STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK VPN CLIENT EXCLUSIVE

NOTES DE VERSION

Version 7

Dernière mise à jour du document : 3 août 2023

Référence : sns-fr-vpn_client-exclusive-notes_de_version-v7.4

Table des matières

Dans la documentation, Stormshield Network VPN Client Exclusive est désigné sous la forme abrégée : SN VPN Client Exclusive et Stormshield Network Security sous la forme SNS.

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

Compatibilité

Stormshield Network Firewall

3.7, 3.11 et 4.x

Systèmes d'exploitation

Windows 10 64 bits sur processeurs x86-64
Windows 11 64 bits sur processeurs x86-64

NOTE
SN VPN Client Exclusive n'est pas compatible avec les ordinateurs, téléphones et tablettes équipés d'un processeur ARM.

Mode "Diffusion Restreinte (DR)" des firewalls SNS

SN VPN Client Exclusive version 7.4.018 est compatible avec le mode "Diffusion Restreinte (DR)" des versions SNS 4.3.12 et supérieures.

Compatibilité des fichiers de configuration

Les fichiers de configuration issus de versions précédentes du logiciel ne peuvent pas être importés dans la nouvelle version. Lors d'une mise à jour d'une version précédente, l'installateur de la nouvelle version convertit automatiquement la configuration. Ne désinstallez donc pas la version précédente avant de lancer l'installateur de la nouvelle version.

Nouvelles fonctionnalités et améliorations de la version 7.4.018

Fonctionnalités principales

- Le **Panneau TrustedConnect** gère désormais plusieurs connexions, y compris en mode GINA et lorsque le Mode filtrant est actif,
- Les demandes d'activation par le TAS sont étalées jusqu'à 90 jours avant la fin de l'abonnement afin d'éviter une surcharge du serveur TAS lorsqu'un grand nombre de licences doivent être renouvelées à la même date,
- Prise en charge de la sélection automatique du certificat utilisateur indépendamment de son support : token / carte à puce ou magasin de certificats Windows.

Améliorations

- La fenêtre de la **Console** disponible à partir du **Panneau TrustedConnect** adopte désormais le même comportement que celle disponible à partir du **Panneau des Connexions** :
  - L'option peut être activée ou désactivée dans le menu contextuel du **Panneau TrustedConnect**,
  - Le même raccourci clavier Ctrl+Alt+T pour activer ou désactiver la journalisation est disponible,
  - Un message dans la fenêtre de la **Console** indique désormais si la journalisation est activée ou désactivée, et une icône pour ouvrir le dossier où sont stockés les logs s'affiche lorsque la journalisation est activée.
- Les licences peuvent désormais être activées sur le serveur TAS après l'expiration de la période d'essai ou de l'abonnement lorsque *NoActivWin* et *AutoActiv* sont activés,
- À la suite des modifications que l'ANSSI a apportées à la [RFC 7296] en lien avec la conformité IPsec DR, la charge utile de demande de certificat doit dorénavant utiliser SHA-2 au lieu de SHA-1 pour les versions du logiciel exécutées en mode IPsec DR (nécessite la configuration d'un paramètre dynamique),
- Harmonisation du comportement entre les tunnels SSL/OpenVPN et IKEv2 qui utilisent un certificat client ayant un champ *key usage* incorrect ou une CA manquante : un avertissement s'affiche, mais il est toujours possible d'ouvrir le tunnel,
- Amélioration de la gestion des tunnels OpenVPN sans certificat : la configuration SSL peut toujours être importée, aucune erreur n'est générée dans la **Console** et il est toujours possible d'ouvrir le tunnel,
- Mise à jour d'OpenSSL à la version 1.1.1t,
- Les messages d'avertissement et les codes d'erreur ont été harmonisés entre le **Panneau des Connexions**, le **Panneau TrustedConnect** et le panneau affiché sur l'écran d'ouverture de session Windows lorsque le mode GINA est activé,
- Le tunnel s'ouvre désormais automatiquement lorsqu'une passerelle redondante est définie et que la passerelle principale envoie une demande de suppression (DELETE) suivie d'une demande de création (CREATE),
- Le réseau virtuel est forcé à 32 lorsque le mode CP n'est pas utilisé.

