STORMSHIELD

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK VPN CLIENT EXCLUSIVE

GUIDE DE L'ADMINISTRATEUR

Version 7.5.007

Dernière mise à jour du document : 30 mai 2024

Référence : sns-fr-vpn_client_exclusive-guide-administrateur-v7.5.007

Table des matières

Historique des modifications

Date	Description
30 mai 2024	Nouveau document

Avant de commencer

Bienvenue dans le guide de l'administrateur de SN VPN Client Exclusive v7.5.007.

Ce guide est destiné aux administrateurs de SN VPN Client Exclusive. Il comporte toutes les informations permettant de mettre en œuvre et de configurer le logiciel pour permettre l'ouverture de tunnels VPN sécurisés.

Pour le déploiement du logiciel, un document complémentaire nommé « **Guide de déploiement** » est également disponible.

Dans cette documentation, Stormshield Network VPN Client Exclusive est désigné sous la forme abrégée SN VPN Client Exclusive. Certaines images présentes dans cette documentation sont issues du logiciel du partenaire éditeur TheGreenBow. Dans votre logiciel SN VPN Client Exclusive, l'apparence graphique peut varier mais l'expérience utilisateur est identique.

Installation

Introduction

L'installation de SN VPN Client Exclusive s'effectue en exécutant le programme téléchargeable sur le site web MyStormshield.

L'installation par défaut, en double cliquant sur l'icône du programme téléchargé, ouvre une fenêtre permettant de personnaliser l'installation.

L'installation du logiciel est configurable, via un ensemble d'options de ligne de commande et de fichiers de configuration VPN. Ces options et possibilités sont détaillées dans le document « Guide de déploiement ».

Voir la section Procédure d'installation.

Conditions d'installation

SN VPN Client Exclusive fonctionne sur Windows 10 et 11 64 bits.

La configuration minimale requise pour installer le logiciel est la suivante :

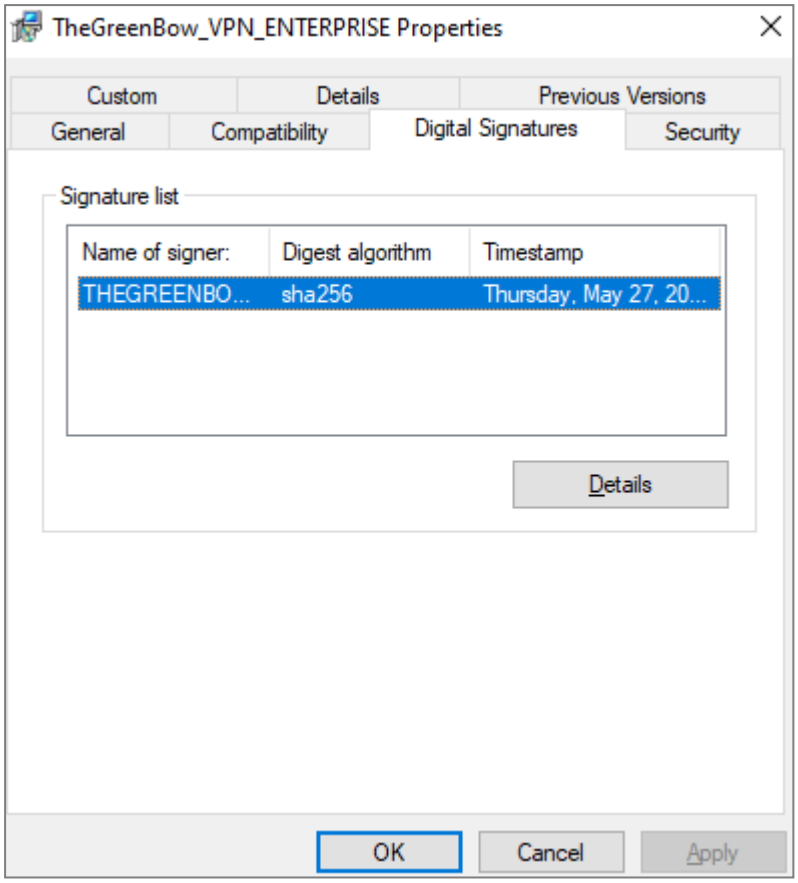
- Processeur : processeur 1 GHz ou plus rapide
- RAM : 2 Go
- Espace disponible sur le disque dur : 40 Mo

Lorsque le logiciel n'est pas installé à partir d'un compte administrateur, un écran s'affiche demandant de saisir le nom d'utilisateur et le mot de passe d'un compte administrateur sur la machine.

Signature numérique et version

Le logiciel installeur de SN VPN Client Exclusive est signé par le certificat de THEGREENBOW SA. Ceci permet à l'installateur ou à l'utilisateur de vérifier l'intégrité du programme d'installation.

L'authenticité du logiciel peut être vérifiée en visualisant les propriétés du programme (clic droit sur l'installeur MSI), puis en sélectionnant l'onglet **Signatures numériques**.



La version de SN VPN Client Exclusive peut être vérifiée par l'utilisateur dans la fenêtre **À propos…** du logiciel.

Procédure d'installation

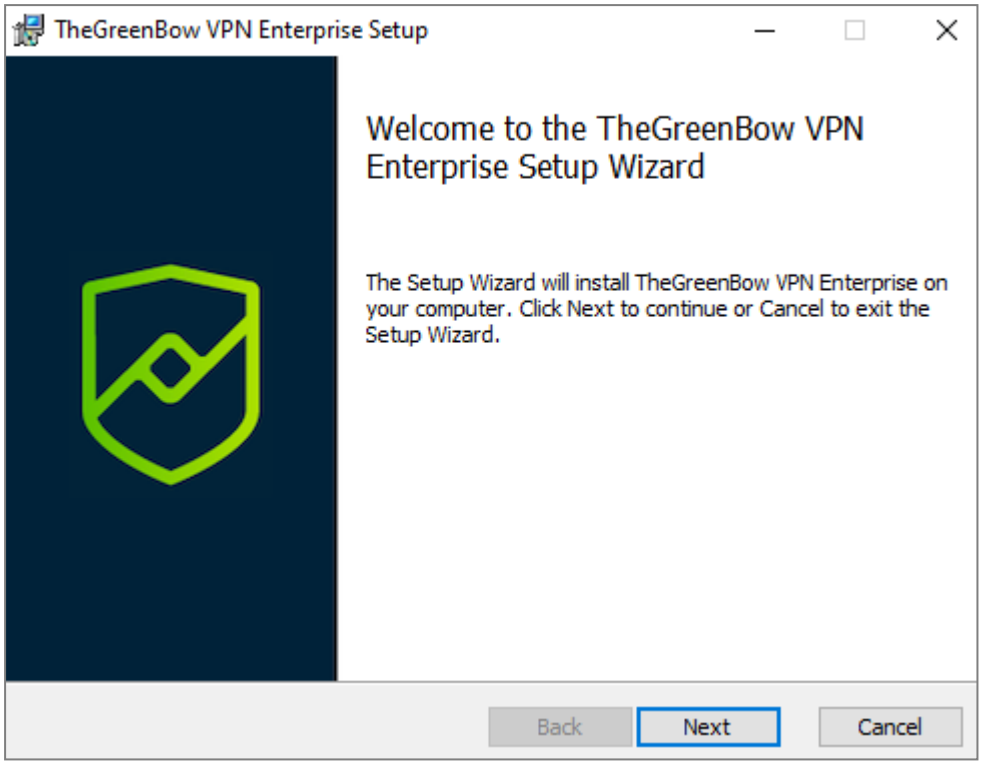
Après avoir téléchargé le programme d'installation de SN VPN Client Exclusive et vérifié son authenticité (voir section Signature numérique et version ci-dessus), vous pouvez procéder à son installation en suivant les étapes décrites ci-dessous.

La procédure d'installation est identique qu'il s'agisse d'une première installation ou d'une mise à jour (cf. chapitre Mise à jour). Lors d'une mise à jour, les paramètres du logiciel, la configuration VPN existante et la licence sont conservés. Dans certains cas, voir section Mise à jour de la configuration VPN.

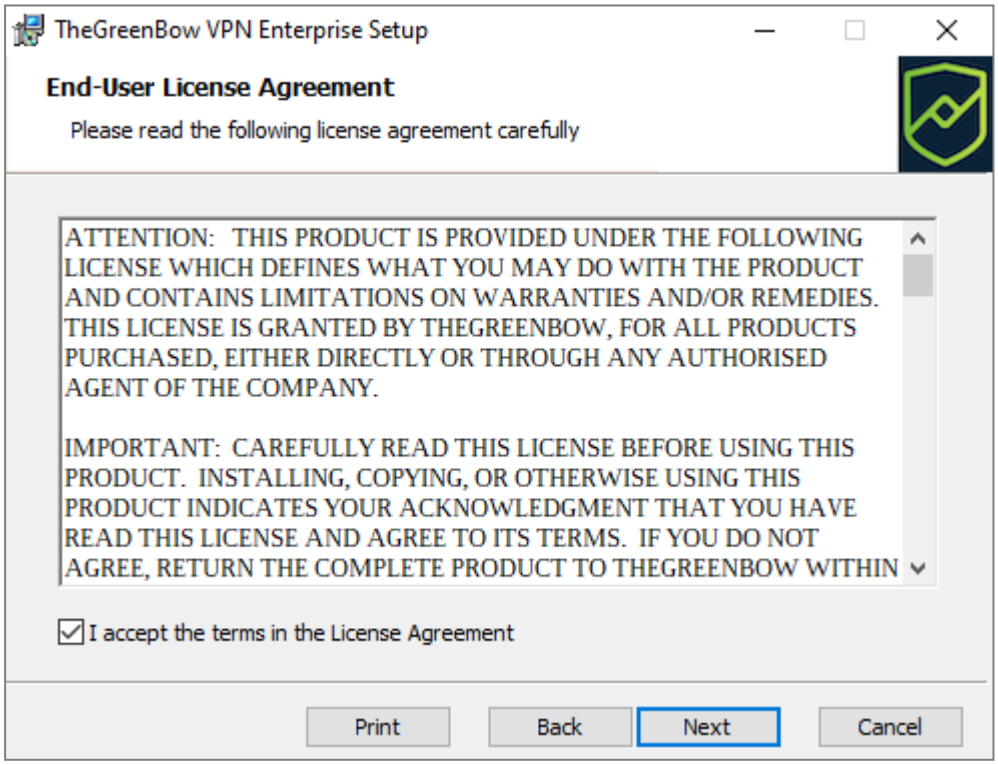
IMPORTANT
La mise à jour du logiciel ne peut se faire que si votre abonnement est toujours en cours (cf. section Comment obtenir une mise à jour).

NOTE
Si vous souhaitez effectuer une installation silencieuse, passer des paramètres spécifiques lors de l'installation ou effectuer un déploiement à grande échelle, reportez-vous au « Guide de déploiement ».

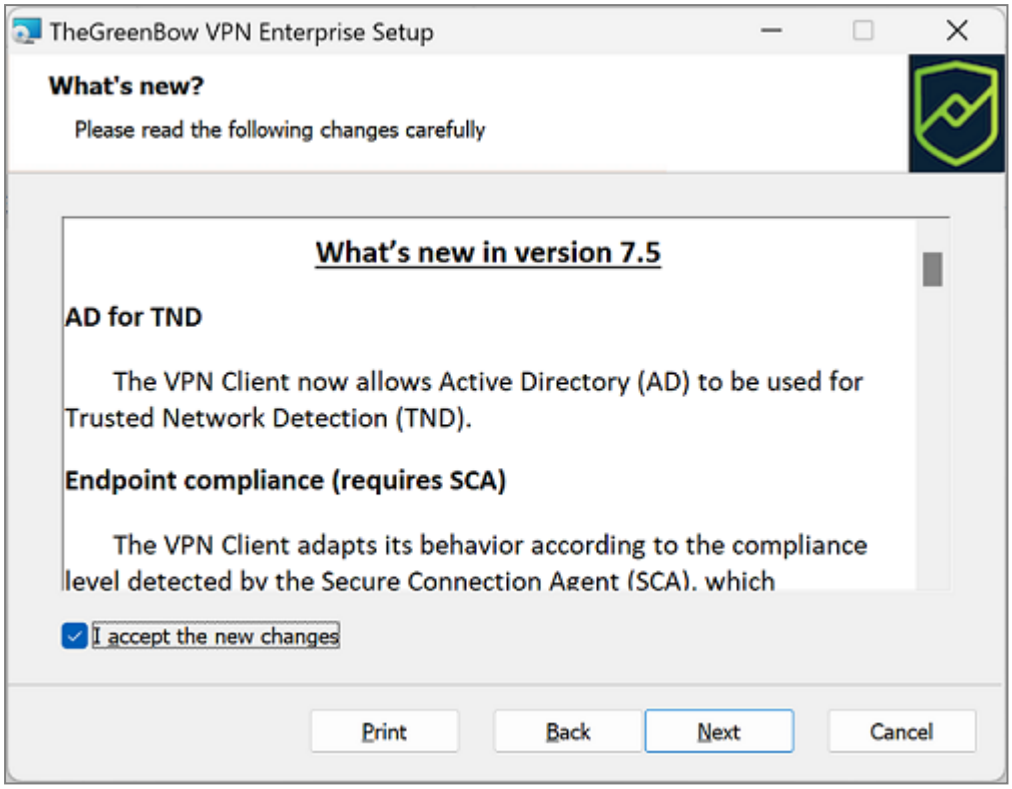
1. Double-cliquez sur le programme d'installation que vous avez téléchargé. La fenêtre suivante s'affiche :



