STORMSHIELD DATA SECURITY ENTERPRISE

NOTES DE VERSION

Version 11

Dernière mise à jour du document : 24 novembre 2025

Référence : sds-fr-sdse_notes_de_version-v11.4.2

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.

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

Changements de comportement

Changements introduits en version 11.4

Lors de l'installation de SDS Enterprise 11.4, les journaux d'événements sont désormais activés par défaut. Ils sont accessibles par l'intermédiaire de l'observateur d'événements Windows sur les postes des utilisateurs.

Vous pouvez désactiver tout ou partie des journaux via une GPO. Pour plus d'informations, reportez-vous à la section **Consulter les journaux d'événements** du *Guide d'administration*.

Les utilisateurs doivent désormais accepter le changement de signataire de politique de sécurité avant de se connecter à leur compte SDS Enterprise. Pour plus d'informations, reportez-vous à la section **Modifier le signataire d'une politique de sécurité** du *Guide d'administration*.

Changement introduit en version 11.3

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.

Changement introduit en version 11.1.1

À partir de la version 11.1.1 de SDS Enterprise, l'agent est désormais installé par défaut avec une politique de sécurité, qui s'applique si vous n'utilisez pas votre propre politique de sécurité.

Changements introduits en version 11.0

Le répertoire dans lequel sont stockés les fichiers temporaires lors des opérations de co-signature et contre-signature de la fonctionnalité Stormshield Data Sign est désormais toujours *%temp%*. Vous ne pouvez plus le personnaliser au moyen du paramètre TmpFolder dans le fichier *SBox.ini*.

L'outil d'administration Stormshield Data Authority Manager a été remplacé par l'interface d'administration web Stormshield Data Management Center. Il n'est pas possible de paramétrer dans SDMC les politiques définies dans Stormshield Data Authority Manager. Pour obtenir de l'aide sur la reproduction des politiques de sécurité dans SDMC et la migration des clés de chiffrement et signature des utilisateurs de la version 10 vers la version 11 de SDS Enterprise, veuillez contacter votre équipe commerciale Stormshield.

Dans les Propriétés de l'agent SDS Enterprise, les icônes des fonctionnalités suivantes ne sont plus disponibles : **File**, **Shredder**, **Virtual Disk** et **Mail**, ainsi que l'icône **Mise à jour automatique**. Ces fonctionnalités sont dorénavant entièrement paramétrables via la console d'administration SDMC.

La fonctionnalité Stormshield Data Mail pour Lotus Notes a été supprimée du produit SDS Enterprise.

Les cmdlets ou API .NET permettant la connexion ou déconnexion et le verrouillage ou déverrouillage du compte SDS Enterprise, disponibles via le composant Connector, sont désormais désactivées dans le cas où les utilisateurs se connectent à leur compte SDS Enterprise via le mode SSO.

L'agent SDS Enterprise version 11.0 est uniquement disponible pour les postes de travail sous Microsoft Windows 64 bits.

Correctifs de SDS Enterprise 11.4.2

Stormshield Data Team

Références support STORM-58628, STORM-59406

Il est désormais possible de déplacer un fichier protégé par Stormshield Data Team depuis un serveur de fichiers vers un espace non protégé de l'ordinateur sans provoquer un écran bleu.

Référence support STORM-48

Correction d'une anomalie empêchant Stormshield Data Team de chiffrer des fichiers de taille inférieure ou égale à 4 Ko.

Stormshield Data Connector

Référence support STORM-59113

Correction d'une incompatibilité entre l'agent SDS Enterprise et la dernière version de PowerShell 5. L'installation du composant Stormshield Data Connector sur les postes de travail rendait PowerShell 5 inutilisable.

Compatibilité

Consultez le document Cycle de vie produits pour connaître les informations de compatibilité avec les versions de Microsoft Windows.

Navigateurs web (serveur)

Microsoft Edge	Dernière version stable
Google Chrome	Dernière version stable
Mozilla Firefox	Dernière version stable

Synchroniseurs pour la protection automatique de documents

SharePoint Online/Office 365
OneDrive Entreprise/for Business dans Office 365
SharePoint 2016 (on-premises)

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SDS Enterprise est consultable sur la Base de connaissances Stormshield (anglais uniquement). Pour vous connecter à la Base de connaissances, utilisez les mêmes identifiants que sur votre espace client MyStormshield.

Précisions sur les cas d'utilisation

Stormshield Data Management Center

SDMC ne permet pas de gérer une infrastructure à clé publique (PKI), contrairement à Stormshield Data Authority Manager version 10.

Cartes à puce/tokens

Pour que le middleware SDS Enterprise fonctionne correctement, les "Smart Card Minidrivers" du support cryptographique concerné doivent être installés sur le poste de travail.

Le changement de lecteur pour un même support cryptographique au cours d'une même session Windows n'est pas supporté. Si vous avez commencé à utiliser une carte dans un lecteur donné, vous devez redémarrer votre session Windows pour pouvoir utiliser cette carte dans un autre lecteur.

La création d'un compte sur une carte virtuelle n'est possible qu'avec des clés RSA d'une taille de 2048 bits maximum. Cette limitation vaut également pour un compte de type SSO dont les clés sont stockées sur une carte virtuelle.