Correctifs de la version 7.4.018

- Correction d'un problème avec OpenVPN où la validation du certificat de la passerelle était désactivée par défaut,
- Correction d'un problème où la modification d'un port de balise TND n'était pas prise en compte,
- Correction d'un problème où la génération d'une charge utile d'authentification échouait lors de l'utilisation d'un certificat chargé automatiquement dans le magasin de certificats Windows lors de l'insertion d'une carte à puce ou d'un token, mais dont la clé privée reste sur la carte à puce ou le token,
- Correction d'un problème où l'onglet **Certificat** n'était plus mis à jour lors de l'insertion ou du retrait d'un token ou d'une carte à puce,
- Dans le cadre de l'utilisation de plusieurs cartes à puce, correction d'un problème où un tunnel était fermé de manière inopinée lors du retrait d'une carte à puce qui n'est pas utilisée avec le Client VPN,
- Correction d'un problème où l'installation du Client VPN était abandonnée sous Windows 11,
- En présence d'une passerelle redondante, la taille du SPI dans la proposition SA_INIT est définie à 8 au lieu de 0 lorsque le Client VPN bascule sur la passerelle redondante,
- Correction d'un problème où l'anneau indicateur de l'état de connexion du **Panneau TrustedConnect** restait gris pendant et après la détection d'un réseau de confiance (TND),
- Correction d'un problème où un tunnel qui n'utilise pas de token était fermé lors du retrait d'un token,
- Correction d'un problème où un tunnel ne se fermait pas côté client lorsqu'une passerelle envoie des demandes de suppression (DELETE) et ne répond plus,
- Correction d'un problème où un tunnel ne s'ouvrait pas lorsque le code PIN correct est saisi après une première saisie d'un code PIN incorrect,
- Correction d'un problème où le Client VPN ne demandait pas explicitement le code PIN lorsqu'une carte à puce est retirée puis réinsérée,
- Correction d'un problème où une réinitialisation IKE était déclenchée lors de l'insertion d'une carte à puce lorsque la CPD est activée,
- Correction d'un problème où l'écriture et la suppression des clefs *path* et *ngpath* était possible,
- Correction d'un problème où un nom de serveur syslog trop long entraînait un dépassement de mémoire tampon,
- Correction d'un problème où une erreur de « format incompatible » se produisait lors de la récupération d'une configuration à partir d'un ancien modèle de passerelle,
- Correction d'un problème où le Client VPN n'acceptait pas un fichier de configuration provenant d'un nouveau modèle de passerelle qui prend en charge les algorithmes de signature SHA-2,
- Correction d'un problème où le Client VPN n'acceptait pas un certificat auto-signé ou un certificat utilisé par les deux points de terminaison distant et local,
- L'algorithme de hachage SHA-1 a été réintroduit pour prendre en charge les équipements plus anciens,
- Correction d'un problème où le **Panneau de Configuration** restait accessible depuis l'icône en barre des tâches alors que l'option **Restreindre l'accès du panneau de configuration aux administrateurs** était activée,

- Le schéma de signature RSASSA-PKCS1-V1_5 a été rétabli en tant que schéma par défaut pour prendre en charge des équipements plus anciens.

Limitations et précisions sur les cas d'utilisation

- Mode USB : l'option **Avec cet ordinateur uniquement** n'est pas disponible,
- L'utilisation d'IPv4 au sein d'une connexion IPv6 ne fonctionne pas avec toutes les configurations,
- Un **Local ID** de type *ID_DER_ASN1_DN* ne peut pas être utilisé avec des clés partagées,
- Authentification : les clés partagées ne peuvent pas contenir des caractères spéciaux,
- Si la fenêtre **À propos...** est ouverte juste après une installation en ligne de commande, la mention *Version d'évaluation* apparaît toujours même si l'activation s'est correctement déroulée,
- La barre de défilement peut parfois disparaître de l'onglet **Automatisation**,
- Avec certaines résolutions d'écran, la barre d'état du **Panneau de Configuration** peut ne pas s'afficher la première fois que le client est lancé,
- Le changement de langue dans le **Panneau de Configuration** ne s'applique pas au **Mode GINA**,
- Désinstaller le client en double-cliquant sur le paquet MSI n'est pas supporté,
- En configuration VPN SSL, le choix de la suite de chiffrement ne doit pas être configuré en "auto" mais sélectionné spécifiquement parmi la liste des suites de chiffrement proposées,
- L'établissement d'un tunnel mobile en mode standard (non DR) avec une autorité de certification (CA) et certificats basés sur l'algorithme Brainpool 256 n'est pas fonctionnel,
- L'établissement d'un tunnel mobile en mode DR sans utilisation du mode *Config* (option **Obtenir la configuration depuis la passerelle** décochée) provoque un échec de la renégociation en phase 2.

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 et pour accéder aux vidéos créées par l'équipe du support technique (Technical Assistance Center).

Télécharger cette version

Suivez les étapes ci-dessous pour télécharger la version 7.4.018 de SN VPN Client Exclusive.

