GUIDE
STORMSHIELD SSL VPN CLIENT

GUIDE DE CONFIGURATION ET D'UTILISATION

Version 4

Dernière mise à jour du document : 20 avril 2026

Référence : sns-fr-ssl_vpn_client_guide_configuration_utilisation-v4

Table des matières

Historique des modifications

Date	Description
20 avril 2026	• La note technique a été renommée "Guide de configuration et d'utilisation du client VPN SSL Stormshield v4". • Changements mineurs.
22 mai 2025	• Ajout du paramètre "Activer l'accélération noyau DCO" et d'informations relatives aux réseaux assignés aux clients VPN ainsi qu'au nombre maximal de tunnels VPN autorisés dans la section "Configurer le service VPN SSL" pour les versions SNS 5. • La configuration de la vérification des postes clients (ZTNA) dispose à présent de sa propre section dans le document et son contenu a été modifié. • Ajout d'un nouveau problème concernant l'affichage d'un avertissement lié la fonctionnalité de compression LZ4 dans la section "Résoudre les problèmes".
13 mars 2025	• Sortie du client VPN SSL Stormshield 4.0.10. • Ajout de précisions concernant la mise à jour vers une version inférieure à la version 4 dans la section "Spécificités du client VPN SSL Stormshield". • Modification des informations relatives aux journaux des connexions VPN SSL dans la section "Consulter les journaux du client VPN SSL Stormshield". • Ajout de deux problèmes dans la section "Résoudre les problèmes".
6 février 2025	• Ajout du champ "Autoriser l'établissement de tunnels pour des clients VPN SSL Stormshield Linux ou Mac" dans la section "Configurer le service VPN SSL > Configurer la politique de vérification de la conformité des postes clients (cas du ZTNA)".

13 novembre 2024	• Sortie du client VPN SSL Stormshield 4.0.9.
	• Ajout d'un paragraphe "Limitations et précisions sur les cas d'utilisation" dans la section "Spécificités du client VPN SSL Stormshield".
	• Modification des informations concernant l'utilisation du Mode Push :
	  ◦ Avec le carnet d'adresses dans la section "Configurer le client VPN SSL Stormshield",
	  ◦ Dans la section "Établir un tunnel VPN avec le client VPN SSL Stormshield".
	• Suppression de la note concernant les utilisateurs partageant un poste de travail Windows avec d'autres utilisateurs dans la section "Établir un tunnel VPN avec le client VPN SSL Stormshield".

7 octobre 2024	• Ajout de précisions sur le délai avant renégociation des clés dans la section "Configurer le service VPN SSL".
	• Ajout de précisions concernant l'utilisation du Mode Push :
	  ◦ Avec le carnet d'adresses dans la section "Configurer le client VPN SSL Stormshield",
	  ◦ Dans la section "Établir un tunnel VPN avec le client VPN SSL Stormshield".

22 août 2024	• Sortie du client VPN SSL Stormshield 4.0.
	• Le contenu lié à OpenVPN Connect a été déplacé dans une annexe et celui du client VPN SSL Stormshield dispose à présent de ses propres sections.
	• Le contenu lié au client VPN SSL Stormshield a été enrichi :
	  ◦ Ajout de nouvelles spécificités,
	  ◦ Ajout du format *.exe* pour le programme d'installation,
	  ◦ Ajout des procédures de déploiement via une stratégie de groupe (GPO) et via un script,
	  ◦ Modification du nom de certains champs dans les procédures,
	  ◦ Ajout d'informations concernant les journaux disponibles.
	• Le contenu de la section "Suivre les utilisateurs connectés au VPN SSL sur le firewall Stormshield SSL VPN Client" a été enrichi.
	• Ajout du cas de la mise en œuvre d'un accès réseau *Zero Trust* (ZTNA).

Avant de commencer

Bienvenue dans le guide de configuration et d'utilisation de Stormshield SSL VPN Client version 4.

> **NOTE**
> Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée à des ressources, internes à une entreprise ou non, en passant par le firewall Stormshield SSL VPN Client.

Pour qu'un tunnel VPN SSL puisse s'établir avec le firewall Stormshield SSL VPN Client, un client VPN SSL doit être installé sur le poste de travail ou le terminal mobile de l'utilisateur. Les communications entre le firewall Stormshield SSL VPN Client et l'utilisateur sont alors encapsulées et protégées via un tunnel TLS chiffré.

L'établissement de ce tunnel est basé sur l'authentification de l'utilisateur dans un canal de communication TLS chiffré par des certificats serveur et client communs signés par une autorité de certification (CA) présente sur le firewall Stormshield SSL VPN Client. Cette solution garantit donc confidentialité, intégrité et non-répudiation.

Ce guide présente :

- L'activation et la configuration du service VPN SSL des firewalls Stormshield SSL VPN Client en version 4.x,
- La mise en œuvre d'un accès réseau *Zero Trust* (ZTNA) avec des firewalls Stormshield SSL VPN Client en version 4.8 ou supérieure et des clients VPN SSL Stormshield en version 4.0 ou supérieure,
- L'installation du client VPN SSL Stormshield en version 4.x, sa configuration, son utilisation jusqu'à l'établissement d'un tunnel VPN SSL, certaines de ses spécificités (compatibilités, modes de connexion, ...) et l'accès à ses journaux,
- Le suivi des utilisateurs connectés au VPN SSL,
- Certaines informations concernant le logiciel OpenVPN Connect.

Dans la suite du document, Stormshield SSL VPN Client peut également être nommé "client VPN SSL Stormshield".

Prérequis

Les prérequis pour réaliser les manipulations de ce guide sont les suivants.

Disposer d'un client VPN SSL compatible

Chaque poste de travail ou terminal mobile doit disposer d'un client VPN compatible pour établir des tunnels VPN SSL avec le firewall Stormshield SSL VPN Client. Les clients VPN compatibles sont :

- **Stormshield SSL VPN Client** en version 4 : ce guide présente son installation, sa configuration, son utilisation jusqu'à l'établissement d'un tunnel VPN SSL et certaines de ses spécificités (compatibilités, modes de connexion, ...),
- **OpenVPN Connect**.

Pour plus d'informations sur les versions et les systèmes d'exploitation compatibles des logiciels Stormshield, reportez-vous au Guide de cycle de vie Network Security & Tools.

NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Disposer d'un firewall SNS adapté

Le nombre maximal de tunnels VPN SSL autorisés par les firewalls Stormshield SSL VPN Client est différent selon le modèle utilisé. Choisissez un modèle adapté à vos besoins. Retrouvez cette information sur le site de Stormshield, rubrique Gamme produits (SNS) en sélectionnant votre modèle.

Avoir connecté le firewall Stormshield SSL VPN Client à un annuaire

Le firewall Stormshield SSL VPN Client doit être connecté à un annuaire pour afficher dans ses modules les listes d'utilisateurs et groupes d'utilisateurs. Ceci permettra de définir les utilisateurs et groupes d'utilisateurs autorisés à établir des tunnels VPN SSL.

Vérifiez cette connexion dans l'interface d'administration du firewall Stormshield SSL VPN Client dans **Configuration > Utilisateurs > Authentification**, onglet **Méthodes disponibles**. Une ligne **LDAP** doit apparaître dans la grille. Pour plus d'informations sur la configuration des annuaires, reportez-vous à la section Configuration des annuaires du *manuel utilisateur de la version Stormshield SSL VPN Client utilisée*.