Les cartes virtuelles (Virtual Smart Card de Microsoft) et certains types de cartes à puce associées à leur middleware ne supportent pas l'algorithme de chiffrement RSA-OAEP-SHA-256. Cette incompatibilité empêche le déchiffrement des fichiers *.sdsx*. Pour plus d'informations, reportez-vous à la Base de connaissances (anglais uniquement).

Kernel

Après l'installation de l'agent SDS Enterprise ou un changement dans la politique de sécurité, il est nécessaire de redémarrer le poste de travail pour que la politique soit correctement prise en compte.

Brancher simultanément deux supports cryptographiques (token ou/et carte) sur une machine peut entraîner des dysfonctionnements. Cette restriction ne s'applique pas lorsque le middleware Stormshield Smartcard Support est utilisé.

Lorsque le paramétrage Windows d'affichage des éléments est configuré à plus de 100%, le bandeau SDS de la mire de connexion ou de la fenêtre « A propos » ne prend pas toute la taille de la fenêtre.

Lors d'un import de clés PGP, le redimensionnement de la fenêtre **Mot de passe requis** entraîne un mauvais positionnement des boutons **Annuler** et **OK**.

Lors de la sélection d'un correspondant depuis l'annuaire LDAP pour une opération de chiffrement, dans le cas où le correspondant dispose de plusieurs certificats, SDS Enterprise propose toujours le certificat le plus récent même si celui-ci est révoqué. L'opération de

chiffrement échoue donc. Nous vous recommandons de supprimer les certificats révoqués de votre annuaire LDAP.

Lors de l'installation sur le poste de travail d'un utilisateur d'un compte *.usi* provenant du SDAM, les valeurs des paramètres issues du fichier de configuration de la politique *.json* prévalent au démarrage du kernel et à la connexion de l'utilisateur.

Le type de compte SSO pour se connecter au compte SDS Enterprise s'appuie sur le fonctionnement du type de compte Carte ou token USB. L'installation de l'extension carte des agents est donc nécessaire pour le faire fonctionner.

En cas de blocage d'un compte SDS Enterprise, seul le déblocage de compte Mot de passe via le mot de passe de secours est possible.

Il n'est pas possible de désactiver un protocole de téléchargement de listes de révocation en particulier (HTTP, FILE, etc.).

La date de dernier téléchargement de la liste de révocation n'est plus affichée dans le contrôleur de révocation. Cependant une entrée dans le journal d'événements Windows est générée.

Le certificat du compte de recouvrement doit disposer des usages de chiffrement de données (Data Encipherment) et de chiffrement de clés (Key Encipherment).

Stormshield Data File

Gestion des accès des utilisateurs - il n'est pas possible d'utiliser le menu "Modifier l'accès" en sélectionnant à la fois des fichiers et des dossiers.

Les documents Microsoft OneNote ne sont actuellement pas supportés par SDS Enterprise.

Lorsqu'on protège un fichier au format *.sdsx* ou que l'on retire la protection d'un fichier .sdsx, les droits Windows appliqués sur le fichier sont restreints au seul utilisateur de la session et à l'héritage du dossier parent.

Si la sauvegarde d'un document protégé en cours d'édition est impossible (le document a été renommé ou supprimé entre temps, ou bien le document se trouve sur un partage réseau et la connexion est interrompue), l'utilisateur doit modifier l'emplacement de sauvegarde ou renommer son document.

Les clés RSA des certificats strictement inférieures à 2048 bits ne sont pas supportées pour le format SDSX.

La protection des dossiers de déchiffrement temporaire en local avec la fonctionnalité Team n'est pas supportée.

Stormshield Data Share

La protection automatique de dossiers n'est pas supportée pour les dossiers déjà protégés par Team.

Par défaut, les applications Microsoft ne sont pas autorisées à "Enregistrer sous" dans les espaces collaboratifs synchronisés afin d'éviter de diffuser les fichiers en clair.

Lorsque la protection automatique de documents est activée sur un dossier et que vous utilisez la fonction "Enregistrer sous" sur les applications concernées, vous devez fermer l'application à l'origine de l'enregistrement pour que le fichier soit visible dans le dossier protégé automatiquement.

Le chemin du document à partir de la racine du dossier synchronisé ne doit pas contenir plus de 185 caractères, extension comprise (e.g., .pptx, .sdsx). Sinon, le document ne sera pas protégé et ne sera plus accessible.

Lorsqu'on applique une règle de protection automatique sur le contenu d'un dossier ou lorsqu'on retire la protection du contenu d'un dossier après désactivation d'une règle de protection automatique, les droits Windows appliqués sur les fichiers contenus dans le dossier sont restreints au seul utilisateur de la session et à l'héritage du dossier.

La fonctionnalité Share n'est pas supportée sur un partage réseau, un serveur de fichiers ou un lecteur externe.

Si l'icône "cadenas" n'est pas visible sur un dossier protégé, vérifiez dans la base de registre, dans "Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers", que les clés suivantes sont bien positionnées au-dessus des clés existantes dans l'arborescence :

- EncrypterOverlayIcon
- SDSShareOverlayIcon

Si ce n'est pas le cas, ajoutez des espaces devant leur nom puis redémarrez l'Explorateur pour prendre en compte la modification.