1. Connectez-vous à votre espace personnel MyStormshield.
2. Rendez-vous dans **Téléchargements > Téléchargements**.
3. Dans les catégories, sélectionnez **Stormshield Network Security > VPN CLIENT EXCLUSIVE**.
4. Selon la langue souhaitée et la version de Windows concernée, cliquez sur le programme d'installation du SN VPN Client Exclusive (fichier *.msi*). Le téléchargement se lance automatiquement.
5. Vérifiez l'intégrité des binaires récupérés grâce à l'une des commandes suivantes :
   - Système d'exploitation Linux : *sha256sum <filename>*
   - Système d'exploitation Windows : *CertUtil -hashfile <filename> SHA256*

   Comparez ensuite le résultat obtenu avec l'empreinte (hash) indiquée sur MyStormshield. Pour la visualiser, cliquez sur **Afficher** dans la colonne **SHA256** du fichier concerné.

NOTE
Pour rappel, lors d'une mise à jour d'une version précédente, l'installateur de la nouvelle version convertit automatiquement la configuration. Ne désinstallez pas la version précédente avant de lancer l'installateur de la nouvelle version.

Versions précédentes de SN VPN Client Exclusive 7

Retrouvez dans cette section les nouvelles fonctionnalités, vulnérabilités résolues et correctifs des versions précédentes de SN VPN Client Exclusive 7.

7.3.007	Nouvelles fonctionnalités	Correctifs
7.0.115	Nouvelles fonctionnalités	

Nouvelles fonctionnalités et améliorations de la version 7.3.007

Fonctionnalités principales

- Ajout d'une fenêtre **Console** au **Panneau TrustedConnect**,
- Permet l'ouverture d'un tunnel dans le **Panneau TrustedConnect** même en cas de détection d'un réseau de confiance,
- Le **Panneau TrustedConnect** peut désormais être réouvert automatiquement lorsque l'on quitte l'application ou si elle s'arrête de manière inopinée,
- La CRL peut maintenant être téléchargée dans un cache et un délai d'expiration peut être défini pour la CRL en cache,
- Ajout d'une fonctionnalité associant le filtrage des flux de données et la Détection du portail captif (CPD),
- La vérification de la CRL du certificat utilisateur est maintenant facultative.

Améliorations

- Augmentation du nombre de sous-réseaux supportés à 16,
- La hauteur de la fenêtre du **Panneau de connexion** peut désormais être augmentée ou réduite,
- Support de plusieurs adresses IP source sur l'interface réseau,
- Le nombre de règles pour le mode filtrage a été augmenté de 12 à 30,
- Le *Local ID* peut maintenant être rempli automatiquement avec le DNS ou une adresse e-mail en plus d'objet du certificat,
- Les mots de passe servant à chiffrer des configurations exportées doivent désormais se conformer aux recommandations de l'ANSSI, c'est-à-dire être composés d'au moins 16 caractères dans un alphabet de 90 symboles, dont au moins un caractère en majuscule, un en minuscule et un caractère spécial,
- Le client VPN accepte désormais la valeur `id-kp-ipsecIKE` dans l'extension *Extended Key Usage* pour un certificat de la passerelle VPN,
- Meilleur support des passerelles IPsec DR :
  - La renégociation des clés de la *Child SA* demande maintenant le même *TS* que celui de la *SA* d'origine,
  - La taille *NONCE* est de 16 octets lorsque *PRF_HMAC_SHA2_256* est utilisé.
- Meilleur support des tokens/cartes à puce :
  - La fenêtre de saisie du code PIN précise désormais la carte à puce/token concerné,
  - PKCS#11 ne provoque plus l'arrêt inopiné du Client VPN avec les lecteurs CNG,
  - Un tunnel n'est plus fermé lorsqu'un token non relatif au tunnel est extrait.
- Amélioration de la stabilité du module IKE,
- Meilleure performance du chiffrement AES-GSM,
- Suppression d'algorithmes considérés comme faibles pour SSL et OpenVPN : MD5, SHA1, suite de chiffrement TLS à faible niveau de sécurité et BF-CBC.

Correctifs de la version 7.3.007

- Les champs DSCP sont maintenant gérés correctement dans les paquets ESP créés,
- Le Client VPN ne s'arrête plus de manière inopinée à la sortie du mode veille,
- Le module d'activation lit maintenant tous les fichiers `tgbcode` et utilise celui disposant de la date de renouvellement la plus récente,
- Correction d'un problème où la **Console** n'enregistrait plus de logs quand l'utilisateur quittait son poste de travail ou verrouillait sa session,
- Correction d'un problème où le serveur d'activation retournait un message d'erreur injustifié,
- Correction d'un problème où le tunnel s'arrêtait avec le message d'erreur "unsupported payload 53 for this exchange",
- Correction d'un problème de menu contextuel pour Windows en mode tablette,
- Diverses améliorations cosmétiques et de stabilité.