Permettre aux utilisateurs d'accéder au portail captif du firewall Stormshield SSL VPN Client

Le portail captif du firewall Stormshield SSL VPN Client doit être activé et les utilisateurs qui se connecteront en VPN SSL doivent pouvoir y accéder. Cet accès permet notamment :

- Aux clients VPN SSL Stormshield de récupérer leur configuration VPN SSL,
- Au firewall Stormshield SSL VPN Client et aux clients VPN SSL Stormshield d'appliquer la politique de vérification de la conformité des postes clients dans le cas où un accès réseau *Zero Trust* est utilisé.

Vous pouvez vérifier la configuration du portail captif dans l'interface d'administration du firewall Stormshield SSL VPN Client dans **Configuration > Utilisateurs > Authentification**, onglets **Portail captif** et **Profils du portail captif**. Pour plus d'informations sur la configuration du portail captif, reportez-vous à la section Authentification du *manuel utilisateur de la version Stormshield SSL VPN Client utilisée*.

Cas de l'authentification multifacteur

Dans le cas où une authentification multifacteur pour les connexions VPN SSL est utilisée :

Pour une authentification multifacteur utilisant la solution TOTP Stormshield

- Le firewall Stormshield SSL VPN Client doit être en version 4.5 ou supérieure,
- La solution TOTP doit être déjà configurée. Pour plus d'informations, reportez-vous à la note technique Configurer et utiliser la solution TOTP Stormshield.

Pour une authentification multifacteur utilisant une solution tierce et un serveur RADIUS

- La solution d'authentification multifacteur choisie doit être déjà configurée,
- Le serveur RADIUS permettant de faire le lien entre le firewall Stormshield SSL VPN Client et la solution d'authentification multifacteur choisie doit être déjà configuré.

Cas de la mise en œuvre d'un accès réseau *Zero Trust* (ZTNA)

Dans le cas où un accès réseau *Zero Trust* est utilisé :

- Le firewall Stormshield SSL VPN Client doit être en version 4.8 ou supérieure,
- Chaque poste de travail doit utiliser le client VPN SSL Stormshield en version 4.0 ou supérieure,
- Le Client VPN SSL Stormshield doit être configuré en mode automatique.

NOTE

Un accès réseau *Zero Trust* (ZTNA) consiste à ne faire confiance aux utilisateurs et aux appareils qu'après leur vérification. On parle d'accès réseau *Zero Trust* (ZTNA) lorsque plusieurs composantes sont réunies :

- Une garantie de la conformité du canal de communication grâce au chiffrement TLS des tunnels VPN,
- Une vérification des utilisateurs grâce à l'authentification multifacteur (par exemple avec la solution TOTP Stormshield),
- Une politique de vérification de la conformité des postes clients et des utilisateurs,
- Un filtrage fin pour limiter l'accès des utilisateurs aux seules ressources nécessaires.

Spécificités du client VPN SSL Stormshield v4

Cette section présente certaines spécificités du client VPN SSL Stormshield v4.

NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Compatibilité

Versions et systèmes d'exploitation compatibles

Pour plus d'informations, reportez-vous au Guide de cycle de vie Network Security & Tools.

Méthodes d'authentification multifacteur compatibles

- Mot de passe + Code OTP.
  Cette méthode est compatible avec la solution TOTP Stormshield. Le firewall Stormshield SSL VPN Client doit être en version 4.5 ou supérieure pour utiliser cette solution,
- Code OTP seulement,
- Mode Push (utilisation d'une application tierce pour approuver la connexion).

Modes de connexion

Mode automatique

Avec ce mode, le client VPN SSL Stormshield récupère automatiquement et de manière sécurisée sa configuration VPN SSL sur le firewall Stormshield SSL VPN Client. Il fonctionne de la manière suivante :

À la première connexion :

- Le client VPN SSL Stormshield s'authentifie une première fois sur le firewall Stormshield SSL VPN Client :
  - Le client VPN SSL Stormshield récupère automatiquement sa configuration VPN ,
  - Le firewall Stormshield SSL VPN Client et le client VPN SSL Stormshield appliquent la politique de vérification de la conformité des postes clients (cas du ZTNA).
- Si la première authentification aboutit, le client VPN SSL Stormshield s'authentifie une seconde fois sur le firewall Stormshield SSL VPN Client afin d'établir le tunnel VPN SSL.

Lors des connexions suivantes :

- Le client VPN SSL Stormshield vérifie si une nouvelle configuration VPN est disponible :
  - S'il n'existe pas de nouvelle configuration, le client VPN SSL Stormshield s'authentifie sur le firewall Stormshield SSL VPN Client afin d'établir le tunnel VPN SSL,
  - Si une nouvelle configuration est disponible, le client VPN SSL Stormshield s'authentifie deux fois comme lors d'une première connexion.

Mode manuel

Avec ce mode, vous devez importer la configuration VPN dans un profil de connexion.

Vous pouvez récupérer la configuration VPN (fichier *.ovpn*) depuis le portail captif du firewall hébergeant le service VPN SSL ou depuis l'interface d'administration du firewall. Cette manipulation est décrite dans la section Récupérer la configuration VPN SSL (fichier .ovpn).

Matrice de compatibilité des modes de connexion

Ce tableau récapitule les fonctionnalités compatibles selon le mode de connexion utilisé.

Fonctionnalité	Mode automatique	Mode manuel
Carnet d'adresses	✓	✗
Gestion des profils	✗	✓
Vérification de la conformité des postes clients (ZTNA) *Version SNS 4.8 ou supérieure requise*	✓	✗

Fonctionnalités du client VPN SSL Stormshield

Carnet d'adresses (Mode automatique requis)

Le client VPN SSL Stormshield dispose d'un carnet d'adresses permettant de mémoriser les informations de connexion à différents firewalls : adresse de connexion au firewall (adresse IPv4 ou FQDN), identifiant, mot de passe et utilisation d'une authentification multifacteur.

Exécution de scripts

Sous Windows, le client VPN SSL Stormshield peut exécuter automatiquement des scripts sur le poste de travail de l'utilisateur à chaque ouverture et fermeture d'un tunnel VPN SSL. Pour cela, vous devez au préalable ajouter les scripts à exécuter dans la configuration du service VPN SSL du firewall Stormshield SSL VPN Client.

Limitations et précisions sur les cas d'utilisation

Mise à jour vers une version inférieure à la version 4

La mise à jour vers une version inférieure à la version 4 du client VPN SSL Stormshield n'est pas supportée.

Lorsqu'un carnet d'adresses provenant d'une version 3 ou 2 du client VPN SSL Stormshield est ouvert avec une version 4, son format est mis à jour automatiquement et il ne peut plus être utilisé avec sa version d'origine. Si nécessaire, vous pouvez conserver une copie du fichier du carnet d'adresses en version 3 ou 2 avant de mettre à jour le client VPN SSL Stormshield en version 4.

Affichage de l'icône dans la barre des tâches sous Windows 11

Sous Windows 11, assurez-vous que l'affichage de l'icône du client VPN SSL Stormshield dans la barre des tâches Windows est activé dans **Paramètres de la barre des tâches > Autres icônes de barre d'état système > Menu d'icône masqué**. Dans le cas contraire, les fonctionnalités du client VPN SSL Stormshield sont inaccessibles car elles nécessitent un accès à l'icône du logiciel pour en ouvrir le menu.

