



STORMSHIELD



GUIDE

**STORMSHIELD NETWORK SSL VPN
CLIENT**

GUIDE DE CONFIGURATION ET D'UTILISATION

Version 5.1

Dernière mise à jour du document : 22 octobre 2025

Référence : sns-fr-ssl_vpn_client_guide_configuration_utilisation-v5.1



Table des matières

Historique des modifications	3
Prendre en main le client VPN SSL Stormshield	4
Présentation de l'interface graphique et des menus du client VPN SSL Stormshield	5
Présentation de l'interface graphique	5
Présentation du menu général	5
Présentation du menu contextuel	6
Établir une connexion sécurisée	7
Établir une connexion enregistrée	7
Établir une connexion sans enregistrer d'informations	8
Utiliser l'authentification unique pour établir une connexion	8
En cas d'erreur de connexion	9
Gérer les connexions enregistrées	11
Ajouter, modifier ou supprimer une connexion enregistrée	11
Ajouter une connexion	11
Modifier une connexion	13
Supprimer une connexion	14
Importer des connexions enregistrées	14
Exporter les connexions enregistrées	15
Protéger l'accès aux connexions enregistrées par un mot de passe	15
Protéger l'accès aux connexions enregistrées	15
Modifier le mot de passe d'accès	16
Supprimer la protection	16
En cas de perte du mot de passe d'accès	16
Gérer la liste des connexions favorites	17
Activer l'option de connexion automatique	17
Vérifier si l'option de connexion automatique est activée	18
Activer l'option de connexion automatique sur une connexion enregistrée	18
Consulter les journaux de connexion	19
Utiliser et configurer de manière avancée le client VPN SSL Stormshield	20
Consulter les journaux de débogage (paramètres avancés)	20
Activer les journaux de débogage	20
Accéder aux journaux de débogage	20
Configurer le client VPN SSL Stormshield via une interface en ligne de commande	21
Utiliser l'interface en ligne de commande	21
Liste des commandes	21
Pour aller plus loin	22
Annexe : récupérer le fichier de configuration VPN SSL (fichier OVPN)	23
Récupérer le fichier OVPN depuis le portail captif du firewall SNS	23
Récupérer le fichier OVPN depuis l'interface Web d'administration du firewall SNS	24



Historique des modifications

Date	Description
22 octobre 2025	- Des informations concernant l'authentification unique ont été ajoutées à la section "Établir une connexion sécurisée" - Des informations concernant le message "Risque probable de sécurité" ont été ajoutées à la section "Établir une connexion sécurisée" - Des informations concernant les champs d'une connexion ont été ajoutées à la section "Ajouter, modifier ou supprimer une connexion enregistrée" - Des informations concernant la perte du mot de passe d'accès ont été ajoutées à la section "Protéger l'accès aux connexions enregistrées par un mot de passe" - Des informations concernant l'utilisation de l'option de connexion automatique ont été ajoutées à la section "Activer l'option de connexion automatique" - Ajout d'une nouvelle section "Annexe : récupérer le fichier de configuration VPN SSL (fichier OVPN)" - Ajout d'une nouvelle section "Configurer le client VPN SSL Stormshield via une interface en ligne de commande" - Ajout d'un lien vers le guide d'administration du client VPN SSL Stormshield v5
29 juillet 2025	Nouveau document



Prendre en main le client VPN SSL Stormshield

Bienvenue dans le guide de configuration et d'utilisation de Stormshield Network SSL VPN Client version 5.1.

Dans ce guide, Stormshield Network SSL VPN Client est nommé "client VPN SSL Stormshield".

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

Ce guide présente :

- L'interface graphique et les menus du client VPN SSL Stormshield,
- L'utilisation du client VPN SSL Stormshield, notamment la manière d'établir une connexion sécurisée,
- La configuration du client VPN SSL Stormshield, notamment la gestion des connexions enregistrées.



Présentation de l'interface graphique et des menus du client VPN SSL Stormshield

Le client VPN SSL Stormshield dispose d'une interface graphique qui permet d'établir une connexion sécurisée et de configurer ses paramètres.

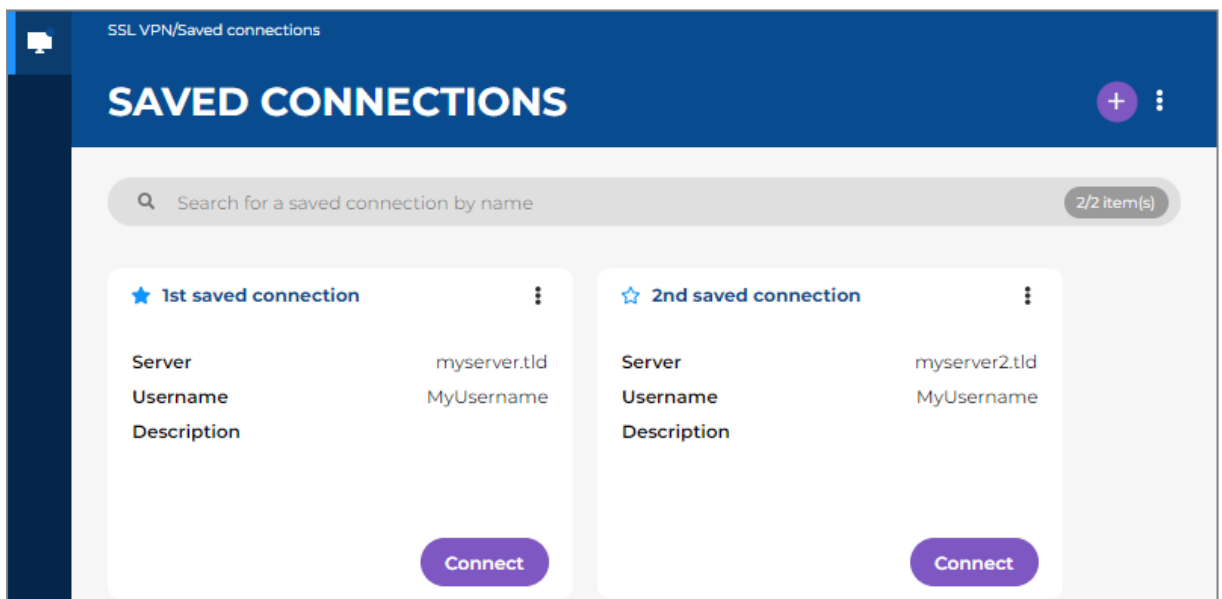
L'interface graphique est disponible en français et en anglais. La langue utilisée dépend de la langue choisie dans les paramètres de la session de l'utilisateur. Si la langue choisie n'est pas prise en charge, le client VPN SSL Stormshield utilise l'anglais par défaut.

Présentation de l'interface graphique

Pour ouvrir l'interface graphique :

- Sous Windows et certains environnements Linux : cliquez sur l'icône  du client VPN SSL Stormshield dans la barre d'état système.
- Sous macOS et certains environnements Linux : cliquez sur l'icône  du client VPN SSL Stormshield dans la barre d'état système, puis cliquez sur **Ouvrir**.

L'interface graphique se compose d'un menu général accessible en survolant l'icône  en forme d'écran et d'une fenêtre principale contenant les informations du menu sélectionné. La capture d'écran ci-dessous montre la fenêtre du menu **Connexions enregistrées**.