Fonctionnalités principales de SN VPN Client Exclusive 7.0

SN VPN Client Exclusive est une solution de type client VPN. Installée sur un ordinateur Windows, elle permet de monter un tunnel VPN avec un pare-feu Stormshield Network Security afin de sécuriser une communication entre un utilisateur distant et un réseau protégé par un pare-feu SNS.

La solution SN VPN Client Exclusive peut être installée sur les environnements suivants :

- Windows 10 64 bits,
- Windows 11 64 bits.

Pour plus d'information concernant SN VPN Client Exclusive 7.0, consultez le *Guide de l'administrateur* sur le site de Documentation Technique Stormshield.

La version SN VPN Client Exclusive 7.0 fournit les fonctionnalités principales suivantes.

Haut niveau de sécurité

Le client SN VPN Client Exclusive a été développé en suivant les recommandations du NIST et de l'ANSSI. Il prend en compte les fonctions d'authentification disponibles sur le système d'information, et inclus à ce titre des mécanismes d'intégration avec les PKI existantes. L'ensemble des protocoles et algorithmes mis en œuvre dans le logiciel en font un client universel pour se connecter à toutes les passerelles VPN du marché, qu'elles soient logicielles ou matérielles.

Mode GINA

Le mode GINA permet d'ouvrir des connexions VPN avant l'ouverture d'une session Windows. Cette fonction permet par exemple d'établir une connexion sécurisée vers un serveur de gestion des droits d'accès de façon à obtenir les droits d'accès au poste utilisateur avant l'ouverture de la session utilisateur.

TND (Trusted Network Detection)

Cette fonctionnalité consiste à détecter que le poste est connecté au réseau de l'entreprise (réseau de confiance) ou non. Lorsque le Client VPN détecte que le poste n'est pas sur le réseau de l'entreprise, le tunnel prédéfini est ouvert automatiquement.

TrustedConnect utilise les deux méthodes suivantes pour détecter si le poste est sur un réseau de confiance ou non :

- Vérification que l'un des suffixes DNS des interfaces réseau présentes sur le poste fait partie de la liste des suffixes DNS de confiance (liste configurée dans le logiciel, cf. ci-dessous),
- Accès automatique en HTTPS à un serveur Web de confiance, et vérification de la validité de son certificat.

Mode Always-On

La fonctionnalité Always-On assure le maintien de la sécurité de la connexion à chaque changement d'interface réseau.

Les type d'interfaces réseaux pris en charge sont les suivants :

- Adaptateur virtuel (ex : vmware),
- Wi-Fi,
- Ethernet,
- Modem USB (type smartphone),
- Modem Bluetooth (type smartphone).

Les événements réseau déclenchant la reconnexion automatique du tunnel (et la détection du réseau de confiance, le cas échéant) sont les suivants :

- Connexion à un réseau (adresses APIPA ignorées),
- Déconnexion d'un réseau,
- Un adaptateur change d'adresse IP ou passage DHCP à statique et vice versa,
- ipconfig /release,
- ipconfig /renew,
- Passage en mode avion.

Microsoft Windows Installer (MSI)

En s'appuyant sur les capacités offertes par l'installeur Windows (MSI), les administrateurs peuvent déployer et administrer le Client SN VPN Client Exclusive avec des outils de gestion de parc et des groupes d'utilisateurs (GPO). Outre l'installation silencieuse, les scripts, les multiples options de personnalisation et de pré-configuration comme la personnalisation de l'interface utilisateur, le paramétrage des fonctions PKI sont gérables de manière totalement centralisée.

Certificat sur carte à puce ou sur token

Le client SN VPN Client Exclusive implémente un mécanisme de détection automatique de l'insertion d'une carte à puce. Ainsi, les tunnels associés au certificat contenu sur la carte à puce sont montés automatiquement à l'insertion de cette carte à puce. Réciproquement, l'extraction de la carte à puce ferme automatiquement tous les tunnels associés.

Logs administrateur, console et traces

Le client SN VPN Client Exclusive propose trois types de logs :

- Les logs "administrateur" sont spécifiquement dédiés au rapport d'activité et d'utilisation du logiciel. Les logs collectés peuvent être au choix et/ou simultanément :
  - Stockés dans un fichier local,
  - Journalisés dans le journal d'évènements Windows,
  - Envoyés au format syslog à un serveur Syslog.
- La "Console" détaille les informations et les étapes des ouvertures et fermeture des tunnels. Elle est principalement constituée des messages IKE et apporte une information de haut niveau sur l'établissement du tunnel VPN. Elle est destinée à l'administrateur, pour l'aider à identifier d'éventuels incidents de connexions VPN.
- Le mode "traçant" fait produire par chaque composant du logiciel le log de son fonctionnement interne. Ce mode est destiné au support éditeur pour le diagnostic d'incident logiciels.

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** > **Rapporter un incident / Suivre un incident**.

- +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.