Il n'est pas possible de modifier la protection d'un dossier si vous avez déjà protégé ou modifié l'accès d'un de ses sous-dossiers ou d'un de ses dossiers parents.

Gestion des accès des utilisateurs - il n'est pas possible d'utiliser le menu "Modifier l'accès" :

- en sélectionnant à la fois des fichiers et des dossiers.
- sur une sélection simultanée de plusieurs dossiers protégés ou sur un dossier non protégé.

Partage des règles de protection

Pour qu'une règle de protection partagée sur un dossier s'applique à un utilisateur, il doit être connecté à son compte SDS Enterprise, figurer parmi les destinataires de la règle et naviguer dans le dossier concerné.

Une règle de protection automatique définie localement sur un dossier d'espace collaboratif par un utilisateur et sans partage est écrasée si un autre utilisateur définit une règle partagée sur le même dossier, incluant le premier utilisateur.

Si deux utilisateurs définissent une règle de protection partagée différente sur le même dossier, la règle la plus récente est prise en compte.

Lorsqu'un utilisateur supprime un dossier portant une règle de protection partagée en le plaçant dans la corbeille, la règle reste active tant que la corbeille n'est pas vidée.

Il n'est pas possible de transformer une règle de protection partagée en une règle non partagée, et inversement.

Stormshield Data Mail

La fonctionnalité de rappel de messages de Microsoft Outlook n'est pas compatible avec le chiffrement de Stormshield Data Mail.

Il n'est pas possible d'envoyer un message chiffré vers un destinataire sur Microsoft Exchange en mode hors connexion dans Microsoft Outlook. La connexion est nécessaire à la résolution des adresses SMTP.

Il n'est parfois pas possible d'ouvrir un fichier .sdsx joint à un message chiffré. Il est donc préférable de télécharger la pièce jointe avant de l'ouvrir.

Il n'est pas possible d'ouvrir un message PGP reçu en pièce jointe (.msg) en faisant un glisser-déposer dans un dossier d'Outlook.

Lorsque le volet de lecture Outlook est désactivé, un simple double-clic ne permet pas d'ouvrir un message chiffré volumineux. Vous devez double-cliquer deux fois sur le message.

La rédaction d'un nouveau message chiffré via le menu **Démarrer**, alors qu'Outlook est arrêté, ne fait pas apparaître le bandeau de chiffrement. Ce message sera cependant correctement chiffré.

L'add-in Mail est incompatible avec Kaspersky Outlook Anti-Virus Addin. Dans le cas où les certificats du destinataire ne sont pas accessibles, des messages peuvent être envoyés non chiffrés.

Retirer la carte à puce pour verrouiller un compte carte SDS Enterprise pendant une sauvegarde de message n'est pas recommandé car la sauvegarde ne sera pas effectuée.

Il n'est pas possible d'ouvrir un fichier *.msg* chiffré ou signé avec Outlook via l'Explorateur Windows. Dans ce cas, veuillez appliquer le contournement décrit dans la Base de connaissances Stormshield (authentification nécessaire).

Stormshield Data Virtual Disk

Il n'est pas recommandé d'utiliser un volume Virtual Disk sur un espace distant. Une perte de connexion pourrait rendre l'accès au disque impossible ou entraîner la perte de modifications réalisées sur le disque.

Stormshield Data Team

Stormshield Data Team n'est pas compatible avec l'outil de sauvegarde Veeam. Cet outil rend le chiffrement de dossier protégé par une règle Team impossible.

Sous Microsoft Windows 10 et 11, lorsque l'on chiffre un dossier, l'icône SDS Enterprise en forme de cadenas n'apparaît pas toujours sur les fichiers chiffrés. Les fichiers sont cependant correctement chiffrés.

Le système de sauvegarde de volumes Shadow Copy, sur lequel repose notamment la gestion des versions sous Windows Explorer, n'est pas supporté par Stormshield Data Team.

Les répertoires synchronisés de type SharePoint, Dropbox, Office 365, Google Drive on premise, etc. ne sont pas supportés par Stormshield Data Team et ne peuvent donc pas être sécurisés par le module. Nous vous recommandons d'exclure ces répertoires des dossiers analysés par Stormshield Data Team grâce au paramètre avancé **Exclusion de dossiers** disponible dans la configuration de la fonctionnalité Team dans la console d'administration SDMC.

L'utilisateur doit être connecté à son compte SDS Enterprise ou doit le déverrouiller lorsqu'il souhaite copier-coller un fichier dans un dossier sécurisé par Stormshield Data Team s'il existe déjà un fichier du même nom dans le dossier. S'il réalise l'opération sans être connecté, le contenu du fichier est vidé.

L'utilisateur doit être connecté à son compte SDS Enterprise ou doit le déverrouiller s'il souhaite modifier un dossier compressé *.zip* contenu dans un dossier sécurisé par Stormshield Data Team. S'il modifie un dossier *.zip* sans être connecté, les fichiers à l'intérieur sont supprimés.

Stormshield Data Shredder

Il n'est pas possible de supprimer définitivement des dossiers synchronisés OneDrive avec la fonctionnalité Shredder. Néanmoins les fichiers contenus dans ces dossiers peuvent être supprimés avec Shredder.

