur sur le réseau, les autres postes qui utilisent le

partage peuvent avoir pendant un certain temps des entrées de cache incorrectes et donc des statuts incorrects dans l'explorateur Windows. En conséquence, les nouveaux états ne seront pas pris en compte immédiatement.

Pour limiter ces incohérences, vous pouvez prendre les mesures suivantes :

- Sécurisez un dossier dès sa création lorsqu'il est encore vide,
- Prévenez les utilisateurs pour qu'ils évitent de se servir du partage au moment critique,
- Évitez de détruire un dossier puis de le recréer avec le même nom et des caractéristiques différentes. Si cette opération doit être effectuée, laissez passer entre les deux opérations le temps nécessaire à la mise à jour des caches (délai de 15 minutes ou redémarrage de la machine de l'utilisateur pour prise en compte instantanée),
- Effectuez les opérations conséquentes sur une arborescence de fichiers (sécurisation/désécurisation) à des heures où pas ou peu d'utilisateurs sont connectés (par exemple pendant la pause déjeuner ou en fin de journée).

L'ajout ou la suppression de collaborateurs à une règle existante ne pose pas de problème particulier et il n'y a donc pas de précaution à prendre.

14. Gérer les clés d'accès à l'API publique de SDMC

SDMC dispose d'une API publique permettant d'interroger votre serveur SDMC via vos propres outils d'orchestration, pour en extraire par exemple les logs d'administration.

Pour autoriser ces requêtes, vous devez fournir des clés aux outils tiers.

L'administrateur doit disposer du droit *Gérer les clés API*. Pour plus d'informations, reportez-vous à la section Gérer les administrateurs dans SDMC.

Le menu **Clés API** de la console SDMC permet de consulter les clés API générées pour un compte d'entreprise, d'en créer et également de les révoquer en les supprimant. Une fois générée dans SDMC, vous ne pouvez plus consulter la valeur des clés. Assurez-vous de les conserver dans un emplacement sécurisé.

Par défaut, les clés API expirent au bout d'un an.

ATTENTION
Une clé API donne directement des droits d'administration sur le serveur SDMC. Pour éviter toute faille de sécurité, assurez-vous que les postes depuis lesquels les requêtes sur l'API SDMC sont effectuées soient sains et dans un périmètre d'administration restreint, par exemple sur un réseau d'administration dédié.

Pour visualiser des exemples d'utilisation de l'API avec des clés, consultez https://github.com/stormshield/sds-sample-api.

Pour des informations plus générales sur l'API SDMC et son utilisation, consultez la documentation de l'API.

14.1 Générer une clé API

1. Sélectionnez le menu de gauche **Clés API**.
   Ce menu n'est visible que si vous disposez du droit d'administration *Gérer les clés API*.
2. Cliquez sur **Ajouter** en haut à droite.
3. Entrez un nom pour la clé en caractères alpha-numériques. Le nom ne peut pas dépasser 200 caractères.
4. Cliquez sur **Ajouter**.
   La zone **Clé API** indique la chaîne de caractères correspondant à la clé.
5. Cliquez sur **Copier** et collez cette chaîne dans un emplacement sécurisé. Cette étape est indispensable si vous voulez utiliser la clé, car pour des raisons de sécurité, elle ne sera ensuite plus affichée.
6. Cliquez sur **Fermer** pour revenir à la fenêtre des clés API.
   La clé générée s'affiche dans la liste. Elle est valable pendant un an et sa date d'expiration est affichée. La fenêtre affiche toutes les clés générées pour votre compte d'entreprise.

14.2 Révoquer une clé API

Pour révoquer une clé API, c'est-à-dire la rendre inutilisable pour faire des requêtes auprès de l'API, vous devez la supprimer de la liste.

1. Sélectionnez le menu de gauche **Clés API**.
2. Cliquez sur  à droite de la clé que vous souhaitez révoquer.
3. Cliquez sur **Supprimer définitivement**.

14.3 Utiliser l'API de SDMC

Les requêtes possibles via l'API de SDMC sont documentées sur cette page. Vous pouvez notamment utiliser ces requêtes pour extraire les logs d'administration du serveur.

15. Résoudre les problèmes

En cas de problème, vous pouvez consulter les journaux d'événements dans l'Observateur d'événements Windows et en complément, utiliser le système de prise de traces afin d'établir un diagnostic avec le Technical Assistance Center SDS Enterprise.

15.1 Consulter les journaux d'événements

Tous les événements liés à SDS Enterprise sont accessibles par l'intermédiaire de l'observateur d'événements Windows sur les postes des utilisateurs.

Lors d'une nouvelle installation de SDS Enterprise, les journaux d'événements sont activés par défaut.

Pour consulter la liste des journaux d'événements disponibles dans SDS Enterprise, reportez-vous à la section Liste des journaux de SDS Enterprise.

En cas de problèmes rencontrés avec l'utilisation de SDS Enterprise, reportez-vous à la section Établir un diagnostic.

Vous pouvez désactiver les journaux d'événements en suivant la procédure ci-dessous.

15.1.1 Comprendre les types de messages

Les messages d'erreur générés par SDS Enterprise peuvent être de trois types différents :

- messages d'information : il s'agit d'une simple information qui ne met pas en jeu la sécurité,
- messages d'avertissement : il s'agit d'une indication qui signale un problème potentiel à l'administrateur,
- messages d'erreur : il s'agit d'un réel problème qui empêche le fonctionnement du produit.

15.1.2 Comprendre le détail des informations journalisées

Les journaux permettent de visualiser les informations suivantes :

- **Type de message** : information, avertissement ou erreur,
- **Date** : date à laquelle le message a été généré,
- **Heure** : heure à laquelle le message a été généré,
- **Source** : source à partir de laquelle l'événement a été généré,
- **Catégorie** : brève description de la source de l'événement,
- **Événement** : numéro correspondant au type du message généré,
- **Utilisateur** : nom de l'utilisateur de SDS Enterprise,
- **Ordinateur** : nom (NetBIOS) de l'ordinateur.

15.1.3 Désactiver les journaux d'événements

La procédure s'effectue par le biais de l'éditeur de stratégie de groupe locale (*gpedit.msc*).

La GPO de Microsoft Windows utilise des fichiers *.admx* pour les paramètres de configuration, et des fichiers de langue *.adml*, où tous les textes relatifs à ces paramètres sont référencés.

L'installation de SDS Enterprise place :

- le fichier *Sbsuite.admx* dans le dossier *%SystemRoot%\PolicyDefinitions*
- le fichier de langue *Sbsuite.adml* dans le dossier *%SystemRoot%\PolicyDefinitions\en-US*

Ces fichiers sont chargés automatiquement lors du lancement de *gpedit*.

1. Lancez l'éditeur de stratégie de groupe locale : **Démarrer** > **Exécuter** > puis tapez *gpedit.msc*.
2. Cliquez sur **Modèles d'administration** > **Composants Stormshield Data Security**.
3. Double-cliquez sur l'entrée **Activer la fonctionnalité de journalisation des événements générés par Stormshield Data Security pour tous les modules**.
4. Sélectionnez l'option **Désactivé**. Il s'agit d'un interrupteur global. Aucun événement ne sera alors généré, quel que soit le réglage effectué pour chaque fonctionnalité sous **Composants Stormshield Data Security**.

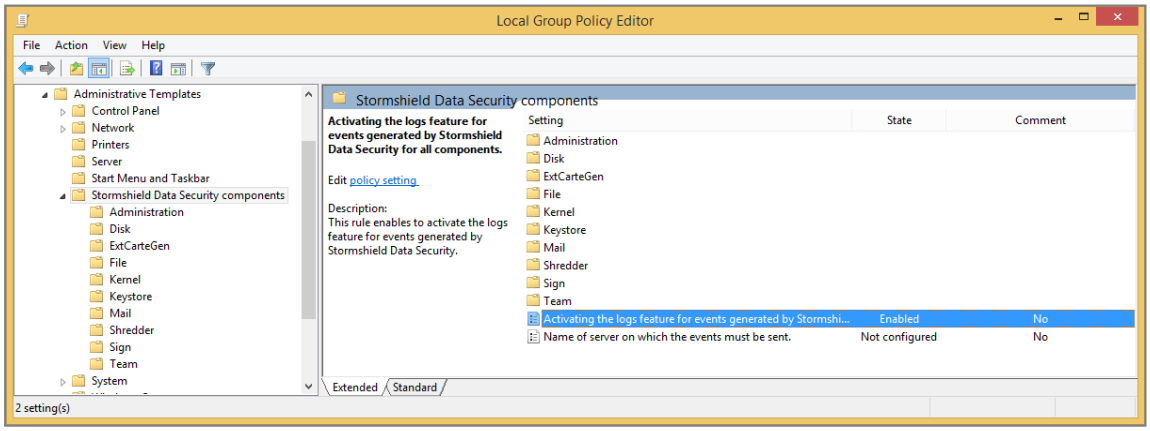
Vous pouvez également choisir de ne désactiver que les événements de certaines fonctionnalités.

