SOPHOS

Cybersecurity made simple.

Sophos Connect

Aide

Table des matières

1 À propos de Sophos Connect

Sophos Connect est un client VPN pour Windows et Mac. Il vous permet de vous connecter à distance aux réseaux derrière le pare-feu XG, par exemple le réseau de votre entreprise. Votre administrateur de pare-feu configurera les informations de connexion sur Sophos XG Firewall et vous enverra le package d'installation et les fichiers de configuration de la connexion.

Ce guide vous fournit tous les renseignements utiles sur l'utilisation de Sophos Connect :

- Retrouvez plus de renseignements sur l'installation et la désinstallation de Sophos Connect à la section Installation de Sophos Connect (page 1).
- Retrouvez plus de renseignements sur l'importation des fichiers de connexion et sur la gestion des connexions à la section Connexions (page 2).
- Retrouvez plus de renseignements sur les événements et sur la manière de résoudre les erreurs à la section Événements (page 11).
- Pour résoudre les problèmes qui n'apparaissent pas sous la section Événements, consultez la section Dépannage général (page 18).

1.1 Installation de Sophos Connect

Installer Sophos Connect sur Windows

- Ouvrez le programme d'installation.
- Acceptez le contrat de licence et cliquez sur **Installer**.
- Une fois l'installation terminée, cliquez sur **Terminer**. Il est possible de lancer Sophos Connect après avoir fermé le programme.

Installer Sophos Connect sur Mac

- Ouvrez le programme d'installation.
- Choisissez la destination de l'installation. Assurez-vous d'avoir assez d'espace libre dans le dossier de destination choisi, par exemple, Lecteur système.
- Cliquez sur **Installer**.
- Une fois l'installation terminée, cliquez sur **Terminer**.

1.2 Désinstallation de Sophos Connect

Désinstaller Sophos Connect de Windows

- Dans le **Panneau de configuration** sous **Programmes**, cliquez sur **Désinstaller un programme**.
- Cliquez sur Sophos Connect avec le bouton droit de la souris et sélectionnez **Désinstaller**.

Désinstaller Sophos Connect de Mac

- Ouvrez l'ordinateur.
- Accédez à « root » et exécutez le script de désinstallation depuis l'emplacement dans lequel Sophos Connect est installé :

  ```
  sudo /Library/Sophos Connect/uninstall.sh
  ```

Vous allez recevoir le message suivant si la désinstallation s'est déroulée avec succès :

```
Sophos Connect a été désinstallé
```

1.3 Connexions

Vous pouvez importer, établir, afficher et modifier des connexions.

Sophos Connect prend en charge SSL VPN SSL et IPsec VPN.

1.3.1 Importer les connexions

Le client Sophos Connect peut se connecter à XG Firewall à l'aide de connexions SSL VPN ou IPsec VPN. Vous pouvez importer des connexions dans le client Sophos Connect.

Introduction

Pour la version 2.0 du client Sophos Connect, vous pouvez importer des connexions SSL VPN et IPsec VPN. Si vous utilisez une version antérieure du client Sophos Connect, seules les connexions IPsec peuvent être importées.

Cette page indique la marche à suivre pour :

- Importer une connexion IPsec à l'aide d'un fichier fourni par votre administrateur.
- Importer une connexion SSL à l'aide d'un fichier fourni par votre administrateur.
- Importer une connexion SSL en téléchargeant un fichier à partir du portail utilisateur.

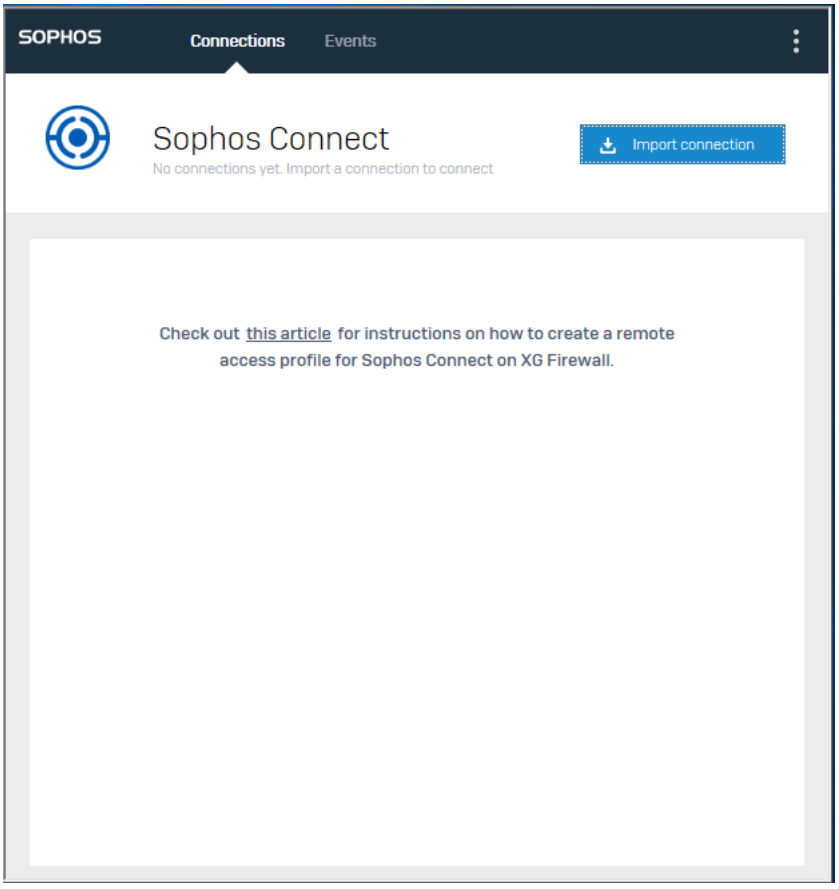
Importer une connexion IPsec

Un fichier de connexion vous a été fourni. Ce fichier a une extension `tgb`, par exemple `Connexion_entreprise.tgb`.