Configurer le firewall Stormshield SSL VPN Client

La mise en œuvre de tunnels VPN SSL nécessite de configurer plusieurs modules dans l'interface web d'administration du firewall Stormshield SSL VPN Client. Pour plus d'informations, reportez-vous au **Guide d'administration VPN SSL des firewalls SNS et des clients VPN SSL Stormshield**.

Installer le client VPN SSL Stormshield v4

Cette section explique comment installer le client VPN SSL Stormshield v4 de manière classique avec le programme d'installation, via une stratégie de groupe (GPO) ou via un script.

NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

NOTE
Le retour à une version précédente du client VPN SSL Stormshield n'est pas supporté. De plus, une fois le client VPN SSL installé, assurez-vous qu'il dispose d'un accès à la zone de notification de la barre des tâches sous Windows 11. Pour plus d'informations, reportez-vous à la section Limitations et précisions sur les cas d'utilisation.

Télécharger le client VPN SSL Stormshield v4

Le programme d'installation du client VPN SSL Stormshield est disponible dans deux formats :

Format	Description
.exe	Un seul fichier exécutable regroupant toutes les langues et les versions de Windows supportées. À utiliser pour une installation classique ou un déploiement via un script.
.msi	Plusieurs packages *.msi* disponibles selon les langues et les versions de Windows supportées. À utiliser pour un déploiement via une stratégie de groupe (GPO) ou via un script.

Vous pouvez télécharger le client VPN SSL Stormshield au format souhaité depuis :

- **Votre espace MyStormshield.**
  Connectez-vous à votre espace MyStormshield et rendez-vous dans **Téléchargements** > **Téléchargements** > **Stormshield Network Security** > **VPN SSL**.

Vous pouvez vérifier l'intégrité des binaires récupérés grâce à la commande suivante :

```
CertUtil -hashfile <filename> SHA256
```

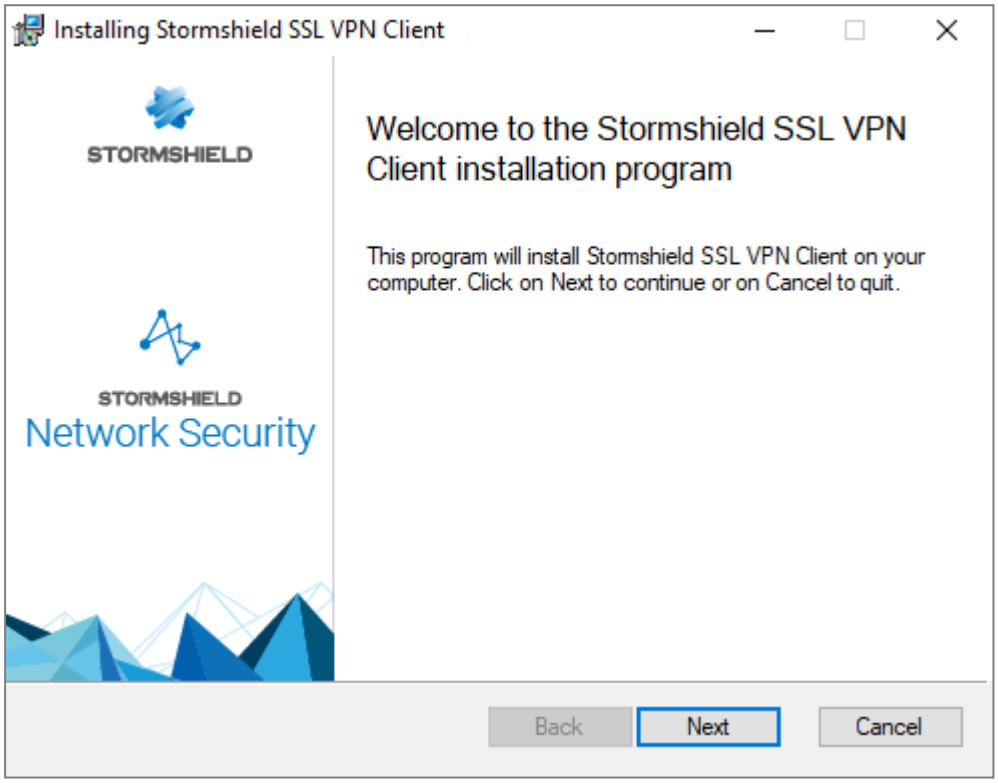
Comparez le résultat obtenu avec l'empreinte (hash) indiquée dans votre espace MyStormshield dans la colonne **SHA256** du tableau des téléchargements.

Installer le client VPN SSL Stormshield avec le programme d'installation *.exe*

Vous devez être administrateur local du poste de travail ou fournir le nom et le mot de passe d'un compte administrateur pour installer le client VPN SSL Stormshield.

1. Connectez-vous à la session utilisateur sur laquelle installer le client VPN SSL Stormshield.
2. Exécutez le programme d'installation (fichier *.exe*) téléchargé au préalable.

3. Suivez les étapes de l'assistant d'installation.
   Vous pouvez personnaliser les paramètres à utiliser par défaut pour se connecter au VPN :
   - L'adresse IP ou le FQDN du firewall,
   - Si la configuration VPN est récupérée avec le mode automatique,
   - Si une authentification multifacteur est utilisée,
   - Si l'utilisateur Windows de la session en question est utilisé comme identifiant.



Déployer le client VPN SSL Stormshield via une stratégie de groupe (GPO)

Vous pouvez déployer directement le package *.msi* téléchargé au préalable ou le modifier pour faciliter la connexion des utilisateurs au VPN SSL en personnalisant certains paramètres.

Créer un package *.mst* pour personnaliser les paramètres à utiliser par défaut pour se connecter au VPN

Vous pouvez personnaliser les paramètres suivants :

- L'adresse IP ou le FQDN du firewall,
- Si la configuration VPN est récupérée avec le mode automatique,
- Si une authentification multifacteur est utilisée,
- Si l'utilisateur Windows de la session en question est utilisé comme identifiant.

Pour créer le package *.mst* :

1. Depuis un poste de travail disposant de l'outil Microsoft Orca, accédez au dossier où se trouve le package *.msi* du client VPN SSL Stormshield, faites un clic-droit et choisissez **Edit with Orca**.
2. Cliquez sur **Transform** > **New Transform**.

3. Sélectionnez la table **Property**.
4. Pour que l'utilisateur Windows de la session en question soit utilisé comme identifiant, indiquez dans le champ **Value** de la propriété *USE_DEFAULT_USERNAME* la valeur *1*.
5. Pour que le client VPN SSL utilise par défaut le mode manuel, indiquez dans le champ **Value** de la propriété *AUTOMATIC_MODE* la valeur *0*,
6. Pour personnaliser l'adresse IP ou le FQDN du firewall :
   1. Faites un clic droit et choisissez **Add Row**.
   2. Dans le champ **Property**, indiquez *DEFAULT_ADDRESS*.
   3. Dans le champ **Value**, indiquez l'adresse IP ou le FQDN du firewall.
   4. Cliquez sur **OK**.
7. Pour indiquer si une authentification multifacteur doit être utilisée :
   1. Faites un clic droit et choisissez **Add Row**.
   2. Dans le champ **Property**, indiquez *ENABLE_OTP*.
   3. Dans le champ **Value**, indiquez *1* pour utiliser une authentification multifacteur ou *0* pour ne pas l'utiliser.
   4. Cliquez sur **OK**.
8. Cliquez sur **Transform > Generate Transform**.
9. Enregistrez le package *.mst* dans le même répertoire que le package *.msi*.