2. Cliquez sur **Suivant**. La fenêtre suivante s'affiche :



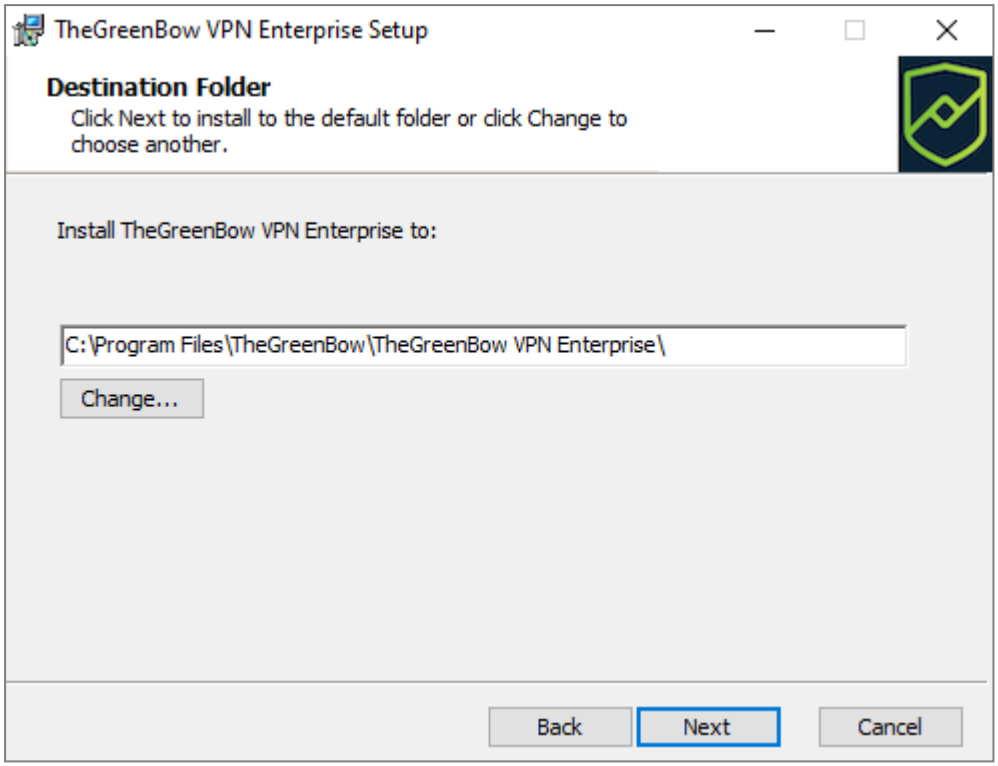
3. Lisez attentivement le Contrat de licence de l'utilisateur final (CLUF). Si vous acceptez tous les termes du contrat, cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**. Dans le cas contraire, vous ne pourrez pas poursuivre l'installation de SN VPN Client Exclusive. La fenêtre suivante s'affiche :



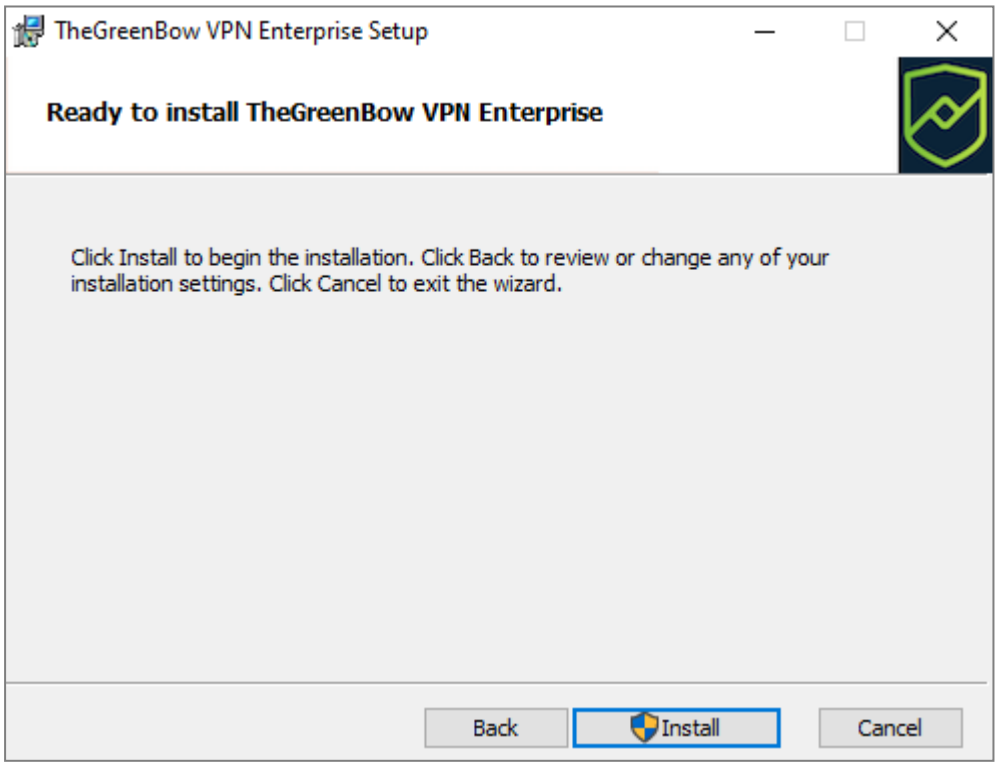
4. Lisez attentivement les informations relatives aux nouveautés et la note de mise à jour concernant la conversion de la configuration VPN existante.

> **IMPORTANT**
> Une fois l'installation terminée, vous ne pourrez pas revenir à une version antérieure du logiciel sans intervention manuelle. En cas de doute, effectuez une sauvegarde de votre configuration VPN dans un dossier distinct ou sur un support amovible.

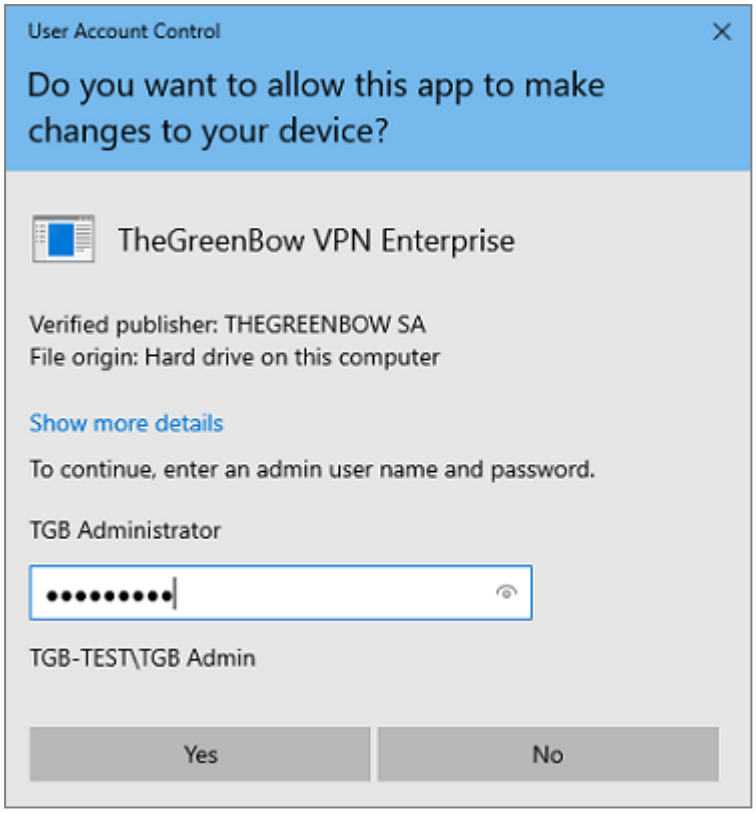
Si vous acceptez les changements introduits, cochez la case **J'accepte les changements introduits**, puis cliquez sur **Suivant**. La fenêtre suivante s'affiche :



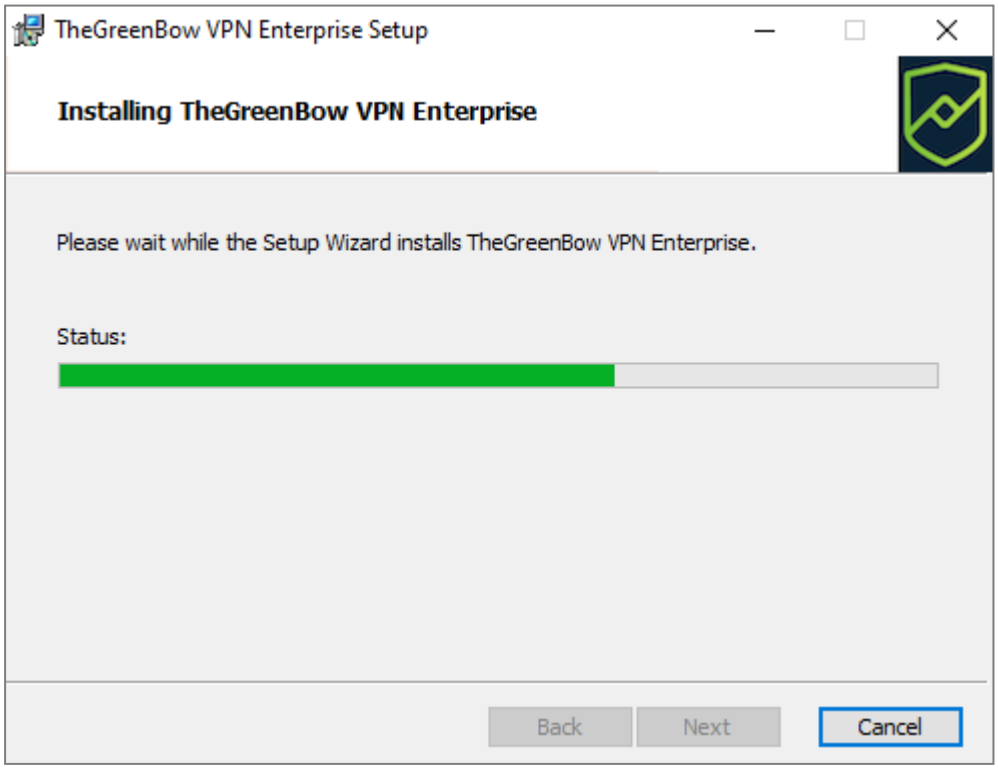
5. Si vous souhaitez installer SN VPN Client Exclusive dans un répertoire particulier, cliquez sur **Modifier…** et sélectionnez le répertoire souhaité. Sinon, vous pouvez conserver le répertoire par défaut. Cliquez ensuite sur **Suivant**. La fenêtre suivante s'affiche :



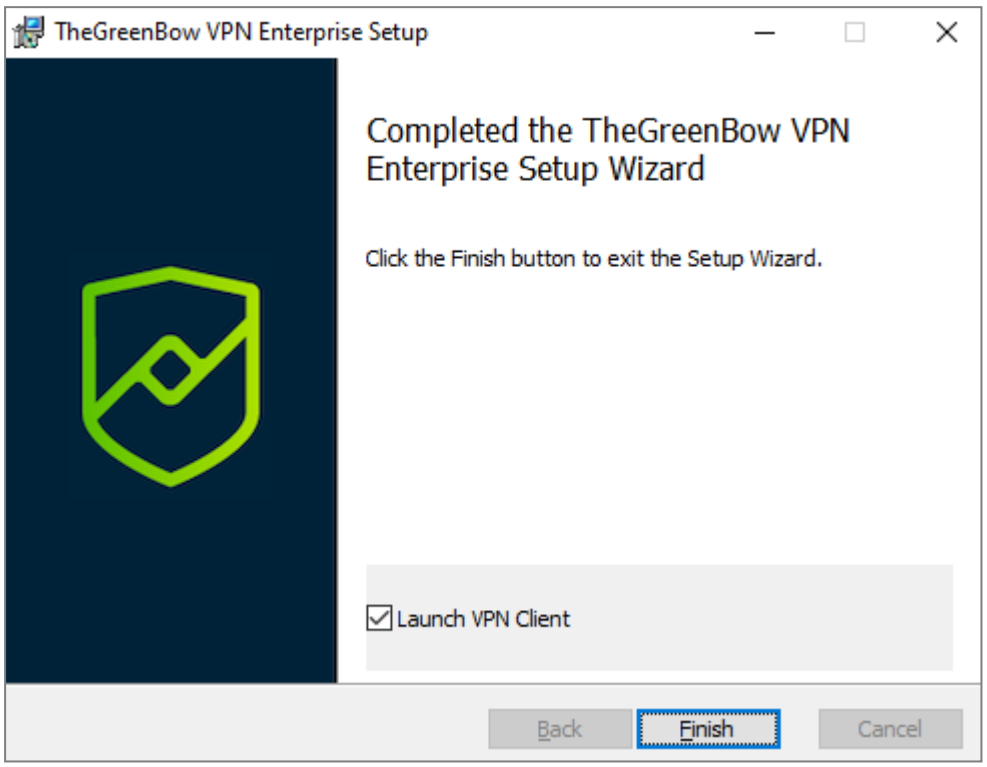
6. Le programme est prêt à installer. Si vous souhaitez revenir en arrière pour vérifier ou modifier vos paramètres d'installation, cliquez sur **Précédent**. Sinon, cliquez sur **Installer**. Si vous effectuez l'installation à partir d'un compte qui ne dispose pas des droits d'administration, la fenêtre suivante s'affiche :



