STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSL VPN CLIENT

NOTES DE VERSION

Version 3

Dernière mise à jour du document : 30 mai 2024

Référence : sns-fr-ssl_vpn_client-notes_de_version-v3.2.4

Table des matières

Historique des modifications 3
Changements de comportement 4
Vulnérabilités résolues de la version 3.2.4 5
Compatibilité 6
Problèmes connus 7
Ressources documentaires 8
Télécharger cette version 9
Versions précédentes de SN SSL VPN Client 3 10
Contact 26

Dans la documentation, Stormshield Network SSL VPN Client est désigné sous la forme abrégée : SN SSL VPN Client et Stormshield Network Security 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
30 mai 2024	Nouveau document

Changements de comportement

Cette section liste les changements de comportements automatiques liés à la mise à jour de SN SSL VPN Client en version 3.2.4 depuis la dernière version 2 disponible.

Changements introduits en version 3.2.3

En savoir plus

- Groupe local "OpenVPN Administrators" - Il n'est désormais plus nécessaire que l'utilisateur Windows appartienne au groupe local "OpenVPN Administrators".
  Le changement introduit en version 3.2.0 n'est donc plus d'actualité.

Changements introduits en version 3.2.0

- Groupe local "OpenVPN Administrators" - L'utilisateur Windows doit dorénavant appartenir au groupe local "OpenVPN Administrators". En cas contraire, SN SSL VPN Client ne pourra pas établir de tunnels VPN.
  Pour vérifier que l'utilisateur appartient au groupe, exécutez dans l'invite de commandes Windows `net localgroup "OpenVPN Administrators"`. Pour ajouter manuellement l'utilisateur au groupe, exécutez `net localgroup "OpenVPN Administrators" "myuser" /add` (remplacez myuser par l'utilisateur concerné).

  Cette exigence n'est plus d'actualité à partir de la version 3.2.3.

Changements introduits en version 3.0.0

En savoir plus

- Compatibilité - SN SSL VPN Client en version 3.0.0 est désormais un service 64 bits. Il devient donc uniquement compatible avec les systèmes d'exploitation 64 bits.

Vulnérabilités résolues de la version 3.2.4

OpenVPN

Une vulnérabilité de sévérité faible a été corrigée dans OpenVPN.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2024-014.

Compatibilité

Pour plus d'informations, reportez-vous à la section VPN SSL Client du *Guide de cycle de vie produits*.

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

Méthodes d'authentification multifacteur

Ce tableau récapitule les méthodes d'authentification multifacteur compatibles selon la version installée sur le firewall SNS et le mode de connexion utilisé par **SN SSL VPN Client**.

Versions SNS	Mode de connexion utilisé par SN SSL VPN Client	Mot de passe + Code OTP	Code OTP seulement	Mode Push	TOTP
4.7 ou supérieures	Tous les modes	✓	✓	✓	✓
4.3 LTSB	Tous les modes	✓	✓	✓	✗
3.7 LTSB 3.11 LTSB	Mode automatique	✗	✗	✗	✗
	Mode manuel	✓	✓	✗	✗

Problèmes connus

La liste actualisée des problèmes connus relatifs à cette version du 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.

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 3.2.4 de SN SSL VPN Client.

1. Connectez-vous à votre espace personnel MyStormshield.
2. Rendez-vous dans **Téléchargements > Téléchargements**.
3. Dans les catégories, sélectionnez **Stormshield Network Security > VPN SSL**.
4. Selon la langue souhaitée et la version de Windows concernée, cliquez sur le programme d'installation du SN SSL VPN Client (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
Vous pouvez également télécharger cette version depuis le site Stormshield VPN SSL ou depuis le portail captif du firewall SNS hébergeant le service VPN SSL. Vous devrez vous connecter à MyStormshield pour vérifier l'intégrité des binaires.