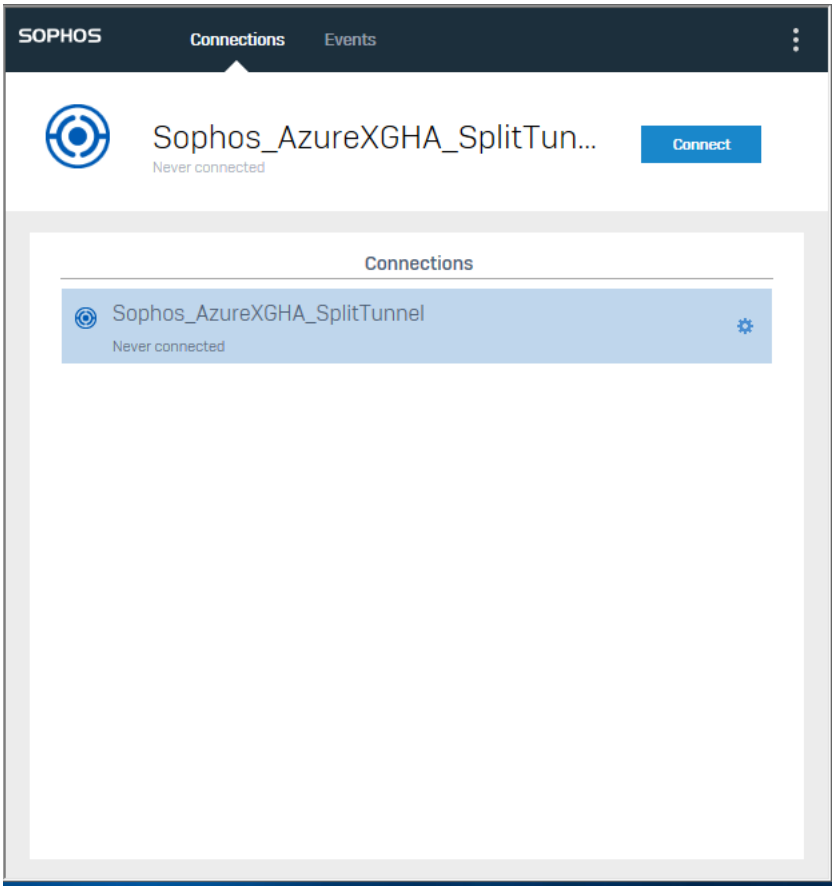
Pour importer une connexion :

1. Cliquez sur **Importer la connexion** sur la page **Connexions**.

   Si des connexions existent, cliquez sur le bouton menu et sélectionnez **Importer la connexion** dans le menu déroulant.



2. Naviguez jusqu'au fichier `tgb` et double-cliquez dessus.
   La connexion s'affiche sous **Connexions**.



Vous pouvez à présent établir la connexion.

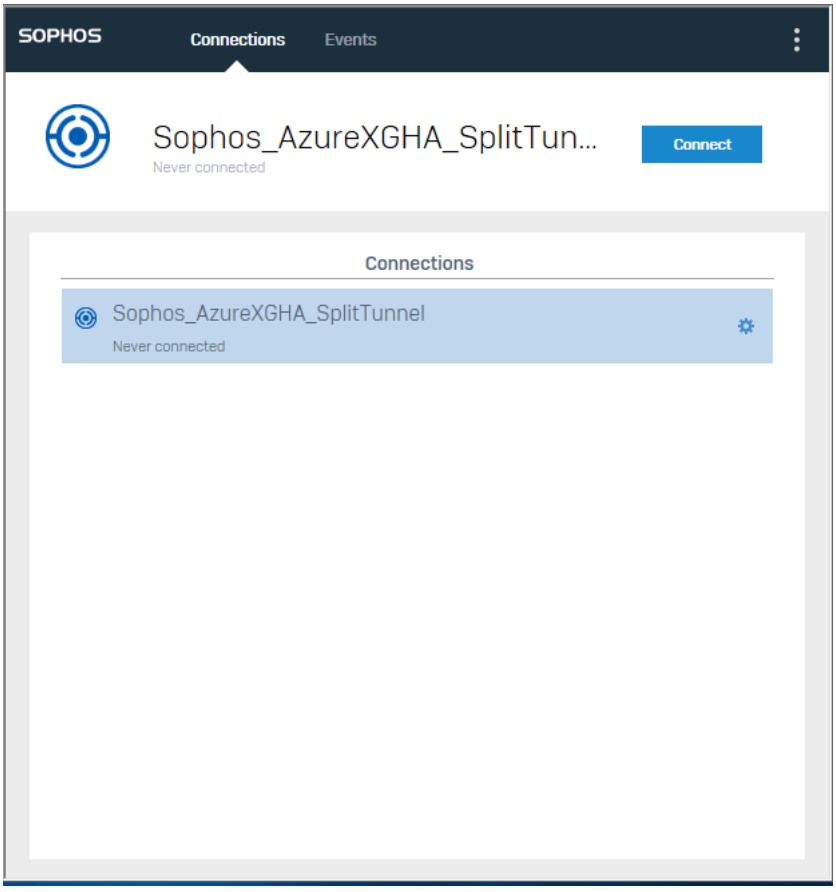
Remarque
Vous pouvez importer plusieurs connexions.

Importer une connexion SSL

Un fichier de connexion vous a été fourni. Ce fichier a une extension `pro`, par exemple `Connexion_entreprise.pro`.

Pour importer une connexion :

Recherchez le fichier `.pro` et double-cliquez dessus.
La connexion est importée automatiquement et Sophos Connect s'ouvre. La connexion s'affiche sous **Connexions**.



Vous pouvez à présent établir la connexion.

Remarque
Vous pouvez importer plusieurs connexions.

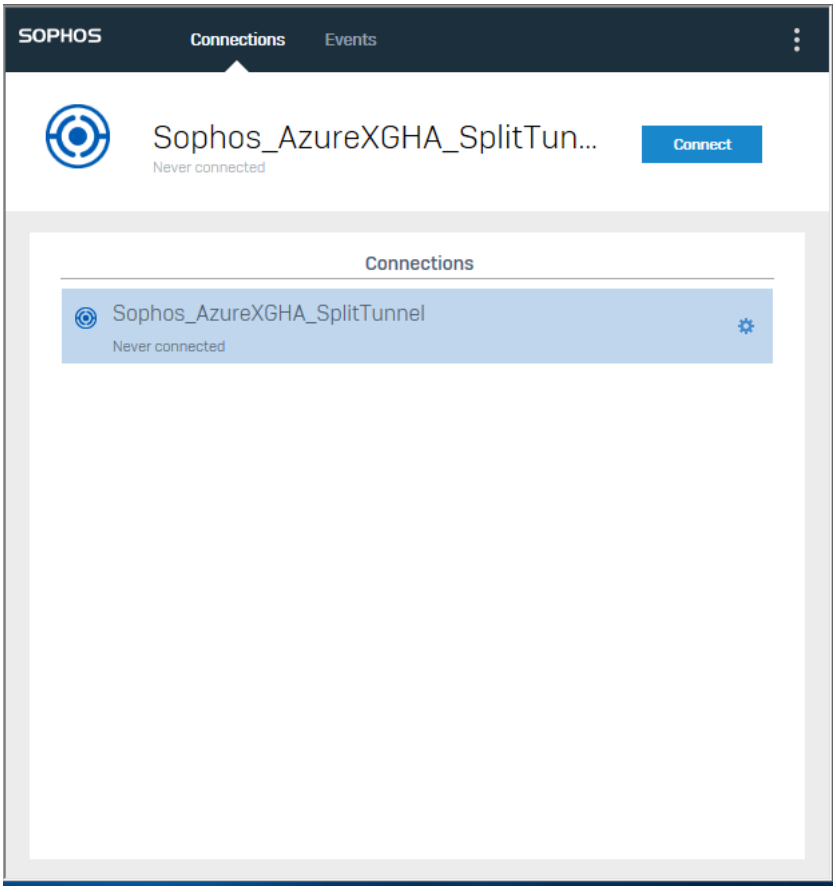
Importer une connexion SSL à partir du portail utilisateur