Par exemple, pour désactiver les événements de la fonctionnalité Virtual Disk seulement :

1. Conservez la journalisation des événements générés par SDS Enterprise activée pour toutes les fonctionnalités.
2. Désactivez la journalisation d'événements de la fonctionnalité Virtual Disk sous **Composants Stormshield Data Security**.

Une fonctionnalité dont l'option “Non configuré” est sélectionnée est active si l'interrupteur global est activé.

Un changement de la stratégie de groupe modifie directement les valeurs correspondantes en base de registre. Celles-ci s'appliquent pour chaque utilisateur unitairement. Elles sont présentes sous la clé HKEY_CURRENT_USER de la base de registre. En revanche, une stratégie de groupe (spécifiée à distance par Active Directory) est prioritaire sur les changements effectués localement.



15.2 Établir un diagnostic

En cas de problèmes rencontrés lors de l'utilisation du produit, SDS Enterprise possède un système de prise de traces. Il permet ainsi de fournir au Technical Assistance Center SDS Enterprise des informations utiles à l'analyse des problèmes. Ces traces sont activables « à chaud », c'est-à-dire sans redémarrer la machine, ni la session Windows.

15.2.1 Comprendre le fonctionnement de la prise de traces

Pour activer la prise de traces SDS Enterprise, vous pouvez double-cliquer sur un fichier portant l'extension *.sbdiag* fourni par le Technical Assistance Center SDS Enterprise ou bien sélectionner le menu **Prise de traces Stormshield** dans le menu **Démarrer** de Windows.

Lors d'une prise de traces, les éléments suivants sont enregistrés dans une archive *.zip* qui se trouve dans le dossier **C:/ProgramData/Arkoon/Security BOX/Traces** :

- Les traces SDS Enterprise produites (fichier *Trace.etl*).
- Les événements SDS Enterprise (fichier *audits.evtx*) : la génération de ce fichier est paramétrable dans l'interface ou dans le fichier d'extension *.sbdiag*. L'activation des journaux d'événements est nécessaire. Pour les activer, reportez-vous à la section Consulter les journaux d'événements.
- Une empreinte de la machine (fichier *sbdiag.xml*) : elle contient des informations sur le système et sur l'installation de SDS Enterprise et de la suite Microsoft Office,
- Une trace PSR (Problem Steps Recorder) : cet outil, livré avec les systèmes d'exploitation Windows à partir de Windows 7, permet de visualiser les actions effectuées lors de la reproduction d'un problème sur la machine. La génération de ce fichier est paramétrable dans l'interface ou dans le fichier d'extension *.sbdiag*.

15.2.2 Utiliser le système de prise de traces

Depuis un fichier *.sbdiag*

1. Double-cliquez sur le fichier *.sbdiag* fourni par le Technical Assistance Center SDS Enterprise pour démarrer l'interface de prise de traces en mode préconfiguré.
2. Cliquez sur le bouton **Démarrer la session de trace**.
3. Attendez que le message **Session de trace en cours** s'affiche.
4. Reproduisez la séquence d'actions à tracer.
5. Une fois la reproduction terminée, cliquez sur le bouton **Arrêter la session de trace**.
6. Dans la fenêtre suivante, ajoutez si besoin des commentaires à l'attention du Technical Assistance Center SDS Enterprise. Donnez des informations supplémentaires sur la méthode de reproduction, des repères temporels, des noms de fichiers, etc.
7. Patientez jusqu'à ce que le dossier contenant la session de trace s'ouvre. Envoyez le fichier zip *Trace <horodatage>.zip* au Technical Assistance Center SDS Enterprise.

Dans ce mode préconfiguré, les paramètres ne sont pas modifiables.

Depuis l'interface de prise de traces

Si vous ne possédez pas de fichier *.sbdiag* ou si vous souhaitez personnaliser la session de trace, sélectionnez le menu **Prise de traces Stormshield** dans le menu **Démarrer** de Windows :

1. Pour démarrer la session, ouvrez la boîte de dialogue des paramètres en cliquant sur l'icône de l'engrenage.

2. Il est recommandé de cocher les deux options du panneau supérieur des paramètres. L'activation des journaux d'événements est nécessaire pour l'extraction des événements SDS Enterprise. Pour les activer, reportez-vous à la section Consulter les journaux d'événements.

> **NOTE**
> L'outil PSR (Problem Steps Recorder) peut enregistrer des captures d'écran lors de la prise de traces.

3. Sélectionnez le module Kernel et le module impacté par la prise de traces uniquement.
4. Après avoir cliqué sur **OK** dans cette boite de dialogue, un fichier d'extension *.sbdiag* est automatiquement créé et la session de trace peut être démarrée comme décrit dans la section ci-dessus.

16. Désinstaller SDS Enterprise sur les postes des utilisateurs

1. Ouvrez le **Panneau de configuration**.
2. Ouvrez les **Programmes et fonctionnalités**.
3. Sélectionnez dans la liste la ligne correspondant à SDS Enterprise.
4. Cliquez sur **Désinstaller**.
5. Suivez les indications à l'écran.

Vous pouvez également utiliser la commande Setup du package d'installation qui propose d'installer, désinstaller et modifier l'installation.

17. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

Annexe A. Liste des journaux de SDS Enterprise

Consultez la liste des journaux d'événements par fonctionnalité dans les sections suivantes.

Pour activer les journaux dans l'observateur d'événements Windows et comprendre les informations journalisées, reportez-vous à la section Consulter les journaux d'événements.

A.1 Administration

Installation de la Suite Stormshield Data Security

Numéro	Type	Description
300	Information	L'installation de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5 • Société : %6
301	Information	La modification de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5
302	Information	La désinstallation de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5
303	Information	L'installation du patch de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : - • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5 • Société : %6
304	Information	La modification du patch de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : - • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5

Numéro	Type	Description
305	Information	La désinstallation du patch de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : - • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5
306	Erreur	Le setup deStormshield Data Security s'est interrompu de façon inattendue.
307	Erreur	Le setup de Stormshield Data Security a été arrêté avant qu'il ne se termine correctement.
308	Erreur	La politique de groupe définit l'envoi des événements vers le serveur '%2', mais l'utilisation de cette adresse échoue avec le code d'erreur %3 : "%4". Veuillez contacter votre administrateur.
309	Erreur	La politique n'est pas disponible : %2.
310	Erreur	La politique est incomplète, vérifiez les paramètres suivants : %2.
311	Avertissement	En l'absence de politique de sécurité personnalisée, la politique par défaut sera utilisée.
1925	Erreur	Vous ne disposez pas de privilèges suffisants pour exécuter cette installation pour tous les utilisateurs de cet ordinateur. Ouvrez une session en tant qu'administrateur, puis réessayez d'exécuter cette installation.

Administration de l'annuaire

Numéro	Type	Description
700	Information	La mise à jour automatique de l'annuaire s'est effectuée avec succès.
701	Erreur	La mise à jour automatique de l'annuaire a échoué.
702	Information	La mise à jour manuelle de l'annuaire s'est effectuée avec succès.
703	Erreur	La mise à jour de l'annuaire a échoué.
704	Information	La mise à jour de l'annuaire à la connexion s'est effectuée avec succès.
705	Erreur	La mise à jour de l'annuaire à la connexion a échoué.
706	Information	La mise à jour de l'annuaire après déverrouillage s'est effectuée avec succès.
707	Erreur	La mise à jour de l'annuaire après déverrouillage a échoué.
708	Information	L'exportation de %4 certificat(s) de l'annuaire au format '%3' a été réalisée avec succès dans le fichier '%2'.
709	Erreur	L'exportation de %4 certificat(s) de l'annuaire au format '%3' dans le fichier '%2' a échoué.
710	Information	L'importation de %2 certificat(s) dans l'annuaire a été réalisée avec succès.
711	Erreur	L'importation de %2 certificat(s) dans l'annuaire a échoué.

