



STORMSHIELD



STORMSHIELD NETWORK SECURITY
STORMSHIELD NETWORK SSL VPN CLIENT

NOTES DE VERSION

Version 5

Dernière mise à jour du document : 22 octobre 2025

Référence : sns-fr-ssl_vpn_client-notes_de_version-v5.1.2



Table des matières

Historique des modifications	3
Changements de comportement	4
Nouvelles fonctionnalités et améliorations de la version 5.1.2	6
Correctifs de la version 5.1.2	7
Compatibilité	8
Problèmes connus	9
Limitations et précisions sur les cas d'utilisation	10
Ressources documentaires	12
Installer cette version	13
Versions précédentes de SN SSL VPN Client v5	14
Contact	17

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

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



Historique des modifications

Date	Description
22 octobre 2025	Nouveau document



Changements de comportement

Cette section liste les changements de comportements automatiques liés à la mise à jour du client VPN SSL Stormshield en version 5.1.2 depuis la dernière version 4 disponible.

Changements introduits en version 5.1.1 EA

En savoir plus

- Langues disponibles - Le client VPN SSL Stormshield est disponible en français et en anglais. L'allemand n'est plus disponible.
- Certificats obsolètes - Les algorithmes SHA-1 et MD5 ne sont plus supportés par le client VPN SSL Stormshield. Si vous utilisez dans la configuration VPN SSL du firewall SNS un certificat signé avec un algorithme qui n'est plus supporté, vous devez le modifier.
Ceci concerne les certificats du service VPN SSL, et si vous utilisez des clients VPN SSL Stormshield configurés en **Mode Stormshield** (anciennement Mode automatique), ceci concerne également le certificat du portail captif. Vous pouvez vérifier l'algorithme de signature de vos certificats dans l'interface Web d'administration du firewall SNS dans le module **Certificats et PKI**.
Si vous devez modifier :
 - Les certificats du service VPN SSL, reportez-vous à la section [Configurer le service VPN SSL](#) du *Guide d'administration VPN SSL*. Pour mettre à jour les certificats VPN SSL générés par défaut sur le firewall SNS, reportez-vous à l'article [How can I regenerate the sslvpn-full-default-authority?](#) de la base de connaissances Stormshield (anglais uniquement).
 - Le certificat du portail captif, reportez-vous à la section [Personnaliser le certificat du portail captif](#) du *Guide d'administration VPN SSL*.
- Certificats - À la première connexion, certains utilisateurs devront indiquer de nouveau le certificat du firewall SNS comme étant de confiance.
- Mode manuel / Fichiers OVPN importés - Une nouvelle méthode d'import des fichiers OVPN est disponible. Lors d'une mise à jour depuis une version 4 ou inférieure vers une version 5, les anciens fichiers OVPN importés ne sont pas récupérés. Vous devez donc les importer de nouveau à l'issue de la mise à jour.
- Carnet d'adresses / Connexions enregistrées - Le "**Carnet d'adresses**" est désormais intitulé "**Connexions enregistrées**". Lors d'une mise à jour depuis une version 4 ou inférieure vers une version 5, les entrées du carnet d'adresses sont ajoutées aux connexions enregistrées, soit automatiquement, soit en renseignant au premier démarrage du client VPN SSL Stormshield le mot de passe du carnet d'adresses si ce dernier est protégé. Le carnet d'adresses d'origine n'est pas modifié et est conservé à son emplacement d'origine.
- Mise à jour depuis une version inférieure à la version 5 - Le programme d'installation de la version 5 ne prend plus en charge la désinstallation des versions 3 et inférieures. Dans le cas d'une mise à jour depuis ces versions, vous devez désinstaller au préalable la version d'origine avant d'installer la version 5.
- Le trafic du client VPN SSL Stormshield est désormais initié par un compte de service. Dans le cas où une configuration durcie est utilisée sur les postes de travail (utilisation d'un pare-feu par exemple), le client VPN SSL Stormshield doit pouvoir joindre les ports suivants pour établir des connexions VPN SSL. Les ports mentionnés proviennent d'une configuration par défaut, adaptez-les si nécessaire.