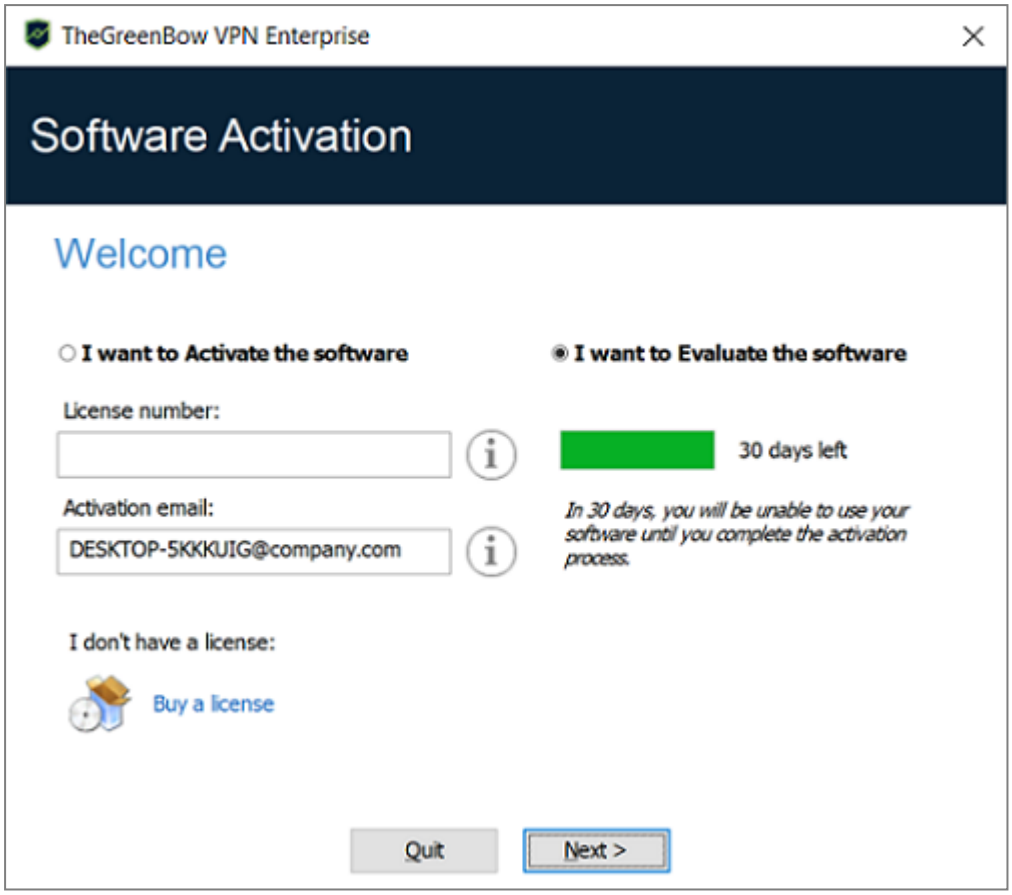
7. Pour poursuivre l'installation, vous devez entrer un nom et mot de passe d'administrateur pour autoriser le programme d'installation d'apporter des modifications à votre ordinateur. Dans le cas contraire, le logiciel ne sera pas installé.
   Si vous effectuez l'installation à partir d'un compte d'administrateur, vous n'avez pas besoin de saisir de mot de passe. Il vous suffit de confirmer que vous autorisez l'application à apporter des modifications à votre appareil.
8. L'installation commence et la fenêtre suivante s'affiche :



9. Attendez la fin de la l'installation de l'ensemble des composants de SN VPN Client Exclusive. Lorsque l'installation a réussi, la fenêtre suivante s'affiche :



10. Si vous ne souhaitez pas lancer SN VPN Client Exclusive immédiatement, décochez la case correspondante. Pour quitter l'assistant d'installation, cliquez sur **Terminer**.
L'écran d'activation du logiciel s'affiche :



11. SN VPN Client Exclusive est désormais installé sur votre poste de travail.

Si vous possédez déjà une licence SN VPN Client Exclusive :

- sélectionnez **Je veux activer le logiciel**,
- entrez le numéro de licence et l'e-mail d'activation,
- puis cliquez sur **Suivant >**.

Pour en savoir davantage sur la procédure d'activation, reportez-vous au chapitre Activation.

Si vous souhaitez évaluer SN VPN Client Exclusive :

- sélectionnez **Je veux évaluer le logiciel**,
- puis cliquez sur **Suivant >**.

Vous pourrez alors utiliser le logiciel pendant une période d'évaluation de 30 jours. Pour en savoir davantage sur la période d'évaluation, reportez-vous à la section Période d'évaluation.

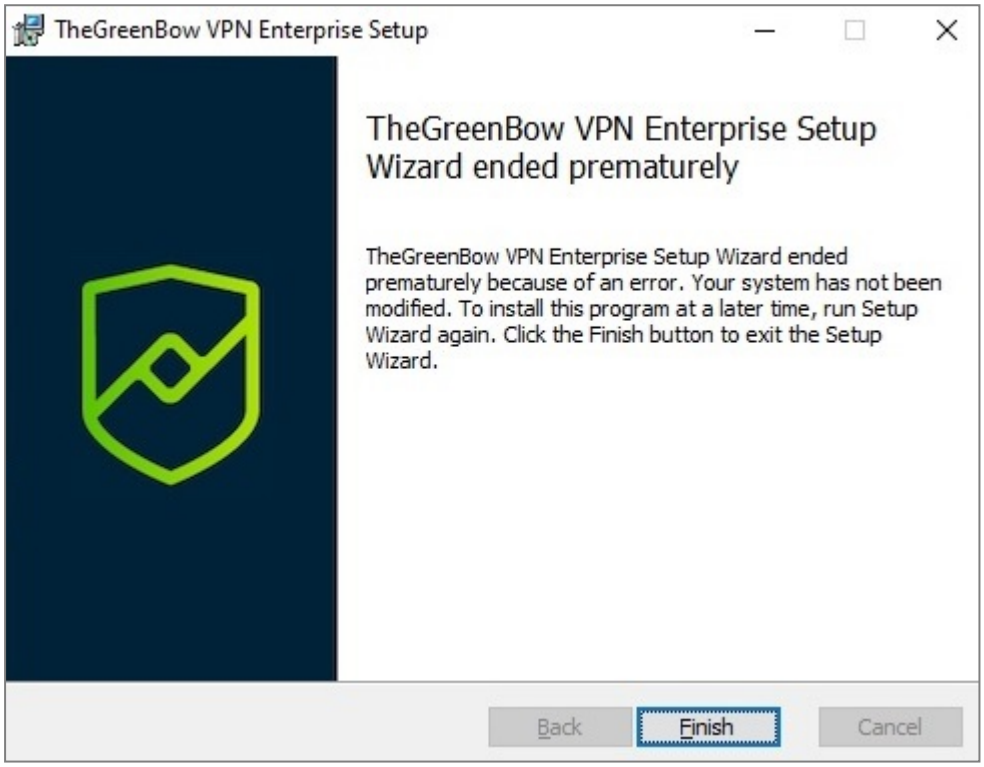
Vous êtes désormais prêt à utiliser le logiciel. Vous pouvez poursuivre avec les étapes suivantes :

- Pour commencer à utiliser SN VPN Client Exclusive immédiatement, reportez-vous au chapitre Prise en main du logiciel.
- Pour utiliser l'**Assistant de Configuration** pour créer une connexion VPN rapidement, reportez-vous au chapitre Assistant de Configuration.
- Pour importer une configuration VPN compatible avec cette version du logiciel, reportez-vous à la section Importer une configuration VPN.
- Pour une présentation détaillée des interfaces disponibles, reportez-vous aux chapitres Panneau des Connexions, Panneau de Configuration et Panneau TrustedConnect.

- Pour une explication complète de l'ensemble des options de configuration d'un tunnel VPN, reportez-vous au chapitre Configurer un tunnel VPN.
- Pour désinstaller SN VPN Client Exclusive, reportez-vous au chapitre Désinstallation.

Interruption de l'installation

Si vous interrompez l'assistant d'installation avant d'avoir cliqué sur le bouton « Installer », la fenêtre suivante s'affiche :

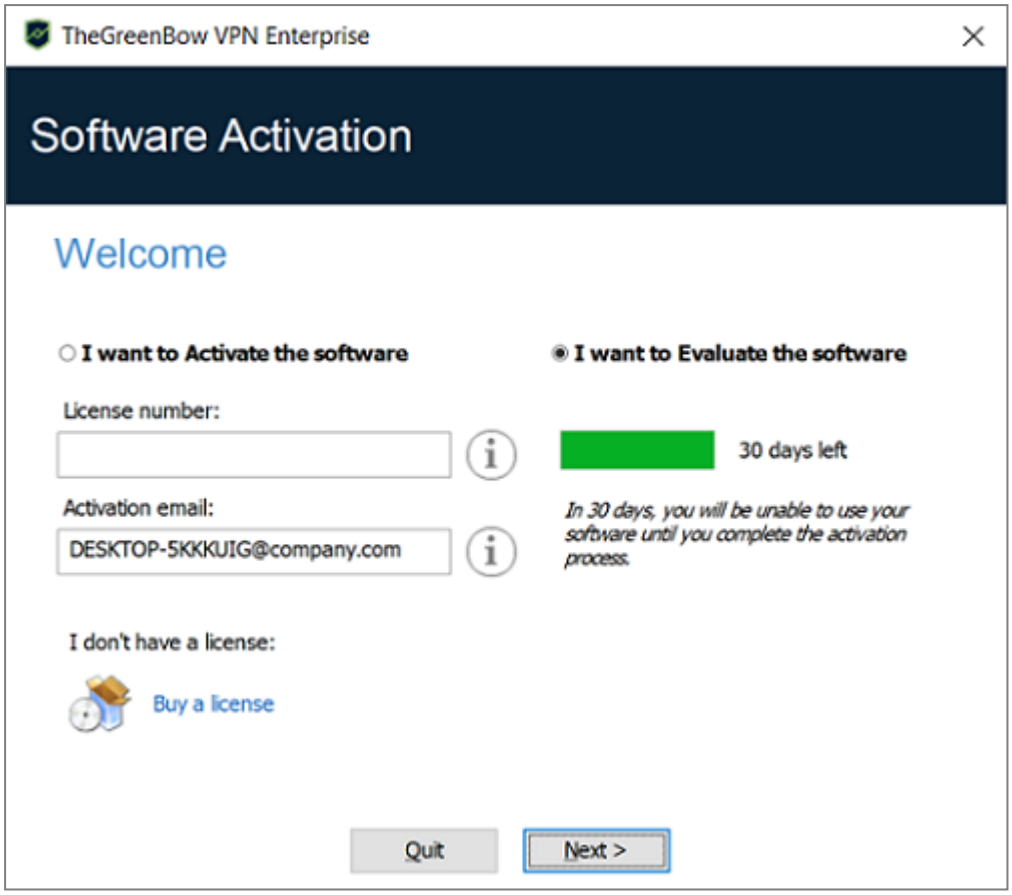


Votre système n'a pas été modifié et vous pouvez reprendre l'installation ultérieurement.

Période d'évaluation

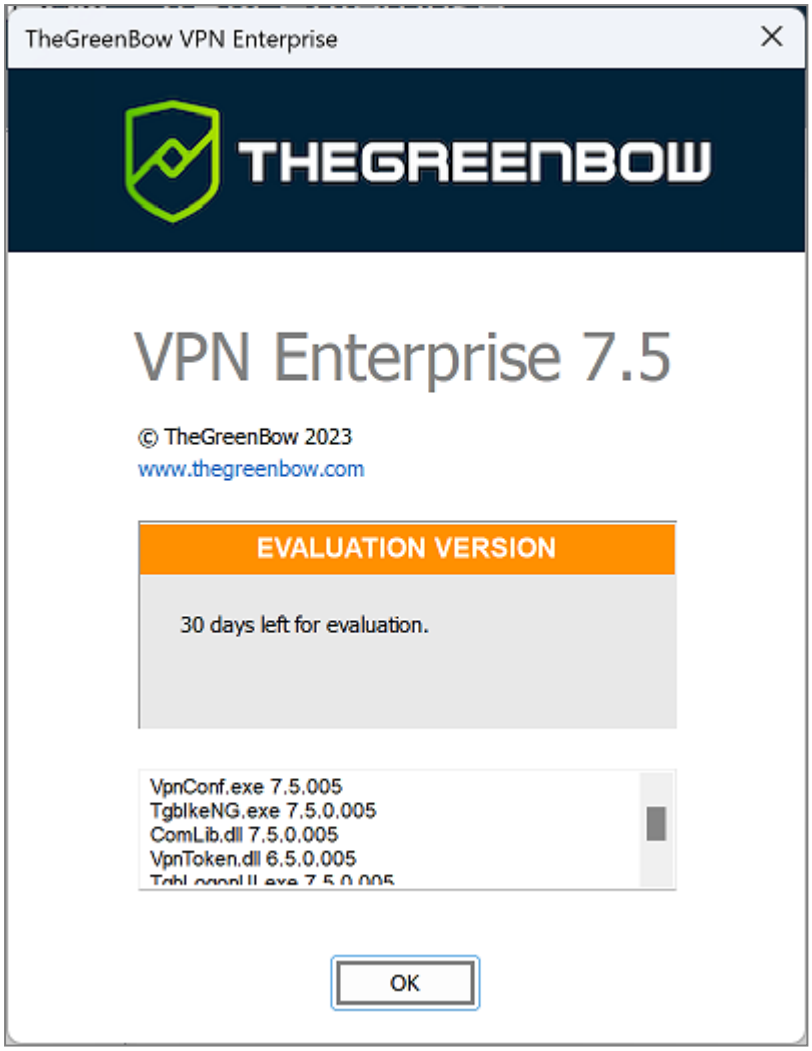
À la première installation sur un poste, si une clé de licence n'est pas fournie à l'installeur, le Client VPN entre en période d'évaluation de 30 jours. Pendant cette période d'évaluation, le Client VPN est complètement opérationnel : toutes les fonctions sont disponibles.

Pendant la période d'évaluation, la fenêtre d'activation est affichée à chaque démarrage du logiciel. Elle indique le nombre de jours d'évaluation restants.

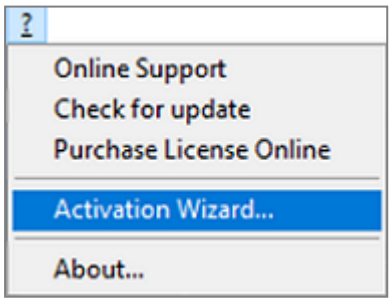


Sélectionnez **Je veux évaluer le logiciel**, puis cliquez sur **Suivant >** pour lancer le logiciel.

Pendant la période d'évaluation, la fenêtre **À propos…** affiche le nombre de jours d'évaluation restants.



Pendant la période d'évaluation, il est toujours possible d'accéder à la fenêtre d'activation via le menu **?** > **Assistant d'activation** de l'interface principale (**Panneau de Configuration**).