Configurer le déploiement par GPO

1. Sur le contrôleur de domaine, lancez le gestionnaire de serveur.
2. Dans la barre supérieure de menu, cliquez sur **Outils > Gestion des stratégies de groupe**.
3. Dans la liste de gauche, faites un clic droit sur le nom du domaine Microsoft Active Directory et sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici...**.
4. Nommez la GPO et cliquez sur **OK**.
5. Dans la liste de gauche, faites un clic droit sur le nom de la GPO que vous venez de créer et sélectionnez **Modifier**.
   La fenêtre d'édition de la GPO s'ouvre.
6. Dans le menu de gauche de la GPO, dépliez le menu **Configuration ordinateur > Stratégies > Paramètres du logiciel**.
7. Faites un clic droit sur **Installation de logiciel**, sélectionnez **Nouveau > Package**, puis sélectionnez le package *msi* d'installation du client VPN SSL Stormshield.
8. Choisissez le mode **Avancé** et cliquez sur **OK**.
   La fenêtre d'édition de la GPO s'ouvre.
9. Vous pouvez renommer cette instance d'installation si vous le souhaitez.
10. Dans l'onglet **Modifications**, vous pouvez associer le package *.mst* précédemment créé à la GPO d'installation du client VPN SSL Stormshield. Pour cela, cliquez sur **Ajouter...**, sélectionnez le package *.mst* et cliquez sur *Ouvrir*.
11. Cliquez sur **OK**.

L'installation est automatique lorsqu'un poste de travail se connecte au réseau de l'entreprise.

Déployer le client VPN SSL Stormshield via un script

1. Ouvrez une invite de commande en tant qu'administrateur.
2. Allez dans le dossier où se trouve le fichier *.exe* ou le package *.msi* téléchargé au préalable.
3. Tapez la commande correspondante :
   - Pour un fichier *.exe* :
     ```
     Stormshield_SSLVPN_Client_4.X.Y_x64.exe [PARAMETERS]
     ```
   - Pour un package *.msi* :
     ```
     msiexec /i Stormshield_SSLVPN_Client_4.X.Y_language_x64.msi
     [PARAMETERS] /qn
     ```

   Vous pouvez faciliter la connexion des utilisateurs au VPN SSL en complétant la commande avec les paramètres suivants :
   - DEFAULT_ADDRESS=[adresse IP ou FQDN du firewall],
   - AUTOMATIC_MODE=[0 pour le mode manuel, 1 pour le mode automatique],
   - USE_DEFAULT_USERNAME=[0 pour que le champ reste vide, 1 pour que l'utilisateur Windows de la session en question soit utilisé comme identifiant],
   - ENABLE_OTP=[0 pour ne pas utiliser une authentification multifacteur, 1 pour en utiliser une].
4. Exécutez la commande.

Exemple de commande permettant de déployer le fichier *.exe* :

```
Stormshield_SSLVPN_Client_4.0.0_x64.exe DEFAULT_ADDRESS=vpn.company.tld
```

Exemple de commande permettant de déployer un package *.msi* :

```
msiexec /i Stormshield_SSLVPN_Client_4.0.0_en_x64.msi DEFAULT_
ADDRESS=vpn.company.tld AUTOMATIC_MODE=1 ENABLE_OTP=0 /qn
```

L'installation est automatique lorsqu'un poste de travail se connecte au réseau de l'entreprise. Une invite de commande s'affiche sur le bureau et une barre de progression indique l'état de l'installation.

Configurer le client VPN SSL Stormshield v4

Vous devez configurer le client VPN SSL Stormshield v4 selon le mode de connexion souhaité. Reportez-vous à la section Matrice de compatibilité des modes de connexion pour vérifier les fonctionnalités compatibles selon le mode de connexion utilisé.

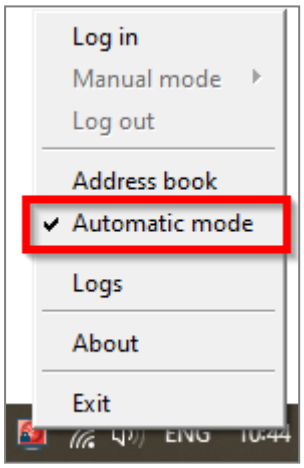
NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Activer le Mode automatique

En **Mode automatique**, le client VPN SSL Stormshield récupère automatiquement la configuration VPN après authentification et validation du droit à l'utilisation du VPN SSL.

1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows.
2. Cliquez sur **Mode automatique**.

Pour vous connecter, poursuivez vers la section Établir un tunnel VPN en Mode automatique.

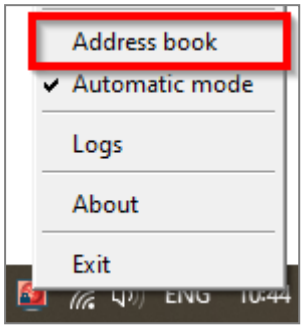


Configurer le carnet d'adresses (Mode automatique requis)

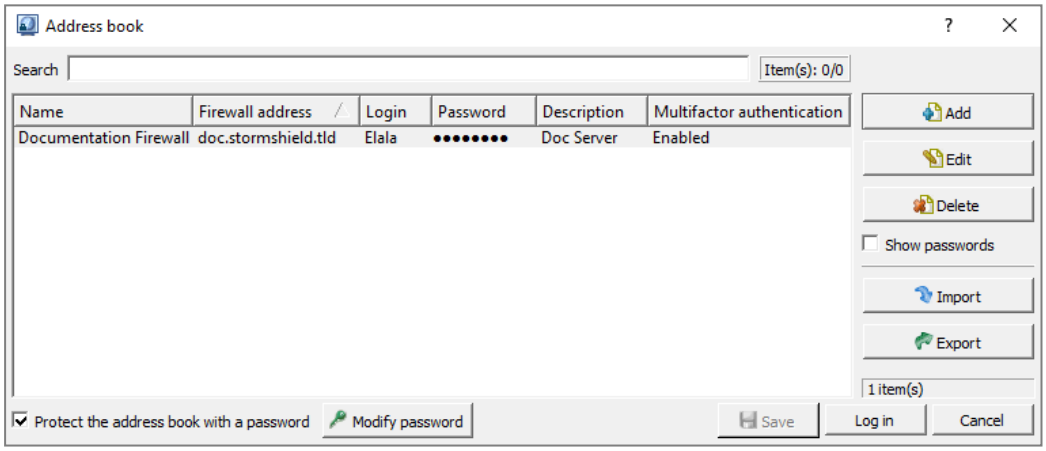
Le client VPN SSL Stormshield dispose d'un carnet d'adresses permettant de mémoriser les informations de connexion à différents firewalls : adresse de connexion au firewall (adresse IPv4 ou FQDN), identifiant, mot de passe et utilisation d'une authentification multifacteur.

Ouvrir le carnet d'adresses

1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows.
2. Cliquez sur **Carnet d'adresses**. Le **Mode automatique** doit être activé.



3. Si le carnet d'adresses est protégé par un mot de passe, renseignez-le pour l'ouvrir. Vous pouvez protéger le carnet d'adresses grâce aux options **Protéger le carnet d'adresses par un mot de passe** et **Modifier le mot de passe**.