Numéro	Type	Description
712	Information	Option COMPATIBILITY_MODE : Valeur: %2 Acces %3
713	Information	Option ALLOW_MANUAL_UPDATE : Valeur : %2 Acces %3
714	Information	Option DISABLE_CHECK_ON_DISPLAY: Valeur: %2 Acces %3
715	Information	Option ACTIVATE : Valeur: %2 Acces %3
716	Information	Option ALLOW_DOWNLOAD_CRL : Valeur: %2 Acces %3
717	Information	Option REPLACE_FROM_LDAP : Valeur: %2 Acces %3
718	Information	Option START_ON_CONNECTION : Valeur: %2 Acces %3
719	Information	Option REPLACE_FROM_LDAP_OUTOFDATE_CERT : Valeur: %2 Acces %3
720	Information	Option REPLACE_FROM_LDAP_REVOKEDCERT : Valeur: %2 Acces %3
721	Information	Option DELETE_IF_OUTOFDATE : Valeur: %2 Acces %3
722	Information	Option DELETE_IF_REVOKE : Valeur: %2 Acces %3
723	Information	Option DELETE_IF_NOT_ON_LDAP : Valeur: %2 Acces %3
724	Information	Option SB_EVT_ADMINISTRATION_INFO_REPLACE_ON_VALID_CERT : Valeur: %2 Acces %3
725	Information	Option TIMER : Valeur: %2 Acces %3
726	Information	Option COMMON_NAME_REPLACE : Valeur: %2 Acces %3
727	Information	Option COMMON_NAME_OUT_OF_DATE : Valeur: %2 Acces %3
728	Information	Option COMMON_NAME_REVOKE : Valeur: %2 Acces %3
729	Information	Option COMMON_NAME_NOT_ON_LDAP: Valeur: %2 Acces %3
730	Avertissement	La mise à jour LDAP du certificat dont l'e-mail est '%2' n'a pas été effectuée car la liste de révocation n'est pas disponible.

Administration de la liste de révocation

Numéro	Type	Description
1100	Information	La mise à jour de la liste de révocation %2 a été effectuée avec succès.
1101	Erreur	La mise à jour de la liste de révocation %2 a échoué.
1102	Information	La mise à jour de la liste de révocation %2 à partir du cache a été effectuée avec succès.
1103	Erreur	La mise à jour automatique de la liste de révocation %2 à partir du cache a échoué.
1104	Information	La base de données de CRL %2 à été réinitialisée.
1105	Erreur	La DLL %2 n'a pas pu être chargée.

A.2 Virtual Disk

Gestion des volumes

Numéro	Type	Description
8300	Information	Le montage du volume automatique '%2' sur '%3' en mode '%4' s'est déroulé avec succès.
8301	Erreur	Le montage du volume automatique '%2' sur '%3' en mode '%4' a échoué.
8302	Information	Le volume '%2' a été monté avec succès sur '%3' en mode '%4'.
8303	Erreur	Le montage du volume '%2' sur '%3' en mode '%4' a échoué.
8304	Information	Le démontage du volume automatique '%2' monté sur '%3' a été un succès.
8305	Erreur	Le démontage du volume automatique '%2' monté sur '%3' a échoué.
8306	Information	Le volume '%2' monté sur '%3' a été démonté avec succès.
8307	Erreur	Le démontage du volume '%2' monté sur '%3' a échoué.
8308	Information	Le volume '%2' monté sur '%3' a été verrouillé avec succès.
8309	Erreur	Le verrouillage du volume '%2' monté sur '%3' a échoué.
8310	Information	Le volume '%2' monté sur '%3' a été déverrouillé avec succès.
8311	Erreur	Le déverrouillage du volume '%2' monté sur '%3' a échoué.
8312	Information	Le volume '%2' a été créé avec succès.
8313	Erreur	La création du volume '%2' a échoué.
8314	Information	Le volume '%2' a été ajouté avec succès à la liste des volumes automatiques. Il sera monté sur '%3'.
8315	Erreur	L'ajout du volume '%2' à la liste des volumes automatiques a échoué.
8316	Information	Le volume '%2' monté sur '%3' a été supprimé avec succès de la liste des volumes automatiques.
8317	Erreur	La suppression du volume '%2' (monté sur '%3') de la liste des volumes automatiques a échoué.

A.3 File

Chiffrement / Déchiffrement vers

Numéro	Type	Description
18300	Information	L'utilisateur a chiffré avec succès le fichier '%2' en mode auto-déchiffrable.
18301	Erreur	Le chiffrement du fichier '%2' en mode auto-déchiffrable a échoué.
18302	Information	L'utilisateur a chiffré avec succès le dossier '%2' en mode auto-déchiffrable.

Numéro	Type	Description
18303	Erreur	Le chiffrement du dossier '%2' en mode auto-déchiffrable a échoué.
18304	Information	L'utilisateur a chiffré avec succès le fichier '%2' en utilisant SecurityBOX SmartFile.
18305	Erreur	Le chiffrement du fichier '%2' en utilisant SecurityBOX SmartFile a échoué.
18306	Information	L'utilisateur a chiffré avec succès le dossier '%2' en utilisant SecurityBOX SmartFile.
18307	Erreur	Le chiffrement du dossier '%2' en utilisant SecurityBOX SmartFile a échoué.
18308	Information	L'utilisateur a chiffré avec succès le fichier '%2' pour les correspondants suivants : %3.
18309	Erreur	Le chiffrement du fichier '%2' pour les correspondants suivants a échoué : %3.
18310	Information	L'utilisateur a chiffré avec succès le dossier '%2' pour les correspondants suivants : %3.
18311	Erreur	Le chiffrement du dossier '%2' pour les correspondants suivants a échoué : %3.
18312	Information	Les collaborateurs suivants ont été ajoutés avec succès au fichier '%2' : %r%3.
18313	Erreur	L'ajout des collaborateurs suivants au fichier '%2' a échoué : %r%3.
18314	Information	Les collaborateurs suivants ont été supprimés avec succès du fichier '%2' : %r%3.
18315	Erreur	La suppression des collaborateurs suivants du fichier '%2' a échoué : %r%3.
18316	Erreur	Une erreur s'est produite avec le certificat de '%2'.
18317	Information	Les fichiers suivants n'ont pas été traités car ils n'étaient pas chiffrés :%2.
18318	Information	Les fichiers suivants n'ont pas été traités car ils n'étaient pas chiffrés pour l'utilisateur connecté :%2.

Chiffrement / Déchiffrement

Numéro	Type	Description
18700	Information	L'utilisateur a chiffré le fichier '%2' avec succès.
18701	Erreur	Le chiffrement du fichier '%2' a échoué.
18702	Information	L'utilisateur a déchiffré le fichier '%2' avec succès.
18703	Erreur	Le déchiffrement du fichier '%2' a échoué.
18704	Erreur	Le chemin '%2' n'a pas été déchiffré car il est protégé par Share.
18705	Erreur	Le dossier '%2' n'a pas été déchiffré car il contient un sous-dossier protégé par Share.
18706	Information	L'utilisateur a lancé la conversion en .sdsx du fichier '%2'.

Numéro	Type	Description
18707	Information	La conversion du fichier '%2' en .sdsx a réussi.
18708	Erreur	La conversion du fichier '%2' en .sdsx a échoué.
18709	Information	La conversion du fichier '%2' en .sdsx a réussi. Le fichier original a été déplacé à l'emplacement '%3'.
18710	Erreur	La conversion du fichier '%2' en .sdsx a réussi. Le déplacement du fichier original dans le dossier '%3' a échoué.
18711	Avertissement	L'ouverture des fichiers et la conversion en .sdsx n'a pas eu lieu car l'utilisateur a sélectionné plusieurs fichiers et/ou dossiers contenant au moins un fichier .sbox.