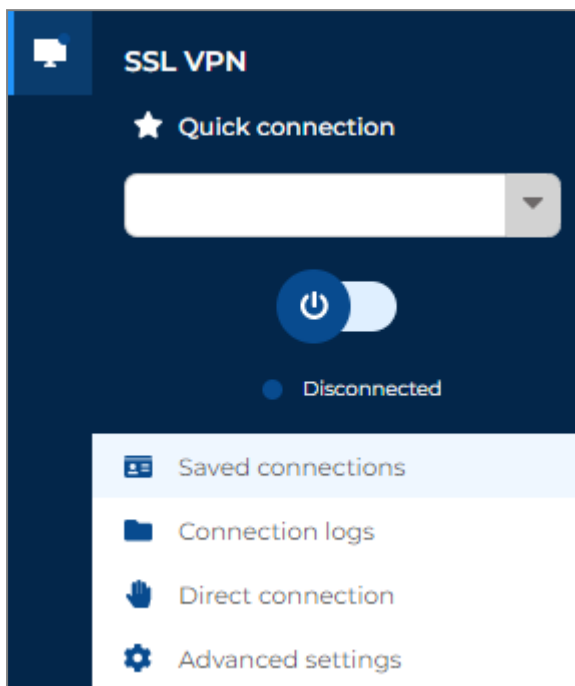
Présentation du menu général

Pour ouvrir le menu général, survolez l'icône  en forme d'écran à gauche. Depuis le menu général, vous pouvez accéder aux menus suivants :

- **Connexion rapide** : permet de sélectionner dans la liste déroulante la dernière connexion utilisée ou une connexion favorite, puis d'établir la connexion grâce au bouton de connexion . L'état actuel de la connexion établie est également affiché.
- **Connexions enregistrées** : permet d'enregistrer des connexions et d'établir une connexion enregistrée.



- **Journaux de connexion** : permet d'afficher les événements de connexion.
- **Connexion directe** : permet d'établir une connexion sans enregistrer d'informations.
- **Paramètres avancés** : permet d'accéder aux paramètres avancés.

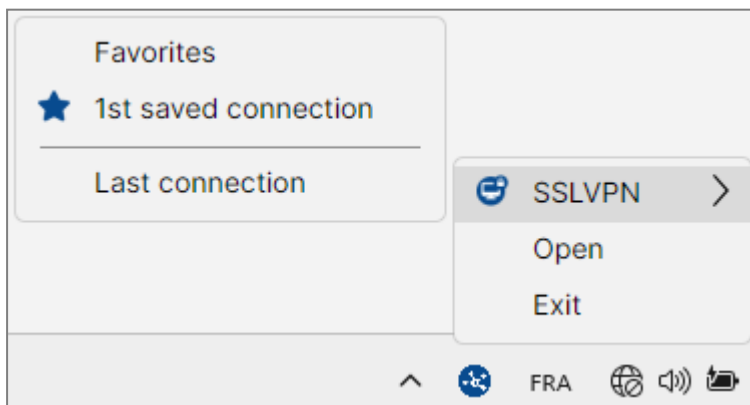


Présentation du menu contextuel

Pour ouvrir le menu contextuel, faites un clic droit sur l'icône  du client VPN SSL Stormshield dans la barre d'état système. Depuis le menu contextuel, vous pouvez accéder aux menus suivants :

- **VPNSSL** : permet d'établir la dernière connexion utilisée ou à une connexion favorite. Il est également possible de se déconnecter si une connexion est actuellement établie.
- **Ouvrir** : permet d'ouvrir l'interface graphique du client VPN SSL Stormshield.
- **Fermer** : permet de quitter l'application.

La capture d'écran ci-dessous montre le menu contextuel sous Windows. Le visuel peut être différent selon le système d'exploitation utilisé.





Établir une connexion sécurisée

i NOTE

Vous ne pouvez établir qu'une seule connexion à la fois.

Établir une connexion enregistrée

Pour établir une connexion enregistrée, les informations de la connexion concernée doivent avoir été enregistrées au préalable. Pour plus d'informations, reportez-vous à la section [Gérer les connexions enregistrées](#).

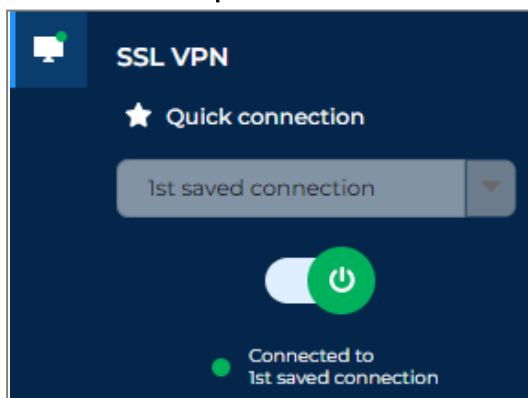
1. Vous pouvez établir une connexion enregistrée dans les menus suivants :
 - Dans le menu **Connexion rapide** : sélectionnez dans la liste déroulante une **connexion favorite** ou la dernière connexion utilisée et cliquez sur le bouton de connexion
 - Dans le menu **Connexions enregistrées** : dans le cadre de la connexion enregistrée à laquelle vous souhaitez vous connecter, cliquez sur **Se connecter**.
 - Dans le **Menu contextuel** de l'icône du client VPN SSL Stormshield : sélectionnez **VPNSSL** et cliquez sur une **connexion favorite** ou la dernière connexion utilisée.
2. Si des informations supplémentaires sont requises pour établir la connexion, comme un code OTP, saisissez-les. Si vous utilisez l'authentification unique, authentifiez-vous sur le portail qui s'ouvre automatiquement dans votre navigateur Web pour établir la connexion.

Une fois connecté, l'icône du client VPN SSL Stormshield et le bouton de connexion deviennent verts. En cas d'erreur, consultez la section [En cas d'erreur de connexion](#).

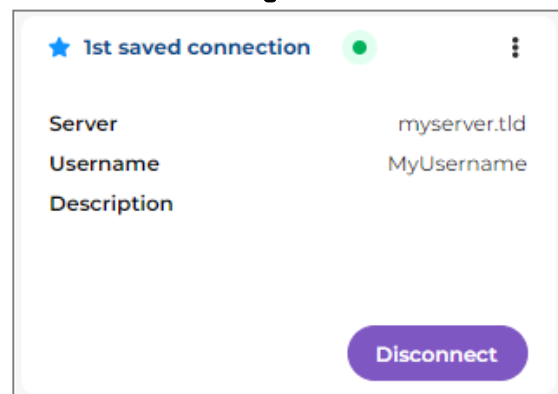
Si vous utilisez l'authentification unique, la date d'expiration de votre authentification s'affiche. Pour plus d'informations, reportez-vous à la section [Utiliser l'authentification unique pour établir une connexion](#).

Vous pouvez vous déconnecter en cliquant sur **Se déconnecter** ou sur le bouton de connexion.

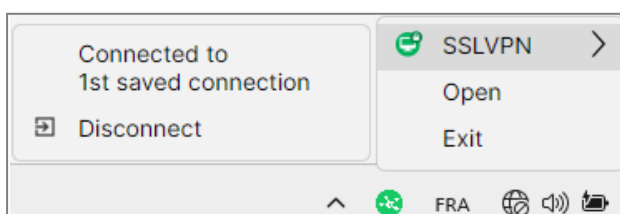
Menu **Connexion rapide**



Menu **Connexions enregistrées**



Menu **contextuel**





Établir une connexion sans enregistrer d'informations

1. Rendez-vous dans le menu **Connexion directe**.

SSL VPN/Direct connection

DIRECT CONNECTION

Stormshield mode Import OVPN file

General

Server * Port *

443

Authentication

☐ Connect with single sign-on

Username

Password

☐ Use an OTP

Connect

2. Choisissez parmi le **Mode Stormshield** ou **Import de fichier OVPN** et complétez les champs.

i NOTE

Si vous avez besoin d'aide pour choisir le mode ou pour compléter les champs, reportez-vous aux descriptions disponibles dans la section [Ajouter, modifier ou supprimer une connexion enregistrée](#). Les modes et les champs sont similaires dans les deux menus, sauf quelques exceptions mentionnées dans les descriptions.

