STORMSHIELD DATA SECURITY ENTERPRISE

NOTES DE VERSION

Version 11

Dernière mise à jour du document : 5 juin 2024

Référence : sds-fr-sdse_notes_de_version-v11.1.1

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 11.0

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 cmdlet 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.

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.

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

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

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 clés publiques (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 un module TPM 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 un module TPM.

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.). Tous les protocoles sont correctement gérés.

La date de dernier téléchargement de la liste de révocation n'est plus affichée dans le contrôleur de révocation. Cependant un journal d'événement Windows est généré.

Stormshield Data File

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.

Dans le cas où 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 devra modifier l'emplacement de sauvegarde ou renommer son document.

Un document protégé par SDS Enterprise et stocké sur un partage réseau, qui est en cours de modification par un utilisateur autorisé, ne bloque pas la modification simultanée par un autre utilisateur autorisé.

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 autorisées, 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.

Afin que les documents déplacés dans un espace synchronisé Dropbox soient automatiquement protégés, utilisez le glisser-déplacer ou le copier-coller. Si vous utilisez le menu contextuel **Déplacer vers Dropbox** sur un document, celui-ci ne sera pas protégé.

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'arboresence :

- 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.

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, 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.

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 11.1.1 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.

11.1	Nouvelles fonctionnalités	Correctifs
11.0	Nouvelles fonctionnalités	Correctifs

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 11.1 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

11.1 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 11.1 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** > **Rapporter un incident/Suivre un incident**.
- +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.

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.