STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD CLIENT VPN IPSEC

NOTES DE VERSION

Version 1

Dernière mise à jour du document : 28 octobre 2026

Référence : sns-fr-client_vpn_ipsec-notes_de_version-v1.2

Table des matières

Historique des modifications 3
Version 1.2 4
Compatibilité 6
Problèmes connus 7
Ressources documentaires 8
Installer cette version 9
Versions précédentes du client VPN IPsec Stormshield v1 10
Contact 18

Dans la documentation, "Stormshield Client VPN IPsec" est nommé "client VPN IPsec Stormshield", et "Stormshield Network Security" est désigné sous la forme abrégée "SNS".

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

Historique des modifications

Date	Description
28 octobre 2026	Nouveau document

Version 1.2

Cette section liste les dernières évolutions de la version 1.2 du client VPN IPsec Stormshield.

Dernières évolutions de la licence Premium

Authentification

L'utilisation de la carte à puce pour l'authentification utilisateur a été simplifiée. La configuration d'un tunnel sur carte à puce ne nécessite plus la présence du certificat client. Par conséquent, la carte peut être absente au moment de la configuration.
Le certificat présent sur la carte lors de l'établissement du tunnel peut différer de celui présent lors de la configuration initiale, pour traiter par exemple le cas d'usage du renouvellement ou de remplacement du certificat.
L'utilisation de la carte à puce s'active désormais en cochant une case dédiée depuis l'interface du client VPN.

Pour plus d'informations, reportez-vous à la section Configuration manuelle du tunnel du *Guide d'installation et d'utilisation Stormshield Client VPN IPsec*.

Connexion automatique

Il est désormais possible d'établir automatiquement un tunnel utilisateur à l'ouverture de la session Windows (Mode "Always-on").
L'administrateur configure cette fonctionnalité depuis l'interface du client VPN via l'option **Connexion automatique**, puis exporte la configuration sur les postes cibles.
Si l'option est activée, l'utilisateur ne peut ni arrêter ni démarrer manuellement le tunnel. Il peut néanmoins « redémarrer » le tunnel en cas problème persistant.

Pour plus d'informations, reportez-vous à la section Configuration manuelle du tunnel du *Guide d'installation et d'utilisation Stormshield Client VPN IPsec*.

Réseau

Il est désormais possible de bloquer le trafic avant la connexion VPN si celle-ci n'est pas établie ou si elle est interrompue ("lock down"). Ceci permet d'empêcher que le trafic destiné au tunnel VPN quitte l'ordinateur en clair.

L'option **Bloquer le trafic avant la connexion VPN** est disponible si le mode **Connexion automatique** est activé. Elle doit être utilisée uniquement en cas de "full tunneling", car elle empêche d'accéder au trafic qui doit passer en dehors du tunnel VPN.

Pour plus d'informations, reportez-vous à la section Configuration manuelle du tunnel du *Guide d'installation et d'utilisation Stormshield Client VPN IPsec*.

Installation et configuration

Les certificats clients dont le champ "Utilisation de la clé" n'est pas conforme à un usage IKEv2 ne sont plus exploitables dans l'application : ils ne s'affichent pas dans la liste des certificats et ne peuvent pas être sélectionnés.

Extended Key Usage (EKU) est désormais supporté, ce qui permet d'enrichir les filtres liés à la sélection de certificats.
Le paramétrage des filtres s'effectue dans le fichier d'export JSON. Seules les valeurs officiellement reconnues et testées sont acceptées. À ce jour, la seule valeur supportée est *1.3.6.1.5.5.7.3.2* (clientAuth).

Pour plus d'informations, reportez-vous à la section **Configuration administrée du tunnel** du *Guide d'installation et d'utilisation Stormshield Client VPN IPsec*.

Compatibilité

Pour plus d'informations, reportez-vous à la section **VPN IPsec Client** du document *Cycle de vie produits Network Security & Tools*.

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version du client VPN IPsec Stormshield 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**.