SDS Encryption Portal

En mode "PKI externe" et sur téléphone mobile uniquement, lorsque les utilisateurs du portail de chiffrement se connectent via la solution Microsoft Entra ID, si la double authentification n'est pas paramétrée, ils doivent s'authentifier une première fois puis cliquer de nouveau sur **Se connecter avec Microsoft**.

Ressources documentaires

Les ressources documentaires techniques suivantes sont disponibles sur le site de Documentation Technique Stormshield. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

Guides

- Stormshield Data Security Enterprise - Guide d'administration
- Stormshield Data Security Enterprise - Guide de configuration avancée
- Stormshield Data Security Enterprise - Guide d'utilisation avancée
- Stormshield Data Security Enterprise - Guide de l'utilisateur
- Stormshield Data Security Enterprise - Guide Architecture et sécurité
- Stormshield Data Authority Manager - Guide d'utilisation
- Stormshield Data Connector - Guide d'utilisation

Télécharger cette version

Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel MyStormshield afin de télécharger la version 11.4.2 de Stormshield Data Security Enterprise :

1. Connectez-vous à votre espace MyStormshield avec vos identifiants personnels.
2. Dans le panneau de gauche, sélectionnez la rubrique **Téléchargements**.
3. Dans le panneau de droite, sélectionnez le produit qui vous intéresse puis la version souhaitée.

Vérifier l'intégrité des binaires

Afin de vérifier l'intégrité des binaires Stormshield Data Security Enterprise :

1. Entrez l'une des commandes suivantes en remplaçant `filename` par le nom du fichier à vérifier :
   - Système d'exploitation Linux : `sha256sum filename`
   - Système d'exploitation Windows : `CertUtil -hashfile filename SHA256`
2. Comparez le résultat avec les empreintes (hash) indiquées sur votre espace client MyStormshield, rubrique **Téléchargements**.

Versions précédentes de SDS Enterprise v11

Retrouvez dans cette section les nouvelles fonctionnalités et correctifs des versions précédentes de Stormshield Data Security Enterprise 11.x.

11.4.1	Nouvelles fonctionnalités	
11.4	Nouvelles fonctionnalités	Correctifs
11.3	Nouvelles fonctionnalités	Correctifs
11.2.1		Correctifs
11.2	Nouvelles fonctionnalités	Correctifs
11.1.1		Correctifs
11.1	Nouvelles fonctionnalités	Correctifs
11.0	Nouvelles fonctionnalités	Correctifs

Nouvelles fonctionnalités et améliorations de SDS Enterprise 11.4.1

Stormshield Data Management Center (SDMC)

Un nouvel onglet **Politiques** > **Comptes** > **Connexion** permet de configurer le comportement de l'agent SDS Enterprise lors :

- De l'activation de l'économiseur d'écran,
- Du verrouillage de la session Windows,
- Du retrait de la carte à puce ou token USB.

Vous pouvez également configurer ces paramètres dans le fichier des politiques de sécurité au format *.json*.

En savoir plus

Agent SDS Enterprise

Virtual Disk

Le raccourci Virtual Disk est désormais disponible dans l'onglet **Propriétés** > **Configuration** de l'agent SDS Enterprise. Ce raccourci permet d'accéder aux volumes de l'utilisateur.

Paramètres de connexion

Dans les propriétés de l'agent SDS Enterprise, l'onglet **Écran de veille** n'existe plus dans le menu **Connexion**. Les options permettant de configurer le comportement de l'agent lors de l'activation de l'économiseur d'écran et du verrouillage de la session Windows sont désormais configurables dans SDMC.

Nouvelles fonctionnalités et améliorations de SDS Enterprise 11.4

Administration de SDS Enterprise

Arrêt du support du fichier de configuration *SBox.ini*

Afin de simplifier le déploiement et l'administration de SDS Enterprise, les paramètres qui se trouvaient dans le fichier de configuration *SBox.ini* ont été déplacés et ce fichier n'est plus nécessaire.

Les paramètres de configuration se trouvent désormais soit dans le fichier au format *.json* des politiques de sécurité soit dans la base de registre Windows. Certains autres paramètres ont été remplacés par des valeurs fixes dans le code ou bien supprimés.

Pour vous aider :

- un outil de migration est disponible sur demande,
- un *Guide de migration* est disponible sur le site de la Documentation technique.

En savoir plus

Stormshield Data Management Center (SDMC)

Conversion des fichiers chiffrés *.sbox* au format *.sdsx*

Afin de vous aider à convertir vos fichiers chiffrés de l'ancien format *.sbox* au nouveau format plus sécurisé *.sdsx*, vous pouvez désormais configurer dans la politique de sécurité la conversion automatique de ces fichiers lorsque l'utilisateur les ouvre. L'opération est transparente pour lui et le format *.sdsx* permet, entre autre, de ne pas avoir à rechiffrer les fichiers après utilisation. Retrouvez ces nouvelles options dans le menu **Politiques** > **Fonctionnalités** > **File** de SDMC et dans les paramètres du fichier de configuration *.json*.

En savoir plus

Gestion du porte-clés des utilisateurs

Dans le nouvel onglet **Porte-clés** du menu **Politiques** > **Comptes**, vous choisissez d'afficher ou non les onglets permettant de gérer les clés de chiffrement, de signature, de déchiffrement et de recouvrement du porte-clés des utilisateurs.