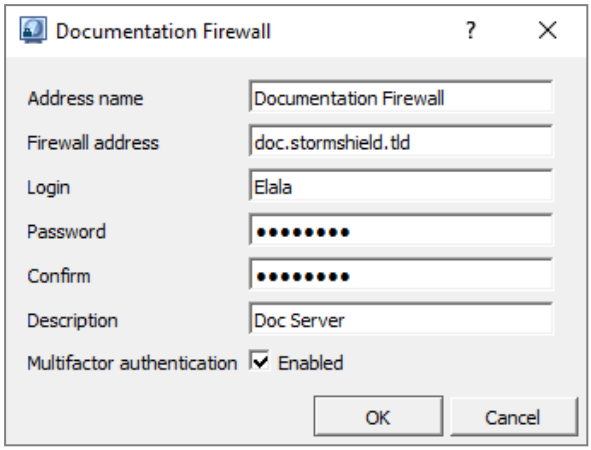


Ajouter ou modifier une adresse dans le carnet d'adresses

1. Cliquez sur **Ajouter** pour ajouter une nouvelle adresse. Pour modifier une adresse existante, sélectionnez-la puis cliquez sur **Modifier**.
2. Complétez les champs.

Champ / Case	Description
Nom de l'adresse	Nom de l'adresse.
Adresse du firewall	Adresse IPv4 ou FQDN du firewall Stormshield SSL VPN Client à joindre pour établir le tunnel VPN. Si le port du portail captif du firewall n'est pas celui par défaut (TCP/443), renseignez l'adresse et le port séparés par deux points (adresse:port).
Identifiant	Identifiant de l'utilisateur.
Mot de passe Confirmer	Mot de passe de l'utilisateur. Si une authentification multifacteur **Code OTP seulement** ou **Mode Push** est utilisée, laissez ces champs vides.
Description	Description de l'adresse, si nécessaire.
Authentification multifacteur	Si une authentification multifacteur est utilisée (**Mot de passe + Code OTP**, **Code OTP seulement** ou **Mode Push**), cochez la case **Activée**.

3. Cliquez sur **OK**, puis sur **Sauvegarder**.



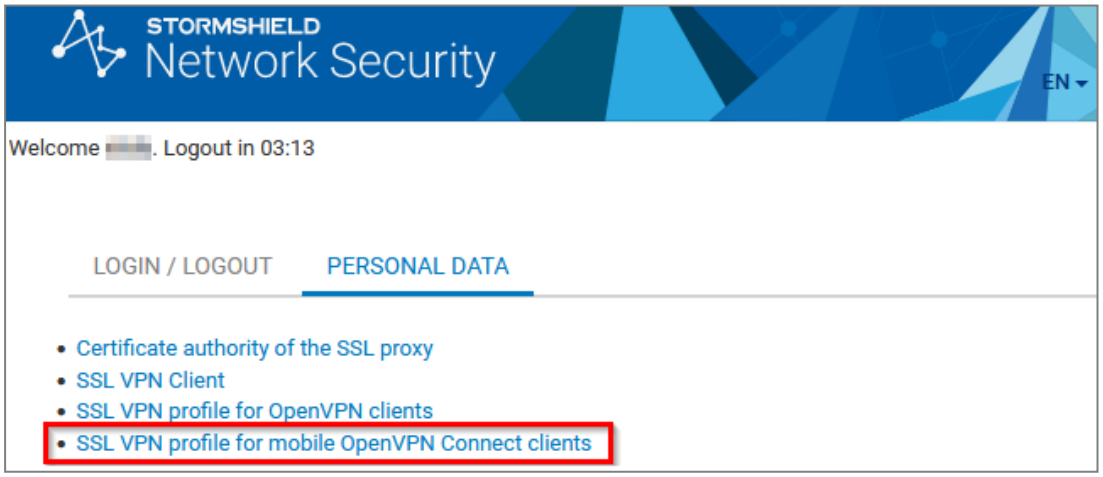
Configurer le Mode manuel

En **Mode manuel**, vous devez importer les éléments de configuration (autorité de certification, certificat, clé privée, ...) que le client VPN SSL Stormshield doit utiliser, rassemblés dans un fichier *.ovpn*.

Récupérer la configuration VPN SSL (fichier *.ovpn*)

Vous pouvez récupérer la configuration VPN SSL Stormshield depuis :

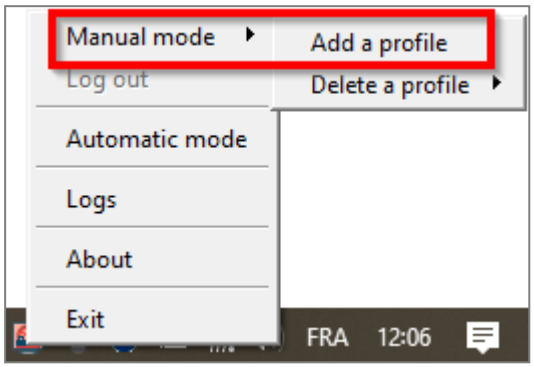
- **Le portail captif du firewall Stormshield SSL VPN Client hébergeant le service VPN SSL.**
  En étant connecté sur le réseau de l'entreprise, authentifiez-vous à l'adresse *https://adresseIP_du_firewall/auth*, puis dans l'onglet **Données personnelles**, cliquez sur *Profil VPN SSL pour clients mobile OpenVPN Connect (fichier unique .ovpn)*,



- **L'interface d'administration du firewall Stormshield SSL VPN Client.**
  Rendez-vous dans **Configuration > VPN > VPN SSL > Configuration avancée** et cliquez sur **Exporter le fichier de configuration**.

Ajouter un profil de connexion

1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows.
2. Cliquez sur **Mode manuel** > **Ajouter un profil**. Le **Mode automatique** doit être désactivé.



3. Sélectionnez le fichier *.ovpn*.
4. Définissez un nom au profil de connexion.
5. Cliquez sur **OK**.

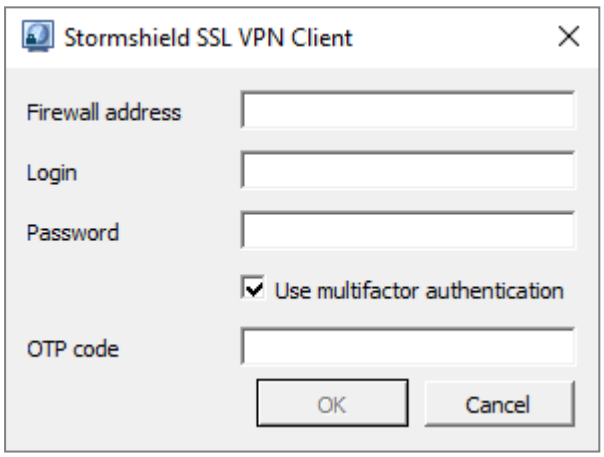
Établir un tunnel VPN avec le client VPN SSL Stormshield v4

Le firewall Stormshield SSL VPN Client et le client VPN SSL Stormshield v4 étant configurés, vous pouvez établir un tunnel VPN.

NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Établir un tunnel VPN en Mode automatique

1. Double cliquez sur l'icône dans la barre des tâches Windows pour ouvrir la fenêtre de connexion.



2. Dans le champ **Adresse du firewall**, indiquez l'adresse IPv4 ou le FQDN du firewall Stormshield SSL VPN Client à joindre pour établir le tunnel VPN. Si le port du portail captif du firewall n'est pas celui par défaut (TCP/443), renseignez l'adresse et le port séparés par deux points (adresse:port).
3. Dans le champ **Identifiant**, renseignez l'identifiant de l'utilisateur.
4. Complétez le reste des champs selon l'authentification qui s'applique.
Dans le tableau, ✅ signifie que les champs doivent être renseignés, ❌ signifie qu'ils doivent rester vides, et - signifie qu'ils ne sont pas visibles.

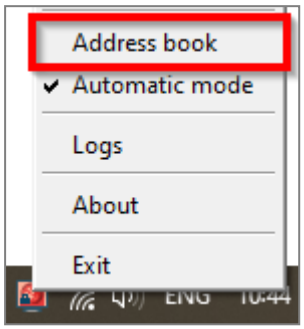
Authentification	Mot de passe	Authentification multifacteur	Code OTP
Classique	✅	❌	-
Multifacteur **Mot de passe + Code OTP**	✅	✅	✅
Multifacteur **Code OTP seulement**	❌	✅	✅
Multifacteur **Mode Push**	❌	✅	❌

5. Cliquez sur **OK**.

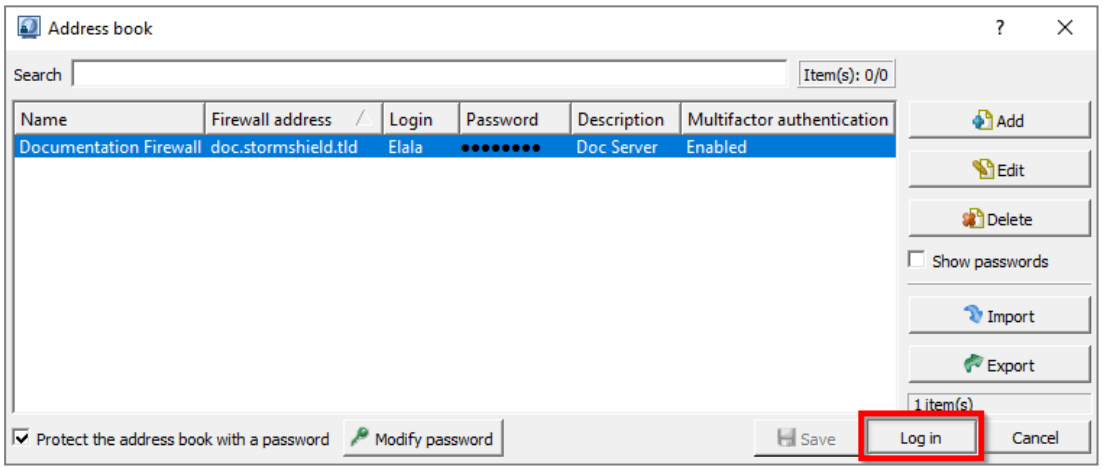
Le client VPN SSL Stormshield s'authentifie sur le firewall Stormshield SSL VPN Client. Si l'authentification n'aboutit pas, consultez la section Que faire si le tunnel VPN ne s'établit pas.

Établir un tunnel VPN en utilisant le carnet d'adresses

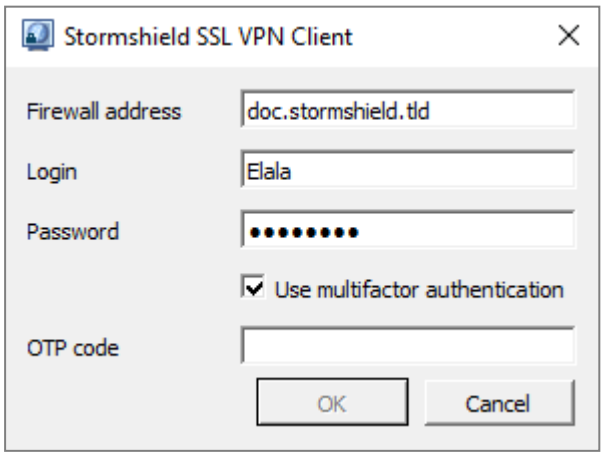
1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows, puis cliquez sur **Carnet d'adresses**. Pour rappel, le **Mode automatique** doit être activé.



2. Si le carnet d'adresses est protégé par un mot de passe, renseignez-le pour l'ouvrir.
3. Sélectionnez l'adresse sur laquelle vous connecter et cliquez sur **Se connecter**.



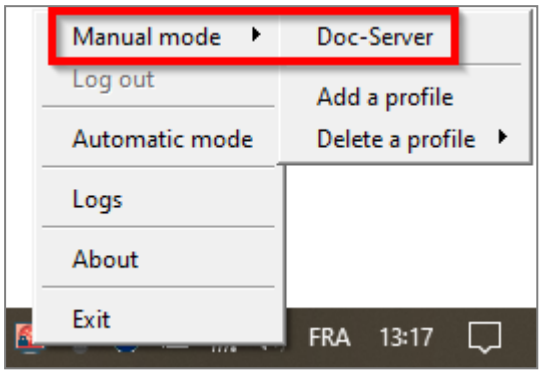
4. La fenêtre de connexion s'affiche.
   - Pour une authentification classique, la connexion se lance automatiquement,
   - Pour une authentification multifacteur **Mot de passe + Code OTP** ou **Code OTP seulement**, renseignez un **Code OTP** (mot de passe à usage unique) et cliquez sur **OK**,
   - Pour une authentification multifacteur **Mode Push**, cliquez sur **OK** et approuvez la connexion sur l'application tierce.



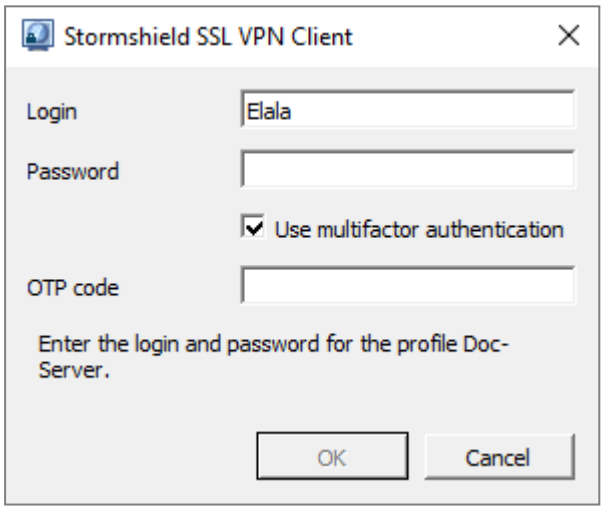
Le client VPN SSL Stormshield s'authentifie sur le firewall Stormshield SSL VPN Client. Si l'authentification n'aboutit pas, consultez la section Que faire si le tunnel VPN ne s'établit pas.

Établir un tunnel VPN en Mode manuel

1. Effectuez un clic-droit sur l'icône dans la barre des tâches Windows, puis cliquez sur **Mode manuel** et sur le profil concerné.



La fenêtre de connexion s'ouvre.



2. Dans le champ **Identifiant**, renseignez l'identifiant de l'utilisateur.
3. Complétez le reste des champs selon l'authentification qui s'applique.
Dans le tableau, ✅ signifie que les champs doivent être renseignés, ❌ signifie qu'ils doivent rester vides, et - signifie qu'ils ne sont pas visibles.