A.4 Kernel

Démarrage / Arrêt

Numéro	Type	Description
25300	Information	Le démarrage du kernel a été effectué avec succès.
25301	Erreur	Le démarrage du kernel a échoué.
25302	Information	L'arrêt du kernel a été effectué avec succès.
25303	Erreur	L'arrêt du kernel a échoué.
25304	Erreur	Une erreur dans la politique de sécurité empêche Stormshield Data Security de fonctionner. Le paramètre erroné est %2.
25305	Erreur	Une erreur dans la configuration en base de registre empêche Stormshield Data Security de fonctionner. Le paramètre erroné est %s.
25306	Avertissement	La valeur du paramètre %2 configurée en base de registre est invalide.

Authentification LDAPS

Numéro	Type	Description
25700	Avertissement	Avertissement de sécurité SSL : certificat serveur invalide. Délivré à : %2 Délivré par : %3 Valide du %4 au %5. Veuillez contacter votre administrateur.
25701	Erreur	Erreur de sécurité SSL : certificat serveur invalide. Délivré à : %2 Délivré par : %3 Valide du %4 au %5. Veuillez contacter votre administrateur.
25702	Erreur	Toutes les méthodes d'authentification soumises au serveur LDAP %2 ont échoué.
25703	Information	L'utilisateur est authentifié auprès du serveur LDAP %2 avec la méthode : %3.

Sélection du composant cryptographique

Numéro	Type	Description
26100	Information	L'utilisateur a sélectionné le middleware '%2'.

A.5 Keystore

Connexion / Déconnexion

Numéro	Type	Description
31300	Information	L'utilisateur s'est connecté à son porte-clés Stormshield Data Security.
31301	Erreur	La connexion au porte-clés Stormshield Data Security a échoué.
31302	Information	L'utilisateur s'est déconnecté de son porte-clés Stormshield Data Security.
31303	Erreur	L'utilisateur n'a pas pu se déconnecter de son porte-clés Stormshield Data Security.
31304	Information	La session Stormshield Data Security de l'utilisateur a été verrouillée.
31305	Erreur	Le verrouillage de la session Stormshield Data Security de l'utilisateur a échoué.
31306	Information	Le déverrouillage de la session Stormshield Data Security de l'utilisateur s'est déroulé normalement.
31307	Erreur	Le déverrouillage de la session Stormshield Data Security de l'utilisateur a échoué.
31308	Avertissement	Un utilisateur est déjà connecté à Stormshield Data Security dans une autre session Windows.
31309	Avertissement	Le code secret saisi est incorrect.
31310	Avertissement	L'identifiant '%2' ne correspond à aucun compte Stormshield Data Security.
31311	Avertissement	La session Stormshield Data Security ne peut pas être déverrouillée car la carte présente dans le lecteur n'est pas la bonne carte.
31312	Erreur	Le compte Stormshield Data Security ou la carte est bloqué.
31313	Information	La carte a été retirée du lecteur.
31314	Erreur	La carte est bloquée.
31315	Erreur	Impossible de notifier un composant.
31316	Erreur	Impossible de charger un composant: '%2'.

Administration de compte

Numéro	Type	Description
31700	Information	Le compte a été créé avec succès

Numéro	Type	Description
31701	Avertissement	L'installation du compte Stormshield Data Security a rencontré une erreur non bloquante.
31702	Erreur	L'installation du compte Stormshield Data Security a échoué.
31703	Information	La désinstallation du compte Stormshield Data Security s'est terminée normalement.
31704	Erreur	La désinstallation du compte Stormshield Data Security a échoué.
31705	Information	La politique de sécurité a été mise à jour.
31706	Erreur	La mise à jour de la politique de sécurité a échoué avec l'erreur suivante : %2.
31707	Information	L'export du compte Stormshield Data Security s'est terminé normalement.
31708	Erreur	L'export du compte Stormshield Data Security a échoué.
31709	Information	Le changement du code secret associé au compte s'est terminé normalement.
31710	Erreur	Le changement du code secret associé au compte a échoué.
31711	Erreur	Le nombre d'erreurs dans le changement du code secret associé au compte a dépassé la limite autorisée.
31712	Erreur	Impossible de créer un nouveau compte Stormshield Data Security parce que la carte est bloquée.
31713	Avertissement	Le code secret saisi est incorrect.
31714	Erreur	Le contenu de la carte ne permet pas la création de compte automatique.
31715	Erreur	Impossible de créer un nouveau compte Stormshield Data Security parce que le modèle est bloqué.
31716	Erreur	Impossible de créer un nouveau compte Stormshield Data Security parce que le modèle est inaccessible.
31717	Information	Un nouveau signataire des politiques de sécurité a été défini.
31718	Avertissement	La mise à jour de la politique de sécurité n'a pas été prise en compte parce que le nouveau signataire a été rejeté par l'utilisateur.
31719	Information	Téléchargement de la politique de sécurité depuis '%2'.
31720	Avertissement	Erreur de téléchargement de la politique de sécurité depuis '%2'.
31721	Information	La mise à jour de la politique de sécurité n'a pas été prise en compte parce que le compte est à jour.
31722	Erreur	La mise à jour de la politique de sécurité n'a pas été prise en compte parce que la signature du fichier est incorrecte.
31723	Erreur	La mise à jour de la politique de sécurité n'a pas été prise en compte pour la raison suivante : '%2'.
31724	Avertissement	La mise à jour de la politique de sécurité a été prise en compte malgré l'avertissement : %2.

Numéro	Type	Description
31725	Erreur	Le paramètre 'MasterPolicies' interdit la copie du fichier '%2'.
31726	Erreur	Création automatique de compte carte %2 : %3.

Administration des clés

Numéro	Type	Description
32100	Information	L'exportation de la clé de chiffrement par l'utilisateur s'est terminée normalement.
32101	Erreur	L'exportation de la clé de chiffrement par l'utilisateur a échoué.
32102	Information	Le renouvellement de la clé de chiffrement par l'utilisateur s'est terminé normalement.
32103	Erreur	Le renouvellement de la clé de chiffrement par l'utilisateur a échoué.
32104	Information	L'exportation de la clé de signature par l'utilisateur s'est terminée normalement.
32105	Erreur	L'exportation de la clé de signature par l'utilisateur a échoué.
32106	Information	Le renouvellement de la clé de signature par l'utilisateur s'est terminé normalement.
32107	Erreur	Le renouvellement de la clé de signature par l'utilisateur a échoué.
32108	Information	L'exportation de la clé par l'utilisateur s'est terminée normalement.
32109	Erreur	L'exportation de la clé par l'utilisateur a échoué.
32110	Information	Le renouvellement de la clé par l'utilisateur s'est terminé normalement.
32111	Erreur	Le renouvellement de la clé par l'utilisateur a échoué.
32112	Information	L'exportation du certificat de la clé de chiffrement par l'utilisateur s'est terminée normalement.
32113	Erreur	L'exportation du certificat de la clé de chiffrement par l'utilisateur a échoué.
32114	Information	L'exportation du certificat de la clé de signature par l'utilisateur s'est terminée normalement.
32115	Erreur	L'exportation du certificat de la clé de signature par l'utilisateur a échoué.
32116	Information	L'exportation du certificat de la clé par l'utilisateur s'est terminée normalement.
32117	Erreur	L'exportation du certificat de la clé par l'utilisateur a échoué.
32118	Information	Un certificat pour la %2 n'a pas été importé dans le compte de l'utilisateur car il était périmé.
32119	Information	Un certificat pour la %2 n'a pas été importé dans le compte de l'utilisateur car ses usages étaient insuffisants.

Administration du porte-clés

Numéro	Type	Description
32500	Information	La clé de déchiffrement a été importée avec succès.
32501	Erreur	L'import de la clé de déchiffrement a échoué.
32502	Information	La clé de recouvrement a été importée avec succès.
32503	Erreur	L'import de la clé de recouvrement a échoué.