En savoir plus

Agent SDS Enterprise

Icône SDS Enterprise personnalisée sur les dossiers d'espaces collaboratifs synchronisés protégés

Désormais pour personnaliser l'icône des dossiers d'espaces collaboratifs synchronisés protégés par la fonctionnalité Stormshield Data Share et permettre de les identifier facilement, vous pouvez ajouter une clé de registre. Elle permet de remplacer l'icône de dossier Windows par défaut par une icône SDS Enterprise.

En savoir plus

Correctifs de SDS Enterprise 11.4

Agent SDS Enterprise

Référence support STORM-52916

SDS Enterprise en mode SSO démarre désormais correctement, même si un certificat du magasin personnel est mal formaté.

Choix des correspondants

Référence support STORM-51540

La fenêtre de choix des correspondants récupère désormais le bon statut de la liste de révocation lors de l'ajout d'un collaborateur à un fichier chiffré.

Stormshield Data Team

Référence support STORM-50534

Correction d'une anomalie empêchant l'ajout d'un collaborateur alors que son certificat est valide.

Lorsque l'utilisateur déplace des fichiers dans un dossier sécurisé par Stormshield Data Team :

- Si le certificat d'un collaborateur avec qui le dossier est partagé présente une erreur (e.g., révoqué, chaîne de parenté révoquée ou indisponible), alors le chiffrement a systématiquement lieu **sauf** pour le collaborateur en question.
- Si le certificat d'un collaborateur avec qui le dossier est partagé présente un avertissement (e.g., expiré, CRL expirée ou indisponible), alors le chiffrement a systématiquement lieu, **y compris** pour le collaborateur en question.

  Auparavant, dans ces mêmes cas, l'utilisateur pouvait annuler l'action de chiffrement.

Stormshield Data Shredder

Référence support STORM-51107

SDS Enterprise demande désormais confirmation à l'utilisateur avant de broyer le premier fichier d'une sélection multiple.

Stormshield Data Virtual Disk

Référence support STORM-11289

Correction d'une anomalie empêchant le démontage des volumes sécurisés.

Nouvelles fonctionnalités et améliorations de SDS Enterprise 11.3

Politique de sécurité SDS Enterprise

Chiffrement et signature automatiques des messages avec Microsoft Purview

Si votre société utilise le système d'étiquettes de confidentialité proposé par Microsoft Purview Information Protection, vous pouvez dorénavant déclarer ces étiquettes dans les paramètres de la fonctionnalité Mail d'une politique de sécurité et y associer une action automatique de l'agent. Lorsque l'utilisateur applique une étiquette à un message, l'agent vérifie alors la présence de l'étiquette dans la politique et déclenche l'action de sécurisation correspondante : chiffrement seul du message, signature seule du message ou la combinaison des deux actions.

En savoir plus

Gestion des règles de protection partagées

Dans les paramètres de la fonctionnalité Share d'une politique de sécurité, vous pouvez désormais rendre obligatoire ou bien interdire la création de règles partagées lorsqu'un utilisateur crée une règle de protection automatique d'un dossier directement depuis son poste de travail. Par défaut, l'utilisateur a le choix de partager ou non une règle lorsqu'il la crée.

En savoir plus

Chiffrement Windows automatique du répertoire temporaire de déchiffrement de fichiers

Dans les paramètres de la fonctionnalité File d'une politique de sécurité, vous pouvez désormais activer le chiffrement Windows automatique du répertoire SDS Enterprise, appelé *Decrypted*, qui permet de stocker temporairement les fichiers *.sdsx* lorsqu'ils sont en cours de modification par l'utilisateur.

En savoir plus

SDS Encryption Portal

Le portail SDS Encryption Portal, permettant de lire et protéger des documents confidentiels dans un navigateur internet, offre désormais la possibilité d'utiliser votre propre solution de PKI, en choisissant le mode d'utilisation "PKI externe" lors de la création du tenant de votre organisation. Vous utilisez ainsi les clés de chiffrement des utilisateurs qui sont déjà en vigueur dans l'organisation. Dans ce mode, l'authentification des utilisateurs auprès du portail fonctionne exclusivement avec la solution de gestion des identités Microsoft Entra ID.

Ce mode permet également à SDS Encryption Portal d'être interopérable avec SDS Enterprise. Les documents chiffrés via le portail web, au format *.sdsx*, peuvent être maintenant déchiffrés via l'agent SDS Enterprise et inversement.

Le mode "PKI externe" est actuellement disponible en version Bêta. Contactez votre commercial Stormshield si vous souhaitez mettre en place cette solution.

Pour en savoir plus sur SDS Encryption Portal, consultez le ***Guide d'administration et d'utilisation*** et les ***Nouveautés*** du portail.

Correctifs de SDS Enterprise 11.3

Stormshield Data Team

Référence support STORM-6995

Il est désormais possible de chiffrer des fichiers *.pdf* dans un dossier sécurisé par Stormshield Data Team lorsqu'ils sont enregistrés via le navigateur Microsoft Edge.

Recherche de correspondants

Référence support STORM-12166

Résolution d'un problème d'affichage lors de la recherche de correspondants préalable à une opération de chiffrement.