Authentification	Mot de passe	Authentification multifacteur	Code OTP
Classique	✅	❌	-
Multifacteur **Mot de passe + Code OTP**	✅	✅	✅
Multifacteur **Code OTP seulement**	❌	✅	✅
Multifacteur **Mode Push**	❌	✅	❌

4. Cliquez sur **OK**.

Le client VPN SSL Stormshield s'authentifie sur le firewall Stormshield SSL VPN Client. Si l'authentification n'aboutit pas, consultez la section Que faire si le tunnel VPN ne s'établit pas.

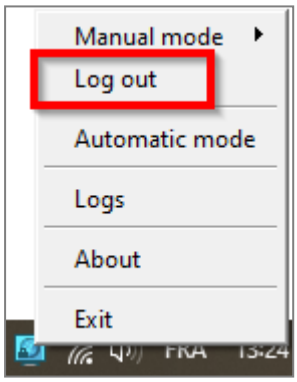
Afficher les informations de connexion du tunnel VPN SSL

La couleur de l'icône du client VPN SSL Stormshield située dans la barre des tâches Windows permet de connaître son état de connexion.

Icône	Description
	Le client VPN SSL Stormshield est connecté. Survolez l'icône avec la souris afin d'afficher des informations sur le tunnel VPN SSL (nom d'utilisateur et l'adresse du firewall Stormshield SSL VPN Client, heure où la connexion s'est établie avec le firewall Stormshield SSL VPN Client, adresse IP du poste au travers du tunnel VPN SSL et nombre d'octets échangés).
	Le client VPN SSL Stormshield est en train de se connecter.
	Le client VPN SSL Stormshield n'est pas connecté ou une tentative de connexion a échoué.

Déconnecter le tunnel VPN SSL

1. Effectuez un clic-droit sur l'icône  dans la barre des tâches Windows.
2. Cliquez sur **Se déconnecter**.



Que faire si le tunnel VPN ne s'établit pas

Dans le cas où le tunnel VPN ne s'établit pas, suivez ces quelques recommandations :

- Prenez connaissance du message d'erreur qui s'affiche,
- Vérifiez les informations de connexion dans la fenêtre de connexion ainsi que dans le carnet d'adresses si utilisé,
- Vérifiez la validité du code OTP si renseigné. Le client VPN SSL Stormshield effectue plusieurs tentatives de connexion en cas de non réponse, le code OTP peut donc avoir expiré entre temps,
- Vérifiez la configuration du profil de connexion importé (pour le Mode manuel). Par exemple, si la configuration VPN SSL du firewall Stormshield SSL VPN Client a été modifiée, cette dernière doit être importée sur le client VPN SSL Stormshield,
- Consultez la section Résoudre les problèmes.

Consulter les journaux du client VPN SSL Stormshield v4

Cette section présente les journaux disponibles du client VPN SSL Stormshield v4.

NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Journaux en cas d'erreurs d'installation, de désinstallation ou de mise à jour

Des journaux sont créés lorsqu'une erreur est rencontrée lors de l'installation, la désinstallation ou la mise à jour du client VPN SSL Stormshield. Vous pouvez les retrouver à cet emplacement :

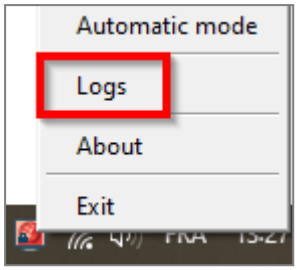
```
%programfiles%\Stormshield\Stormshield SSL VPN Client\install_logs
```

Nom du fichier	Contenu
install_driver.log	Erreurs rencontrées lors de l'installation du driver OpenVPN
uninstall_driver.log	Erreurs rencontrées lors de la suppression du driver OpenVPN
backward_update_sites.log	Erreurs rencontrées lors de la copie des profils de connexion depuis le client VPN SSL Stormshield en version 3.2.3 ou inférieure
generate_ovpn_auth.log	Erreurs rencontrées lors de la génération de la clé privée utilisée pour sécuriser l'accès à l'interface de gestion OpenVPN
tap_create.log	Erreurs rencontrées lors de l'installation de l'interface réseau pour OpenVPN
tap_delete.log	Erreurs rencontrées lors de la suppression de l'interface réseau pour OpenVPN
update_ovpn_admin.log	Erreurs rencontrées lors de la mise à jour de la valeur *ovpn_admin_group* dans la clé *HKEY_LOCAL_MACHINE\SOFTWARE\StormshieldSSLVPN*
clean_previous_version.log	Informations de la désinstallation de la version 3.2.3 ou inférieure
install_certs.log	Erreurs rencontrées lors de l'installation du certificat
set_dacls.log	Erreurs rencontrées lors de la mise à jour des droits d'accès aux dossiers
service_update.log	Erreurs rencontrées lors de la mise à jour du service VPN SSL

Journaux des connexions VPN SSL

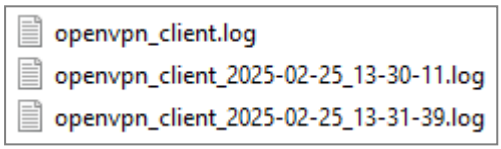
Vous pouvez retrouver les journaux des connexions VPN SSL en effectuant un clic-droit sur l'icône  dans la barre des tâches Windows puis en cliquant sur **Journaux (logs)**, ou dans l'explorateur de fichiers Windows à cet emplacement :

```
%localappdata%\Stormshield\Stormshield SSL VPN Client\log\openvpn_
client.log
```



À l'établissement d'un tunnel VPN SSL :

- Si la taille du fichier *openvpn_client.log* est supérieure à 1 Mo, celui-ci est renommé selon le format suivant "*openvpn_client_yyyy-MM-dd_hh-mm-ss.log*" et un nouveau fichier *openvpn_client.log* est créé,
- Si la taille totale des fichiers *.log* est supérieure à 100 Mo, le plus ancien est supprimé.



Journaux accessibles dans l'observateur d'événements Windows

Les journaux liés au client VPN SSL Stormshield sont accessibles par l'intermédiaire de l'observateur d'événements Windows sur les postes des utilisateurs.

Par défaut, seuls les journaux d'erreur sont accessibles dans l'observateur d'événements.

Pour accéder aux journaux du client VPN SSL Stormshield :

1. Ouvrez l'**Observateur d'événements** Windows.
2. Sélectionnez **Journaux des applications et des services > Stormshield SSL VPN service**.