Source	Destination	Protocole / Port (par défaut)	Objectif de la connexion
Client (SSLVPNService) Mode Stormshield uniquement	Passerelle OpenVPN du firewall SNS	TCP/443 (portail captif)	Récupération de la configuration VPN SSL et envoi au firewall SNS des informations pour vérifier la conformité du poste client utilisé (ZTNA).
Client (OpenVPN)	Passerelle OpenVPN du firewall SNS	UDP/1194 (VPN SSL)	Établissement de la connexion VPN SSL
Client (OpenVPN)	Passerelle OpenVPN du firewall SNS	TCP/443 (VPN SSL)	Établissement de la connexion VPN SSL (Compatibilité)



Nouvelles fonctionnalités et améliorations de la version 5.1.2

Connexion

Utilisation d'un code OTP avec les connexions OpenVPN

Il est désormais possible d'utiliser un code OTP pour établir une connexion OpenVPN (fichier OVPN importé) dans les menus "**Connexions enregistrées**" et "**Connexion directe**".

Pour plus d'informations sur comment établir une connexion avec le client VPN SSL Stormshield ou gérer les connexions enregistrées, reportez-vous au [Guide de configuration et d'utilisation du client VPN SSL Stormshield v5](#).

Configuration via une interface en ligne de commande

Import de connexions enregistrées

Il est désormais possible d'importer des connexions enregistrées dans le client VPN SSL Stormshield à l'aide de la nouvelle commande CLI "*import-addressbook*".

Pour plus d'informations, reportez-vous à la section [Configurer le client VPN SSL Stormshield via une interface en ligne de commande](#) du *Guide de configuration et d'utilisation du client VPN SSL Stormshield v5*.

Compatibilité

Nouvelle compatibilité macOS

Le client VPN SSL Stormshield en version 5.1.2 peut être installé sur macOS Tahoe 26 (arm64) M1 et modèles suivants.

Pour retrouver tous les systèmes d'exploitation compatibles, reportez-vous à la section [VPN SSL Client](#) du document *Cycle de vie produits Network Security & Tools* qui est la page de référence concernant les compatibilités du client VPN SSL Stormshield.



Correctifs de la version 5.1.2

Migration des entrées du carnet d'adresses dans les connexions enregistrées

Lors d'une mise à jour depuis une version 4 ou inférieure vers une version 5.1.2, le port personnalisé des entrées du carnet d'adresses (serveur:port) est désormais correctement converti dans les connexions enregistrées.

Si des ports personnalisés mal convertis sont toujours présents dans les connexions enregistrées depuis la mise à jour en version 5.1.1 EA, ils seront automatiquement corrigés lors de la mise à jour en version 5.1.2.

Communication avec le firewall SNS

Sur certains environnements Windows, le client VPN SSL Stormshield en version 5.1.1 EA ne pouvait pas communiquer avec le firewall SNS car le certificat de son portail captif n'était pas présenté à l'utilisateur. Ce problème a été corrigé.

Authentification multifacteur via une application tierce

L'authentification multifacteur via une application tierce installée sur un appareil de confiance, utilisée par exemple avec la solution Trustbuilder (anciennement inWebo), est désormais fonctionnelle avec la version 5.1.2 du client VPN SSL Stormshield. Cette solution permet notamment à l'utilisateur d'approuver l'établissement de la connexion grâce à une notification *push* sur son appareil ou de générer un code OTP.



Compatibilité

Pour plus d'informations, reportez-vous à la section [VPN SSL Client](#) du document *Cycle de vie produits Network Security & Tools*.



Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version de SN SSL VPN Client 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](#).



Limitations et précisions sur les cas d'utilisation

Cette section liste les limitations et précisions sur les cas d'utilisation avec le client VPN SSL Stormshield.

Installation

Installation sous Windows de la version 5 bloquée par une ancienne version 3

Dans le cas où l'installation de la version 5 du client VPN SSL Stormshield est bloquée par une ancienne version 3, même si cette dernière a été désinstallée, vous devez utiliser un script fourni par Stormshield pour nettoyer les clés de registre et les fichiers résiduels qui n'ont pas été correctement supprimés par le programme de désinstallation de la version 3.

Pour plus d'informations, reportez-vous à l'article [Unable to install SSL VPN Client v5 on Windows due to previous v3 installation](#) de la *Base de connaissances Stormshield* (anglais uniquement).

Installation multi-comptes sous Linux et macOS

Nous recommandons à chaque utilisateur partageant un poste de travail Linux ou macOS avec d'autres utilisateurs de veiller à bien fermer leur connexion VPN SSL après chaque utilisation sur le poste de travail.