Correctifs de SDS Enterprise 11.2.1

Stormshield Data Team

Lorsque vous créez via l'explorateur Windows une archive *.zip* d'un sous-dossier dans un dossier sécurisé avec Stormshield Data Team, l'archive est désormais correctement chiffrée.

Les fichiers déplacés dans un dossier se trouvant sur un partage réseau et sécurisé par Stormshield Data Team sont désormais correctement chiffrés.

Référence support STORM-48

En présence de l'antivirus McAfee, les fichiers de moins de 2 Ko sont désormais correctement chiffrés par Stormshield Data Team.

Référence support STORM-50

Les caractères "~00" ne s'affichent plus dans le nom des fichiers lors du chiffrement de certains fichiers par Stormshield Data Team.

Stormshield Data Shredder

Référence support STORM-10612

La suppression définitive du contenu de la corbeille Windows avec Stormshield Data Shredder fonctionne désormais correctement.

Recherche de collaborateurs

Référence support STORM-8943

Dans la fenêtre **Choix de vos correspondants**, la recherche LDAP sur les adresses de messagerie et à la fois sur le nom commun de collaborateurs est désormais possible.

Comptes Single Sign-On (SSO)

Référence support STORM-8068

Il est désormais possible de créer un compte utilisateur SSO même si des certificats expirés sont présents dans le magasin Windows.

Nouvelles fonctionnalités et améliorations de SDS Enterprise 11.2

AVERTISSEMENT AVANT LA MISE À JOUR DE L'AGENT
À partir de la version 11.1.1 de SDS Enterprise, l'agent est désormais installé par défaut avec une politique de sécurité.
Par conséquent, si vous utilisez déjà une politique de sécurité personnalisée sur votre parc, elle sera remplacée par la politique par défaut lors de la mise à jour de l'agent. Vous devrez alors déployer de nouveau votre politique après la mise à jour.
Ce redéploiement de politique personnalisée ne sera pas nécessaire lors des prochaines mises à jour de l'agent d'une version 11.1.1 vers une version supérieure.

Agent SDS Enterprise

Partage des règles de protection avec la fonctionnalité Stormshield Data Share

Lorsque vous utilisez la fonctionnalité Stormshield Data Share pour protéger automatiquement des dossiers synchronisés avec vos espaces collaboratifs, vous pouvez maintenant partager les règles de protection avec vos collaborateurs. Une fois que la règle est créée sur un dossier, elle s'applique automatiquement à tous les collaborateurs listés dans la règle et leurs fichiers sont protégés lorsqu'ils sont placés dans le dossier.

Cette fonctionnalité est disponible dans l'interface de l'agent via une case à cocher dans la fenêtre de sélection des collaborateurs, ainsi que via les commandes PowerShell utilisables avec Stormshield Data Connector.

En savoir plus

Modification de l'accès des collaborateurs à un fichier ou un dossier

Le nouveau menu **Modifier l'accès** permet aux utilisateurs présents dans une règle de protection de donner ou de supprimer l'accès à des collaborateurs. Le menu peut être utilisé sur un dossier, sur un fichier ou sur plusieurs fichiers à la fois.

En savoir plus

Correctifs de SDS Enterprise 11.2

Stormshield Data File

Référence support : STORM-3352

Une erreur qui pouvait bloquer le chiffrement simultané de deux fichiers a été corrigée.

Stormshield Data Virtual Disk

Référence support : STORM-171

La vitesse de création des disques virtuels a été augmentée.

Stormshield Data Team

Référence support : STORM-44

Une erreur de traitement pouvant empêcher le déchiffrement de fichiers avec la fonctionnalité Stormshield Data Team a été corrigée.

Recherche de collaborateurs

Référence support : STORM-108

Le temps de recherche dans l'annuaire LDAP via la fenêtre d'ajout de collaborateurs lors de chiffrement de fichiers, de dossiers ou de disques virtuels a été amélioré.

Correctif de SDS Enterprise 11.1.1

AVERTISSEMENT AVANT LA MISE À JOUR DE L'AGENT
À partir de la version 11.1.1 de SDS Enterprise, l'agent est désormais installé par défaut avec une politique de sécurité.
Par conséquent, si vous utilisez déjà une politique de sécurité personnalisée sur votre parc, elle sera remplacée par la politique par défaut lors de la mise à jour de l'agent. Vous devrez alors déployer de nouveau votre politique après la mise à jour.
Ce redéploiement de politique personnalisée ne sera pas nécessaire lors des prochaines mises à jour de l'agent d'une version 11.1.1 vers une version supérieure.

Stormshield Data Virtual Disk

Référence support : STORM-154
Un crash mémoire qui pouvait bloquer la mise à jour de l'agent SDS Enterprise d'une version 10 vers une version 11 a été corrigé.

Nouvelles fonctionnalités et améliorations de SDS Enterprise 11.1

Stormshield Data Management Center (SDMC)

Gestion des clés pour l'utilisation de l'API SDMC

Un nouvel onglet **Clés API** est disponible dans SDMC. Il permet aux administrateurs possédant le droit **Gérer les clés API** de créer des clés API, valables un an par défaut. Les clés API permettent d'utiliser l'API publique de SDMC, notamment afin d'accéder aux logs d'administration. Les administrateurs peuvent également supprimer définitivement ces clés.