3. Cliquez sur **Se connecter**.
4. Si vous utilisez l'authentification unique, authentifiez-vous sur le portail qui s'ouvre automatiquement dans votre navigateur Web pour établir la connexion.

Une fois connecté, l'icône  du client VPN SSL Stormshield et le bouton de connexion  deviennent verts. En cas d'erreur, consultez la section [En cas d'erreur de connexion](#).

Si vous utilisez l'authentification unique, la date d'expiration de votre authentification s'affiche. Pour plus d'informations, reportez-vous à la section [Utiliser l'authentification unique pour établir une connexion](#).

Vous pouvez vous déconnecter en cliquant sur **Se déconnecter** ou sur le bouton de connexion.

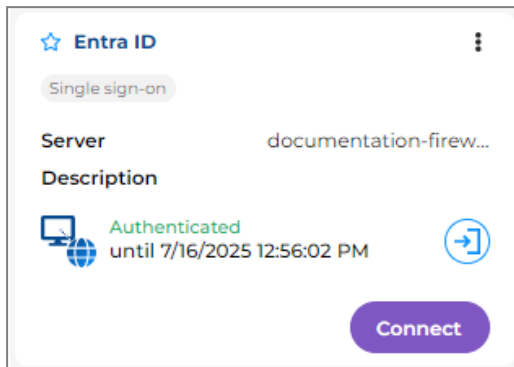
Utiliser l'authentification unique pour établir une connexion

Si vous utilisez l'authentification unique pour établir une connexion dans le menu **Connexions enregistrées** ou **Connexion directe**, la date d'expiration de votre authentification s'affiche dans l'interface graphique une fois la connexion établie.

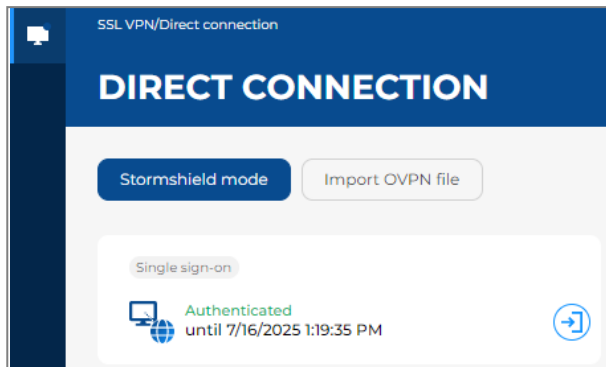
Tant que cette date n'est pas atteinte et que l'authentification est toujours effective sur le firewall SNS, vous n'avez pas besoin de vous authentifier de nouveau pour établir la connexion.



Menu Connexions enregistrées



Menu Connexion directe

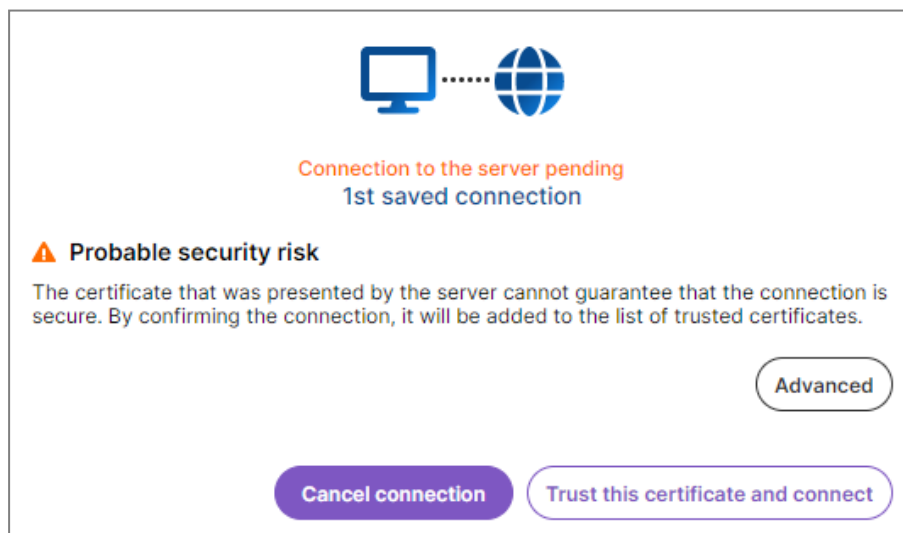


Sur demande d'un administrateur de votre organisation, vous pouvez annuler votre authentification avant qu'elle n'expire :

1. Cliquez sur le bouton  à droite de la date d'expiration de votre authentification.
2. Cliquez sur **Valider**. Cette action ne déconnecte pas une connexion actuellement établie.

En cas d'erreur de connexion

- Prenez connaissance du message d'erreur qui s'affiche. Si besoin, vous pouvez le retrouver dans le menu [Journaux de connexion](#).
- Vérifiez les informations de connexion qui ont été saisies, soit dans le menu [Connexion directe](#), soit dans les [informations de la connexion enregistrée](#). Si un code OTP a été utilisé, vérifiez sa validité. Le client VPN SSL Stormshield effectue plusieurs tentatives de connexion en cas de non réponse, le code OTP peut donc avoir expiré entre temps.
- Si le message "*Risque probable de sécurité*" s'affiche, c'est que le certificat présenté au client VPN SSL Stormshield ne peut pas être validé automatiquement. Vous devez alors indiquer si vous souhaitez faire confiance et vous connecter, ou annuler la connexion.



Pour cela, affichez les informations du certificat et de sa chaîne de certification en cliquant sur **Avancée...** > **Afficher le certificat** pour vérifier que la connexion est sûre. Si vous ne savez pas quoi décider, contactez un administrateur de votre organisation.

Si vous décidez de faire confiance et de vous connecter, cette décision est sauvegardée pour la connexion utilisée. Le message s'affichera de nouveau si vous utilisez une autre connexion enregistrée ou issue du menu **Connexion directe**.