Configuration de Windows

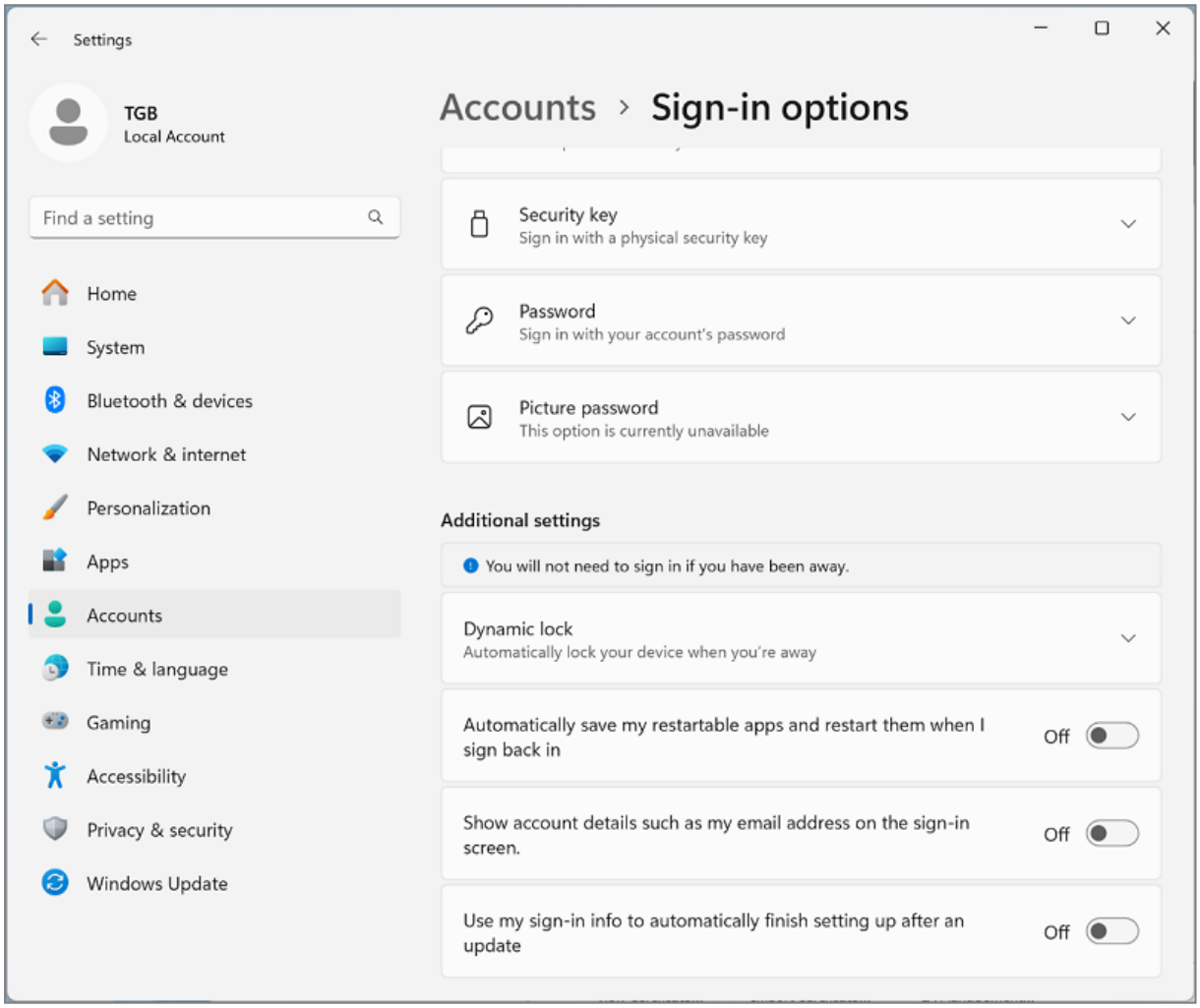
Une fois l'installation terminée, il convient de s'assurer de la désactivation d'une option de connexion dans les paramètres de Windows.

NOTE
Cette option n'est pas disponible (Windows 10) ou grisée (Windows 11) si votre poste est intégré

à un domaine, ou si votre organisation a appliqué des stratégies professionnelles ou de messagerie électronique à votre poste.

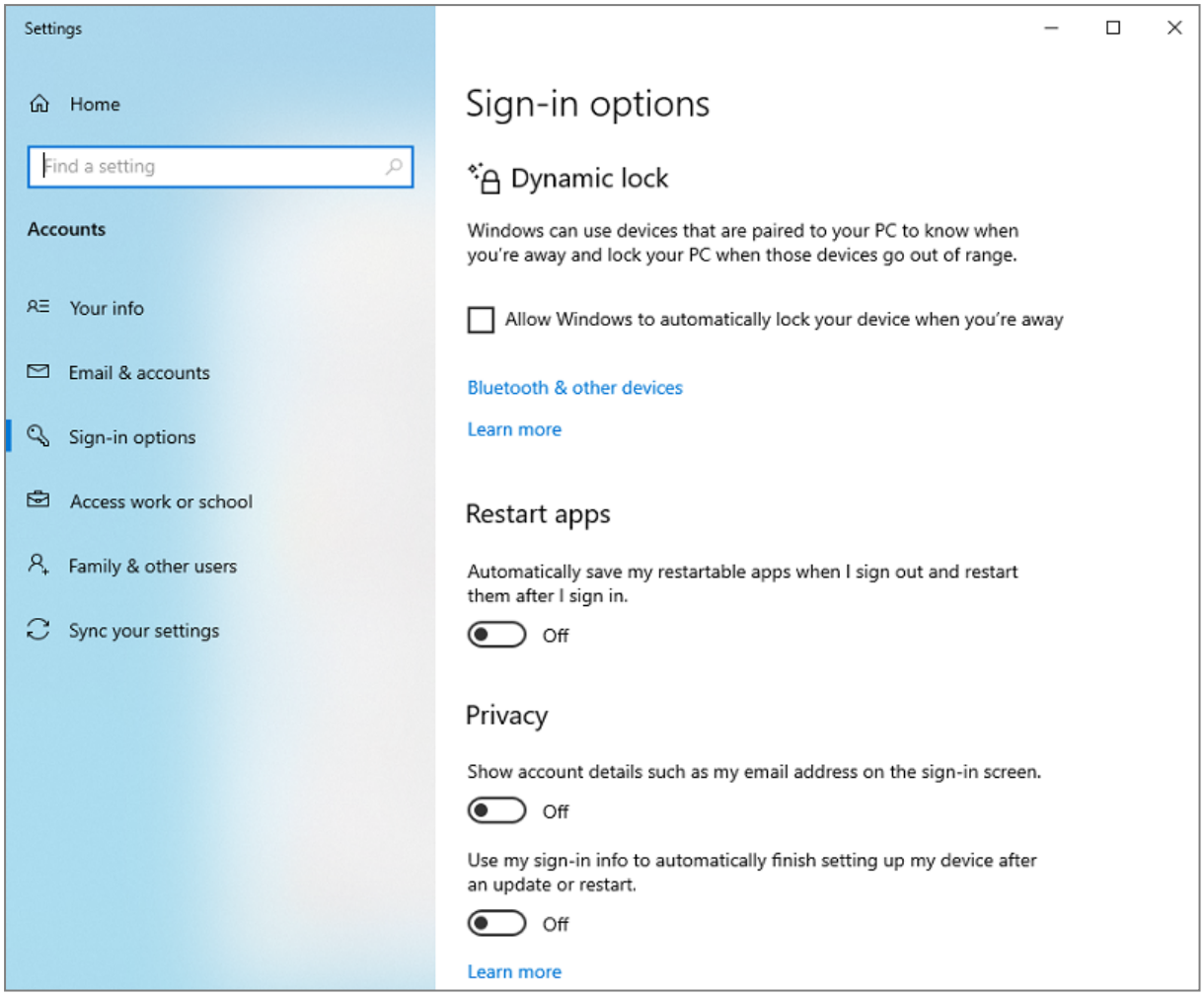
Windows 11

Sous Windows 11, sélectionnez **Démarrer**, puis **Paramètres > Comptes > Options de connexion** et sous **Paramètre supplémentaires** désactivez **Utiliser mes infos de connexion pour terminer automatiquement la configuration après une mise à jour**, comme indiqué dans la capture d'écran ci-dessous :



Windows 10

Sous Windows 10, sélectionnez **Démarrer**, puis **Paramètres > Comptes > Options de connexion** et sous **Confidentialité** désactivez **Utiliser mes infos de connexion pour terminer automatiquement la configuration de mon appareil et rouvrir mes applications après une mise à jour ou un redémarrage**, comme indiqué dans la capture d'écran ci-dessous :


Settings
Home
Find a setting
Accounts
Your info
Email & accounts
Sign-in options
Access work or school
Family & other users
Sync your settings
Sign-in options
Dynamic lock
Windows can use devices that are paired to your PC to know when you're away and lock your PC when those devices go out of range.
Allow Windows to automatically lock your device when you're away
Bluetooth & other devices
Learn more
Restart apps
Automatically save my restartable apps when I sign out and restart them after I sign in.
Off
Privacy
Show account details such as my email address on the sign-in screen.
Off
Use my sign-in info to automatically finish setting up my device after an update or restart.
Off
Learn more

Activation

Si l'activation n'a pas été réalisée lors de l'installation silencieuse (cf. « Guide de déploiement ») – le Client VPN doit être activé pour fonctionner en dehors de la période d'évaluation.

La procédure d'activation est accessible soit à chaque lancement du logiciel, soit via le menu **?** > **Assistant d'activation** de l'interface principale.

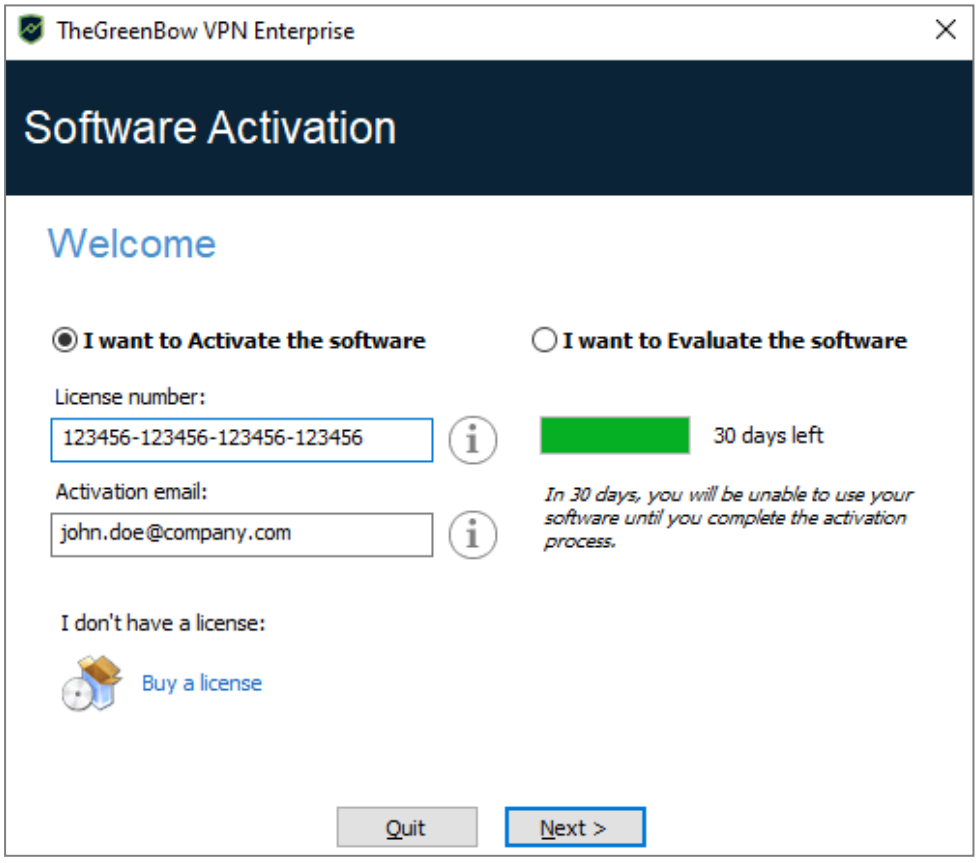
Étape 1

Dans le champ **Numéro de licence**, entrez le numéro de licence reçu par e-mail.

Le numéro de licence peut être copié-collé depuis l'e-mail de confirmation d'achat directement dans le champ.

Le numéro de licence est uniquement composé de caractères [0..9] et [A..F], éventuellement regroupés par 6 et séparés par des tirets.

Dans le champ **Email d'activation**, entrez l'adresse e-mail permettant d'identifier votre activation. Cette information permet de retrouver, en cas de perte, les informations sur votre activation.



NOTE

Le champ **Email d'activation** est rempli par défaut avec le nom d'utilisateur du poste sur lequel le logiciel est installé (sous la forme *nom_utilisateur@entreprise.com*). Ce mécanisme propose à l'administrateur qui gère une licence logicielle « maître » une façon d'identifier unitairement

chaque poste activé. Cela lui permet de gérer les activations et désactivations logicielles de façon déterministe.

Étape 2

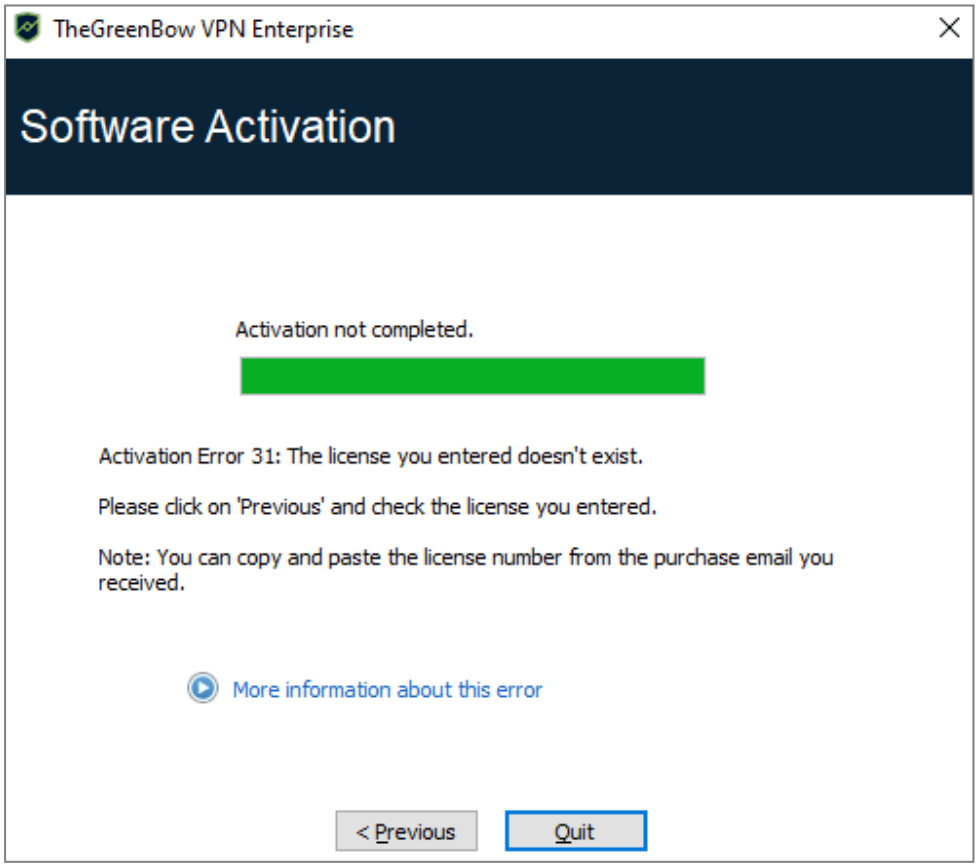
Cliquez sur **Suivant >**. Le processus d'activation en ligne s'exécute automatiquement.