Ressources documentaires

Les ressources documentaires techniques 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.

Merci de consulter la **Base de connaissances** Stormshield pour obtenir des informations techniques spécifiques créées par l'équipe du support technique (Technical Assistance Center).

Installer cette version

Pour installer ou mettre à jour le client VPN IPsec Stormshield, reportez-vous au **Guide d'installation et d'utilisation Stormshield Client VPN IPsec v1**.

Versions précédentes du client VPN IPsec Stormshield v1

Retrouvez dans cette section les nouvelles fonctionnalités, les vulnérabilités résolues et correctifs des versions précédentes du client VPN IPsec Stormshield v1.

1.1.1	Consulter
1.1	Consulter
1.0.1	Consulter
1.0	Consulter

Version 1.1.1

Cette section liste les dernières évolutions de la version 1.1.1 du client VPN IPsec Stormshield.

Dernières évolutions des licences Essential et Premium

Réseau
Dans certains cas, une anomalie pouvait empêcher l'établissement du tunnel VPN. Cette anomalie a été résolue.

Version 1.1

Cette section liste les dernières évolutions de la version 1.1 du client VPN IPsec Stormshield.

Introduction des licences Essential et Premium

Deux licences sont désormais disponibles pour le client VPN IPsec Stormshield. Selon la licence dont vous disposez, Essential ou Premium, vous bénéficiez de fonctionnalités avancées supplémentaires pour améliorer l'expérience de vos administrateurs et de vos utilisateurs.

Liste des fonctionnalités	Licence Essential	Licence Premium
VPN IPsec / IKEv2		
Profils IPsec standards	✓	✓
Profil IPsec DR ANSSI (Diffusion Restreinte)		✓
Configuration multi-tunnels VPN		✓
Fragmentation IKE, NAT-T	✓	✓
Mode Config	✓	✓
Négociation ESN	✓	✓
Childless IKEv2		✓
Authentification et gestion des certificats		
Clé partagée (PSK)	✓	✓
Certificat dans le magasin de certificats Windows	✓	✓
Certificat dans une carte à puce ou token		✓
Vérification et révocation des certificats (OCSP)	✓	✓
Mode de lancement du tunnel VPN		
Manuel	✓	✓
Fonctionnalités réseau avancées		
Dead Peer Detection (DPD)	✓	✓
Déploiement et configuration du client VPN		
Installation en local ou administrée	✓	✓
Configuration en local	✓	✓
Configuration administrée (EMM / GPO)		✓
Journaux d'événements Windows	✓	✓
Gestion des licences		
Mode SaaS avec libération automatique	✓	✓

Dernières évolutions de la licence Essential

Gestion des licences

Il est désormais possible d'importer et d'activer une clé de licence depuis l'interface utilisateur du client VPN IPsec Stormshield ou via un fichier de configuration. L'activation des licences s'effectue sur un serveur distant hébergé dans le Cloud. L'interface utilisateur permet de visualiser le type de licence souscrit (Essential ou Premium) et sa date d'expiration.

Pour plus d'informations, reportez-vous à la section **Licence** du *Guide d'installation et d'utilisation Stormshield Client VPN IPsec*.

Dernières évolutions de la licence Premium

Toutes les dernières évolutions de la licence Essential sont incluses.

Authentification utilisateur par certificat

L'authentification utilisateur par certificat X.509 v3 stocké dans une carte à puce est désormais supportée. Pour plus d'informations sur les références de cartes à puce testées, reportez-vous à la section **Annexe** du *Guide d'installation et d'utilisation Stormshield Client VPN IPsec*.

Configuration administrée - Sélection du certificat

L'administrateur peut désormais simplifier la sélection du certificat utilisateur en filtrant sur un ou plusieurs critères définis dans le fichier de configuration *.json*. Pour plus d'informations, reportez-vous à la section **Configuration administrée du tunnel** du *Guide d'installation et d'utilisation Stormshield Client VPN IPsec*.

