



**STORMSHIELD**



**STORMSHIELD NETWORK SECURITY**  
STORMSHIELD NETWORK SSL VPN CLIENT

# NOTES DE VERSION

Version 3

Dernière mise à jour du document : 22 février 2022

Référence : sns-fr-ssl\_vpn\_client-notes\_de\_version-v3.0.0



# Table des matières

Nouvelles fonctionnalités de la version 3.0.0 .....	3
Vulnérabilités résolues de la version 3.0.0 .....	4
Correctifs de la version 3.0.0 .....	5
Compatibilité .....	6
Préconisations .....	7
Documentation .....	8
Télécharger cette version .....	9
Contact .....	10

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.



# Nouvelles fonctionnalités 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 mot de passe à usage unique (OTP) dans un champ distinct.

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

- **Mot de passe + mot de passe à usage unique** : pour utiliser cette méthode, la case précisant l'utilisation d'une authentification multifacteur doit être cochée et les champs **Mot de passe** et **OTP** doivent être complétés,
- **Mot de passe à usage unique seulement** : pour utiliser cette méthode, la case précisant l'utilisation d'une authentification multifacteur doit être cochée, le champ **Mot de passe** doit être laissé vide et le champ **OTP** doit être complété,
- **Mode Push** : pour utiliser cette méthode, la case précisant l'utilisation d'une authentification multifacteur doit être cochée et les champs **Mot de passe** et **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](#).



## Vulnérabilités résolues de la version 3.0.0

---

### Systeme

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

---

## Systeme

### 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.



## Compatibilité

Les plate-formes suivantes sont compatibles avec SN SSL VPN Client 3.0.0.

### Stormshield Network Firewall

2.x, 3.x et 4.x

### Systèmes d'exploitation

Windows 8.1 64 bits  
Windows 10 64 bits

#### **i** 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**.

Version SNS	Mode de connexion du SN SSL VPN Client	Méthodes d'authentification multifacteur compatibles
4.3 et supérieures	Mode Automatique	<ul style="list-style-type: none"><li>• Mot de passe + mot de passe à usage unique</li><li>• Mot de passe à usage unique seulement</li><li>• Mode Push</li></ul>
	Mode Sites (manuel)	
3.x, 4.2 et inférieures	Mode Automatique	<ul style="list-style-type: none"><li>• Non compatible</li></ul>
	Mode Sites (manuel)	<ul style="list-style-type: none"><li>• Mot de passe + mot de passe à usage unique</li><li>• Mot de passe à usage unique seulement</li></ul>



# Préconisations

---

## Installation

Lorsque SN SSL VPN Client a été installé sur la machine à l'aide d'un package msi, il est impératif de le désinstaller avant d'installer la nouvelle version.



## Documentation

---

Les ressources documentaires techniques suivantes sont disponibles sur le site de [Documentation Technique Stormshield](#) ou sur le site [Institute](#) de Stormshield. Nous vous invitons à vous appuyer sur ces ressources pour exploiter au mieux l'ensemble des fonctionnalités de cette version.

### Guides

- Stormshield Network Firewall - Manuel d'utilisation et de configuration

### Notes techniques

- Tunnels VPN SSL

Merci de consulter la [Base de connaissance](#) 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

---

### Se rendre sur votre espace personnel MyStormshield

Vous devez vous rendre sur votre espace personnel [MyStormshield](#) afin de télécharger la version 3.0.0 de SN SSL VPN Client :

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 SN SSL VPN Client :

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 l'espace client [MyStormshield](#), rubrique Téléchargements.



## 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**.



## STORMSHIELD

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

*Copyright © Stormshield 2022. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.*