Lorsque l'activation aboutit, cliquez sur **Démarrer** pour lancer le logiciel.

NOTE
L'activation du logiciel est liée au poste sur lequel le logiciel est installé. Ainsi, un numéro de licence qui ne permet qu'une seule activation ne peut, une fois activé, être réutilisé sur un autre poste. Réciproquement, l'activation de ce numéro de licence peut être annulée en désinstallant le logiciel.

Erreurs d'activation

L'activation du logiciel peut ne pas aboutir pour différentes raisons. Chaque erreur est indiquée sur la fenêtre d'activation. Elle est accompagnée, le cas échéant, par un lien qui permet d'obtenir des informations complémentaires, ou qui propose une opération permettant de résoudre le problème.



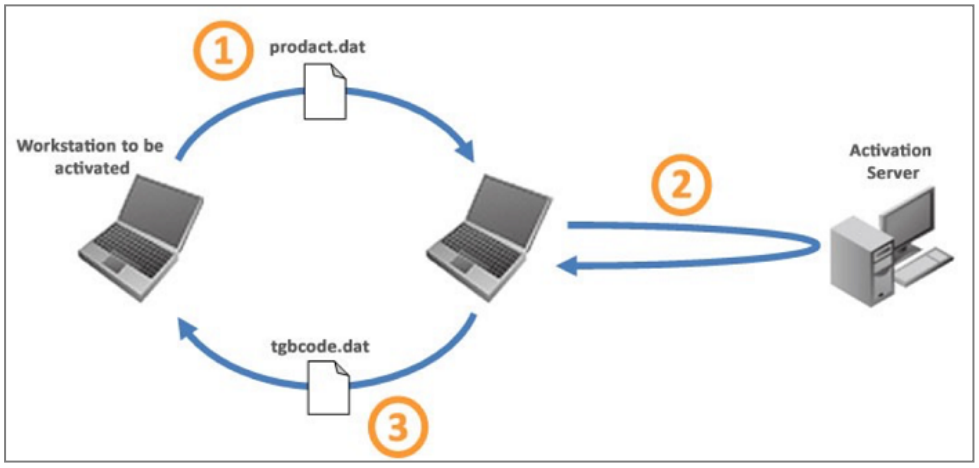
TheGreenBow indique sur son site web toutes les erreurs d'activation ainsi que les procédures de résolution des problèmes d'activation.

Les erreurs d'activation les plus courantes sont les suivantes :

N°	Signification	Résolution
31	Le numéro de licence n'est pas correct	Vérifier le numéro de licence.
33	Le numéro de licence est déjà activé sur un autre poste	Désinstaller le logiciel du poste sur lequel a été activée la licence, ou contacter l'équipe commerciale Stormshield.
53, 54	La communication avec le serveur d'activation est impossible	Vérifier que le poste est bien connecté à internet. Vérifier que la communication n'est pas filtrée par un firewall ou pour un proxy. Le cas échéant, configurer le pare-feu pour laisser passer la communication, ou le proxy pour la rediriger correctement.

Activation manuelle

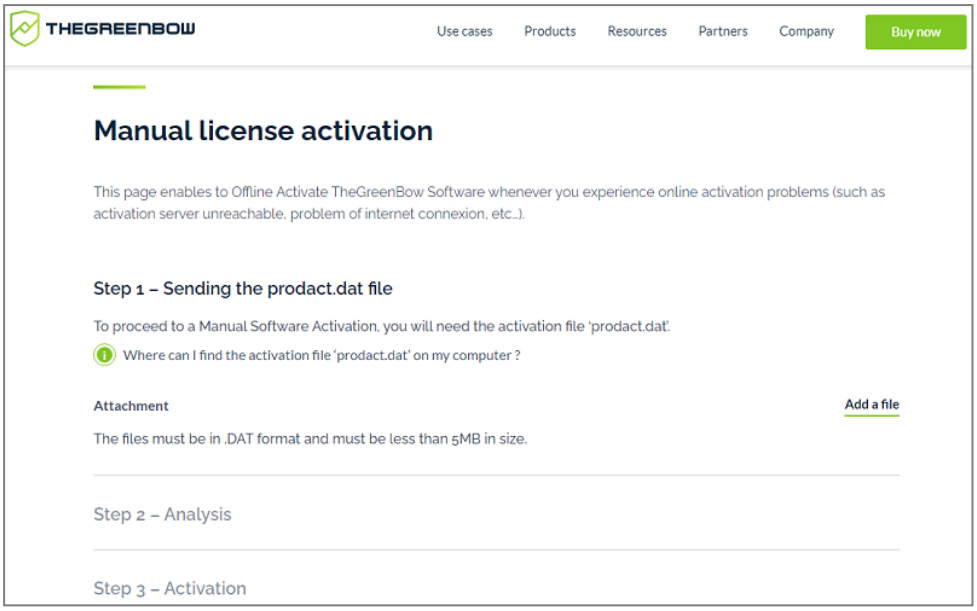
Lorsque l'activation échoue à cause d'un problème de communication avec le serveur d'activation, il est toujours possible d'activer manuellement le logiciel sur le site web TheGreenBow. La procédure est la suivante :



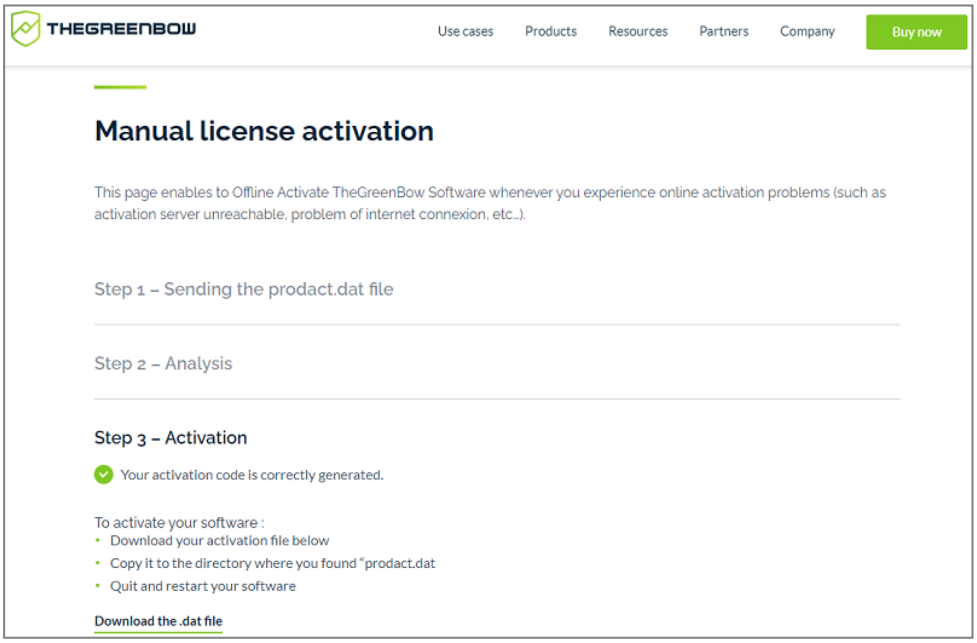
1	Fichier *prodact.dat*	Sur le poste à activer, récupérez le fichier *prodact.dat* situé dans le répertoire Windows **Documents**. Le fichier *prodact.dat* est un fichier texte qui contient les éléments du poste utilisés pour l'activation. Si ce fichier n'existe pas dans le répertoire **Documents**, effectuer sur le poste une activation : même si elle échoue, elle a pour effet de créer ce fichier.
2	Activation	Sur un poste connecté au serveur d'activation (le serveur d'activation est le serveur TheGreenBow, accessible sur internet), ouvrez la page d'activation manuelle (se reporter à la procédure détaillée ci-dessous), postez-y le fichier *prodact.dat* et récupérez le fichier *tgbcode* créé automatiquement par le serveur.
3	Fichier *tgbcode*	Copiez ce fichier *tgbcode* dans le répertoire Windows **Documents** du poste à activer. Lancez le logiciel : il est activé.

Pour procéder à l'activation manuelle, suivez les étapes ci-dessous :

1. Sur un poste ayant une connexion au site web TheGreenBow ouvrez la page web suivante : https://thegreenbow.com/fr/support/gestion-des-licences/activation-manuelle-dune-licence/



2. Cliquez sur le bouton **Ajouter un fichier** et ouvrez le fichier *prodact.dat* créé sur le poste à activer.
3. Cliquez sur **Envoyer**. Le serveur d'activation vérifie la validité des informations du fichier *prodact.dat*.
4. Cliquez sur **Effectuer**. Le serveur d'activation présente en téléchargement le fichier contenant le code d'activation destiné au poste à activer.



Ce fichier a un nom de la forme : *tgbcode_[date]_[code].dat* (par exemple : *tgbcode_20210615_1029.dat*).

Licence et logiciel activé

Lorsque le logiciel est activé, le numéro de licence et l'adresse e-mail utilisés pour l'activation sont consultables dans la fenêtre **À propos…** du logiciel.


TheGreenBow VPN Enterprise
THEGREENBOW
VPN Enterprise 7.5
© TheGreenBow 2023
www.thegreenbow.com
Subscription valid until: 11-25-2025
VpnConf.exe 7.5.006
TgbIkeNG.exe 7.5.0.006
ComLib.dll 7.5.0.006
VpnToken.dll 6.5.0.006
OK

Mise à jour

Comment obtenir une mise à jour

L'obtention d'une mise à jour du logiciel suit les règles suivantes :

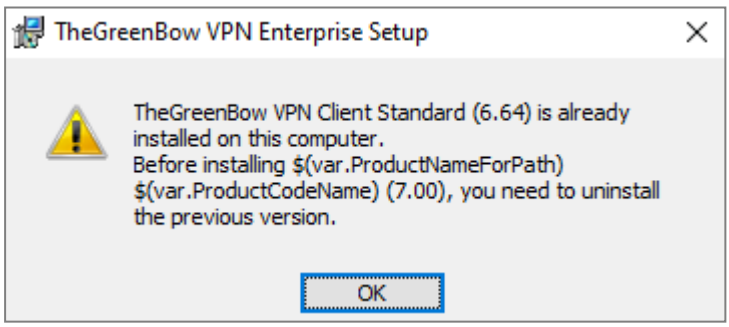
En cours d'abonnement	Je peux installer toute mise à jour L'abonnement démarre à la date d'achat du logiciel.
Hors période d'abonnement	Je ne peux pas utiliser le logiciel ni faire de mise à jour

IMPORTANT
La mise à jour de SN VPN Client Standard vers SN VPN Client Exclusive et vice-versa n'est pas autorisée.

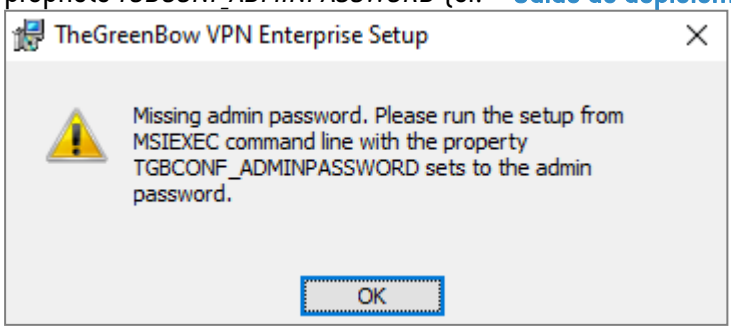
Procédure de mise à jour

La mise à jour de SN VPN Client Exclusive permet de passer à une version plus récente du logiciel tout en conservant les paramètres, la configuration VPN et la licence. Elle s'effectue comme une installation normale (cf. section Procédure d'installation) à deux exceptions près :

1. Si la licence du produit installé n'est pas compatible avec SN VPN Client Exclusive 7.5.007, alors la mise à jour n'est pas possible et l'écran suivant s'affiche. Il vous faudra alors désinstaller la version précédente du logiciel avant de procéder à l'installation de la nouvelle version.



2. Si l'accès au **Panneau de Configuration** de la version déjà installée est protégé par un mot de passe, la mise à jour ne peut pas se faire par l'interface graphique du programme d'installation. Dans ce cas, l'écran suivant s'affiche. Vous pouvez soit supprimer le mot de passe protégeant l'accès au **Panneau de Configuration** dans la version installée, puis procéder à la mise à jour, ou effectuer la mise à jour en ligne de commande à l'aide de la propriété *TGBCONF_ADMINPASSWORD* (cf. « Guide de déploiement »).



Mise à jour de la configuration VPN

Au cours d'une mise à jour, la configuration VPN est sauvegardée et restaurée.

> **NOTE**
> Si l'accès au **Panneau de Configuration** est verrouillé par un mot de passe, ce mot de passe est demandé au cours de la mise à jour, pour autoriser la restauration de la configuration VPN.