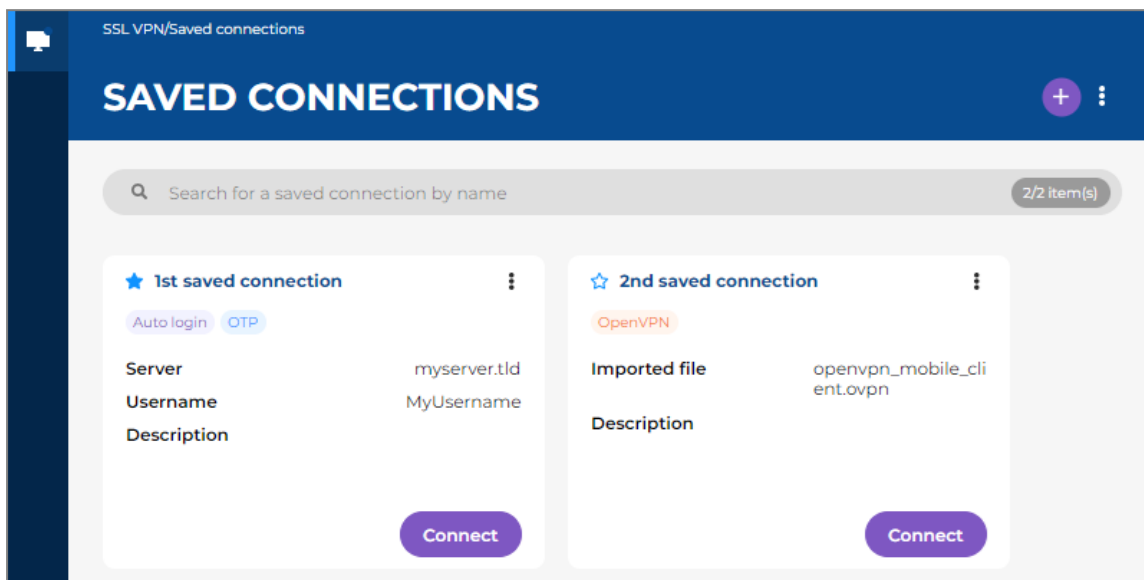


- Assurez-vous (ou un administrateur de votre organisation) que le client VPN SSL Stormshield puisse joindre le firewall SNS :
 - Vérifiez la configuration du service VPN SSL et des éléments associés en vous reportant au [Guide d'administration VPN SSL des firewalls SNS et des clients VPN SSL Stormshield](#).
 - Dans le cas où une configuration durcie est utilisée sur les postes de travail de l'organisation (utilisation d'un pare-feu par exemple), il est possible que le client VPN SSL Stormshield ne parvienne pas à se connecter si certains ports sont injoignables. Pour plus d'informations sur les ports et protocoles, reportez-vous au [Guide d'installation du client VPN SSL Stormshield v5](#).



Gérer les connexions enregistrées

Vous pouvez enregistrer des connexions et les gérer dans le menu **Connexions enregistrées**.



Dans la fenêtre, chaque cadre représente une connexion enregistrée. Vous y retrouvez notamment le nom de la connexion, son serveur, ainsi que des étiquettes.

Étiquette	Description
Code OTP	L'utilisation d'un code OTP est activée sur la connexion.
Connexion automatique	Une connexion automatique est activée sur la connexion.
Authentification unique	L'utilisation de l'authentification unique est activée sur la connexion.
OpenVPN	Connexion de type OpenVPN (import de fichier OVPN).

Ajouter, modifier ou supprimer une connexion enregistrée

Ajouter une connexion

1. Dans le menu **Connexions enregistrées**, cliquez sur le bouton  en haut à droite. Si aucune connexion enregistrée n'existe, vous pouvez également cliquer sur le bouton **Ajouter une connexion** au centre.
2. Choisissez parmi les deux modes proposés :

Mode	Description
Mode Stormshield	Ce mode permet au client VPN SSL Stormshield : • De récupérer automatiquement la configuration VPN SSL et de vérifier à chaque fois qu'il se connecte si elle doit être mise à jour. • De transmettre au firewall SNS les informations permettant de vérifier la conformité du poste client (ZTNA) à chaque fois qu'il se connecte.
Import de fichier OVPN	Ce mode permet d'importer un fichier de configuration OpenVPN (OVPN) fourni par le firewall SNS, et de se connecter à sa passerelle OpenVPN.



3. Complétez les champs selon le mode sélectionné.

Mode Stormshield

Champ / Case	Description
Nom	Nom de la connexion enregistrée. Ce champ ne s'affiche pas dans le menu Connexion directe .
Serveur	Adresse IPv4 ou FQDN du firewall SNS à joindre établir la connexion.
Port	Port du serveur (par défaut 443). Si le port du portail captif du firewall SNS n'est pas celui par défaut (TCP/443), renseignez le port utilisé ici.
Description	Description de la connexion enregistrée. Ce champ ne s'affiche pas dans le menu Connexion directe .
Se connecter avec l'authentification unique	Cochez la case pour utiliser l'authentification unique. Pour établir la connexion, vous devez alors vous authentifier sur un portail qui s'ouvre automatiquement dans votre navigateur Web. Pour plus d'informations, reportez-vous à la section Utiliser l'authentification unique pour établir une connexion. En cochant cette case, les champs Nom d'utilisateur, Mot de passe et Utiliser un code OTP sont masqués. ! IMPORTANT Vous devez disposer d'un firewall SNS en version 5 pour utiliser l'authentification unique. Vous ne pouvez pas établir de connexion si le firewall SNS utilise une version antérieure à la version 5.
Nom d'utilisateur	Nom d'utilisateur.
Mot de passe	Mot de passe de l'utilisateur. Si vous utilisez une authentification multifacteur via une application tierce (mode <i>Push</i>), laissez ce champ vide.
Utiliser un code OTP	Si vous utilisez une solution d'authentification multifacteur, comme la solution TOTP Stormshield, cochez la case. Pour établir la connexion, vous devez alors renseigner un code OTP (code à usage unique). Si vous utilisez une authentification multifacteur via une application tierce (mode <i>Push</i>), cochez la case mais laissez le champ Code OTP vide pour établir une connexion.
Se connecter automatiquement	Cochez la case pour établir automatiquement la connexion enregistrée au démarrage du client VPN SSL Stormshield. Cette option ne peut être activée que sur une seule connexion enregistrée. Elle ne s'affiche pas dans le menu Connexion directe. Une action manuelle reste toutefois requise pour établir la connexion dans certains cas (connexions enregistrées protégées par un mot de passe, code OTP ou mot de passe à renseigner). Pour plus d'informations, reportez-vous à la section Activer l'option de connexion automatique.



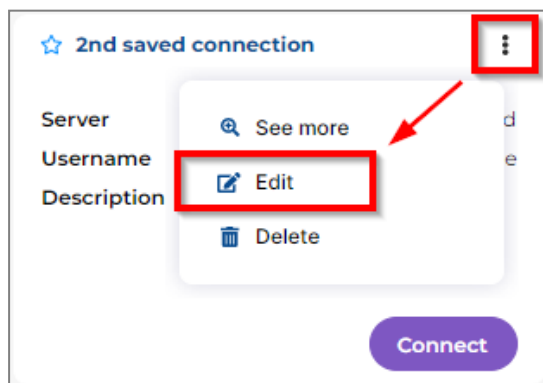
Import de fichier OVPN

Champ	Description
Glisser-déposer / Parcourir	Fichier OVPN que vous souhaitez importer. Pour récupérer le fichier OVPN, reportez-vous à la section Annexe : récupérer le fichier de configuration VPN SSL (fichier OVPN) .
Nom	Nom de la connexion enregistrée. Ce champ ne s'affiche pas dans le menu Connexion directe .
Description	Description de la connexion enregistrée. Ce champ ne s'affiche pas dans le menu Connexion directe .
Nom d'utilisateur	Nom d'utilisateur.
Mot de passe	Mot de passe de l'utilisateur. Si vous utilisez une authentification multifacteur via une application tierce (mode <i>Push</i>), laissez ce champ vide.
Utiliser un code OTP	Si vous utilisez une solution d'authentification multifacteur, comme la solution TOTP Stormshield, cochez la case. Pour établir la connexion, vous devez alors renseigner un code OTP (code à usage unique). Si vous utilisez une authentification multifacteur via une application tierce (mode <i>Push</i>), cochez la case mais laissez le champ Code OTP vide pour établir une connexion.
Se connecter automatiquement	Cochez la case pour établir automatiquement la connexion enregistrée au démarrage du client VPN SSL Stormshield. Cette option ne peut être activée que sur une seule connexion enregistrée. Elle ne s'affiche pas dans le menu Connexion directe . Une action manuelle reste toutefois requise pour établir la connexion dans certains cas (connexions enregistrées protégées par un mot de passe, code OTP ou mot de passe à renseigner). Pour plus d'informations, reportez-vous à la section Activer l'option de connexion automatique .