Pour importer une connexion :

1. Connectez-vous au portail utilisateur.
2. Accédez à **SSLVPN** et cliquez sur **Télécharger la configuration pour les autres systèmes d'exploitation**.
3. Ouvrez le client Sophos Connect.
4. Cliquez sur **Importer la connexion** sur la page **Connexions**.

   Si des connexions existent, cliquez sur le bouton menu et sélectionnez **Importer la connexion** dans le menu déroulant.
5. Naviguez jusqu'au fichier `.ovpn` et ouvrez-le.

La connexion s'affiche sous **Connexions**.



Vous pouvez à présent établir la connexion.

Remarque
Vous pouvez importer plusieurs connexions.

1.3.2 Connecter

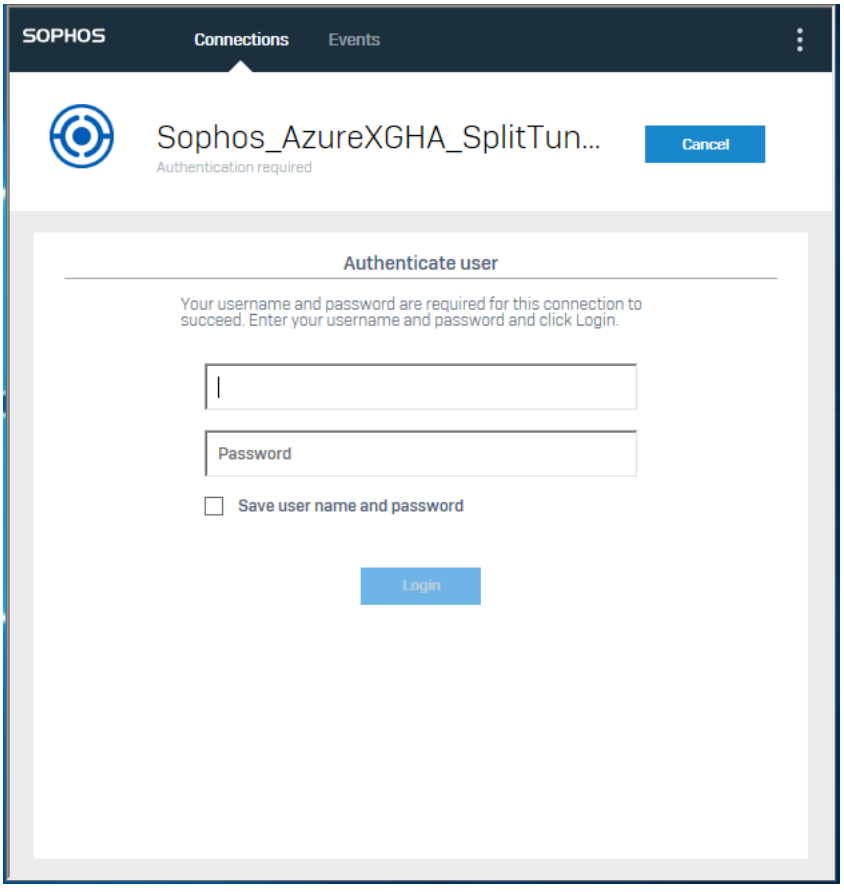
Assurez-vous qu'il y ait au moins une connexion importée disponible et que vous disposez des codes d'accès nécessaires à la connexion.

Pour établir une connexion :

1. Sélectionnez une connexion sur la page **Connexions**.
2. Cliquez deux fois sur la connexion.

   Vous pouvez également cliquer sur **Connecter**.

   L'écran de connexion apparaît.

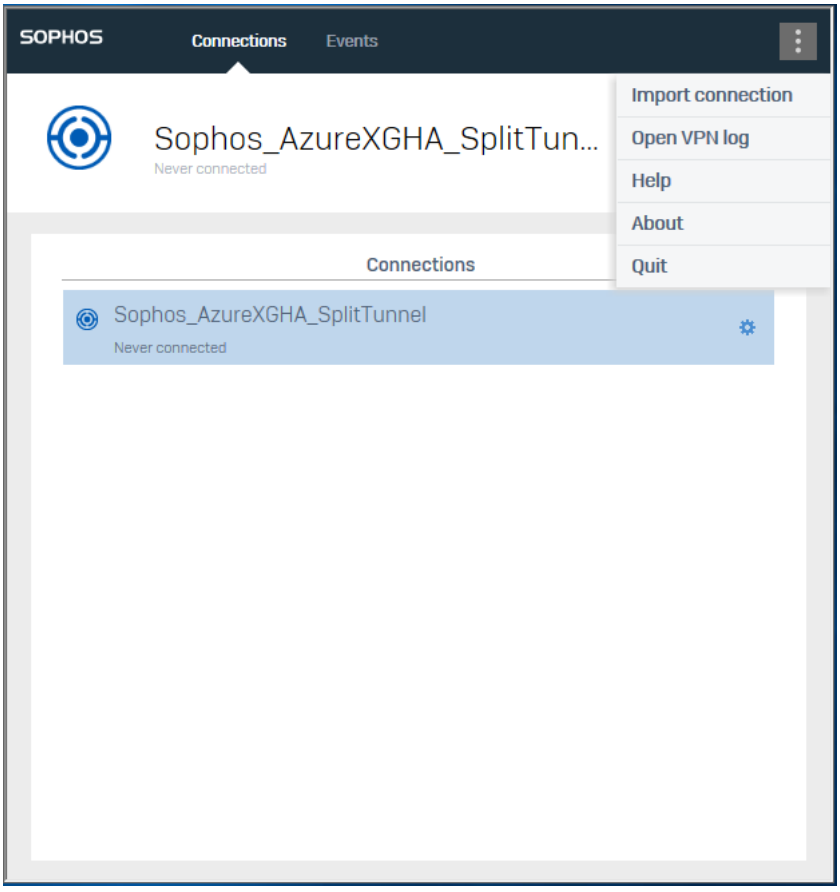


3. Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Connexion**.
   Votre administrateur a peut-être configuré l'authentification à deux facteurs.
   - Si votre administrateur a configuré OTP, vous devez saisir votre mot de passe OTP à 6 chiffres en plus de votre nom d'utilisateur et votre mot de passe.
   - Si votre administrateur a configuré l'authentification DUO, vous recevrez peut-être une ou deux invites DUO pendant le processus de connexion.