Automatisation

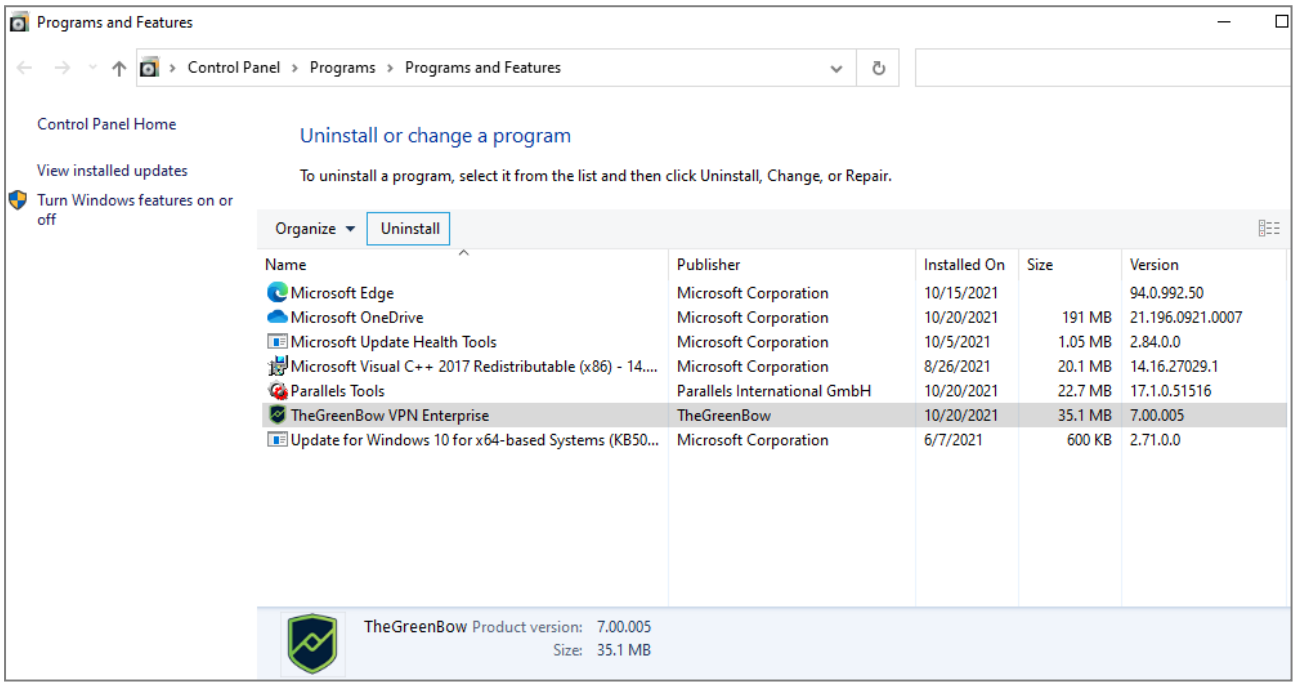
L'exécution d'une mise à jour est configurable, en utilisant une liste d'options de ligne de commande, ou en utilisant un fichier d'initialisation.

Ces options sont décrites dans le document « Guide de déploiement ».

Désinstallation

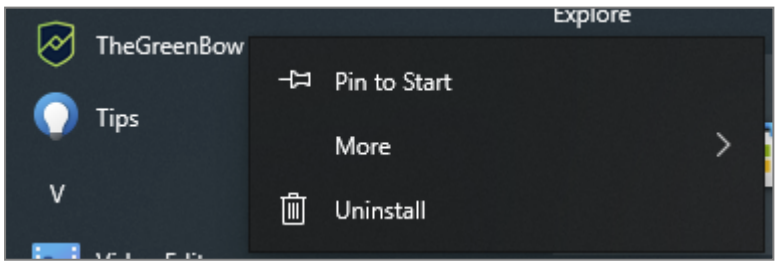
Pour désinstaller le Client VPN, suivez les étapes ci-dessous :

1. Ouvrez le **Panneau de configuration** Windows.
2. Sélectionnez **Désinstaller un programme**.
3. Sélectionnez **SN VPN Client Exclusive** dans la liste de programmes.
4. Cliquez sur **Désinstaller** et suivez les instructions pour désinstaller le programme.



Ou

1. Ouvrez le menu **Démarrer** de Windows.
2. Cliquez avec le bouton droit de la souris sur le programme **SN VPN Client Exclusive**, puis sélectionnez **Désinstaller**.



3. Le **Panneau de configuration** Windows s'affiche. Sélectionnez **SN VPN Client Exclusive** dans la liste de programmes.
4. Cliquez sur **Désinstaller** et suivez les instructions pour désinstaller le programme.

> **NOTE**
> Pour désinstaller le programme, comme pour l'installer, il faut disposer des droits d'administrateur sur le poste.

Vous pouvez également désinstaller le programme en ligne de commande. Cette procédure est décrite dans le document « Guide de déploiement ».

IMPORTANT
Si vous lancez l'installeur MSI et que vous sélectionnez l'option **Supprimer** pour désinstaller le programme, un message d'erreur s'affiche. Veuillez privilégier l'une des méthodes de désinstallation décrite ci-dessus.

Prise en main du logiciel

Introduction

L'interface graphique du SN VPN Client Exclusive permet :

1. de configurer le logiciel lui-même (mode de démarrage, langue, contrôle d'accès, etc.),
2. de gérer les configurations des tunnels VPN, les certificats, l'importation, l'exportation, etc.,
3. d'utiliser les tunnels VPN (ouverture, fermeture, identification des incidents, etc.),
4. de passer en mode TrustedConnect (ouverture automatique d'un tunnel sur non-détection de réseau de confiance).

L'interface graphique comprend les éléments suivants :

- le Panneau des Connexions (liste des tunnels VPN à ouvrir) ;
- le Panneau de Configuration, affichable depuis le Panneau des connexions ou l'icône en barre des tâches, et composé des éléments suivants :
  - un ensemble de menus de gestion du logiciel et des configurations VPN ;
  - l'arborescence de la configuration VPN ;
  - des onglets de configuration des tunnels VPN ;
  - une barre d'état ;
- le Panneau TrustedConnect permettant de bénéficier des fonctionnalités Always-On et TND (exécutable séparé) ;
- une icône en barre des tâches et son menu associé, différente pour le Panneau TrustedConnect et pour le Panneau des Connexions / de Configuration.

Démarrer le logiciel

Une fois l'installation ou la mise à jour terminée, si vous avez laissé la case **Lancer le client VPN** cochée et que vous n'avez pas activé le logiciel, la fenêtre d'activation s'affiche (cf. chapitre Activation). Lorsque le logiciel est activé ou que vous avez choisi de l'évaluer, le SN VPN Client Exclusive se lance minimisé et l'icône SN VPN Client Exclusive apparaît dans la barre des tâches. L'icône en barre des tâches est décrite en détail dans le paragraphe Icône en barre des tâches ci-dessous.

Si vous avez décoché la case **Lancer le client VPN** en fin d'installation ou de mise à jour, vous pouvez soit double-cliquer sur l'icône de bureau correspondante, soit activer le menu **Démarrer** de Windows, puis sélectionner le programme dans la liste.

Vérification de l'intégrité du Client VPN

Tous les binaires constitutifs du SN VPN Client Exclusive (à l'exception des pilotes) sont signés par le certificat de THEGREENBOW (SISTECH S.A.). Les pilotes (ou drivers) sont eux signés par le certificat de THEGREENBOW SA. Ceci permet à l'utilisateur de vérifier l'intégrité du logiciel et de ses modules.

L'authenticité du logiciel peut être vérifiée en visualisant les propriétés de n'importe quel module du logiciel en faisant un clic droit, puis en sélectionnant l'onglet **Signatures numériques**.

Dans le cas où l'un des modules du logiciel est corrompu, le Client VPN ne sera pas opérationnel. En fonction des cas, soit une pop-up Windows s'affiche ou un message est consigné dans la **Console**.

Démarrer le Client VPN à partir du raccourci sur le bureau

Au cours de l'installation du logiciel, un raccourci vers l'application est créé sur le bureau Windows.

SN VPN Client Exclusive peut être lancé directement en double-cliquant sur cette icône.

Le Client VPN se lance minimisé et l'icône SN VPN Client Exclusive apparaît dans la barre des tâches (cf. paragraphe Icône en barre des tâches ci-dessous).

Démarrer le Client VPN à partir du menu Démarrer

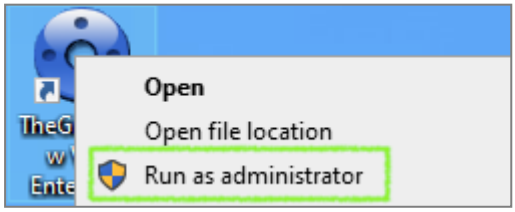
À l'issue de l'installation, le SN VPN Client Exclusive peut être lancé depuis le menu **Démarrer** de Windows en cliquant sur le programme SN VPN Client Exclusive.

Le Client VPN se lance minimisé et l'icône SN VPN Client Exclusive apparaît dans la barre des tâches (cf. paragraphe Icône en barre des tâches ci-dessous).

Démarrer le Client VPN en tant qu'administrateur

Par défaut, l'accès au **Panneau de Configuration** du Client VPN est réservé aux seuls administrateurs Windows.

Pour lancer le Client VPN en mode administrateur, afin de pouvoir accéder au **Panneau de Configuration**, cliquez sur l'icône **SN VPN Client Exclusive** avec le bouton droit de la souris, puis sélectionnez l'option de menu **Exécuter en tant qu'administrateur**.



Icône en barre des tâches

En utilisation courante, l'état du **Panneau des Connexions** / **de Configuration** de SN VPN Client Exclusive est identifié par une icône située en barre des tâches.

L'icône change de couleur si un tunnel VPN est ouvert :

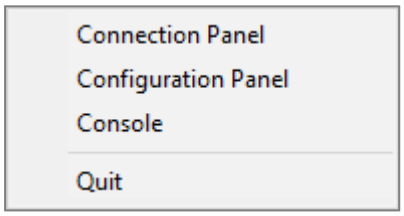
	Icône bleue : aucun tunnel VPN n'est ouvert
	Icône verte : au moins un tunnel VPN est ouvert

L'infobulle de l'icône indique à tout moment l'état du logiciel :

- **VPN Tunnel ouvert** si un ou plusieurs tunnels sont ouverts ;
- **SN VPN Client Exclusive** lorsque le Client VPN est lancé, sans tunnel ouvert.

Un clic gauche sur l'icône ouvre le **Panneau des Connexions**.

Un clic droit sur l'icône du Client VPN en barre des tâches affiche le menu contextuel associé à l'icône :



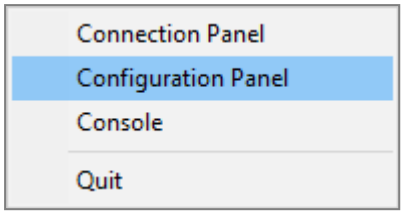
L'administrateur peut limiter les options affichées dans le menu (cf. section Visualisation des options de menu en barre des tâches). Par défaut, les options du menu contextuel sont les suivantes :

1. **Panneau des Connexions** : ouvre le **Panneau des Connexions**.
2. **Panneau de Configuration** : ouvre le **Panneau de Configuration** (si le Client VPN a été exécuté en tant qu'administrateur).
3. **Console** : ouvre la fenêtre des traces VPN.
4. **Quitter** : ferme les tunnels VPN ouverts et quitte le logiciel.

NOTE
Si le logiciel n'a pas été démarré en tant qu'administrateur et que l'option **Restreindre l'accès du panneau de configuration aux administrateurs** n'a pas été désactivée, lorsque l'utilisateur sélectionne l'option **Panneau de Configuration**, un message s'affiche indiquant que le logiciel doit être lancé en tant qu'administrateur pour accéder au **Panneau de Configuration** (cf. paragraphe Démarrer le Client VPN en tant qu'administrateur ci-dessus).

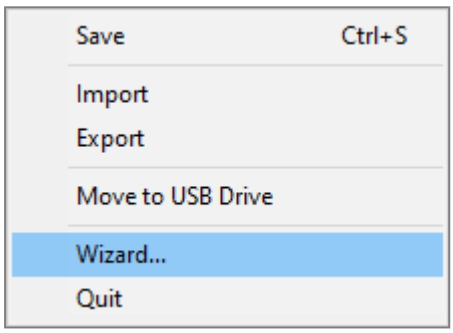
Configurer un tunnel VPN

Pour ouvrir le **Panneau de Configuration**, il faut préalablement avoir lancé le Client VPN en tant qu'administrateur (cf. paragraphe Démarrer le Client VPN en tant qu'administrateur ci-dessus). Si ce n'est pas le cas, quittez et relancer le Client VPN en tant qu'administrateur. Si c'est le cas, cliquez avec le bouton droit de la souris sur l'icône en barre des tâches (cf. paragraphe Icône en barre des tâches ci-dessus), puis sélectionnez l'option **Panneau de Configuration**. Le **Panneau de Configuration** est décrit dans le chapitre Panneau de Configuration.



NOTE
Lorsque l'option **Restreindre l'accès du panneau de configuration aux administrateurs** est désactivée (cf. section Restreindre l'accès au Panneau de Configuration), il n'est pas nécessaire de lancer le Client VPN en tant qu'administrateur pour avoir accès au Panneau de Configuration.

Ensuite, ouvrez l'**Assistant de Configuration** en sélectionnant l'option de menu **Configuration** > **Assistant de Configuration**.



Utiliser l'assistant comme décrit au chapitre Assistant de Configuration ci-dessous.

Automatiser l'ouverture du tunnel VPN

Le SN VPN Client Exclusive permet d'automatiser l'ouverture d'un tunnel VPN. Il peut s'ouvrir automatiquement des manières suivantes :

1. au démarrage de Windows, avant ou après l'ouverture de la session Windows ;
2. sur détection de trafic à destination du réseau distant (cf. chapitre Automatisation) ;
3. sur insertion de la carte à puce ou du token contenant le certificat utilisé pour ce tunnel (cf. section Utiliser un certificat sur carte à puce ou sur token) ;
4. lors de l'utilisation du **Panneau TrustedConnect**, si le Client VPN détecte que le poste ne se trouve pas dans le réseau de confiance (cf. chapitre Gestion du Panneau TrustedConnect).

Ouvrir un tunnel avec le Panneau TrustedConnect

Le **Panneau TrustedConnect** est décrit au chapitre Panneau TrustedConnect. Il permet d'ouvrir une connexion VPN de manière automatisée lorsque le poste est situé en dehors du réseau de confiance, et de garder la connexion ouverte même en cas de changement d'interface réseau.

Le **Panneau TrustedConnect** se lance depuis un exécutable distinct du **Panneau de Configuration**. Si le **Panneau TrustedConnect** n'est pas lancé automatiquement au démarrage de la session, il est possible de l'exécuter à partir du dossier d'installation du Client VPN : l'exécutable se nomme *VpnDialer.exe* (aucun raccourci vers l'application n'est créé sur le bureau de Windows lors l'installation du logiciel).