4. Cliquez sur **Ajouter**.

Modifier une connexion

1. Dans le menu **Connexions enregistrées**, dans le cadre de la connexion que vous souhaitez modifier, cliquez sur le bouton  et sur **Modifier**.

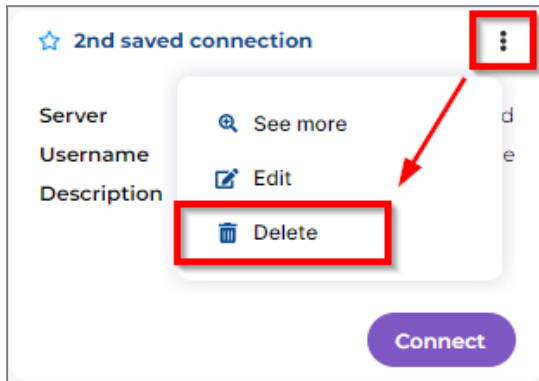


2. Modifiez les informations de la connexion. Si besoin, reportez-vous aux descriptions des champs ci-dessus.
3. Cliquez sur **Modifier** pour enregistrer les modifications.



Supprimer une connexion

1. Dans le menu **Connexions enregistrées**, dans le cadre de la connexion que vous souhaitez supprimer, cliquez sur le bouton  et sur **Supprimer**.



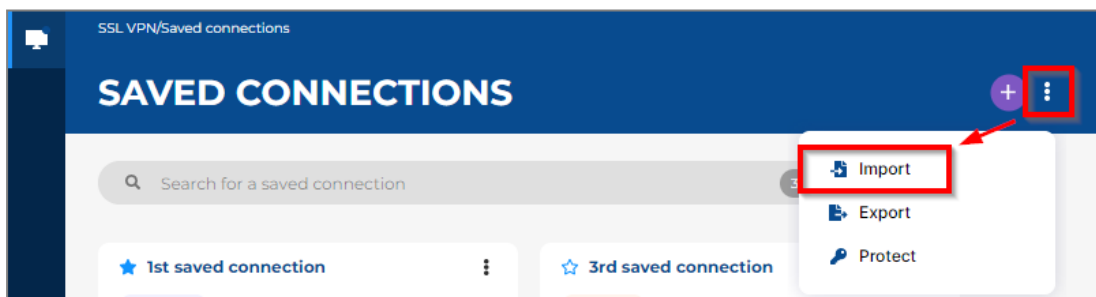
2. Cliquez sur **Supprimer** pour valider la suppression.

Importer des connexions enregistrées

! IMPORTANT

Cette action **écrase et remplace** les connexions enregistrées actuellement disponibles par celles contenues dans le fichier .book importé.

1. Dans le menu **Connexions enregistrées**, cliquez sur le bouton  en haut à droite, puis cliquez sur **Importer**.



2. Sélectionnez le fichier .book contenant les connexions enregistrées que vous souhaitez importer, puis cliquez sur **Ouvrir**.
3. Si le fichier .book est protégé par un mot de passe, renseignez-le dans la fenêtre qui s'affiche, puis cliquez sur **Importer**.

Si vous souhaitez protéger les connexions enregistrées importées, reportez-vous à la section [Protéger l'accès aux connexions enregistrées par un mot de passe](#).

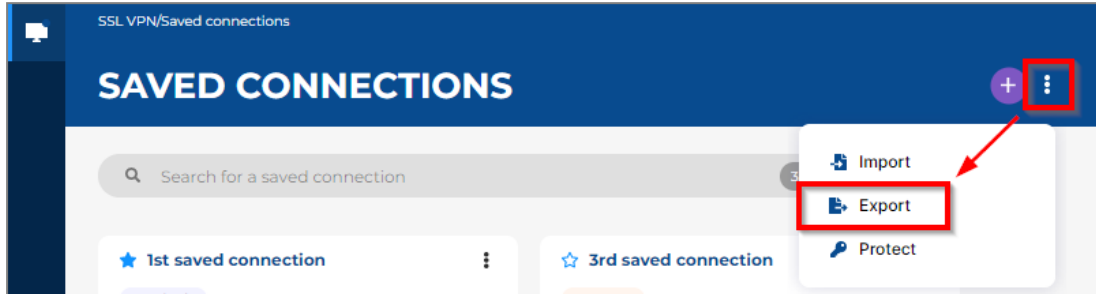
i NOTE

Vous pouvez également importer des connexions enregistrées via l'interface en ligne de commande du client VPN SSL Stormshield. Pour plus d'informations, reportez-vous à la section [Configurer le client VPN SSL Stormshield via une interface en ligne de commande](#).



Exporter les connexions enregistrées

1. Dans le menu **Connexions enregistrées**, cliquez sur le bouton ⓘ en haut à droite, puis cliquez sur **Exporter**.



2. Sélectionnez l'emplacement où enregistrer le fichier .book contenant les connexions enregistrées exportées, définissez-lui un nom, puis cliquez sur **Enregistrer**.
3. Si vous souhaitez protéger avec un mot de passe le fichier .book, définissez un mot de passe dans la fenêtre qui s'affiche. Laissez le champ vide pour ne pas protéger le fichier. Ce mot de passe doit être saisi lors de l'import du fichier.
4. Cliquez sur **Exporter** pour effectuer l'export.

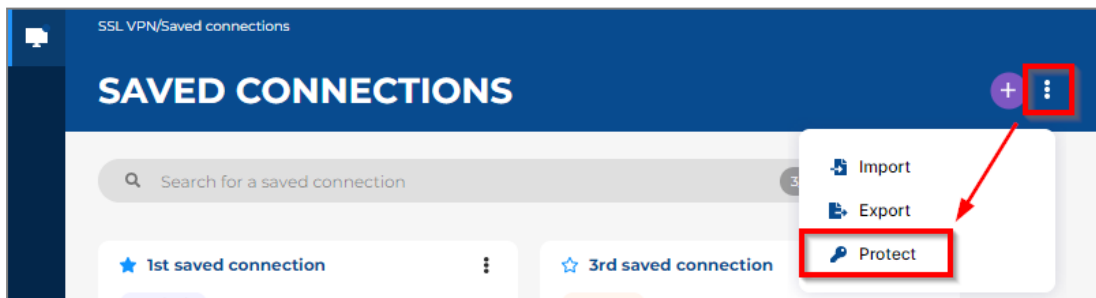
Protéger l'accès aux connexions enregistrées par un mot de passe

Protéger l'accès aux connexions enregistrées

NOTE

Si vous protégez l'accès aux connexions enregistrées par un mot de passe et que l'**option de connexion automatique** est activée sur une connexion, vous devez saisir ce mot de passe à chaque ouverture du client VPN SSL Stormshield pour établir la connexion automatique.