En savoir plus

Accès aux logs d'administration via l'API SDMC

Vous pouvez désormais accéder aux logs de connexion des administrateurs via l'API SDMC. Ces logs indiquent entre autre le mode de connexion employé par les administrateurs (mot de passe ou SAML).

Les logs d'administration qui étaient déjà accessibles depuis la version 1 de SDMC via l'API sont toujours disponibles.

Signature des politiques de sécurité

L'algorithme PS256 est désormais utilisé par défaut lors de la signature des politiques. Le précédent algorithme de signature RS256 reste fonctionnel avec l'utilitaire de signature et l'Agent SDS Enterprise.

En savoir plus

Gestion des clés et certificats des utilisateurs dans les comptes Mot de passe

Dans le menu **Comptes** > **Création** d'une politique de sécurité, puis dans l'encart **Création de compte Mot de passe**, les cases à cocher permettant de sélectionner la provenance des clés et certificats des utilisateurs ont été remplacées par une liste déroulante.

Exclusion de dossiers du chiffrement par la fonctionnalité Team

Dans les paramètres de la fonctionnalité Team d'une politique de sécurité, vous pouvez désormais établir une liste de dossiers sur lesquels un utilisateur ne pourra pas créer de règle de sécurité Team pour sécuriser automatiquement le dossier. La liste est récursive, elle inclut automatiquement les sous-dossiers.

En savoir plus

Mode d'effacement sécurisé d'un fichier avec la fonctionnalité Shredder

Dans les paramètres avancés de la fonctionnalité Shredder d'une politique de sécurité, vous pouvez désormais configurer le mode d'effacement sécurisé des fichiers. Auparavant la fonctionnalité écrivait en plusieurs passes une série de caractères en octets par défaut à la place du contenu du fichier. SDMC permet maintenant de choisir les valeurs des passes successives qui remplacent le contenu à effacer.

En savoir plus

Import de politiques de sécurité dans SDMC

Il est désormais possible d'importer dans SDMC une politique de sécurité au format *.json*, précédemment téléchargée depuis SDMC. Les annuaires LDAP et les certificats des autorités de certification indiqués dans la politique ne sont toutefois pas importés.

En savoir plus

Configuration avancée des politiques de sécurité

Les changement suivants ont été apportés dans les paramètres JSON des politiques de sécurité :

- Dans la section *accountPolicy - creation - automatic*, les paramètres *encryptionKeyAuthorityId* et *signatureKeyAuthorityId* sont dorénavant optionnels.
- Dans la section *accountPolicy - parameters- cryptography*, le nouveau paramètre optionnel *keyEncryptionMethod* permet de choisir l'algorithme à utiliser lors du chiffrement des clés.
- Dans la section *diskPolicy*, le nouveau paramètre *encryptionAlgorithm* permet de choisir l'algorithme à utiliser lors du chiffrement des volumes virtuels sécurisés.

Agent SDS Enterprise

Mise à jour d'un signataire de politique

Les utilisateurs sont désormais informés après la mise à jour du signataire de la politique de sécurité utilisée avec l'agent SDS Enterprise.

En savoir plus

Chiffrement de volumes avec la fonctionnalité Virtual Disk

L'algorithme de chiffrement AES-XTS peut désormais être utilisé pour chiffrer les volumes virtuels sécurisés générés avec l'agent SDS Enterprise.

En savoir plus

Correctifs de SDS Enterprise 11.1

Stormshield Data Mail

Référence support : STORM-56

Une erreur due à une politique invalide ou un certificat de signature expiré s'affichait à l'ouverture de chaque message Outlook. Le problème a été corrigé par l'application de permissions moins restrictives.

Référence support : STORM-57

Un seul clic sur **Envoyer** est désormais suffisant pour envoyer un message lorsque plusieurs serveurs LDAP sont déclarés, et que l'un d'entre eux n'est pas fonctionnel.

Agent SDS Enterprise

Référence support : STORM-15

L'agent SDS Enterprise fonctionne désormais correctement lorsqu'il est installé conjointement avec le logiciel Sentinel One.

Fonctionnalités et améliorations de Stormshield Data Security Enterprise 11.0

Stormshield Data Management Center (SDMC)

Administration de SDS Enterprise

L'administration de SDS Enterprise s'effectue désormais dans l'interface d'administration web 11.3 qui propose entre autres les fonctionnalités suivantes :

- Définir de manière centralisée les annuaires LDAP pour les utiliser ensuite lors de la création de politiques,
- Définir de manière centralisée les certificats d'autorité ainsi que les certificats de recouvrement de données pour les utiliser ensuite lors de la création de politiques,
- Configurer les politiques de sécurité pour les agents SDS Enterprise, puis les générer au format *.json*. Grâce à ces politiques, vous configurez l'utilisation des fonctionnalités de SDS Enterprise,
- Télécharger la dernière version de l'agent SDS Enterprise et l'outil de signature des politiques de sécurité. La signature permet de garantir l'authenticité et l'intégrité des politiques,
- Gérer l'accès des administrateurs d'un compte d'entreprise : vous pouvez inviter des administrateurs, les supprimer, ou modifier leurs droits.