NOTE

Le **Panneau TrustedConnect** (lancé à partir de l'exécutable *VpnDialer.exe*) ne peut être lancé en même temps que le **Panneau de Configuration** ou le **Panneau des Connexions** (tous deux lancés à partir de l'exécutable *VpnConf.exe*, du raccourci sur le Bureau ou du menu **Démarrer**).

Lorsque *VpnConf.exe* est en cours d'exécution et que vous lancez *VpnDialer.exe*, tous les tunnels ouverts dans *VpnConf.exe* seront fermés et *VpnDialer.exe* (TrustedConnect) tentera de lancer automatiquement le tunnel configuré.

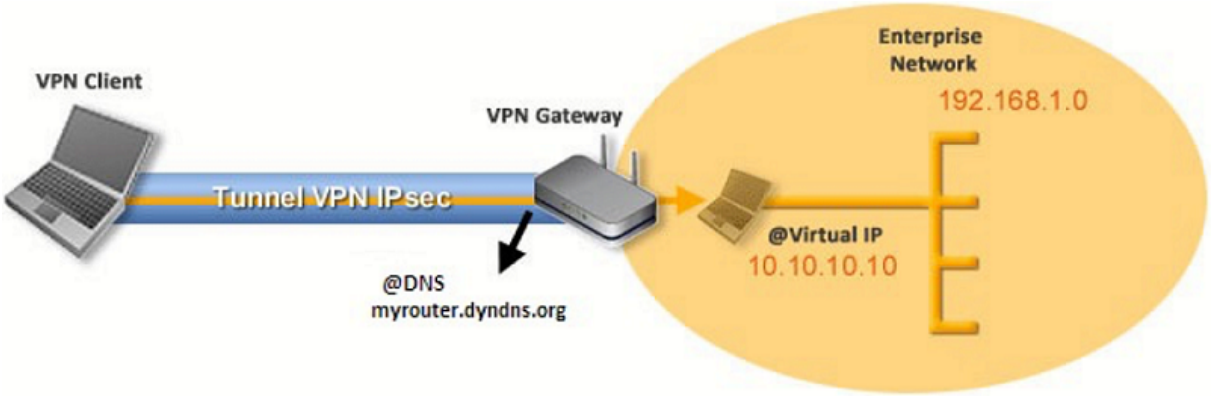
En revanche, lorsque *VpnDialer.exe* (TrustedConnect) est en cours d'exécution, il n'est pas possible de lancer *VpnConf.exe*. Vous devez d'abord quitter *VpnDialer.exe* avant de pouvoir lancer *VpnConf.exe*.

Assistant de Configuration

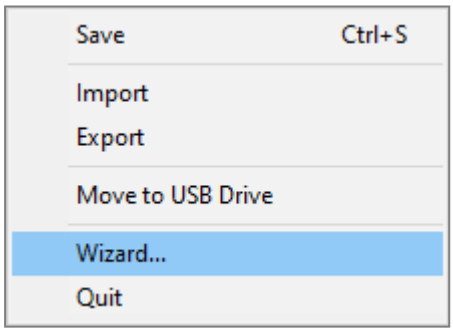
L'**Assistant de Configuration** permet de configurer un tunnel VPN en trois étapes simples.

L'utilisation de l'**Assistant de Configuration** est illustrée par l'exemple suivant :

- Le tunnel est ouvert entre un poste et une passerelle VPN dont l'adresse DNS est « myrouter.dyndns.org ».
- Le réseau local de l'entreprise est 192.168.1.0 (il contient par exemple des machines dont l'adresse IP est 192.168.1.3, 192.168.1.4, etc.).
- Une fois le tunnel ouvert, le poste distant aura comme adresse IP dans le réseau de l'entreprise : 10.10.10.10.



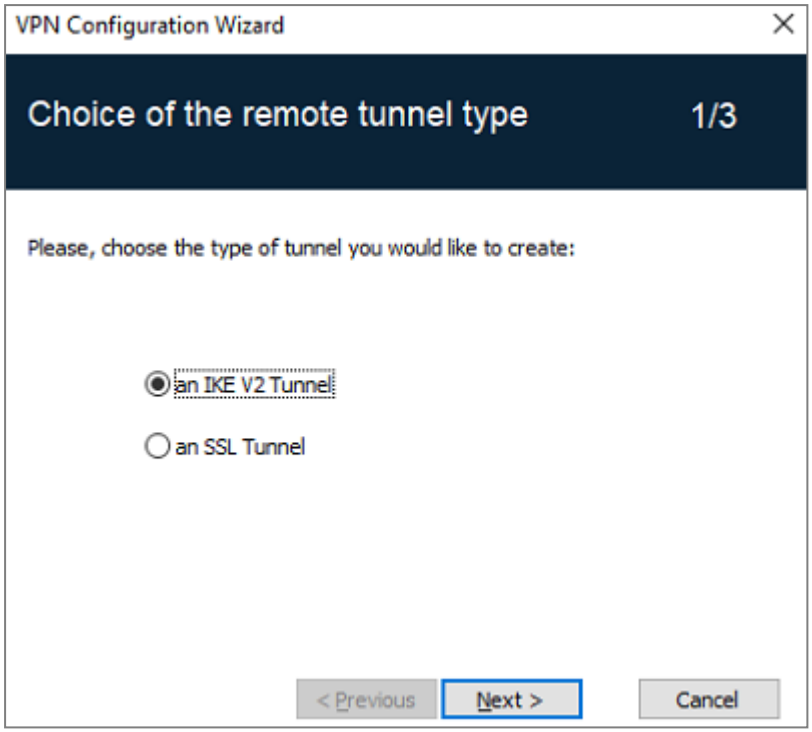
Dans l'interface principale, ouvrez l'**Assistant de Configuration VPN** : **Configuration** > **Assistant de Configuration**.



ASTUCE
Recommandation de sécurité : Il est recommandé de configurer des tunnels IKEv2 avec certificat. Reportez-vous au chapitre Recommandations de sécurité.

Étape 1

Choisissez le protocole VPN à utiliser pour le tunnel : IKEv2 ou SSL.

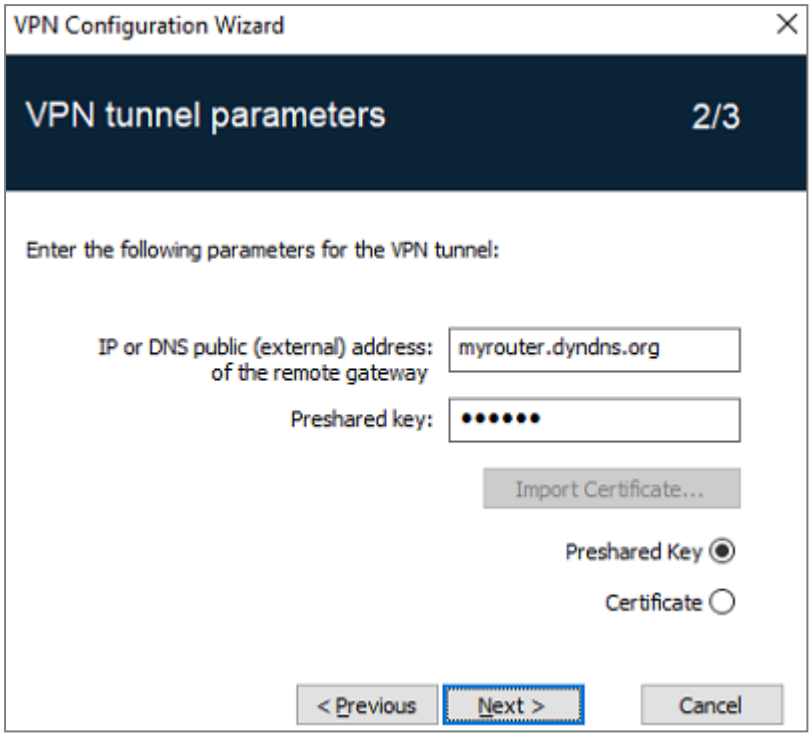


Étape 2

Pour un tunnel IPsec / IKEv2

Entrez les valeurs suivantes :

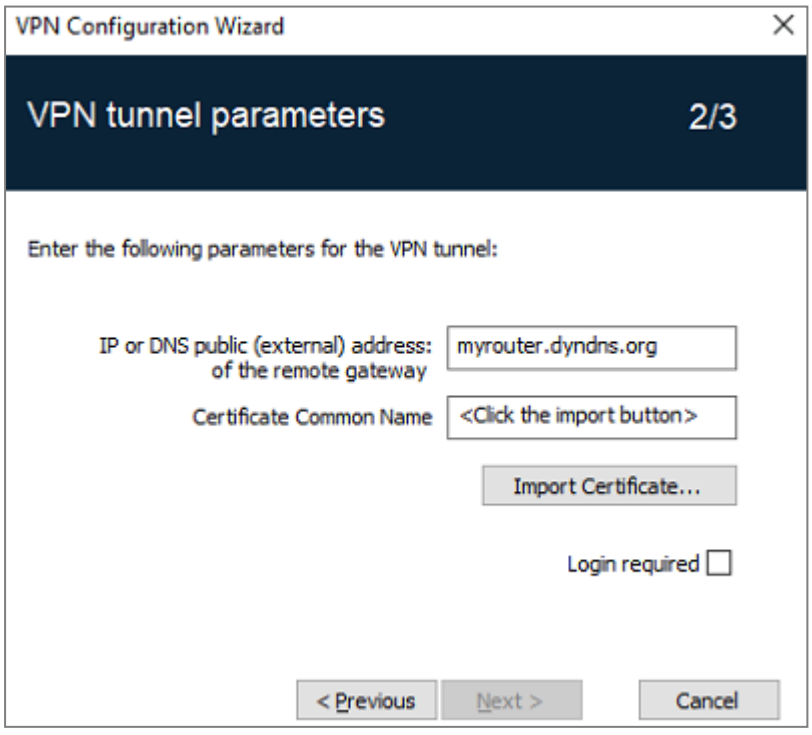
- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (exemple : myrouter.dyndns.org).
- Une clé partagée (« preshared key ») qui doit être configurée de façon identique sur la passerelle.
- OU : Un certificat qui doit être importé grâce au bouton **Importer un Certificat…** (voir section Importer un certificat dans la configuration VPN).



Pour un tunnel SSL (OpenVPN)

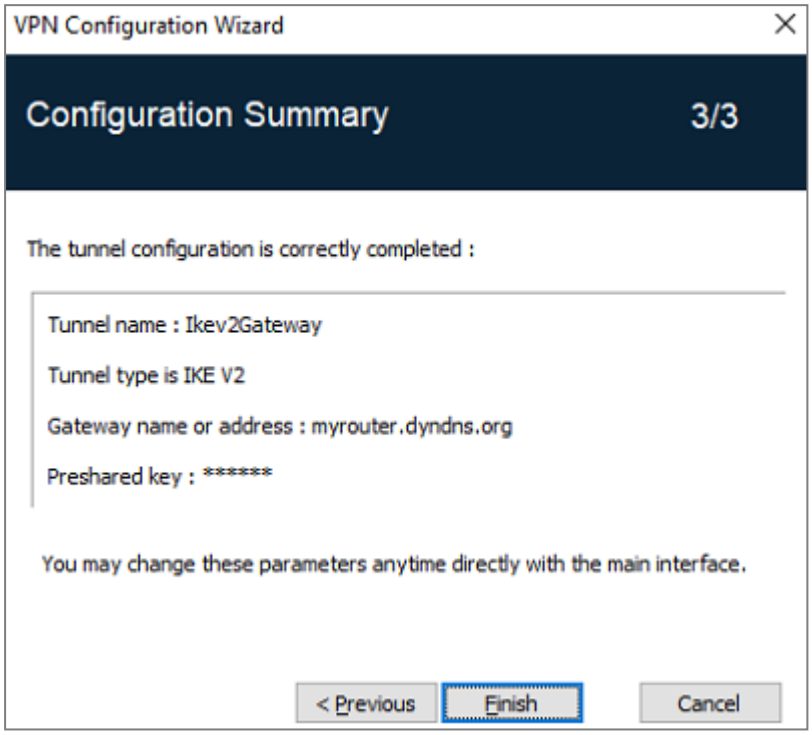
Entrez les valeurs suivantes :

- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (exemple : myrouter.dyndns.org).
- Un certificat qui doit être importé grâce au bouton **Importer un Certificat…** (voir section Importer un certificat dans la configuration VPN).



Étape 3

Vérifiez dans la fenêtre de résumé que la configuration est correcte, puis cliquez sur **Terminer**.

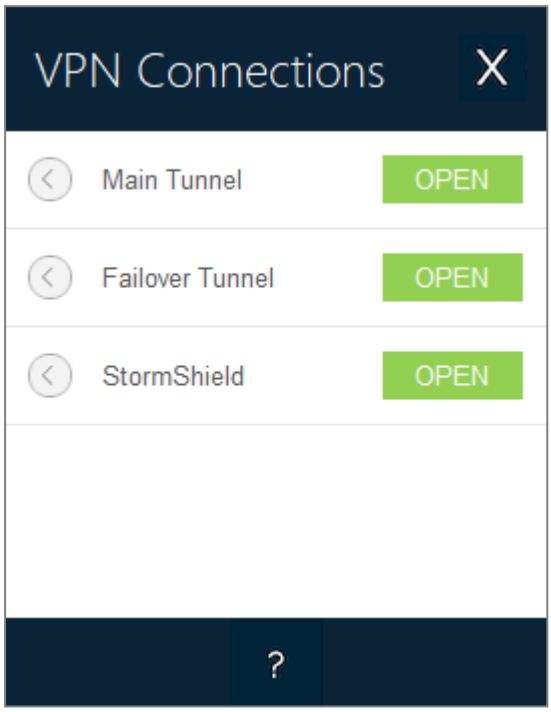


Le tunnel qui vient d'être configuré apparaît dans l'arborescence de la configuration VPN de l'interface principale.

Double-cliquez sur le tunnel pour l'ouvrir, ou affiner la configuration via les onglets de l'interface principale.