1. Dans le menu **Connexions enregistrées**, cliquez sur le bouton ⓘ en haut à droite, puis cliquez sur **Protéger**.

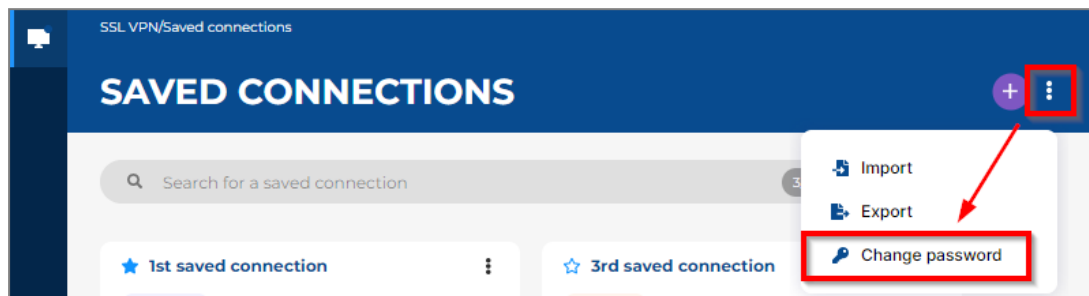


2. Activez le paramètre **Activer la protection par mot de passe** ☒.
3. Définissez le mot de passe d'accès, et confirmez-le. Conservez ce mot de passe dans un espace sécurisé et sauvegardé. En cas de perte, Stormshield n'est pas en mesure de le retrouver. Pour plus d'informations, reportez-vous à la section **En cas de perte du mot de passe d'accès**.
4. Cliquez sur **Modifier le mot de passe**.



Modifier le mot de passe d'accès

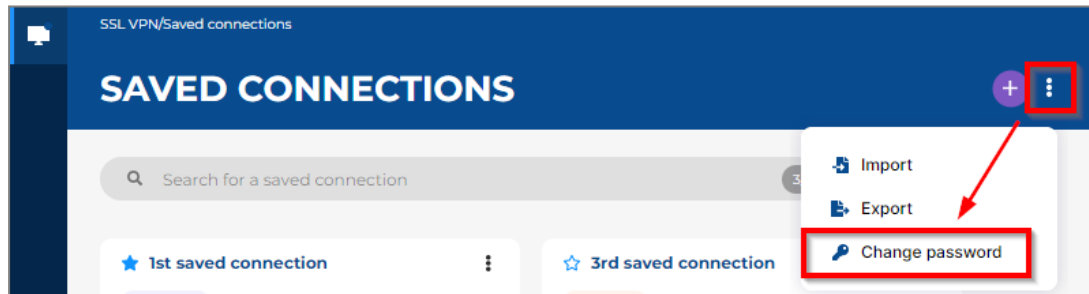
1. Dans le menu **Connexions enregistrées**, cliquez sur le bouton ⓘ en haut à droite, puis cliquez sur **Modifier le mot de passe**.



2. Renseignez le mot de passe d'accès actuel.
3. Définissez le nouveau mot de passe d'accès, et confirmez-le. Conservez ce mot de passe dans un espace sécurisé et sauvegardé. En cas de perte, Stormshield n'est pas en mesure de le retrouver. Pour plus d'informations, reportez-vous à la section [En cas de perte du mot de passe d'accès](#).
4. Cliquez sur **Modifier le mot de passe**.

Supprimer la protection

1. Dans le menu **Connexions enregistrées**, cliquez sur le bouton ⓘ en haut à droite, puis cliquez sur **Modifier le mot de passe**.



2. Désactivez le paramètre **Activer la protection par mot de passe** ☐.
3. Renseignez le mot de passe d'accès.
4. Cliquez sur **Désactiver la protection**.

En cas de perte du mot de passe d'accès

Il n'est pas possible de réinitialiser le mot de passe d'accès, et Stormshield n'est pas en mesure de le retrouver. En dernier recours, vous devez supprimer le dossier contenant le fichier des connexions enregistrées. Ces dernières seront alors perdues définitivement.

Pour accéder à ce dossier et le supprimer, vous devez disposer des droits nécessaires sur le poste de travail. Si vous avez besoin d'aide pour réaliser cette manipulation ou si vous ne disposez pas des droits nécessaires, contactez un administrateur de votre organisation.

Ce dossier se trouve à l'emplacement suivant :

- Sous Windows :
C:\ProgramData\Stormshield\SSL VPN Client\Addressbooks\



- Sous Linux :

```
/var/lib/stormshield/sslvpnclient/addressbooks/
```

- Sous macOS :

```
/Library/Application Support/Stormshield/SSL VPN Client/Addressbooks/
```

Il peut contenir plusieurs sous-dossiers. Si un seul sous-dossier est présent, cela signifie qu'un seul utilisateur du poste de travail a ajouté des connexions enregistrées. Si plusieurs sous-dossiers existent, vous devez identifier le sous-dossier de l'utilisateur concerné :

- Sous Linux et macOS, le nom de chaque sous-dossier correspond à l'identifiant des utilisateurs du poste de travail.
- Sous Windows, le nom de chaque sous-dossier correspond à un identifiant interne Windows qui ne contient pas d'informations permettant d'identifier l'utilisateur. Vous pouvez vous aider des dates de dernière modification pour trouver l'utilisateur concerné.

Une fois prêt, quittez le client VPN SSL Stormshield, supprimez le sous-dossier, puis démarrez le client VPN SSL Stormshield. L'utilisateur peut ensuite de nouveau [ajouter des connexions enregistrées](#), ou en [importer](#).

Gérer la liste des connexions favorites

Dans le menu **Connexions enregistrées**, chaque connexion enregistrée possède à gauche de son nom une icône en forme d'étoile.

Icône	Description
☆	La connexion n'est pas dans la liste des connexions favorites.
★	La connexion est dans la liste des connexions favorites.

Cliquez sur l'icône pour ajouter ou retirer la connexion de la liste des connexions favorites.

The screenshot displays two saved VPN connections in the Stormshield client. Each connection card features a star icon in the top left corner, which is highlighted with a red box. The first connection, '1st saved connection', has a blue star and includes 'Auto login' and 'OTP' toggle buttons. Below these are fields for 'Server' (myserver.tld), 'Username' (MyUsername), and 'Description'. The second connection, '2nd saved connection', also has a blue star and includes an 'OpenVPN' toggle button. Below this are fields for 'Imported file' (openvpn_mobile_client.ovpn) and 'Description'. Both cards have a purple 'Connect' button at the bottom right.

Vous pouvez également retrouver la liste des connexions favorites dans le menu **Connexion rapide** et le **menu contextuel** de l'icône  du client VPN SSL Stormshield.

Activer l'option de connexion automatique

Vous pouvez activer l'option de connexion automatique sur une connexion enregistrée. Ceci permet d'établir automatiquement la connexion au démarrage du client VPN SSL Stormshield.

Cette option ne peut être activée que sur une seule connexion enregistrée.