Version 1.0.1

Cette section liste les dernières évolutions de la version 1.0.1 du client VPN IPsec Stormshield.

Utilisation du client VPN

Réseau

Le tunnel VPN se reconnecte désormais automatiquement en cas de sortie de veille prolongée.

Configuration VPN

La gestion des espaces superflus dans les champs de texte de la configuration du client VPN IPsec Stormshield a été améliorée.

Interface graphique

Le mode sombre du client VPN IPsec Stormshield a été amélioré.

Gestion des tunnels VPN

Les processus de réauthentification IKE et de renégociation des clés (*rekey*) ont été améliorés dans les modes de configuration réseau **Automatique** et **Manuel**.

Sécurité

Certains composants internes du client VPN IPsec Stormshield ont été mis à jour.

Fonctionnalités principales de Stormshield Client VPN IPsec 1.0

Le client VPN IPsec Stormshield vous permet de vous connecter de manière sécurisée à votre réseau d'entreprise. Il intègre les fonctionnalités suivantes.

Compatibilité et interopérabilité du client VPN IPsec Stormshield

- Systèmes d'exploitation : Windows 11, version 22H2 et supérieure. Il est recommandé d'utiliser Windows 11 Professionnel ou Windows 11 Entreprise.
- Firewalls SNS : versions 4.8 LTSB et versions 5, en IPsec standard ou en IPsec DR (Diffusion Restreinte).

VPN IPsec / IKEv2

Profils IPsec standards

Les algorithmes et fonctions cryptographiques suivants sont pris en charge :

Chiffrement	Échange de clés (Diffie-Hellman)
• AES CBC (128, 192 ou 256 bits) • AES CTR (128, 192 ou 256 bits) • AES GCM-16 (128, 192 ou 256 bits)	• Groupe 14 (MODP 2048 bits) • Groupe 15 (MODP 3072 bits) • Groupe 16 (MODP 4096 bits) • Groupe 17 (MODP 6144 bits) • Groupe 18 (MODP 8192 bits) • Groupe 19 (ECP 256 bits) • Groupe 20 (ECP 384 bits) • Groupe 21 (ECP 521 bits) • Groupe 28 (Brainpool ECP 256 bits) • Groupe 29 (Brainpool ECP 384 bits) • Groupe 30 (Brainpool ECP 512 bits)
Intégrité	
• SHA2 256 bits • SHA2 384 bits • SHA2 512 bits	
PRF (Pseudo-Random Function)	
• SHA 256 bits • SHA 384 bits • SHA 512 bits	

Profil IPsec DR ANSSI (Diffusion Restreinte)

Un profil IPsec DR est proposé lors de l'ajout d'une configuration VPN. Ce profil permet de configurer un VPN, tout en respectant le référentiel IPsec DR de l'ANSSI. Les suites cryptographiques suivantes sont proposées :

Suite	Chiffrement	Intégrité	Échange de clés (Diffie-Hellman)	PRF
1	AES GCM-16 256 bits	Aucune*	Groupe 19 (ECP 256 bits)	SHA 256 bits
2	AES GCM-16 256 bits	Aucune*	Groupe 28 (Brainpool ECP 256 bits)	SHA 256 bits
3	AES CTR 256 bits	SHA2 256 bits	Groupe 19 (ECP 256 bits)	SHA 256 bits
4	AES CTR 256 bits	SHA2 256 bits	Groupe 28 (Brainpool ECP 256 bits)	SHA 256 bits

(*) L'intégrité est nativement assurée par le mode de chiffrement GCM.

Configuration multi-tunnels VPN

Le client VPN IPsec Stormshield permet d'ajouter plusieurs configurations VPN. Notez qu'un seul tunnel VPN ne peut être établi à la fois.

Fragmentation IKE

La fragmentation des paquets IKEv2 est activée par défaut avec une taille maximale de 1280 octets. Il est possible de modifier cette taille ou de désactiver la fragmentation dans la configuration d'un VPN (paramètre **Fragmentation**).