Connexion

Vérification des postes clients sous Windows (ZTNA) - Pare-feu et antivirus

Lorsque la vérification des postes clients (ZTNA) est activée sur le firewall SNS et qu'au moins l'un des critères "Antivirus du poste client actif et à jour" ou "Firewall actif sur le poste client" est coché, les utilisateurs doivent attendre quelques minutes après l'ouverture de leur session Windows avant d'établir une connexion avec le client VPN SSL Stormshield.

En effet, le service Windows permettant de vérifier l'état de l'antivirus et du Pare-feu Windows met quelques minutes à démarrer après l'ouverture d'une session. Tant que ce service n'est pas démarré, le client VPN SSL Stormshield n'est pas en mesure de vérifier l'état de ces critères et le firewall SNS refuse alors d'établir la connexion car le poste de travail est considéré comme non conforme.

Certificats signés avec l'algorithme SHA-1

Lorsque la passerelle OpenVPN (le firewall SNS par exemple) présente un certificat signé avec l'algorithme SHA-1, un message d'erreur s'affiche dans la fenêtre de connexion du client VPN SSL Stormshield, indiquant de vérifier les identifiants utilisés pour se connecter. Vous ne devez pas tenir compte de la raison évoquée dans le message : la connexion échoue car l'algorithme SHA-1 n'est plus supporté par le client VPN SSL Stormshield.

Authentification unique - Durée minimale d'authentification autorisée du portail captif du firewall SNS

Dans le cas où l'authentification unique est utilisée pour établir des tunnels VPN SSL avec le firewall SNS, nous recommandons de ne pas diminuer la durée minimale d'authentification autorisée en-dessous de 15 minutes (valeur par défaut). Cette configuration s'effectue dans le module **Authentification > Profils du portail captif** du firewall SNS.



Si vous décidez tout de même d'abaisser cette durée, vous devez indiquer aux utilisateurs de ne pas sélectionner dans le champ "**Durée d'authentification**" du portail captif une valeur inférieure ou égale à 5 minutes. Le client VPN SSL Stormshield ne peut pas établir la connexion si la durée d'authentification choisie par l'utilisateur est inférieure ou égale à 5 minutes.

Utilisation

Fonctionnalité DCO des firewalls SNS v5

Le tableau ci-dessous indique si les clients VPN SSL Stormshield Windows, Linux et macOS peuvent bénéficier des améliorations de la fonctionnalités DCO des firewalls SNS v5.

Client VPN SSL Stormshield sous	Fonctionnalité DCO des firewalls SNS v5
Windows	✔ Bénéficie des améliorations de la fonctionnalité DCO
Linux	✔ Bénéficie des améliorations de la fonctionnalité DCO, seulement si ces deux conditions sont respectées : <ul style="list-style-type: none">• OpenVPN est en version 2.6.0 ou supérieure,• Le paquet openvpn-dco est installé.
macOS	✘ Ne bénéficie pas des améliorations de la fonctionnalité DCO

Pour plus d'informations sur la fonctionnalité DCO, reportez-vous à la section [Configurer le service VPN SSL](#) du *Guide d'administration VPN SSL des firewalls SNS et des clients VPN SSL Stormshield*.



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 SSL Stormshield, reportez-vous au [Guide d'installation du client VPN SSL Stormshield v5](#).



Versions précédentes de SN SSL VPN Client v5

Retrouvez dans cette section les nouvelles fonctionnalités, les vulnérabilités résolues et correctifs des versions précédentes de SN SSL VPN Client v5.

5.1.1 EA

[Nouvelles fonctionnalités](#)



Nouvelles fonctionnalités et améliorations de la version 5.1.1 EA

Nouvelle interface graphique et expérience utilisateur améliorée

L'interface graphique du client VPN SSL Stormshield en version 5 a été repensée et l'expérience utilisateur a été améliorée :