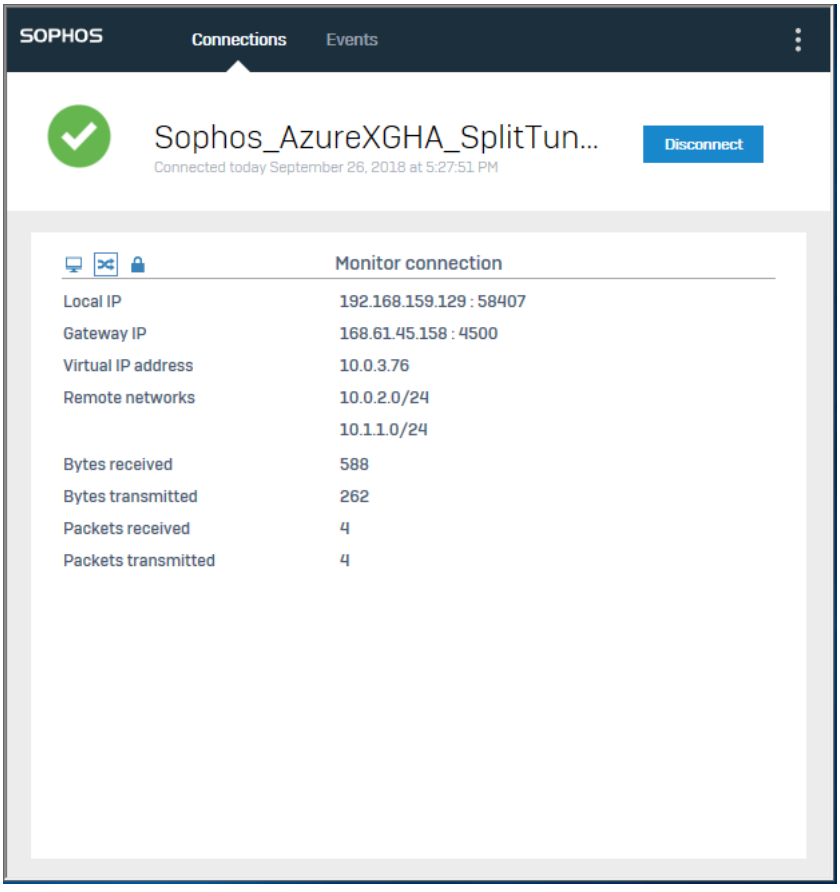
   Remarque
   Si vous avez importé la connexion à l'aide d'un fichier d'approvisionnement, vous recevrez un avertissement indiquant que le certificat du serveur ne peut pas être vérifié. Vous pouvez cliquer sur **OK** pour continuer. Si vous ne souhaitez pas voir le message, contactez votre administrateur.

   Sophos Connect tente d'établir la connexion et de vous authentifier.

   Remarque
   Si vous rencontrez des problèmes de connexion, consultez la page **Événements** et contacter votre service informatique. Vous pouvez également vérifier les journaux VPN en cliquant sur l'icône de menu et en les sélectionnant.



La connexion au serveur distant est établie.



Si la connexion réussie, vous verrez l'icône suivante apparaître sur la barre des tâches :

Si la connexion échoue, vous verrez l'icône suivante apparaître sur la barre des tâches :

Remarque
Si vous avez renommé la connexion, le nom d'origine que vous a donné votre administrateur pare-feu continuera à apparaître dans les informations sur la connexion. Retrouvez plus de renseignements sur la manière de renommer une connexion à la section Options de connexion (page 10).

1.3.3 Options de connexion

Vous pouvez apporter de nombreuses modifications aux connexions dans Sophos Connect en cliquant sur l'icône des paramètres à droite de la connexion.

1. **Auto-connecter** tente d'établir une connexion au démarrage de Sophos Connect.
2. **Supprimer** supprime la connexion. Il faudra donc l'importer de nouveau si vous souhaitez la réactiver.
3. **Renommer** vous donne la possibilité de renommer la connexion.
4. **Effacer les codes d'accès** efface les codes d'accès que vous avez stockés auparavant.

5. **Mettre à jour la stratégie** (disponible uniquement si la connexion a été créée à l'aide d'un fichier d'approvisionnement). Cela vous permet de récupérer la stratégie la plus récente de XG Firewall à la demande.

Conseil
Si la connexion échoue après plusieurs tentatives, lancez une mise à jour de stratégie et retentez la connexion.

1.4 Événements

Cette page permet de voir toutes les actions de Sophos Connect et les résultats de ces actions. Ceci inclut notamment les échecs des actions prises par l'utilisateur ainsi que les échecs de négociations IKE. Retrouvez plus de renseignements sur la manière de résoudre ces erreurs à la section Dépannage des évènements (page 12)

- Si vous voulez plus d'informations sur les erreurs afin de résoudre un problème, cliquez sur **Ouvrir le journal VPN**.
- Pour supprimer les événements de la liste, cliquez sur **Effacer les événements**.