Versions précédentes de SN SSL VPN Client 3

Retrouvez dans cette section les nouvelles fonctionnalités, les vulnérabilités résolues et correctifs des versions précédentes de SN SSL VPN Client 3.

3.2.3			Correctifs
3.2.2			Correctifs
3.2.1		Vulnérabilités résolues	Correctifs
3.2.0	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs
3.1.1			Correctifs
3.1.0		Vulnérabilités résolues	Correctifs
3.0.1			Correctifs
3.0.0	Nouvelles fonctionnalités	Vulnérabilités résolues	Correctifs

Correctifs de la version 3.2.3

Carnet d'adresses - Code OTP

Référence support 84763

Le carnet d'adresses tient désormais compte de l'authentification multifacteur (code OTP) lors de la connexion à une adresse.

Plus d'informations sur la configuration et l'utilisation du SN SSL VPN Client.

Installation

Groupe local Windows "OpenVPN Administrators"

Référence support 85105

Dans certains cas, l'utilisateur Windows n'était pas ajouté au groupe local "OpenVPN Administrators" une fois l'installation du SN SSL VPN Client terminée, empêchant l'utilisateur d'établir des tunnels VPN. Afin de pallier ce problème, il n'est désormais plus nécessaire que l'utilisateur Windows appartienne au groupe local "OpenVPN Administrators".

Variables d'environnement Windows

Références support 85167 - 85168

L'installation du SN SSL VPN Client échouait lorsque la valeur de la variable d'environnement Windows "*Path*" avait été modifiée. Ce problème, qui générait les erreurs "*pnputil.exe failed with return code 9009*" et "*GENERATE_OVPN_AUTH*", a été corrigé. Le mécanisme d'installation du SN SSL VPN Client utilise dorénavant la variable d'environnement Windows "*SystemRoot*" plutôt que la variable "*Path*".

À noter que l'installation du SN SSL VPN Client échouera si la valeur de la variable "*SystemRoot*" a été modifiée et ne correspond plus au dossier d'installation de Windows (par exemple : *C:\Windows*).

Correctifs de la version 3.2.2

NOTE
Dans certains cas, l'installation sur Windows 10 ou Windows 11 du SN SSL VPN Client peut échouer. Si vous êtes concerné par ce problème, veuillez contacter le support Stormshield (référence support 84756).

Installation

Installation sur un profil utilisateur Windows contenant un espace

Référence support 85042

Un problème empêchant l'installation du SN SSL VPN Client lorsque le profil utilisateur Windows contenait un espace a été corrigé. Ce problème survenait notamment si le paramètre du comportement de nom court (nom 8dot3) était désactivé sur Windows.

Déploiement via GPO

Référence support 85010

Un problème rendait difficile le déploiement via GPO du SN SSL VPN Client si une version antérieure avait été installée manuellement sur le poste de l'utilisateur.

Ce problème a été corrigé pour les futurs déploiements : si une version égale ou supérieure à la 3.2.2 a été installée manuellement sur le poste, le déploiement via GPO d'une version supérieure à celle d'origine s'effectuera normalement.

Si une version antérieure à la version 3.2.2 a été installée manuellement sur le poste, le déploiement via GPO d'une version égale ou supérieure à la 3.2.2 s'effectuera mais un redémarrage du poste de l'utilisateur sera nécessaire.

Authentification multifacteur - OTP

Exécution d'un script d'ouverture

Référence support 84754

L'utilisateur devait s'authentifier une seconde fois pour que le tunnel VPN s'ouvre lorsque ces deux éléments étaient configurés :

- Une authentification OTP,
- Un script créé via le bloc-note Windows et à executer à la connexion VPN SSL.

Ce problème a été corrigé.

Système

Interruption du tunnel VPN

Référence support 85070

Lorsque la consommation CPU de la machine Windows atteignait 100% pendant 2 secondes, SN SSL VPN Client considérait que Windows ne répondait plus et interrompait alors le tunnel VPN.