A.6 Mail

Envoi/Réception

Numéro	Type	Description
39312	Information	Le certificat de l'utilisateur '%2' n'a pas été trouvé dans l'annuaire de confiance.
39313	Information	Le certificat de l'utilisateur '%2' est révoqué.
39314	Information	Le certificat de l'utilisateur '%2' n'est plus valide.
39315	Information	La chaîne de parenté de l'utilisateur '%2' est révoquée.
39316	Information	La chaîne de parenté de l'utilisateur '%2' n'est plus valide.
39317	Information	La liste de révocation du certificat de l'utilisateur '%2' n'est pas disponible.
39318	Avertissement	L'utilisateur a reçu un mail chiffré mais ne possède pas la clé de déchiffrement.
39319	Avertissement	L'utilisateur a reçu un message dont la signature est incorrecte. Le message a été signé avec le certificat '%2'.
39320	Information	L'envoi d'un e-mail signé a été effectué avec succès (Destinataire(s): %2).
39321	Information	L'envoi d'un e-mail chiffré a été effectué avec succès (Destinataire(s): %2).
39322	Information	L'envoi d'un e-mail signé et chiffré a été effectué avec succès (Destinataire(s): %2).
39323	Erreur	L'utilisateur a reçu un message dont la signature n'a pas pu être vérifiée. L'adresse d'origine du message est '%2'.
39324	Erreur	L'utilisateur a reçu un message dont le certificat comporte une erreur. Le message a été signé avec le certificat '%2'.
39325	Avertissement	L'utilisateur a reçu un message dont le certificat n'est pas sûr. Le message a été signé avec le certificat '%2'.
39326	Information	Le message envoyé avec l'étiquette de confidentialité %1 a été signé automatiquement.

Numéro	Type	Description
39327	Information	Le message envoyé avec l'étiquette de confidentialité %1 a été chiffré automatiquement.
39328	Information	Le message envoyé avec l'étiquette de confidentialité %1 a été chiffré et signé automatiquement.

Transchiffrement

Numéro	Type	Description
39700	Information	L'utilisateur a lancé le transchiffrement sur le dossier '%2'.
39701	Avertissement	Le transchiffrement des messages a rencontré des problèmes.

Désactivation de la sécurité

Numéro	Type	Description
40100	Information	La sécurité des messages du dossier '%2' a été désactivée.
40101	Information	La sécurité de certains messages a été désactivée (quantité: %2).
40102	Avertissement	La désactivation de la sécurité des messages a rencontré des problèmes.

Administration

Numéro	Type	Description
40500	Information	Le module Stormshield Data Mail est chargé avec succès dans Outlook '%2'.
40501	Information	Le module Stormshield Data Mail est désactivé dans Outlook '%2'.
40502	Information	L'exception suivante a été levée dans le module Stormshield Data Mail : '%2'.
40503	Avertissement	La clé de registre suivante, nécessaire au bon fonctionnement de l'add-in Stormshield Data Mail Édition Outlook, a été modifiée : '%2'.
40504	Avertissement	Des serveurs WKD n'ont pas pu être contactés lors de l'envoi d'un message. Les requêtes sur les URL suivantes n'ont pas abouti : %2.

A.7 Shredder

Numéro	Type	Description
46300	Information	L'opération de broyage a été initiée avec succès.
46301	Erreur	Échec de démarrage de l'opération de broyage.
46302	Information	L'opération de broyage a été terminée avec succès.

Numéro	Type	Description
46303	Erreur	L'opération de broyage a échoué.
46304	Information	La suppression du fichier '%2' a été effectuée avec succès.
46305	Erreur	La suppression du fichier '%2' a échoué.
46308	Information	Le vidage sécurisé de la corbeille a été effectué avec succès.
46309	Erreur	Le vidage sécurisé de la corbeille a échoué.
46310	Information	Le nettoyage de la liste des fichiers a été effectué avec succès.
46311	Erreur	Le nettoyage de la liste des fichiers a échoué.

A.8 Sign

Signature

Numéro	Type	Description
47300	Information	Le fichier '%2' a été signé avec succès.
47301	Erreur	La signature du fichier '%2' a échoué.
47302	Information	Le fichier '%2' a été co-signé avec succès.
47303	Erreur	La co-signature du fichier '%2' a échoué.
47304	Information	Le fichier '%2' a été contre-signé avec succès.
47305	Erreur	La contre-signature du fichier '%2' a échoué.
47306	Information	Le fichier '%2' a été sur-signé avec succès.
47307	Erreur	La sur-signature du fichier '%2' a échoué.
47308	Erreur	Le fichier '%2' est corrompu.

A.9 Team

Gestion des règles

Numéro	Type	Description
49300	Information	Une règle de sécurité a été définie sur le dossier '%2'.
49301	Erreur	Une tentative de sécurisation du dossier '%2' a échoué.
49302	Information	Le dossier '%2' a été remis en clair (non sécurisé).
49303	Erreur	Une tentative de désécurisation du dossier '%2' a échoué.
49304	Information	Les collaborateurs suivants ont été ajoutés avec succès dans la règle du dossier '%2' :%r%3.

Numéro	Type	Description
49305	Erreur	L'ajout des collaborateurs suivants pour la règle du dossier '%2' a échoué :%r%3.
49306	Information	Les collaborateurs suivants ont été supprimés avec succès de la règle du dossier '%2' :%r%3.
49307	Erreur	La suppression des collaborateurs suivants de la règle du dossier '%2' a échoué : %r%3.
49308	Information	Les propriétaires suivants ont été ajoutés avec succès à la règle du dossier '%2' : %r%3.
49309	Erreur	L'ajout de propriétaires pour la règle du dossier '%2' a échoué : %r%3.
49310	Information	Les propriétaires suivants ont été supprimés avec succès de la règle du dossier '%2' : %r%3.
49311	Erreur	La suppression de propriétaires de la règle du dossier '%2' a échoué : %r%3.
49312	Information	Le dossier '%2' a été configuré avec succès en dossier sécurisé (profil).
49313	Erreur	Une tentative de sécurisation du dossier '%2' a échoué (profil).
49314	Information	Le dossier '%2' a été configuré avec succès en dossier non sécurisé (profil).
49315	Erreur	Une tentative de désécurisation du dossier '%2' a échoué (profil).
49316	Information	La règle du dossier '%2' a été modifiée avec succès (profil).
49317	Erreur	La modification de la règle du dossier '%2' a échoué (profil).
49318	Information	Les collaborateurs suivants ont été ajoutés avec succès dans la règle du dossier '%2' (profil) :%r%3.
49319	Erreur	L'ajout des collaborateurs suivants pour la règle du dossier '%2' a échoué (profil) :%r%3.
49320	Information	Les collaborateurs suivants ont été supprimés avec succès de la règle du dossier '%2' (profil) :%r%3.
49321	Erreur	La suppression des collaborateurs suivants de la règle du dossier '%2' a échoué (profil) : %r%3.
49322	Avertissement	La mise à jour du fichier de règles (*.ust*) du dossier '%2' a échoué : en-tête inconsistant.
49323	Avertissement	L'utilisateur ne fait pas partie des utilisateurs autorisés pour la règle sur '%2'.
49324	Avertissement	L'utilisateur accède aux propriétés de la règle sur '%2' alors que son certificat est révoqué.
49325	Information	La règle de sécurité du dossier '%2' a été sauvegardée dans le compte de l'utilisateur.
49326	Avertissement	Le certificat de '%2' n'a pas été trouvé.
49327	Information	Le certificat de '%2' est invalide et a été ignoré.

Numéro	Type	Description
49328	Information	Le certificat de '%2' est invalide, l'opération de chiffrement a été arrêtée par l'utilisateur.
49329	Avertissement	Le certificat de '%2' n'a pas pu être entièrement vérifié et a été utilisé.
49330	Information	Le certificat de '%2' n'a pas pu être entièrement vérifié et a été ignoré.
49331	Avertissement	Le certificat de '%2' est non valide et révoqué, et a été supprimé de la règle.
49332	Information	La règle de sécurité du dossier '%2' a été restaurée depuis le compte de l'utilisateur.
49333	Avertissement	Suspicion d'attaque : la règle de sécurité du dossier '%2' a été remplacée.
49334	Information	La règle de sécurité du dossier '%2' a disparu.
49335	Avertissement	Un collaborateur illégitime a été détecté et ignoré dans la règle de sécurité du dossier '%2'.
49336	Information	La règle de sécurité du dossier '%2' a été restaurée depuis la règle locale.
49342	Avertissement	Impossible de vérifier la chaîne de parenté ou la liste de révocation.