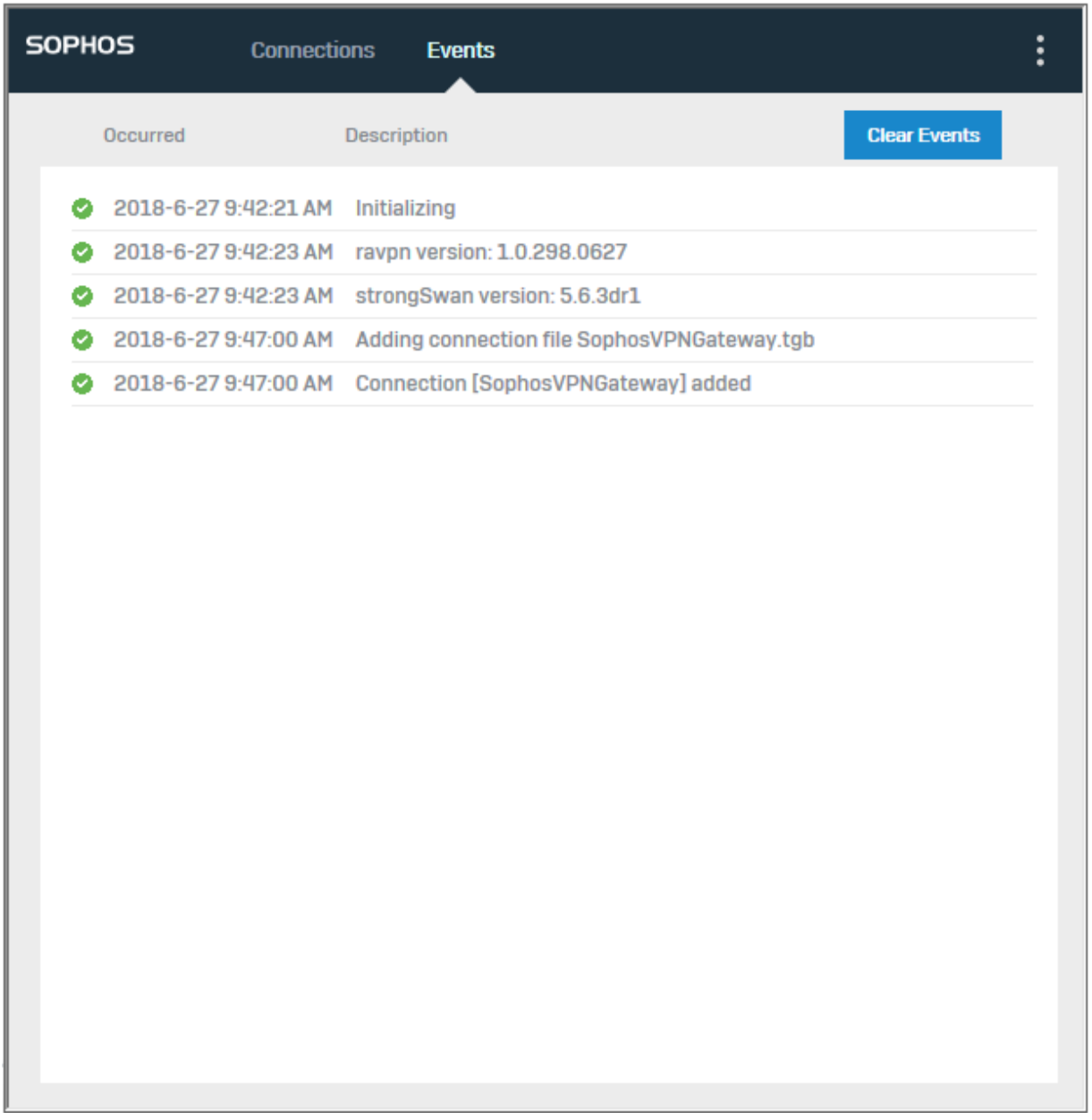


Illustration 1 : Événements

1.4.1 Dépannage des évènements

Si vous ne parvenez pas à vous connecter, cliquez sur **Évènements**, vérifiez le timestamp relatif à l'instant de connexion et trouvez l'erreur.

Cette section couvre les messages d'erreur, leurs causes potentielles et des instructions pour les résoudre. Si vous rencontrez un problème qui n'a pas été couvert ci-dessous, n'hésitez pas à consulter la rubrique Dépannage général.

Veuillez contacter le Support Sophos si vous avez besoin d'aide.

Aucune connexion réseau

Cause: L'adaptateur réseau (Ethernet ou Wi-Fi) n'a pas d'adresse IP.

Action à mener : Vérifiez la validité de votre adresse IP et votre connexion au réseau.

Échec de la résolution DNS

Cause: Le client ne parvient pas résoudre le nom de l'hôte de passerelle.

Action à mener : Vérifiez si un serveur DNS est attribué à l'interface réseau. Exécutez `nslookup` à partir de l'invite de commande (Windows) ou de l'ordinateur (Mac) pour un hôte public, par exemple www.sophos.fr et vérifiez qu'il soit résolu vers une adresse IP. En cas d'échec, contactez votre fournisseur d'accès Internet.

Ports UDP 500/4500 bloqués

Cause: Le pare-feu ou le routeur bloque les ports UDP 500 et 4500.

Action à mener : Vérifiez la configuration de votre pare-feu ou routeur et autorisez le trafic sur ces ports. Si vous n'avez pas accès au pare-feu ou au routeur (par ex. vous êtes dans un hôtel), connectez-vous via votre hotspot mobile et tentez de vous reconnecter.

Aucune réponse de la passerelle : <Passerelle FQDN ou adresse IP utilisée lors de la connexion>

Cause: La passerelle ne répond pas aux messages de négociation IKE. Causes possibles :

- La passerelle à distance (pare-feu ou routeur) a été éteinte.
- L'adresse WAN n'est pas connectée directement à Internet.

Action à mener : Signalez le problème à votre administrateur pare-feu pour résoudre le problème.

Notification NO_PROPOSAL_CHOSEN envoyée par la passerelle

Cause: La passerelle à distance a répondu aux négociations IKE de Sophos Connect avec cette notification d'erreur. Causes possibles :

- La stratégie Sophos Connect n'a pas été pas définie ou activée sur le pare-feu.
- L'administrateur pare-feu a changé les paramètres IKE de phase 1 de la stratégie Sophos Connect du pare-feu et la nouvelle configuration n'a pas été exportée et importée sur le client.

Action à mener : Signalez le problème à votre administrateur pare-feu pour résoudre le problème.

Identifiant distant attendu par le serveur : <valeur d'identifiant attendu>, identifiant reçu : <valeur d'identifiant reçu>

Cause: Le type d'identifiant local ou la valeur configurée dans la stratégie Sophos Connect dans le pare-feu ne correspond pas à la valeur utilisée pour cette connexion. Ceci peut arriver lorsque

l'administrateur pare-feu change l'identifiant local dans le pare-feu et que le nouveau fichier de configuration n'a pas été importé dans Sophos Connect.

Action à mener : Signalez le problème à votre administrateur pare-feu pour résoudre le problème.

Incompatibilité de clé pré-partagée présumée <nom de la connexion>

Cause: La clé prépartagée sur le pare-feu ne correspond pas à la clé utilisée pour cette connexion. Ceci peut arriver lorsque l'administrateur pare-feu change l'ID local dans le pare-feu et que le nouveau fichier de configuration n'a pas été importé dans Sophos Connect.

Action à mener : Signalez le problème à votre administrateur pare-feu pour résoudre le problème.

L'authentification utilisateur de <nom d'utilisateur saisi> a échoué

Cause: Le nom d'utilisateur ou le mot de passe est incorrect.

Action à mener : Tentez de vous reconnecter pour vous assurer que le problème ne provient pas d'une erreur de saisie. Si vous réessayez plusieurs fois sans succès, il est possible que le mot de passe ait changé ou qu'il ait été désactivé dans le pare-feu. Dans ce cas, signalez le problème à votre administrateur pare-feu pour résoudre le problème.