Afin de réduire ces interruptions, ce délai est désormais passé de 2 à 60 secondes et est configurable pour chaque utilisateur dans la clé de registre Windows suivante : **HKEY_CURRENT_USER\SOFTWARE\Stormshield\STORMSHIELD SSL VPN CLIENT\living_timeout**.

Vulnérabilités résolues de la version 3.2.1

OpenSSL

Une vulnérabilité de sévérité moyenne a été corrigée dans OpenSSL.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2023-011.

Correctifs de la version 3.2.1

Authentification multifacteur - OTP

Référence support 85005

Un problème empêchant l'authentification avec un code OTP a été corrigé. Cette régression était apparue en version SN SSL VPN Client 3.2.0.

Scripts *.bat* exécutés par SN SSL VPN Client

Interruption du tunnel VPN après l'exécution d'un script d'ouverture

Référence support 85009

L'exécution d'un script par SN SSL VPN Client à l'ouverture du tunnel VPN avec le firewall SNS interrompait le tunnel si l'exécution du script durait deux secondes ou plus. Ce problème, qui générait l'erreur "*La connexion VPN SSL a été interrompue pendant la mise en veille ou la veille prolongée de Windows. Merci de vous reconnecter.*", a été corrigé.

Suppression des scripts d'ouverture et de fermeture

Référence support 85013

Les scripts exécutés par SN SSL VPN Client à l'ouverture et à la fermeture du tunnel VPN avec le firewall SNS n'étaient pas supprimés du poste de travail Windows lorsqu'ils avaient été retirés de la configuration VPN SSL du firewall SNS. Ces scripts continuaient donc de s'exécuter. Ce problème a été corrigé.

Nouvelles fonctionnalités et améliorations de la version 3.2.0

Installation

La version SN SSL VPN Client 3.2 introduit la possibilité d'installer SN SSL VPN Client sur une machine sans devoir désinstaller au préalable la version d'origine, tant que cette dernière est égale ou supérieure à la version 2.9.

Vulnérabilités résolues de la version 3.2.0

Système

Une vulnérabilité de sévérité forte a été corrigée dans SN SSL VPN Client.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-028/.

Des vulnérabilités de sévérité moyenne ont été corrigées dans SN SSL VPN Client.

Le détail de ces vulnérabilités est disponible sur notre site :

- https://advisories.stormshield.eu/2022-028/,
- https://advisories.stormshield.eu/2022-029/.

Correctifs de la version 3.2.0

Utilisation sur un profil utilisateur Windows avec des caractères spéciaux

Référence support 84668

SN SSL VPN Client fonctionne désormais correctement lorsqu'il est installé sur un profil utilisateur Windows dont le nom d'utilisateur contient des caractères spéciaux (é, ç, ę, ć, ...). Ce problème générait l'erreur "*Échec de l'extraction du fichier de configuration*".

Sortie du mode veille ou de la veille prolongée d'une machine Windows

Référence support 84499

Si le VPN n'était pas déconnecté et que la machine Windows entrait en veille ou veille prolongée, les routes incluses dans la configuration VPN SSL et installées sur le poste n'étaient pas supprimées. Ceci pouvait empêcher le tunnel VPN de fonctionner après la sortie du mode veille ou de la veille prolongée.

Ce comportement a été corrigé et le tunnel VPN est désormais déconnecté automatiquement après la sortie du mode veille ou de la veille prolongée. L'utilisateur en est informé par l'affichage d'une notification.

Correctifs de la version 3.1.1

Système

Installation

Référence support 84687

Un problème empêchant l'installation du SN SSL VPN Client en version 3.1.0 lorsque le pilote réseau TAP était déjà installé sur le système a été corrigé. Ce problème générait l'erreur "*Ce paquet Windows Installer rencontre un problème.*".