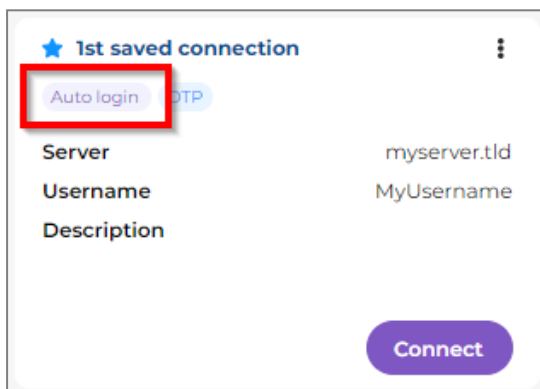
**NOTE**

Une action manuelle reste toutefois requise pour établir la connexion dans les cas suivants :

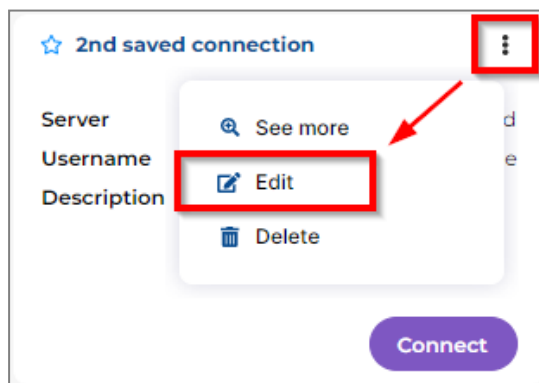
- Si l'**accès aux connexions enregistrées est protégé**, vous devez saisir le mot de passe d'accès à chaque ouverture du client VPN SSL Stormshield pour déverrouiller l'accès aux connexions enregistrées et établir la connexion automatique.
- Si vous devez renseigner des informations supplémentaires pour établir la connexion, comme un code OTP ou le mot de passe de l'utilisateur.

Vérifier si l'option de connexion automatique est activée

Dans le menu **Connexions enregistrées**, une étiquette "*Connexion automatique*" s'affiche dans le cadre d'une connexion enregistrée si l'option **Se connecter automatiquement** est activée.

**Activer l'option de connexion automatique sur une connexion enregistrée**

1. Dans le menu **Connexions enregistrées**, dans le cadre de la connexion que vous souhaitez modifier, cliquez sur le bouton **⋮** et sur **Modifier**.

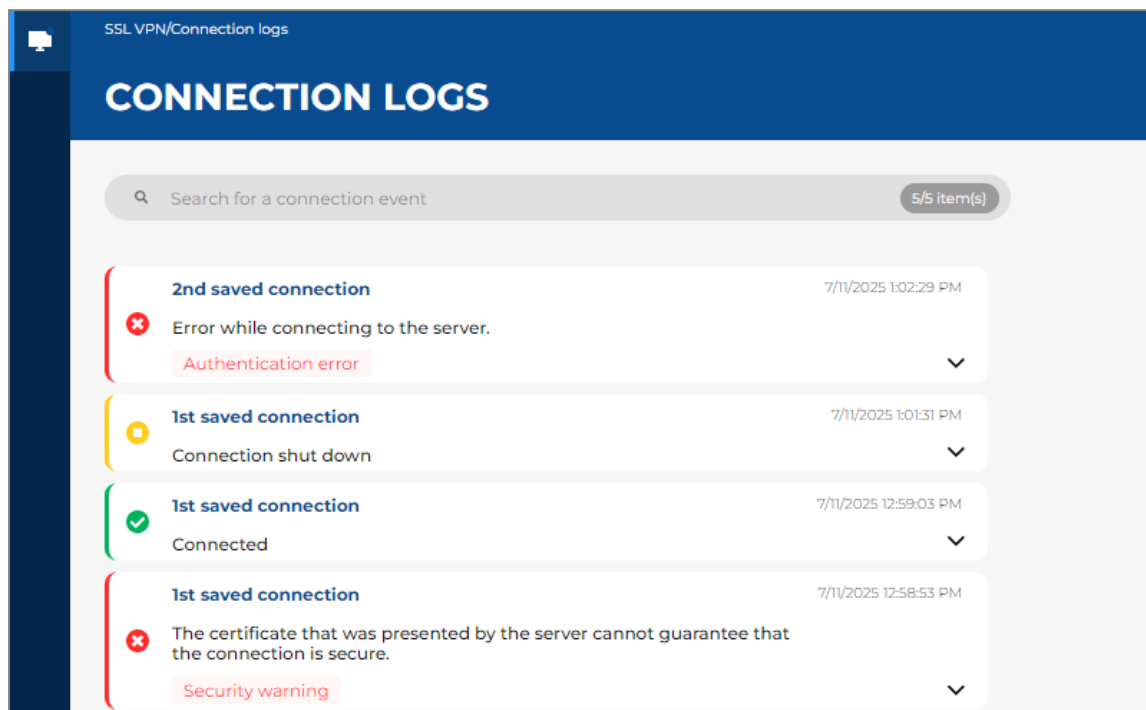


2. Cochez la case **Se connecter automatiquement**.
3. Cliquez sur **Modifier** pour enregistrer la modification.
4. Si l'option de connexion automatique est déjà activée sur une autre connexion enregistrée, vous devez indiquer si vous souhaitez la remplacer par celle en cours de modification. Cliquez sur **Remplacer** pour valider la modification.



Consulter les journaux de connexion

Vous pouvez consulter les événements de connexion du client VPN SSL Stormshield dans le menu **Journaux de connexion**.



Vous retrouvez notamment les événements suivants :

Événement	Description
Connexion établie	La connexion VPN SSL a été correctement établie.
Connexion fermée	La connexion VPN SSL a été fermée, l'utilisateur s'est déconnecté.
Connexion perdue	La connexion VPN SSL avec le serveur a été perdue.
Serveur injoignable	Le client VPN SSL Stormshield n'a pas réussi à joindre le serveur pour établir la connexion.
Avertissement de sécurité	Le certificat présenté par le serveur n'a pas permis de confirmer que la connexion était sûre (risque probable de sécurité). Pour plus d'informations, reportez-vous à la section En cas d'erreur de connexion .
Erreur d'authentification	Le nom d'utilisateur et le mot de passe saisis ne permettent pas d'authentifier l'utilisateur. D'autres raisons peuvent également expliquer la présence de ce message.

Vous pouvez rechercher un événement en saisissant dans le champ de recherche soit le nom de la connexion enregistrée, soit l'adresse du serveur.



Utiliser et configurer de manière avancée le client VPN SSL Stormshield

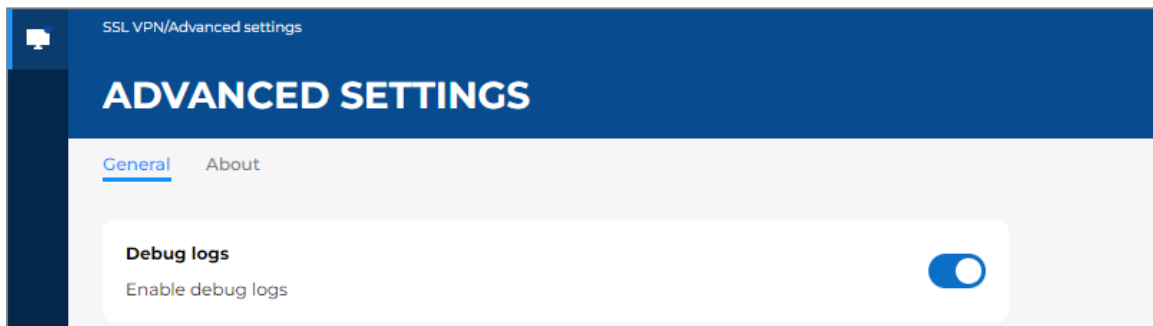
Cette section présente certains cas avancés d'utilisation et de configuration du client VPN SSL Stormshield.

Consulter les journaux de débogage (paramètres avancés)

Un administrateur de votre organisation est susceptible de vous demander d'activer les journaux de débogage. Vous pouvez effectuer cette opération dans le menu **Paramètres avancés**.