Mise à jour des règles Team

Numéro	Type	Description
49337	Avertissement	Le nouveau certificat du collaborateur '%2' n'a pas été trouvé. Ce dernier ne fait plus partie de la règle.
49338	Avertissement	La règle connue sur le dossier '%2' n'est pas à jour. La mise à jour automatique n'a pas pu être effectuée.
49339	Avertissement	Le dossier '%2' sur lequel s'applique la règle est introuvable ou n'est plus sécurisé.
49340	Erreur	La clé de chiffrement du collaborateur '%2' n'a pas été trouvée.
49341	Avertissement	Le collaborateur '%2' n'a pas été trouvé dans la règle.

Chiffrement/Déchiffrement

Numéro	Type	Description
49700	Information	L'utilisateur a sorti le fichier '%2' d'une zone sécurisée avec succès.
49701	Erreur	La sortie du fichier '%2' d'une zone sécurisée a échoué.
49702	Information	L'utilisateur a sorti le dossier '%2' d'une zone sécurisée avec succès.
49703	Erreur	La sortie du dossier '%2' d'une zone sécurisée a échoué.
49704	Information	L'utilisateur a sécurisé le fichier '%2' selon les règles définies.
49705	Erreur	La sécurisation du fichier '%2' selon les règles définies a échoué.
49706	Information	L'utilisateur a sécurisé le dossier '%2' selon les règles définies.

Numéro	Type	Description
49707	Erreur	La sécurisation du dossier '%2' selon les règles définies a échoué.
49708	Information	L'utilisateur a désécurisé le fichier '%2' avec succès.
49709	Erreur	La désécurisation du fichier '%2' a échoué.
49710	Information	L'utilisateur a désécurisé le dossier '%2' avec succès.
49711	Erreur	La désécurisation du dossier '%2' a échoué.
49712	Information	La sécurisation a été annulée.
49713	Information	La désécurisation a été annulée.
49714	Erreur	Impossible de mettre en conformité le dossier '%2' : vous n'avez pas les autorisations Windows.
49715	Avertissement	Impossible de mettre en conformité le dossier caché '%2' : vous n'avez pas les autorisations Windows.

Sauvegarde/Restauration

Numéro	Type	Description
50100	Information	La sauvegarde du fichier '%2' est terminée.
50101	Erreur	La sauvegarde du fichier '%2' a échoué.
50102	Information	La sauvegarde du dossier '%2' est terminée.
50103	Erreur	La sauvegarde du dossier '%2' a échoué.
50104	Information	La restauration du fichier '%2' est terminée.
50105	Erreur	La restauration du fichier '%2' a échoué.
50106	Information	La restauration du dossier '%2' est terminée.
50107	Erreur	La restauration du dossier '%2' a échoué.
50108	Information	La sauvegarde a été annulée.
50109	Information	La restauration a été annulée.
50110	Erreur	Impossible de sauvegarder dans le dossier '%2' : vous n'avez pas les autorisations Windows.
50111	Erreur	Impossible de restaurer dans le dossier '%2' : vous n'avez pas les autorisations Windows.

Driver

Numéro	Type	Description
50500	Avertissement	Le fichier '%2' ne peut pas être ouvert par '%3'.
50501	Erreur	Délai dépassé lors de la tentative d'ouverture du fichier '%2' par '%3'.

Numéro	Type	Description
50502	Erreur	La demande au service Team a échoué : '%2' par '%3'.

A.10 Share

Numéro	Type	Description
14300	Information	Le fichier de configuration de Share '%2' est invalide.
14301	Information	Le fichier de configuration de Share '%2' est manquant.
14302	Information	Impossible de communiquer avec le driver de Share.
14303	Information	L'utilisateur a chiffré avec succès le fichier '%2' en utilisant une règle de protection automatique.
14304	Erreur	Le chiffrement du fichier '%2' en utilisant une règle de protection automatique a échoué.
14305	Information	L'utilisateur a chiffré avec succès le fichier '%2' en utilisant une règle de protection automatique pour les correspondants suivants : %r%3.
14306	Erreur	Le chiffrement du fichier '%2' en utilisant une règle de protection automatique pour les correspondants suivants a échoué : %r%3.
14307	Information	La règle de protection automatique a été appliquée.
14308	Erreur	La règle de protection automatique ne peut pas être appliquée.
14309	Information	L'utilisateur a chiffré avec succès le dossier '%2' en utilisant une règle de protection automatique.
14310	Erreur	Le chiffrement du dossier '%2' en utilisant une règle de protection automatique a échoué.
14311	Information	La règle de protection automatique a été activée.
14312	Erreur	La règle de protection automatique ne peut pas être activée.
14313	Information	La règle de protection automatique a été désactivée.
14314	Erreur	La règle de protection automatique ne peut pas être désactivée.
14315	Information	La règle de protection automatique a été modifiée.
14316	Erreur	La règle de protection automatique ne peut pas être modifiée.

Annexe B. Compatibilité entre SDS Enterprise et les autres solutions de sécurité

Pour fonctionner correctement, SDS Enterprise doit pouvoir accéder aux ressources listées ci-dessous.

Veuillez vous assurer qu'aucune autre solution de sécurité n'empêche l'accès à ces ressources sur les postes des utilisateurs.

Tous les fichier présents dans le dossier "C:\Program Files\Arkoon\Security BOX\" et ses enfants	
Emplacement et noms des pilotes	
C:\Windows\System32\drivers\SBTEAMW8.SYS	
C:\Windows\System32\drivers\SBSWAPW8.SYS	
C:\Windows\System32\drivers\SBOXDISK.SYS	
C:\Program Files\Arkoon\Security BOX\Kernel\SDSCloudDrv.sys	
Extensions propres à SDS Enterprise	
.sbt	.sdsx
.sbox	.vbox
.usr	.ust
.usd	.usx
.usc	.bcrl

Annexe C. Mettre en place la solution d'infrastructure à clé publique (PKI) de Microsoft

Le fonctionnement de SDS Enterprise requiert l'utilisation de clés de chiffrement et de signature pour tous les utilisateurs de l'entreprise. Pour mettre en place la solution de PKI de Microsoft Windows afin de générer les clés de vos utilisateurs, suivez les étapes ci-dessous.

Étapes	Description
1	Ajouter le rôle d'Autorité de certification sur un serveur Windows
2	Configurer la liste de révocation (CRL) de l'autorité de certification
3	Créer un agent de récupération de clé
4	Créer des modèles de certificats
5	Créer un compte signataire des politiques de sécurité SDS Enterprise
6	Créer un compte de recouvrement SDS Enterprise
7	Générer les certificats des utilisateurs

La mise en œuvre de la PKI de Microsoft Windows facilite entre autres la création de comptes utilisateurs en mode SSO, qui nécessitent de stocker les clés dans les magasins de certificats Windows. Pour en savoir plus, consultez la section Créer un compte Single Sign-On (SSO).

C.1 Prérequis

Vous devez disposer d'un serveur Microsoft Windows faisant office de contrôleur de domaine et lui assigner les rôles suivants :

- Serveur DHCP
- Serveur DNS
- Services de domaine Active Directory (AD DS)

C.2 Ajouter le rôle d'Autorité de certification sur le serveur Windows

La première étape consiste à mettre en œuvre une autorité de certification sur votre serveur Windows, à l'aide du rôle **Services de certificats Active Directory** (AD CS). L'autorité de certification émet, révoque et renouvelle les clés des utilisateurs.

La première autorité de certification que vous déployez devient l'autorité racine de votre PKI interne. Par la suite vous pouvez déployer des autorités de certification secondaires et constituer une hiérarchie d'autorités.

Suivez la procédure ci-dessous pour configurer votre autorité de certification et la déclarer dans vos politiques de sécurité SDS Enterprise.

NOTE
Pour plus d'informations sur l'utilisation du **Gestionnaire de serveur** Windows et la mise en œuvre d'une autorité de certification, consultez la documentation de Microsoft.