L'échec d'ajout de la route [réseau/masque] a empêché de terminer la phase 2

Remarque
Les étapes de résolution ci-dessous s'appliquent uniquement à Windows.

Cause: Après l'établissement de la phase 2 SA, l'`ajout de routes` au réseau distant a échoué. Il est possible que le service strongSwan se soit arrêté de fonctionner pendant que le tunnel était actif.

Action à mener : Désactivez puis réactivez l'adaptateur TAP. Ouvrez l'invite de commandes en tant qu'administrateur et saisissez les commandes suivantes :

```
net stop scvpn
net start scvpn
```

Impossible d'ajouter les données de connexion. Une connexion portant le nom <nom de la connexion> existe déjà

Cause: Une connexion du même nom a déjà été importée.

Action à mener : Supprimez la connexion existante de Sophos Connect. Assurez-vous que vous souhaitez vraiment supprimer la connexion existante avant de la supprimer. Sinon, contactez votre administrateur pour résoudre le problème.

Service indisponible

Remarque
Les étapes de résolution ci-dessous s'appliquent uniquement à Windows.

Cause: Le service Sophos Connect (scvpn) a été interrompu.

Action à mener : Ouvrez l'invite de commandes en tant qu'administrateur et saisissez la commande suivante :

```
net start scvpn
```

Impossible de charger les données de connexion vers strongSwan

Remarque
Les étapes de résolution ci-dessous s'appliquent uniquement à Windows.

Cause: Le service strongSwan a été interrompu (Nom de service : charon-svc.exe).

Action à mener : Ouvrez l'invite de commandes en tant qu'administrateur et saisissez la commande suivante :

```
net start strongswan
```

SA désactivé ou supprimé par la passerelle

Cause: La passerelle a envoyé une demande de suppression IKE puis le tunnel a été supprimé. Causes possibles :

- L'administrateur de pare-feu a changé la stratégie sur le pare-feu. Ceci entraine l'envoi d'une demande de suppression IKE à toutes les SA actives connectées au pare-feu.
- L'administrateur pare-feu a supprimé manuellement toutes les connexions IPsec de cet utilisateur sur le pare-feu.

Action à mener : Essayez de vous reconnecter. Si cela ne fonctionne toujours pas, contactez votre administrateur pour résoudre le problème.

Résolution DNS impossible pour la passerelle : <nom de passerelle:port>

Cause: Cette erreur est due à un nom d'hôte non valide.

Action à mener :

- Si la connexion a été ajoutée à l'aide d'un fichier d'approvisionnement, vérifiez le nom d'hôte fourni.
- Si la connexion a été ajoutée en important un fichier `ovpn`, vérifiez les paramètres SSL VPN sur XG Firewall.

Impossible de vérifier le certificat du serveur : <nom de passerelle>. Souhaitez-vous continuer ?

Cause: Le client Sophos Connect importe la configuration SSL VPN en se connectant au portail utilisateur de XG Firewall à l'aide des propriétés du fichier d'approvisionnement. Le portail utilisateur utilise un certificat autosigné qui ne peut pas être vérifié par le client Sophos Connect.

Action à mener : Acceptez l'avertissement de sécurité pour vous connecter et télécharger le fichier de configuration `ovpn` à partir du portail utilisateur. Pour éviter que l'invite ne s'affiche à l'avenir, utilisez l'une des options suivantes :

- Générez un nouveau certificat pour XG Firewall signé par une autorité de certification publique. Importez le certificat dans XG Firewall, puis sélectionnez-le dans les **Paramètres Admin** pour vous connecter à la console d'administration Web.
- Envoyez le certificat d'autorité de certification par défaut du XG Firewall aux ordinateurs distants via l'archivage sécurisé.

Impossible de se connecter au serveur non fiable : <passerelle>

Cause: Vous avez annulé l'invite d'avertissement du certificat et la connexion a été interrompue.

Action à mener : Acceptez l'avertissement de sécurité pour vous connecter et téléchargez la stratégie SSL VPN à partir de XG Firewall. Pour empêcher l'invite de s'afficher lors du téléchargement de la stratégie SSL VPN, utilisez l'une des options suivantes :

- Générez un nouveau certificat pour XG Firewall signé par une autorité de certification publique. Importez le certificat dans XG Firewall, puis sélectionnez-le dans les **Paramètres Admin** pour vous connecter à la console d'administration Web.
- Envoyez le certificat d'autorité de certification par défaut du XG Firewall aux ordinateurs distants via l'archivage sécurisé.

Le fichier d'importation contient une double connexion : <nom de la connexion>

Cause: La connexion importée à partir d'un fichier d'approvisionnement a un nom d'affichage dupliqué.

Action à mener : Vérifiez l'attribut `nom_d'affichage` dans le fichier d'approvisionnement et renommez les noms dupliqués.

Impossible de se connecter à la passerelle de stratégie : <nom de la passerelle>

Cause: Le fichier d'approvisionnement n'est pas configuré correctement. Les raisons suivantes peuvent en être la cause :

1. Nom d'hôte ou adresse IP de passerelle non valide.
2. Port non valide ou port sortant bloqué.
3. La passerelle de stratégie est inaccessible car elle est désactivée.

Action à mener :

Vérifiez les éléments suivants dans le fichier d'approvisionnement :

1. Assurez-vous que la valeur affectée à la `passerelle` est correcte.
2. Assurez-vous que la valeur affectée au `port du portail utilisateur` corresponde au paramètre du port HTTPS du portail utilisateur sur XG Firewall.
3. Si le fichier d'approvisionnement est configuré correctement, contactez votre administrateur pour résoudre le problème.

Aucune stratégie SSL VPN n'est définie pour cet utilisateur : <nom d'utilisateur>

Cause: La stratégie SSL VPN (accès à distance) de XG Firewall ne contient aucun membre de stratégie.

Action à mener : Contactez votre administrateur.

Erreur d'incompatibilité de compression. Retente d'établir la connexion.

Cause: Une stratégie SSL VPN est téléchargée pour la première fois depuis XG Firewall et le tunnel VPN SSL est établi simultanément.

Action à mener : L'erreur est résolue en fonction de la configuration de la connexion :

- Avec un fichier d'approvisionnement : Sophos Connect tente automatiquement de se reconnecter.
- Avec un fichier `ovpn` : Se reconnecter manuellement.

Erreur d'incompatibilité de la stratégie. Télécharge la stratégie et retente la connexion.

Cause: Le client Sophos Connect a essayé d'établir une connexion SSL VPN avec une stratégie existante enregistrée pour cette connexion.

L'administrateur a modifié les paramètres SSL VPN sur XG Firewall après l'établissement et l'enregistrement d'une connexion SSL VPN par Sophos Connect.