Activer les journaux de débogage

Dans le menu **Paramètres avancés**, onglet **Général**, activez le paramètre **Activer les journaux de débogage**.



Accéder aux journaux de débogage

Ces journaux se trouvent aux emplacements suivants. Pour accéder aux journaux du service, vous devez disposer des droits nécessaires sur le poste de travail.

- Sous Windows :
 - Journaux du service :
C:\ProgramData\Stormshield\SSL VPN Client\Logs\
 - Journaux de l'utilisateur :
C:\Users\<user>\AppData\Local\Stormshield\SSL VPN Client\Logs\
- Sous Linux :
 - Journaux du service :
/var/log/stormshield/sslvpnclient/
 - Journaux de l'utilisateur :
\$HOME/.local/share/stormshield/sslvpnclient/logs/
- Sous macOS :
 - Journaux du service :
/Library/Application Support/Stormshield/SSL VPN Client/Logs/
 - Journaux de l'utilisateur :
/Users/<user>/Library/Application Support/Stormshield/SSL VPN Client/Logs/



Configurer le client VPN SSL Stormshield via une interface en ligne de commande

Cette section explique comment configurer le client VPN SSL Stormshield via une interface en ligne de commande.

Utiliser l'interface en ligne de commande

L'exécution des commandes se fait en local sur le poste de travail.

- Sous Windows dans l'invite de commandes :

```
sslvpn-cli.exe [command] [options]
```

- Sous Linux et macOS dans un terminal :

```
sslvpn-cli [command] [options]
```

Si la commande n'est pas détectée par défaut, vous pouvez retrouver le programme à l'emplacement suivant :

- Sous Windows :

```
C:\Program Files\Stormshield\SSL VPN Client\Modules\ssl-vpn\Services\sslvpn-cli.exe
```

- Sous Linux :

```
/usr/bin/sslvpn-cli
```

- Sous macOS :

```
/Applications/Stormshield/SSL VPN Client.app/Contents/MacOS/Modules/ssl-vpn/sslvpn-cli
```

Liste des commandes

import-addressbook

Historique

Ajoutée en version 5.1.2

Description

Importer un fichier .book contenant des connexions enregistrées. Le fichier ne doit pas être protégé par un mot de passe.

Utilisation

- Windows :

```
sslvpn-cli.exe import-addressbook --file <path/file.book>
```

- Linux :

```
sslvpn-cli import-addressbook --file <path/file.book>
```

- macOS :

```
sslvpn-cli import-addressbook --file <path/file.book>
```

Remplacez *<path/file.book>* par le chemin d'accès complet au fichier.



Pour aller plus loin

Pour plus d'informations sur l'installation, la mise à jour et la désinstallation du client VPN SSL Stormshield, reportez-vous au [Guide d'installation du client VPN SSL Stormshield v5](#).

Pour configurer le service VPN SSL du firewall SNS et superviser les utilisateurs connectés, reportez-vous au [Guide d'administration VPN SSL des firewalls SNS et des clients VPN SSL Stormshield](#).

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



Annexe : récupérer le fichier de configuration VPN SSL (fichier OVPN)

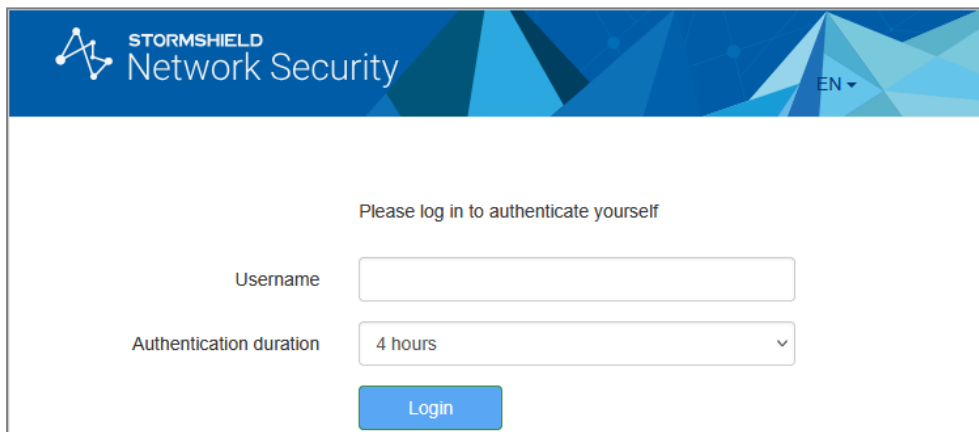
Cette annexe présente comment récupérer le fichier de configuration VPN SSL (fichier OVPN).

Vous devez disposer de ce fichier si vous ajoutez une connexion via l'import d'un fichier OVPN. Un administrateur de votre organisation peut vous demander de récupérer ce fichier OVPN.

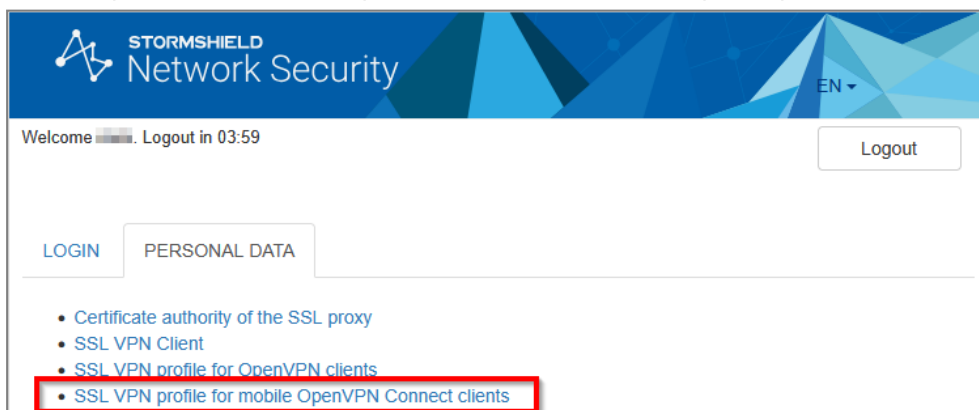
Récupérer le fichier OVPN depuis le portail captif du firewall SNS

1. Assurez-vous d'être connecté au réseau de votre organisation.
2. Ouvrez un navigateur Web et accédez à l'adresse du portail captif du firewall SNS.
Un administrateur de votre organisation doit vous avoir communiqué cette adresse. Elle ressemble généralement à : *mycompany.tld/auth* ou *passerelle.mycompany.tld/auth*.

L'image ci-dessous montre la page de connexion par défaut du portail captif. Notez que cette page peut être personnalisée pour correspondre à votre organisation.



3. Sur la page de connexion, authentifiez-vous en renseignant les informations demandées.
4. Une fois authentifié, rendez-vous dans l'onglet **Données personnelles**, et cliquez sur **Profil VPN SSL pour clients mobile OpenVPN Connect (fichier unique .ovpn)**.



5. Acceptez le téléchargement du fichier OVPN.

Si vous ne parvenez pas à télécharger le fichier OVPN, contactez un administrateur de votre organisation.



Récupérer le fichier OVPN depuis l'interface Web d'administration du firewall SNS

Un administrateur du firewall SNS peut récupérer le fichier OVPN depuis l'interface Web d'administration du firewall SNS. Pour plus d'informations, 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*.



STORMSHIELD

documentation@stormshield.eu

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.