NAT-T (*NAT-Traversal*)

Le NAT-T est pris en charge avec un port configurable pour IKE et ESP encapsulé (par défaut UDP/4500). Le NAT-T permet le passage du protocole IPsec au travers d'un réseau réalisant de la translation d'adresses dynamique.

Mode Config

Un mode automatique (également appelé "Mode Config" ou "*Configuration Payloads*" dans IKEv2, RFC 7296) permet de récupérer la configuration réseau (adresse IP, masque, serveurs DNS) auprès du serveur distant. Cette configuration réseau peut également être définie manuellement.

Négociation ESN

La négociation ESN (*Extended Sequence Number*, RFC 4304) peut être activée dans la configuration d'un VPN (paramètre **Exiger l'ESN**). Elle permet l'utilisation de compteurs 64 bits anti-rejeu sur IKEv2 et CHILD_SA. La négociation ESN est conçue pour gérer des débits élevés et de longues sessions.

Childless IKEv2

L'initiation IKEv2 sans CHILD_SA (RFC 6023) peut être activée dans la configuration d'un VPN (paramètre **Mode childless**). Activez ce paramètre pour des cas d'interopérabilité avancés.

Authentification et gestion des certificats

Clé partagée (PSK)

L'authentification utilisateur par clé pré-partagée est prise en charge.

Certificat stocké dans le magasin de certificats Windows

L'authentification utilisateur par certificat X.509 v3, stocké dans le magasin de certificats Windows, est prise en charge.

Mécanisme de vérification et de révocation des certificats (OCSP)

Le mécanisme de vérification et de révocation des certificats, à l'aide du protocole OCSP, peut être activé dans la configuration d'un VPN (paramètre **Vérification de la révocation du serveur**).

Mode de lancement du tunnel VPN

Manuel

Le tunnel VPN doit être établi manuellement par l'utilisateur après l'ouverture de sa session Windows. L'établissement automatique sera disponible dans une prochaine version du client VPN IPsec Stormshield.

Déploiement et configuration du client VPN

Installation en local ou administrée

Le client VPN IPsec Stormshield peut être installé et mis à jour via un package MSI :

- Soit localement sur un poste de travail en exécutant le package MSI,
- Soit de manière administrée, avec une stratégie de groupe (GPO, EMM ou MDM) ou en ligne de commande (CLI).

Pour plus d'informations, reportez-vous au Guide d'installation et d'utilisation Stormshield Client VPN IPsec v1.

Configuration en local ou administrée

- Le client VPN IPsec Stormshield peut être configuré localement sur un poste de travail en ajoutant des configurations VPN via l'interface graphique.
- Les configuration VPN peuvent être exportées ou importées dans le client VPN IPsec Stormshield. Le format pris en charge est le JSON. Notez que les secrets de la configuration VPN (PSK et certificats) ne sont pas exportés.
- Un parc de clients VPN IPsec Stormshield peut être configuré de manière administrée avec une stratégie de groupe (GPO, EMM ou MDM). Notez que les paramètres récupérés depuis le serveur ne peuvent pas être modifiés par l'utilisateur dans son client VPN IPsec Stormshield.

Journaux

Les journaux du client VPN IPsec Stormshield sont disponibles dans l'Observateur d'événements Windows.

Fonctionnalités réseau avancées

Mécanisme de *split tunneling*

Le mécanisme de *split tunneling* est pris en charge. Il permet de définir les flux qui doivent traverser le tunnel VPN pour atteindre des réseaux distants définis par des adresses IP ou des masques de sous-réseau de destination.

Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/

La soumission d'une requête auprès du support technique doit se faire par le biais du gestionnaire d'incidents présent dans l'espace client MyStormshield, menu **Support technique** > **Gestion des tickets**.

- +33 (0) 9 69 329 129

Afin de pouvoir assurer un service de qualité, il est recommandé de n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace client MyStormshield.



STORMSHIELD

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

Copyright © Stormshield 2026. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.