1. Sur votre serveur Windows, ouvrez le **Gestionnaire de serveur**.
2. Cliquez sur **Ajouter des rôles et des fonctionnalités**.
3. Complétez les écrans suivants.
4. Sur l'écran des rôles de serveurs, sélectionnez **Services de certificats Active Directory**.
5. Ajoutez les services de rôle **Autorité de certification** et **Inscription de l'autorité de certification via le web**.
6. Après l'installation, lors de la configuration des services de certificats Active Directory, sélectionnez **Autorité de certification d'entreprise** dans le **Type d'installation**.
7. Sélectionnez **Autorité de certification racine** dans le **Type d'AC**.
8. Complétez les écrans suivants.
9. Sauvegardez le certificat de l'autorité de certification au format *.cer*, *.crt* ou *.cert*.
10. Importez-le dans la bibliothèque de certificats de SDMC en suivant la procédure Gérer les certificats des autorités de certification et les certificats de recouvrement dans SDMC.
11. Déclarez l'autorité de certification dans vos politiques de sécurité en suivant la procédure Ajouter des autorités de certification et configurer le contrôle de révocation des certificats.

C.3 Configurer la liste de révocation (CRL) de l'autorité de certification

Une autorité de certification peut se référer à une CRL pour vérifier la validité des certificats. Vos politiques de sécurité SDS Enterprise doivent connaître les points de distribution des CRL.

Pour configurer la CRL de votre autorité racine :

1. Sur le serveur, ouvrez le Gestionnaire d'autorités de certification *certsrv.msc* et affichez les propriétés de l'autorité de certification que vous venez de créer.
2. Dans l'onglet **Extensions**, cliquez sur **Ajouter**.
3. Renseignez l'emplacement public qui hébergera la CRL puis validez.
4. Cochez les cases **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta** et **Inclure dans l'extension CDP des certificats émis**.
5. Sélectionnez le lien LDAP dans les emplacements de CRL et décochez la case **Inclure dans l'extension CDP des certificats émis**.
6. Fermez les propriétés de l'autorité.
7. Redémarrez les services de certificats Active Directory.
8. Dans vos politiques de sécurité SDS Enterprise dans SDMC, indiquez les points de distribution des CRL en suivant la procédure Ajouter des autorités de certification et configurer le contrôle de révocation des certificats.

Nous vous recommandons de ne pas stocker le fichier de CRL sur le serveur AD CS. Vous pouvez le stocker sur un serveur web accessible à tous les utilisateurs en HTTPS.

NOTE
Pour plus d'informations sur l'utilisation du Gestionnaire d'autorités de certification, consultez la documentation de Microsoft.

C.4 Créer un agent de récupération de clé

L'agent de récupération de clé est un administrateur Windows autorisé à déchiffrer les clés privées qui sont archivées par la PKI.

Commencez par créer un utilisateur qui tiendra le rôle d'agent de récupération de clé dans votre annuaire Active Directory. Puis créez un modèle de certificat d'agent de récupération de clé et publiez-le :

1. Sur le serveur, ouvrez le Gestionnaire d'autorités de certification *certsrv.msc*.
2. Sur le répertoire **Modèles de certificats** de l'autorité de certification, faites un clic droit et sélectionnez **Gérer**.
3. Dans le panneau de droite, faites un clic droit sur le modèle **Agent de récupération de clé** et sélectionnez **Dupliquer le modèle**.
4. Dans l'onglet **Sécurité**, ajoutez votre agent de récupération de clé.
5. Accordez-lui la permission **S'inscrire**.
6. Validez la création du modèle.
7. Pour publier le nouveau modèle, sur le répertoire **Modèles de certificats** de l'autorité de certification, faites un clic droit et sélectionnez **Nouveau** > **Modèle de certificat à délivrer**.
8. Sélectionnez le modèle de certificat d'agent de récupération de clé.
9. Validez la publication.
   Le nouveau modèle est maintenant disponible dans les **Modèles de certificats** et prêt à être utilisé.

Demandez ensuite un certificat pour l'agent de récupération de clé selon le nouveau modèle ajouté précédemment :

1. Sur un poste de travail du domaine, connectez-vous avec le compte Windows de l'agent de récupération de clé.
2. Ouvrez le Gestionnaire de certificats Windows *certmgr.msc*.
3. Sur le magasin **Personnel** > **Certificats**, faites un clic droit et sélectionnez **Toutes les tâches** > **Demander un nouveau certificat**.
4. Sélectionnez le modèle de certificat d'agent de récupération de clé.
   Le certificat est généré dans le magasin de certificats Windows de l'agent de récupération de clé.

Validez la demande de certificat dans le Gestionnaire d'autorités de certification de nouveau sur le serveur de l'autorité :

1. Ouvrez le gestionnaire *certsrv.msc*.
2. Sélectionnez le répertoire **Demandes en attente** de l'autorité de certification.
3. Sélectionnez le certificat correspondant à la demande.
4. Faites un clic droit et sélectionnez **Toutes les tâches** > **Délivrer**.

Terminez la création en déclarant la clé de l'agent de récupération de clé :

1. Dans le gestionnaire *certsrv.msc*, affichez les propriétés de l'autorité de certification.
2. Dans l'onglet **Agents de récupération**, cochez l'option **Archiver la clé** et ajoutez le certificat de l'agent de récupération de clé.
3. Validez puis redémarrez les services de certificats Active Directory.

Enfin, dans les propriétés des modèles de certificat de chiffrement et de recouvrement que vous allez créer ci-après :

- Assurez-vous d'avoir coché la case **Archiver la clé privée de chiffrement du sujet** dans l'onglet **Traitement de la demande** afin de bien archiver toutes les clés privées dans la PKI.

NOTE
Pour plus d'informations sur l'utilisation du Gestionnaire d'autorités de certification, consultez la documentation de Microsoft.

C.5 Créer des modèles de certificats

Vous devez à présent créer des modèles de certificats pour générer par la suite les certificats de chiffrement et de signature des utilisateurs, et les clés privées associées. Vous avez également besoin de modèles pour les signataires de politiques de sécurité SDS Enterprise et pour les comptes de recouvrement.

Créer les modèles de certificat pour le chiffrement et la signature

1. Sur le serveur, ouvrez le Gestionnaire d'autorités de certification *certsrv.msc*.
2. Sur le répertoire **Modèles de certificats** de l'autorité de certification, faites un clic droit et sélectionnez **Gérer**.
3. Faites un clic droit sur le modèle **Utilisateur** et sélectionnez **Dupliquer le modèle**.
4. Dans l'onglet **Général**, indiquez son nom et sa période de validité, ainsi que la période de renouvellement si nécessaire.
5. Dans l'onglet **Traitement de la demande** :
   - Sélectionnez **Chiffrement** ou **Signature** selon le type de modèle à créer,
   - Dans le cas d'un modèle de certificat pour le chiffrement, cochez la case **Archiver la clé privée de chiffrement du sujet** afin de permettre à l'agent de récupération de clé de déchiffrer les clés privées qui sont archivées par la PKI en cas de besoin,
   - Autorisez éventuellement l'export de la clé privée si cela est autorisé par la politique de sécurité de votre entreprise.
6. Dans l'onglet **Chiffrement**, choisissez 4096 pour la taille minimale de la clé.
7. Dans l'onglet **Extensions**, assurez-vous d'avoir ces extensions avec les options suivantes :

	Options pour le chiffrement	Options pour la signature
Stratégies d'application	Messagerie électronique sécurisée	Messagerie électronique sécurisée
Utilisation de la clé	- Autoriser l'échange de clés uniquement avec le chiffrement (Chiffrement de clés) - Autoriser le chiffrement des données utilisateurs - Rendre cette extension critique	- Signature numérique - Signature faisant preuve de l'origine (Non répudiation) - Rendre cette extension critique

   Veillez à supprimer les autres extensions affichées dans l'onglet afin de garder seulement les deux extensions indiquées dans le tableau.
8. Dans l'onglet **Sécurité**, cochez la permission **S'inscrire** pour les utilisateurs du domaine. Elle est suffisante pour une demande de certificat manuelle.
9. Validez la création du modèle.