- Le "**Mode automatique**" est désormais intitulé "**Mode Stormshield**". Ce mode permet au client VPN SSL Stormshield de récupérer automatiquement la configuration VPN SSL d'une connexion sur le firewall SNS et de lui transmettre les informations permettant de vérifier la conformité du poste client (ZTNA).
- Le "**Carnet d'adresses**" est désormais intitulé "**Connexions enregistrées**".
 - Vous pouvez y enregistrer des connexions, soit en renseignant les informations du firewall SNS en utilisant le "**Mode Stormshield**", soit en important un fichier OVPN.
 - Vous pouvez marquer chaque connexion comme favorite. La liste des connexions favorites est accessible via l'interface graphique du client VPN SSL Stormshield et via le menu contextuel de l'icône du client VPN SSL Stormshield.
 - Vous pouvez activer une option permettant d'établir automatiquement une connexion VPN SSL à l'ouverture du client VPN SSL Stormshield sur la connexion de votre choix. Une action manuelle reste toutefois requise si l'accès aux connexions enregistrées est protégé par un mot de passe ou si un code OTP est utilisé pour la connexion.
- Un nouveau menu intitulé "**Connexion directe**" permet de se connecter en VPN SSL sans avoir à enregistrer une connexion dans le client VPN SSL Stormshield. Dans ce menu, le "**Mode Stormshield**" et l'import d'un fichier OVPN peuvent être utilisés.
- Un nouveau menu intitulé "**Journaux de connexion**" permet de consulter les événements de connexion du client VPN SSL Stormshield, tels que les événements "*Connexion établie*", "*Connexion perdue*", "*Serveur injoignable*", etc.
- Le menu contextuel de l'icône du client VPN SSL Stormshield a été repensé. Depuis ce menu, vous pouvez afficher la dernière connexion utilisée ou la liste des connexions favorites, et établir une connexion VPN SSL en cliquant sur la connexion souhaitée.

Pour plus d'informations, reportez-vous au [Guide de configuration et d'utilisation du client VPN SSL Stormshield v5](#).

Compatibilité étendue

Le client VPN SSL Stormshield en version 5.1.1 EA peut être installé sur les systèmes d'exploitation suivants :

- Windows : Windows 10 (x64) et Windows 11 (x64).
- Linux :
 - Ubuntu Desktop 22.04 LTS (amd64) et Ubuntu Desktop 24.04 LTS (amd64),
 - RHEL 8 (amd64) et RHEL 9 (amd64). Le client VPN SSL Stormshield sous RHEL 8 nécessite l'installation d'un paquet OpenVPN en version minimale 2.5.
- macOS : macOS Sonoma 14 (arm64) M1 et modèles suivants, et macOS Sequoia 15 (arm64) M1 et modèles suivants.



Cette liste peut évoluer dans le temps, notamment selon le cycle de vie des systèmes d'exploitation ci-dessus et des versions mentionnées. Reportez-vous toujours à la section [VPN SSL Client](#) du document *Cycle de vie produits Network Security & Tools* qui est la page de référence concernant les compatibilités du client VPN SSL Stormshield.

Support de l'authentification unique

La version 5 du client VPN SSL Stormshield introduit le support de l'authentification unique. Ceci permet aux utilisateurs de s'authentifier via un portail d'authentification et d'être autorisés à établir une connexion VPN SSL avec un firewall SNS compatible.

Les utilisateurs peuvent s'authentifier :

- Soit sur le portail captif du firewall SNS, par exemple avec leur identité et mot de passe de l'annuaire Active Directory,
- Soit sur le portail d'authentification de la plate-forme d'identité en tant que service (IDaaS) choisie, comme la solution Microsoft Entra ID.

Pour que l'authentification unique fonctionne :

- Le client VPN SSL Stormshield doit être configuré pour utiliser ce mode de connexion en cochant la case **Se connecter avec l'authentification unique** dans les paramètres d'une connexion ou dans le menu **Connexion directe**. Pour plus d'informations, reportez-vous au [Guide de configuration et d'utilisation du client VPN SSL Stormshield v5](#).
- Le firewall SNS utilisé pour la connexion doit être en version 5.0.1 ou supérieure.
- Pour une authentification via la méthode OIDC / Microsoft Entra ID, cette dernière doit être activée et configurée sur le firewall SNS. Pour plus d'informations, reportez-vous à la note technique [Configurer l'authentification OIDC / Microsoft Entra ID](#).

Nouvelle organisation de la documentation du client VPN SSL Stormshield

Dorénavant, la documentation du client VPN SSL Stormshield est répartie dans deux guides :

- [Guide d'installation du client VPN SSL Stormshield v5](#),
- [Guide de configuration et d'utilisation du client VPN SSL Stormshield v5](#).

Auparavant, un seul document regroupant l'installation, la configuration et l'utilisation du client VPN SSL Stormshield était disponible.



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 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.