Action à mener : La connexion a été créée à l'aide d'un fichier d'approvisionnement. Sophos Connect télécharge automatiquement la nouvelle stratégie et rétablit le tunnel SSL VPN.

Remarque
Si l'administrateur modifie la stratégie SSL VPN sur XG Firewall alors que le tunnel est connecté et qu'il s'agit d'un SSL VPN via TCP, le client Sophos Connect détecte et télécharge immédiatement la nouvelle stratégie. S'il s'agit d'un tunnel SSL VPN sur UDP, vous devez attendre que le chronomètre d'inactivité supprime le tunnel. Sophos Connect télécharge ensuite la nouvelle stratégie pour rétablir le tunnel.

Erreur d'incompatibilité de la stratégie. Importez une nouvelle stratégie pour cette connexion.

Cause: Le client Sophos Connect a essayé d'établir une connexion SSL VPN avec une stratégie existante enregistrée pour cette connexion.

L'administrateur a modifié les paramètres SSL VPN sur XG Firewall après l'établissement et l'enregistrement d'une connexion SSL VPN par Sophos Connect.

Action à mener : La connexion a été créée en important un fichier ovpn. L'utilisateur doit télécharger et importer un nouveau fichier ovpn à partir du portail utilisateur de XG Firewall pour rétablir le tunnel SSL VPN.

Remarque
Si l'administrateur modifie la stratégie SSL VPN sur XG Firewall alors que le tunnel est connecté et qu'il s'agit d'un SSL VPN sur tunnel TCP, le client Sophos Connect détecte et déconnecte le tunnel incompatible. S'il s'agit d'un tunnel SSL VPN sur UDP, attendez que le chronomètre d'inactivité supprime le tunnel. L'utilisateur doit télécharger et importer un nouveau fichier ovpn à partir du portail utilisateur de XG Firewall pour rétablir le tunnel SSL VPN.

Délai d'attente de réponse du serveur dépassé.

Cause: La stratégie SSL VPN n'est pas configurée correctement sur XG Firewall. Les causes possibles de la défaillance sont les suivantes :

1. Le nom d'hôte de remplacement est configuré, mais il ne résout pas l'adresse IP publique correcte ou valide.
2. DDNS est configuré, mais il ne résout pas l'adresse IP publique correcte ou valide.
3. Les options **Remplacer le nom d'hôte** et DDNS ne sont pas configurées et le port WAN ne possède pas d'adresse IP publique.

Action à mener : Si vous avez importé la connexion à l'aide d'un fichier d'approvisionnement, mettez à jour le menu des paramètres de connexion de stratégie (sur le client Sophos Connect). Si vous avez utilisé un fichier ovpn pour créer la connexion, exportez un nouveau fichier ovpn à partir du portail utilisateur et réimportez-le dans le client Sophos Connect.

1.5 Dépannage général

Cette rubrique couvre les problèmes qui n'apparaissent pas sur la page Évènements.

Veuillez contacter le Support Sophos si vous avez besoin d'aide.

Le trafic ne passe plus dans le tunnel VPN

Cause: Si vous exécutez une version du firmware antérieure à v17.5, il est possible que le client ait reçu une nouvelle adresse IP virtuelle après le changement de la clé de phase 1.

Action à mener : Déconnectez-vous puis reconnectez-vous. Pour une solution permanente, effectuez une mise à niveau vers la version v17.5.

Impossible d'ouvrir le tableau de bord Sophos Connect

Cause: Si le tableau de bord Sophos Connect ne s'ouvre pas ou qu'il ne répond pas lorsque vous cliquez sur l'icône, ceci indique que l'interface utilisateur graphique de Sophos Connect est bloquée dans une boucle infinie et ne parvient pas à répondre aux commandes extérieures.

Action à mener (Windows): Ouvrez le gestionnaire de tâches et sélectionnez l'onglet Détails. Trouvez scgui.exe et actionnez le clic droit pour terminer la tâche. Redémarrez l'application depuis le raccourci bureau.

Action à mener (Mac): Ouvrez le moniteur d'activités et trouvez le processus Sophos Connect. Ouvrez-le et sélectionnez Sortie forcée. Redémarrez l'application depuis LaunchPad.

La navigation Web cesse de fonctionner lorsque le tunnel est déconnecté

Remarque
Ceci arrive le plus souvent sur Mac.

Cause: Lorsqu'un tunnel unique est déconnecté, les serveurs DNS ne sont pas restaurés à partir des cartes réseau physiques. Cela signifie que les serveurs DNS internes utilisés lorsque vous étiez connecté par VPN sont toujours utilisés. Comme le tunnel n'existe plus, la résolution du nom ne fonctionnera pas.

Action à mener : Déconnectez-vous de votre réseau local, puis reconnectez-vous.

L'interface utilisateur graphique de Sophos Connect affiche le message « Service indisponible »

Remarque
Ceci arrive le plus souvent sur Mac.

Cause: Lorsqu'une déconnexion du tunnel est déclenchée, le démon strongSwan IPsec se bloque dans une boucle infinie. L'interface utilisateur graphique ne reçoit donc pas le message de déconnexion et finit par devenir inactive et afficher le message « Service indisponible ».

Action à mener (Mac):

1. Ouvrez le moniteur d'activités et quittez l'interface utilisateur graphique de Sophos Connect.
2. Ouvrez le terminal et exécutez les commandes suivantes :

   ```
   sudo /bin/launchctl unload -w /Library/LaunchDaemons/
   com.sophos.connect.scvpn.plist
   ```

   ```
   sudo /bin/launchctl load -w /Library/LaunchDaemons/
   com.sophos.connect.scvpn.plist
   ```

3. Ouvrez Sophos Connect et vérifiez que l'erreur « Service indisponible » a été résolue.

Action à mener (Windows):

1. Ouvrez `cmd` en tant qu'administrateur et exécutez les commandes suivantes :

   ```
   net stop scvpn
   ```

   ```
   net start scvpn
   ```

2. Ouvrez Sophos Connect et vérifiez que l'erreur « Service indisponible » a été résolue.

Sophos Connect ne parvient pas à établir un tunnel

Cause: Vous avez probablement installé le client Sophos Connect avant d'installer le client Sophos SSL VPN.

Action à mener : Désinstallez les deux puis réinstallez le client Sophos SSL VPN puis le client Sophos Connect.

Remarque
Ils doivent être installés dans cet ordre là.

Réinitialisation de la connexion reçue de la passerelle : <nom de la passerelle>

Ce message est enregistré dans le fichier `scvpn.log` (dans le dossier d'installation).

Cause: Les paramètres SSL VPN sont modifiés sur XG Firewall, un utilisateur est déconnecté manuellement ou XG Firewall redémarre. Si la connexion utilise SSL VPN sur TCP, XG Firewall envoie une demande de réinitialisation de connexion. Si la connexion utilise SSL VPN sur UDP, il est possible que la connexion se reconnecte automatiquement (selon la période d'inactivité).