Pour publier le modèle nouvellement créé, consultez la section Publier les modèles.

Créer le modèle de certificat pour le signataire de politiques de sécurité SDS Enterprise

Le modèle de certificat pour le signataire est identique au modèle de certificat de signature pour les utilisateurs. Seule la durée de validité du certificat diffère.

1. Suivez la procédure décrite dans la section Créer les modèles de certificat pour le chiffrement et la signature en sélectionnant **Signature** dans l'onglet **Traitement de la demande**.
2. Dans l'onglet **Général**, nous vous recommandons de paramétrer une durée de validité plus élevée que la durée généralement prévue pour les certificats de signature des utilisateurs.

Pour publier le modèle nouvellement créé, consultez la section Publier les modèles.

Créer le modèle de certificat pour le compte de recouvrement

Le modèle de certificat pour le compte de recouvrement est identique au modèle de certificat de chiffrement pour les utilisateurs. Seule la durée de validité du certificat diffère.

1. Suivez la procédure décrite dans la section Créer les modèles de certificat pour le chiffrement et la signature en sélectionnant **Chiffrement** dans l'onglet **Traitement de la demande**.
2. Dans l'onglet **Général**, nous vous recommandons de paramétrer une durée de validité plus élevée que la durée généralement prévue pour les certificats de chiffrement des utilisateurs.

Pour publier le modèle nouvellement créé, consultez la section Publier les modèles.

Publier les modèles

Pour publier les modèles de certificats :

1. Dans le Gestionnaire d'autorités de certification *certsrv.msc*, sur le répertoire **Modèles de certificats** de l'autorité de certification, faites un clic droit et sélectionnez **Nouveau** > **Modèle de certificat à délivrer**.
2. Sélectionnez les modèles créés précédemment.
3. Validez la publication.
   Les nouveaux modèles sont maintenant disponibles dans les **Modèles de certificats** et prêts à être utilisés.

C.6 Créer un compte signataire des politiques de sécurité SDS Enterprise

Les politiques de sécurité SDS Enterprise sont signées par un compte signataire, garantissant leur authenticité et leur intégrité.

Le compte signataire est un compte utilisateur Windows avec une clé de signature uniquement, qui ne sert que pour la signature des politiques de sécurité.

Pour créer le certificat et la clé privée associée du compte signataire de politique, utilisez le modèle de certificat de signataire ajouté précédemment :

1. Sur un poste de travail du domaine, connectez-vous avec le compte Windows de l'agent signataire de politique.
2. Ouvrez le Gestionnaire de certificats Windows *certmgr.msc*.
3. Sur le magasin **Personnel** > **Certificats**, faites un clic droit et sélectionnez **Toutes les tâches** > **Demander un nouveau certificat**.

4. Sélectionnez le modèle de certificat de signataire de politique de sécurité.
   Le certificat est généré dans le magasin de certificats Windows de l'agent signataire de politique.
5. Sauvegardez le certificat au format *.cer*, *.crt* ou *.cert*.
6. Sauvegardez la clé privée au format *.pfx*.

Pour signer une politique de sécurité, reportez-vous à la section Télécharger et signer une politique de sécurité.

NOTE
Pour plus d'informations sur l'utilisation du Gestionnaire de certificats Windows, consultez la documentation de Microsoft.

C.7 Créer un compte de recouvrement SDS Enterprise

Le compte de recouvrement est nécessaire pour sécuriser l'utilisation de SDS Enterprise. Il s'agit d'un compte utilisateur Windows avec une clé de chiffrement uniquement.

Pour en savoir plus sur le fonctionnement du compte de recouvrement, reportez-vous à la section Permettre le recouvrement de données.

Pour créer le certificat et la clé privée associée du compte de recouvrement, utilisez le modèle de certificat pour le compte de recouvrement ajouté précédemment :

1. Sur un poste de travail du domaine, connectez-vous avec le compte Windows de l'agent de recouvrement.
2. Ouvrez le Gestionnaire de certificats Windows *certmgr.msc*.
3. Sur le magasin **Personnel** > **Certificats**, faites un clic droit et sélectionnez **Toutes les tâches** > **Demander un nouveau certificat**.
4. Sélectionnez le modèle de certificat pour le compte de recouvrement.
   Le certificat est généré dans le magasin de certificats Windows de l'agent de recouvrement.
5. Sauvegardez le certificat au format *.cer*, *.crt* ou *.cert*.
6. Sauvegardez la clé privée au format *.pfx*.

   ATTENTION
   Veillez à bien conserver cette clé dans un endroit sécurisé.

7. Importez le certificat dans la bibliothèque de certificats de SDMC en suivant la procédure Gérer les certificats des autorités de certification et les certificats de recouvrement dans SDMC.
8. Indiquez les certificats des comptes de recouvrement à utiliser dans chacune de vos politiques de sécurité en suivant la procédure Permettre le recouvrement de données.

NOTE
Pour plus d'informations sur l'utilisation du Gestionnaire de certificats Windows, consultez la documentation de Microsoft.

C.8 Générer les certificats des utilisateurs

Pour créer des comptes utilisateurs SDS Enterprise en mode SSO, les certificats des utilisateurs doivent être stockés dans les magasins de certificats Windows des postes de travail. Ainsi, lorsqu'un utilisateur se connecte pour la première fois à SDS Enterprise, la création de son compte est automatique, à condition aussi que la politique de sécurité comporte les paramètres nécessaires.

Pour créer et déployer une politique de sécurité SDS Enterprise autorisant la création de comptes en mode SSO, reportez-vous à la section Créer un compte Single Sign-On (SSO).

Deux solutions sont possibles pour gérer les demandes de création de certificats des utilisateurs de la solution SDS Enterprise et pour les stocker dans les magasins Windows :

- le processus d'enrôlement automatique déployé via une stratégie de groupe (GPO).
- la demande manuelle via le Gestionnaire de certificats Windows *certmgr.msc* sur les postes des utilisateurs.

Paramétrer l'enrôlement automatique des utilisateurs

L'enrôlement automatique permet aux utilisateurs de demander un certificat de façon transparente lorsqu'ils se connectent à leur session Windows. Le certificat est alors généré automatiquement via une stratégie de groupe et stocké dans le magasin de certificats Windows de l'utilisateur.

PREREQUIS
Pour mettre en place l'enrôlement automatique, vous devez avoir coché au préalable la permission d'auto-enrôlement pour les utilisateurs du domaine, dans l'onglet **Sécurité** des propriétés de vos modèles de certificats de chiffrement et de signature sur votre serveur faisant office d'autorité de certification.

Sur votre serveur, créez une nouvelle stratégie de groupe :

1. Ouvrez le gestionnaire de stratégies de groupe.
2. Créez une nouvelle stratégie sur le domaine concerné.
3. Dans l'éditeur de stratégies de groupe, sélectionnez le répertoire **Configuration utilisateur** > **Stratégies** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies de clé publique**.
4. Dans le panneau de droite, ouvrez les propriétés de l'objet **Client des services de certificats - Inscription automatique**.
5. Dans **Modèle de configuration**, sélectionnez **Activé**.
6. Cochez les options **Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués** et **Mettre à jour les certificats qui utilisent les modèles de certificats** puis validez.
7. Déployez la nouvelle stratégie de groupe sur les postes des utilisateurs.

NOTE
Pour plus d'informations sur l'utilisation des stratégies de groupe, consultez la documentation de Microsoft.

Faire une demande de certificat manuelle

Chaque utilisateur peut faire une demande de certificat sur son poste de travail. L'utilisateur doit :

1. Ouvrir le Gestionnaire de certificats Windows *certmgr.msc*.
2. Sur le magasin **Personnel** > **Certificats**, faire un clic droit et sélectionner **Toutes les tâches** > **Demander un nouveau certificat**.
3. Sélectionner les modèles de certificats de chiffrement et de signature et compléter la procédure.
   Les certificats sont générés dans le magasin de certificats Windows.

Annexe D. Librairies tierces

SDS Enterprise utilise les librairies suivantes :

- JsonCpp
- OpenSSL
- OssASN1
- ZLib
- Efsw
- Rebex S/MIME for .NET
- Didisoft OpenPGP for .NET

documentation@stormshield.eu