Pour modifier les journaux accessibles dans l'observateur d'événements Windows :

1. Ouvrez l'**Éditeur de Registre** Windows.
2. Modifiez la valeur *log_level* de la clé de registre suivante :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
StormshieldSSLVPNService\Parameters
```

   - 0 : affiche les journaux d'erreur. Il s'agit de la valeur par défaut,
   - 1 : affiche les journaux d'erreur et d'information,
   - 2 : affiche les journaux d'erreur, d'information et de dépannage.

Suivre les utilisateurs connectés au VPN SSL sur le firewall Stormshield SSL VPN Client

Vous pouvez suivre dans l'interface d'administration du firewall Stormshield SSL VPN Client les utilisateurs connectés ou qui se sont connectés au VPN SSL. Pour plus d'informations, reportez-vous au Guide d'administration VPN SSL des firewalls SNS et des clients VPN SSL Stormshield.

Résoudre les problèmes

Ce chapitre liste certains problèmes fréquemment rencontrés lors de l'utilisation du client VPN SSL Stormshield v4. Si celui que vous rencontrez ne se trouve pas dans ce chapitre, nous vous recommandons de consulter la Base de connaissances Stormshield.

NOTE
Si vous utilisez le client VPN SSL Stormshield en version 5, reportez-vous à la documentation Stormshield SSL VPN Client v5.

Les utilisateurs doivent approuver le certificat présenté par le firewall SNS lors d'une première connexion

- *Situation* : Lors du premier établissement du tunnel VPN SSL, les utilisateurs doivent approuver le certificat présenté par le firewall SNS, alors même que ce certificat est certifié par une autorité de certification présente dans le magasin de certificats des utilisateurs.
- *Cause* : L'autorité de certification racine est présente uniquement dans le magasin de certificats des utilisateurs et n'est pas présente dans le magasin de certificats du poste de travail. Par défaut, la vérification du certificat par le client VPN SSL Stormshield utilise le magasin de certificats du poste de travail.
- *Solution* : Modifiez à 1 la valeur **http_request_as_user** dans la base de registre sous la clé :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters
```

Le tunnel VPN SSL ne s'établit pas

Une configuration proxy est définie sur le poste de travail et le client VPN SSL Stormshield ne parvient pas à joindre le firewall SNS

- *Situation* : Lors de la tentative de connexion au VPN SSL sur un poste de travail disposant d'une configuration proxy, le tunnel ne s'établit pas.
- *Cause* : L'accès direct en HTTPS n'est pas autorisé sans utiliser le proxy du poste de travail. Par défaut, les requêtes HTTPS vers le firewall SNS, notamment pour télécharger la configuration VPN, sont effectuées en direct par le client VPN SSL Stormshield sans passer par le proxy.

  NOTE
  Jusqu'à la version 4.0.9, la version 4.0 du client VPN SSL Stormshield utilisait la configuration proxy définie sur le poste de travail pour contacter le firewall SNS en HTTPS. Ce comportement a été modifié en version 4.0.10.

- *Solution* : Modifiez à 1 la valeur **http_use_default_proxy** dans la base de registre sous la clé :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldSSLVPNService\Parameters
```

Le message "*La connexion a été refusée car l'utilisateur ou le poste client utilisé n'est pas conforme à la politique définie sur le firewall*" s'affiche

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*La connexion a été refusée car l'utilisateur ou le poste client utilisé n'est pas conforme à la politique définie sur le firewall*" s'affiche.
- *Cause* : Le poste client utilisé ne respecte pas tous les critères définis dans la politique de vérification de la conformité des postes clients et des utilisateurs (ZTNA).
- *Solutions* :
  - Vérifiez dans les journaux VPN (SSL, IPsec) les critères de vérification non conformes d'un poste client, puis mettez en conformité le poste client concerné,
  - Vérifiez la configuration de la politique de vérification de la conformité des postes clients.

Le message "*Connexion au firewall impossible : Echec de résolution du nom de l'UTM*" s'affiche

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Connexion au firewall impossible : Echec de résolution du nom de l'UTM*" s'affiche.
- *Cause* : L'adresse renseignée est incorrecte ou n'est pas joignable.
- *Solution* : Vérifiez que l'adresse du firewall renseignée est correcte ou est joignable.

Le message "*Identifiant ou mot de passe incorrect*" s'affiche

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Identifiant ou mot de passe incorrect*" s'affiche.
- *Cause* : Le mot de passe de l'utilisateur est incorrect ou ce dernier ne dispose pas des droits pour s'authentifier en VPN SSL.
- *Solutions* :
  - Vérifiez que l'identifiant et le mot de passe sont corrects.
  - Sur le firewall Stormshield SSL VPN Client, vérifiez que la **Politique VPN SSL** est paramétrée sur **Autoriser** dans **Configuration > Utilisateurs > Droits d'accès**, onglet **Accès par défaut** et que l'utilisateur ou le groupe d'utilisateurs concerné est autorisé à établir un tunnel VPN SSL dans **Configuration > Utilisateurs > Droits d'accès**, onglet **Accès détaillé**.

Le message "*Erreur lors de la connexion au service : Connection refused*" s'affiche

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Erreur lors de la connexion au service : Connection refused*" s'affiche.
- *Cause* : Les services **Stormshield SSL OpenVPN Service** et **Stormshield SSL VPN Service** ne sont pas démarrés ou ne fonctionnent pas.
- *Solution* : Vérifiez que les services Windows sont bien démarrés sur le poste de travail ou essayez de les redémarrer.

Les journaux contiennent le message "*Route: Waiting for TUN/TAP interface to come up...*"

- *Situation* : Lors de la tentative de connexion au VPN SSL, le tunnel ne s'établit pas et le message "*Erreur lors de la connexion au service : Connection refused*" s'affiche dans les journaux.
- *Cause* : Un problème avec l'interface **TAP-Windows Adapter** empêche le tunnel VPN de s'établir.
- *Solution* : Dans le **Centre Réseau et Partage** Windows, cliquez sur **Modifier les paramètres de la carte**, effectuez un clic-droit sur l'interface **TAP-Windows Adapter** et cliquez sur **Diagnostiquer**.

Une ressource de l'entreprise n'est pas accessible via le tunnel VPN

- *Situation* : Le tunnel est établi, mais une ressource de l'entreprise n'est pas accessible.
- *Cause* : La politique de filtrage du firewall bloque l'accès à cette ressource ou cette dernière n'est plus accessible. D'autres raisons peuvent être la cause de cette situation.
- *Solutions* :
  - Sur le firewall Stormshield SSL VPN Client, activez temporairement sur la règle du flux concerné le niveau de trace **Avancé** pour collecter des logs (dans **Configuration > Politique de sécurité > Filtrage et NAT > Filtrage**), puis vérifiez dans les logs que la règle s'applique pour ce flux (dans **Monitoring > Logs - Journaux d'audit > Filtrage**),
  - Assurez-vous que la ressource demandée est bien physiquement disponible,
  - Videz le cache ARP du poste de travail en exécutant la commande `arp -d *` dans une console.

Le tunnel VPN se ferme lors de l'envoi d'un fichier dont le poids est très important

- *Situation* : Lors de l'envoi d'un fichier volumineux, le tunnel VPN se ferme.
- *Cause* : Le fichier envoyé est trop volumineux.
- *Solution* : Réalisez l'envoi du fichier en utilisant un protocole qui utilise des blocs plus petits (comme FTP) ou en établissant le tunnel en UDP.

Un avertissement indique que la fonctonnalité de compression LZ4 est obsolète

- *Situation* : Dans l'interface Web d'administration d'un firewall Stormshield SSL VPN Client en version 4.8.5 ou supérieure, un avertissement s'affiche automatiquement à l'ouverture du module VPN SSL si la fonctionnalité de compression LZ4 est activée.
- *Cause* : La fonctionnalité de compression LZ4 est obsolète et il est fortement recommandé de la désactiver pour des raisons de sécurité.
- *Solution* : Dans la fenêtre d'avertissement, acceptez de désactiver cette fonctionnalité. Si vous avez ignoré cet avertissement, un message restera affiché tant qu'elle ne sera pas désactivée et vous devrez utiliser les commandes CLI Serverd pour la désactiver :

```
CONFIG OPENVPN UPDATE compress=0
CONFIG OPENVPN ACTIVATE
```

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur le VPN SSL sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

STORMSHIELD

documentation@stormshield.eu