Action à mener : Importez un nouveau fichier de configuration dans le client Sophos Connect, puis reconnectez-vous. Si votre administrateur ne vous a pas envoyé le fichier, accédez au portail utilisateur et téléchargez-le. Sinon, rendez vous sur le portail utilisateur pour télécharger le fichier `ovpn`.

Les éléments « Connexion automatique » et « Mise à jour de la stratégie » sont grisés dans le menu de la connexion SSL VPN.

Cause: Si la connexion SSL VPN est créée en important un fichier `ovpn`, ces options ne sont pas disponibles.

Action à mener : Pour activer ces options, vous devez créer une connexion à l'aide d'un fichier d'approvisionnement. Ajoutez ces options au fichier d'approvisionnement. L'option **Mise à jour de la stratégie** sera disponible après votre première connexion. Pour activer la **connexion automatique**, vous devez définir un `hôte de connexion automatique` accessible uniquement sur le réseau interne.

Exemple de fichier d'approvisionnement avec la configuration minimale requise pour l'activation de la connexion automatique :

```
[
 {
  "display_name": "<Saisir le nom de la connexion>",
  "gateway": "<Saisir votre nom d'hôte de passerelle ou votre adresse IP>",
  "auto_connect_host":" <Saisir le nom d'hôte ou l'adresse IP de la
 ressource réseau interne>"
 }
]
```

Erreur SSL VPN

Cause: Erreur générée par le service OpenVPN.

Action à mener : Rétablir la connexion. Si cela ne fonctionne pas, redémarrez votre appareil et réessayez.

Port de gestion indisponible

Cause: Sophos Connect ne parvient pas à accéder au port TCP 25340, qui est nécessaire pour communiquer avec OpenVPN.

Action à mener : Vérifiez si une autre application est en cours d'exécution sur l'appareil utilisant ce port. Si possible, quittez l'application. Si vous ne résolvez pas ce problème, Sophos Connect 2.0 ne pourra pas s'exécuter sur votre appareil. Si aucune autre application n'utilise ce port, il s'agit certainement d'un problème temporaire. Le rétablissement de la connexion devrait résoudre le problème.

Impossible de créer le fichier temporaire

Cause: Sophos Connect utilise un fichier temporaire pour transmettre les attributs de connexion au service OpenVPN. Sophos Connect n'a pas réussi à créer le fichier sur cet appareil.

Action à mener : Redémarrez votre appareil.

Service OpenVPN indisponible

Cause: Le service OpenVPN n'a peut-être pas démarré.

Action à mener : Si le type de démarrage du service OpenVPN indique **désactivé**, sélectionnez **manuel** et redémarrez également le service Sophos Connect.

Impossible d'écrire dans le canal.

Cause: Erreur générée par le client Sophos Connect.

Action à mener : Rétablir la connexion. Si cela ne fonctionne pas, redémarrez votre appareil et réessayez.

2 À propos de Sophos Connect Admin

Dans Sophos Connect Admin, vous pouvez importer des fichiers de configuration (`.tgb`) et configurer différentes options pour votre installation VPN.

Remarque
Retrouvez plus de renseignements sur la configuration et l'exportation des fichiers .tgb sur XG Firewall à la section Sophos Connect Client de l'Aide de XG Firewall : Client Sophos Connect.

Les processus d'installation et de désinstallation de Sophos Connect Admin sont identiques à ceux de Sophos Connect. Retrouvez plus de renseignements à la section Installation de l'Aide de Sophos Connect.

2.1 Modification des fichiers de configuration

Vous pouvez modifier vos fichiers de configuration (`.tgb`) dans Sophos Connect Admin, qui offre des options de configuration VPN plus précises.

Ouvrez le fichier `.tgb` exporté à partir de XG Firewall dans Sophos Admin. Vous pouvez :

- Activer **Tout acheminer** pour diriger tout le trafic via la connexion VPN.
- Activer **Envoyer un Security Heartbeat** pour permettre à Sophos Endpoint d'envoyer des informations sur son état de sécurité à XG Firewall. Ceci ne fonctionne que si le client Sophos Endpoint est installé sur l'ordinateur.
- Activer **Autoriser l'enregistrement du mot de passe** pour permettre aux utilisateurs d'enregistrer leur nom d'utilisateur et leur mot de passe sur leur ordinateur. Les informations d'identification de l'utilisateur sont stockées en toute sécurité à l'aide des services de jeu de clés.
- Activer l'**Demander l'authentification à deux facteurs** si vous avez configuré l'authentification à deux facteurs pour les utilisateurs VPN sur XG Firewall.
- Activer le **Tunnel d'auto-connexion** pour activer la connexion automatiquement des que l'utilisateur se connecte à Sophos Connect depuis son ordinateur. Sophos Connect ne lance pas automatiquement la connexion si l'utilisateur est déjà connecté au réseau de l'entreprise.

  La connexion automatique nécessite un paramètre de configuration supplémentaire : **Suffixe DNS/Hôte de surveillance**, qui peut être utilisé pour déterminer si le système local de l'utilisateur se trouve à l'intérieur ou à l'extérieur du réseau de l'entreprise. Veuillez utiliser l'une des valeurs suivantes :

  — Une adresse IP.

  — Un nom de domaine complètement qualifié (FQDN). Le nom d'hôte ne doit être résolu que lors de l'utilisation du serveur DNS interne.

  — Un suffixe DNS.

  Remarque
  Si vous configurez une adresse IP ou un FQDN, le protocole ICMP doit être autorisé sur cet hôte.

- Ajouter, modifier et supprimer les **Réseaux** auxquels l'utilisateur peut se connecter. L'ajout de réseaux spécifiques à la liste permet de partager les tunnels, car l'utilisateur accède aux ressources de ces réseaux via la connexion VPN, mais accède aux ressources Internet directement via sa passerelle distante.

  Remarque
  Le mode **Tout acheminer** est activé si vous supprimez tous les réseaux, et tout le trafic est dirigé via la connexion VPN.

- Modifiez le **Nom de connexion** et l'**Hôte cible**.

  Pour **Effacer** la configuration, réimportez le fichier `.tbg`.

  En cliquant sur **Enregistrer** la configuration sera sauvegardée en tant que fichier `.scx`.

  Remarque
  Vous pouvez importer des fichiers `.scx` et les modifier de nouveau.

Une fois enregistré, le fichier de configuration peut être envoyé à l'utilisateur, qui l'importera dans Sophos Connect. Pour plus de renseignements, cliquez sur Sophos Connect.

3 Mentions légales