Vous pouvez également configurer manuellement les politiques de sécurité directement dans les fichiers de configuration *.json*. Ces fichiers permettent le même niveau de configuration que Stormshield Data Authority Manager.

Pour plus d'informations sur la configuration des politiques et le déploiement des agents sur un parc, reportez-vous au *Guide d'administration* et au *Guide de configuration avancée* SDS Enterprise.

Mode SaaS

SDMC est en mode SaaS ; les nouvelles fonctionnalités et correctifs sont fournis en continu, indépendamment de la version de l'agent SDS Enterprise. À partir de la sortie commerciale de SDS Enterprise version 11, une page listant les dernières évolutions de 11.3 sera disponible sur le site Stormshield Technical Documentation et mise à jour en continu.

Authentification des administrateurs avec SAML

Vous pouvez désormais choisir entre deux modes de connexion pour accéder à SDMC : le mode classique avec adresse e-mail et mot de passe et le mode SAML, permettant de déléguer l'authentification des administrateurs à un fournisseur d'identité.

En savoir plus

Agent SDS Enterprise

Connexion Single Sign-on (SSO)

Grâce au mode SSO de Windows, les utilisateurs SDS Enterprise peuvent maintenant se connecter à l'agent directement via leur session utilisateur Windows. Les clés de chiffrement et de signature des utilisateurs sont stockées dans le Gestionnaire de certificats Microsoft.

En savoir plus

Protection automatique de dossiers et de sous-dossiers en local ou dans un espace synchronisé

La fonctionnalité Stormshield Data Share permet aux utilisateurs d'activer la protection automatique sur un dossier local ou un espace collaboratif. Elle permet aussi aux administrateurs de configurer la protection automatique de tout ou partie des espaces collaboratifs synchronisés de tous les utilisateurs. Les synchroniseurs supportés sont OneDrive, DropBox, SharePoint et Oodrive.

Le composant Stormshield Data Connector qui pilote les fonctionnalités de la solution SDS Enterprise à travers un module PowerShell ou des API .NET, permet désormais d'activer et de désactiver la protection automatique d'un espace synchronisé via la fonctionnalité Stormshield Data Share.

En savoir plus

Mise à jour des politiques de sécurité

Lorsqu'une mise à jour de politique de sécurité est disponible sur un point de distribution, les agents SDS Enterprise l'appliquent désormais automatiquement au démarrage du poste de travail de l'utilisateur.

En savoir plus

Sélection des collaborateurs

Lors de l'utilisation des fonctionnalités File, Team, Share et Virtual Disk, l'utilisateur peut désormais sélectionner des groupes d'utilisateurs avec qui collaborer. Ces groupes peuvent provenir de l'annuaire local de confiance ou d'un annuaire LDAP (Active Directory).

Amélioration des menus contextuels de l'agent

Les menus permettant l'utilisation des fonctionnalités File, Team et Share ont été réorganisés pour faciliter leur utilisation.

Documentation SDS Enterprise

La documentation technique de SDS Enterprise a été restructurée comme suit :

Le document ...	contient ...
Notes de version	• Changements de comportement, • Nouvelles fonctionnalités et améliorations, • Correctifs, • Compatibilité, • Précisions sur les cas d'utilisation.
Guide d'administration	• Installation et désinstallation de la solution, • Configuration et administration via SDMC, • Configuration des fonctionnalités File, Team, Share, Mail et Virtual Disk .

Le document ...	contient ...
Guide de configuration avancée	• Configuration et administration via le fichier de configuration d'une politique de sécurité au format *.json*, • Configuration via le fichier *SBox.ini* et les paramètres avancés de la base de registre, • Configuration des fonctionnalités File, Team, Share, Mail et Virtual Disk.
Guide d'utilisation avancée	• Utilisation avancée des fonctionnalités File, Team, Share, Mail, Shredder, Sign et Virtual Disk, à l'attention des administrateurs de la solution.
Guide de l'utilisateur	• Utilisation quotidienne des fonctionnalités File, Team, Share, Mail, Shredder, Sign et Virtual Disk, à l'attention des utilisateurs finaux de la solution.
Stormshield Data Connector	• Configuration et utilisation de Stormshield Data Connector.
Guide Architecture et Sécurité	• Informations techniques sur la confidentialité, l'intégrité et la disponibilité des données de nos utilisateurs.

Les informations contenues dans les anciens guides Stormshield Data File, Team, Mail, Shredder, Sign et Virtual Disk ont été réparties dans le guide d'administration, le guide de configuration avancée et le guide d'utilisation avancée.

Correctifs de Stormshield Data Security Enterprise 11.0

Stormshield Data Mail

Référence support : 208745CW

La désactivation de la sécurité d'un message est maintenant possible même lorsque le message ne contient pas l'adresse SMTP de l'émetteur.

Référence support : 199751CW

Lors de l'envoi d'un message sécurisé, le problème d'erreur indiquant que le message était trop volumineux dans certains cas a été corrigé.

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/
  La soumission d'une requête auprès du TAC doit se faire par le biais du gestionnaire d'incidents dans l'espace privé https://mystormshield.eu/, menu **Support technique** > **Gestion des tickets**.
- +33 (0) 9 69 329 129
  Afin d'assurer un service de qualité, veuillez n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace https://mystormshield.eu/.

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