Désinstallation

Un problème empêchant la désinstallation du SN SSL VPN Client en version 3.1.0 lorsque le pilote réseau TAP n'était plus présent sur le système a été corrigé.

Vulnérabilités résolues de la version 3.1.0

Système

Une vulnérabilité de sévérité forte a été corrigée dans SN SSL VPN Client.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-004/.

Correctifs de la version 3.1.0

Système

Établissement d'un tunnel

Référence support 82807

Un problème empêchant l'établissement d'un tunnel VPN SSL lorsque des paramètres de proxy étaient configurés dans les propriétés d'Internet Explorer a été corrigé. Cette régression était apparue en version SN SSL VPN Client 2.9.1.

Correctifs de la version 3.0.1

Système

Mode automatique - Saisie d'un port personnalisé

Référence support 84329

En mode automatique, la saisie d'un port personnalisé utilisé pour le portail captif (différent du port par défaut 443) est désormais correctement prise en compte par SN SSL VPN Client.

Fichier *auth_management.txt* manquant après installation du SN SSL VPN Client

Référence support 84348

Dans certaines configurations, même si l'installation du SN SSL VPN Client arrivait à son terme, le fichier *auth_management.txt* n'était pas installé sur le système empêchant alors SN SSL VPN Client de fonctionner. Ce problème a été corrigé.

Nouvelles fonctionnalités et améliorations de la version 3.0.0

Compatibilité

SN SSL VPN Client en version 3.0.0 est désormais un service 64 bits. Il devient donc uniquement compatible avec les systèmes d'exploitation 64 bits.

Authentification multifacteur - OTP

Un utilisateur peut désormais spécifier qu'il utilise une authentification multifacteur en cochant une nouvelle option sur la fenêtre de connexion du SN SSL VPN Client en version 3.0.0. En cochant l'option, l'utilisateur peut alors renseigner un Code OTP dans un champ distinct.

Cet ajout permet au SN SSL VPN Client de supporter les méthodes d'authentification multifacteur suivantes :

- **Mot de passe + Code OTP** : pour utiliser cette méthode, la case **Utiliser une authentification multifacteur** doit être cochée et les champs **Mot de passe** et **Code OTP** doivent être complétés,
- **Code OTP seulement** : pour utiliser cette méthode, la case **Utiliser une authentification multifacteur** doit être cochée, le champ **Mot de passe** doit être laissé vide et le champ **Code OTP** doit être complété,
- **Mode Push** : pour utiliser cette méthode, la case **Utiliser une authentification multifacteur** doit être cochée et les champs **Mot de passe** et **Code OTP** doivent être laissés vides.

Pour plus d'informations sur la compatibilité des méthodes d'authentification multifacteur selon la version installée sur le firewall SNS et le mode de connexion utilisé par SN SSL VPN Client, reportez-vous à la section Compatibilité.

Plus d'information sur la configuration et l'utilisation du VPN SSL des firewalls SNS.

Vulnérabilités résolues de la version 3.0.0

Système

Une vulnérabilité de sévérité moyenne a été corrigée dans SN SSL VPN Client.

Le détail de cette vulnérabilité est disponible sur notre site https://advisories.stormshield.eu/2021-019/.

Correctifs de la version 3.0.0

Système

Déconnexion du tunnel à la fermeture de session

Références support 81985 - 82934 - 83152

Lorsqu'un utilisateur fermait puis rouvrait sa session Windows sans redémarrer sa machine, SN SSL VPN Client ne déconnectait pas le tunnel à la fermeture de la session Windows. Le tunnel était ainsi toujours monté à la réouverture de la session Windows malgré le fait que l'icône du SN SSL VPN Client dans la barre des tâches indiquait le contraire. Ce problème a été corrigé.

Déploiement avec Microsoft Intune

Référence support 82577

SN SSL VPN Client en version 2.9 n'était pas fonctionnel après avoir été déployé avec Microsoft Intune. Ce problème a été corrigé.

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.