Panneau des Connexions

Le **Panneau des Connexions** permet d'ouvrir et de fermer simplement les connexions VPN configurées :



Le **Panneau des Connexions** est configurable. Il est possible de choisir les connexions VPN qui doivent y apparaître. Il est possible de renommer ces connexions VPN et de les ordonner.

Voir le chapitre Gestion du Panneau des Connexions.

Pour ouvrir une connexion VPN, cliquez sur le bouton **OUVRIR** associé.

Pour augmenter la hauteur de la fenêtre du **Panneau des Connexions** afin d'afficher plus de tunnels en même temps à l'écran, appuyez sur la touche Ctrl et la touche + du pavé numérique.

Pour réduire la hauteur de la fenêtre du **Panneau des Connexions**, appuyez sur la touche Ctrl et la touche - du pavé numérique.

L'icône à gauche de la connexion indique les différents états de cette connexion :

	Connexion fermée. Un clic sur cette icône ouvre la configuration VPN de la connexion dans le **Panneau de Configuration**. Attention : l'accès au **Panneau de Configuration** peut être restreint (cf. section Restreindre l'accès au Panneau de Configuration).
	Connexion en cours d'ouverture ou de fermeture.
	Connexion ouverte. Le trafic dans la connexion est représenté par une variation de l'intensité lumineuse du disque central.
	Connexion ayant eu un incident d'ouverture ou de fermeture. Un clic sur l'icône d'alerte ouvre une fenêtre popup qui fournit des informations détaillées ou complémentaires sur le problème rencontré.

Les boutons du **Panneau des Connexions** ont la fonction suivante :

	Ouvre la fenêtre **À propos...**.
	Ouvre le **Panneau de Configuration**. Attention : l'accès au **Panneau de Configuration** peut être restreint (cf. section Restreindre l'accès au Panneau de Configuration).
	Ferme le **Panneau des Connexions**.

Sur le **Panneau des Connexions**, les raccourcis clavier suivants sont disponibles :

Esc (ou Alt+F4)	Ferme le **Panneau des Connexions**.
Ctrl+Entrée	Ouvre le **Panneau de Configuration** (si activé).
Ctrl+O	Ouvre la connexion VPN sélectionnée.
Ctrl+W	Ferme la connexion VPN sélectionnée.
Flèches haut / bas	Déplace le curseur d'une connexion VPN à l'autre.

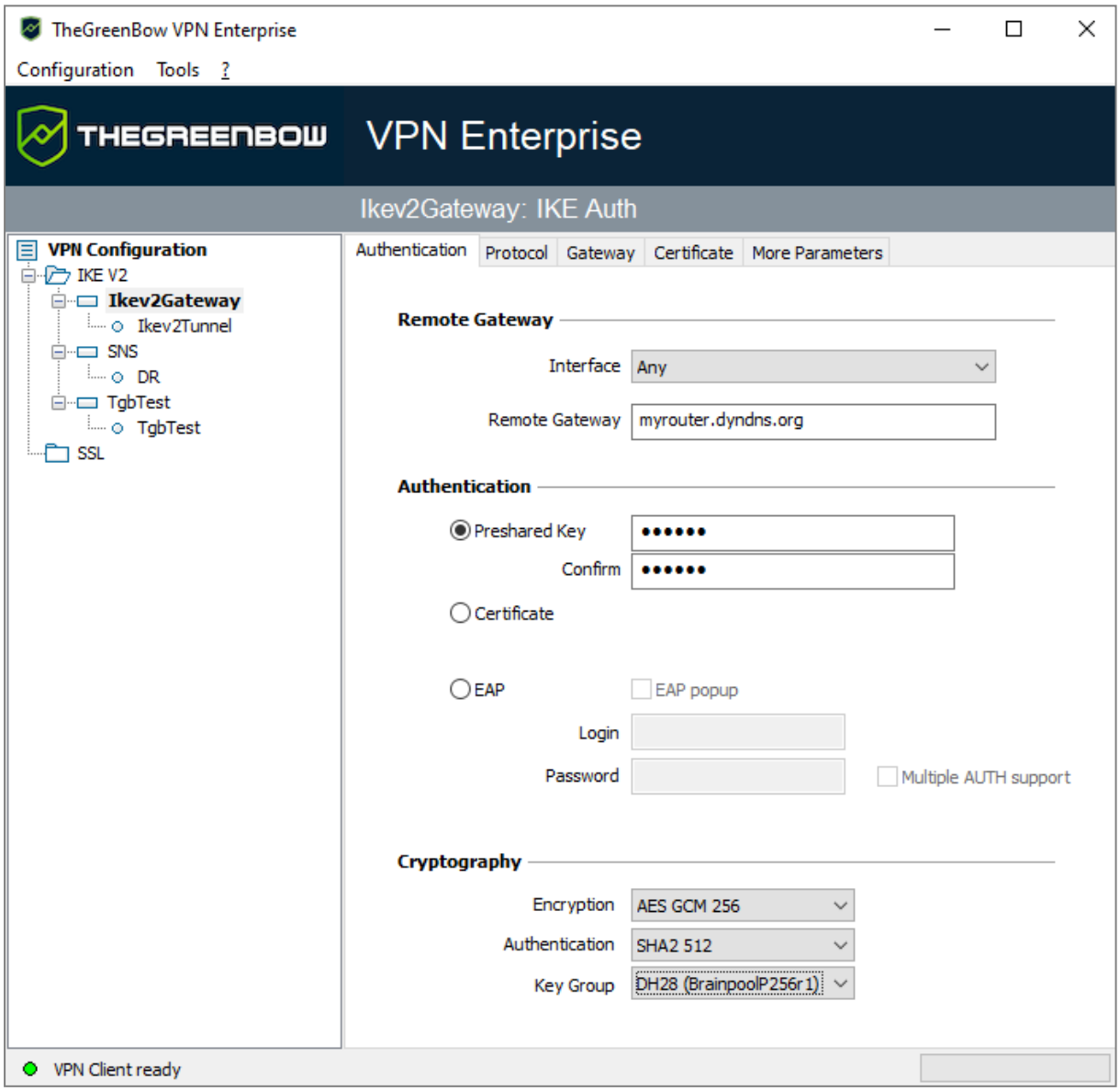
Panneau de Configuration

Le **Panneau de Configuration** est l'interface administrateur de SN VPN Client Exclusive.

Il n'est accessible que si le Client VPN a été lancé en tant qu'administrateur Windows (cf. paragraphe Démarrer le Client VPN en tant qu'administrateur à la section Démarrer le logiciel ci-dessus), ou pour n'importe quel utilisateur si l'option **Restreindre l'accès du panneau de configuration aux administrateurs** a été décochée (non recommandé).

Il est composé des éléments suivants :

- un ensemble de menus permettant la gestion du logiciel et des configurations VPN ;
- l'arborescence de la configuration VPN ;
- des onglets de configuration des tunnels VPN ;
- une barre d'état.



Menus

Les menus du **Panneau de Configuration** sont les suivants :

- Configuration
  - Sauver
  - Importer : Importation d'une configuration VPN
  - Exporter : Exportation d'une configuration VPN
  - Assistant de Configuration
  - Quitter : Fermer les tunnels VPN ouverts et quitter le logiciel
- Outils
  - Panneau des Connexions
  - Configuration des connexions
  - **Console** : Fenêtre de traces des connexions IKE
  - Reset IKE : Redémarrage du service IKE
  - Options : Options de protection, d'affichage, de démarrage, gestion de la langue, gestion des options PKI / IGC
- ?
  - Support Online : Accès au support en ligne
  - Mise à jour : Vérification de la disponibilité d'une mise à jour
  - Acheter une licence en ligne : Accès à la boutique en ligne
  - Assistant d'Activation…
  - À propos…

Barre d'état

La barre d'état en bas de l'interface principale fournit plusieurs informations :

- La « LED » à l'extrémité gauche est verte lorsque tous les services du logiciel sont opérationnels (service IKE).
- Le texte à gauche indique l'état du logiciel (**VPN prêt**, **Sauve configuration**, **Applique Configuration**, etc.).
- Lorsqu'il est activé, le mode traçant est identifié au milieu de la barre d'état.
- L'icône à sa gauche est une icône cliquable qui ouvre le dossier contenant les fichiers de logs générés par le mode traçant.
- La barre de progression à droite de la barre d'état identifie la progression de la sauvegarde d'une configuration.

Raccourcis

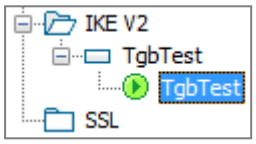
Ctrl+S	Sauvegarde de la configuration VPN
Ctrl+Entrée	Permet de basculer sur le **Panneau des Connexions**
Ctrl+D	Ouvre la fenêtre **Console** de logs VPN

Ctrl+Alt+R	Redémarrage du service IKE
Ctrl+Alt+T	Activation du mode traçant (génération de logs)

Arborescence de la configuration VPN

Utilisation

La partie gauche du **Panneau de Configuration** est la représentation sous forme d'arborescence de la configuration VPN. L'arborescence peut contenir un nombre illimité de tunnels.



Sous la racine « Configuration VPN », deux niveaux permettent de créer respectivement :

- des tunnels IPsec IKEv2, caractérisés par un IKE Auth et un Child SA, chaque IKE Auth pouvant contenir plusieurs Child SA ;
- des tunnels SSL / TLS.

Un clic sur IKE Auth, Child SA ou TLS ouvre dans la partie droite du **Panneau de Configuration** les onglets de configuration VPN associés. Voir dans les sections suivantes :

1. Tunnel IPsec IKEv2
   - IKEv2 (IKE Auth) : Authentification
   - IKEv2 (Child SA) : IPsec
2. Tunnel SSL (OpenVPN)
   - SSL : TLS

Une icône est associée à chaque tunnel (Child SA ou TLS). Cette icône identifie le statut du tunnel VPN :

	Tunnel fermé
	Tunnel en cours d'ouverture
	Tunnel ouvert
	Incident d'ouverture ou de fermeture du tunnel

En cliquant successivement deux fois – sans faire de double-clic - sur un élément de l'arborescence, il est possible d'éditer et de modifier le nom de cet élément.

Toute modification non sauvegardée de la configuration VPN est identifiée par le passage en caractères gras de l'élément modifié. L'arborescence repasse en caractères normaux dès qu'elle est enregistrée.

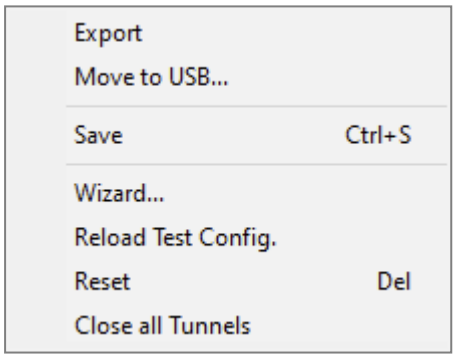
> **NOTE**
> Deux éléments de l'arborescence ne peuvent avoir le même nom. Si l'utilisateur saisit un nom déjà attribué, le logiciel l'en avertit.

Menus contextuels

Configuration VPN

Un clic droit sur la configuration VPN (racine de l'arborescence) affiche le menu contextuel suivant :

Export	Exporte la configuration VPN complète.
Sauver	Sauvegarde la configuration VPN.
Assistant de Configuration	Ouvre l'Assistant de Configuration VPN.
Recharger la configuration par défaut	Ce menu permet de la recharger à tout moment.
Reset	Remet à zéro la configuration VPN après confirmation par l'utilisateur.
Fermer tous les tunnels	Ferme tous les tunnels ouverts.



IKEv2, SSL

Un clic droit sur les éléments **IKEv2** ou **SSL** affiche le menu contextuel suivant, qui permet d'exporter, de sauvegarder, de créer ou de coller un IKE Auth / SSL :

Menu IKEv2

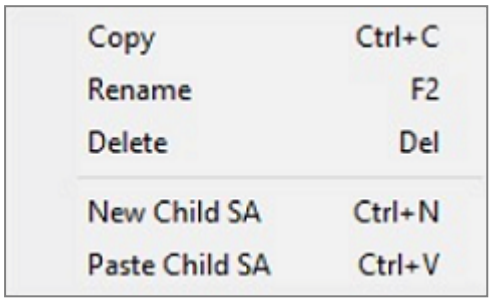
Menu SSL

Export	Exporte tous les tunnels IKEv2.
Sauver	Sauvegarde tous les tunnels IKEv2.
Nouvel IKE Auth **Nouveau TLS**	Crée un nouvel IKE Auth / TLS. Les paramètres de ce nouvel IKE Auth / TLS sont renseignés avec des valeurs par défaut.

Coller IKE Auth **Coller TLS**	Ajoute un IKE Auth / TLS copié précédemment dans le presse-papiers.

IKE Auth

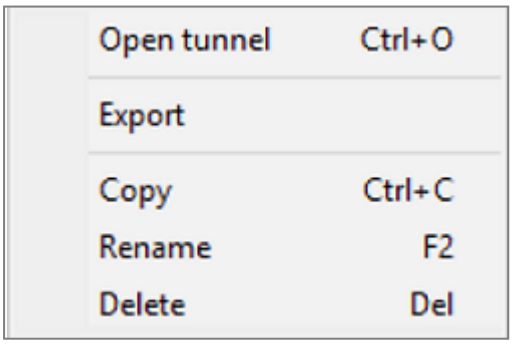
Un clic droit sur un IKE Auth affiche le menu contextuel suivant :



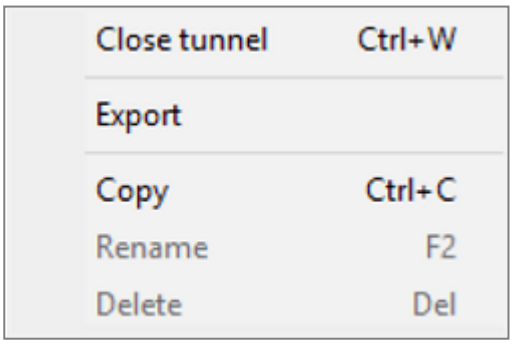
Copier	Copie l'IKE Auth sélectionné dans le presse-papier.
Renommer	Renomme l'IKE Auth. Ce menu est désactivé tant qu'un des tunnels de l'IKE Auth concerné est ouvert.
Supprimer	Supprime l'IKE Auth, y compris tous les Child SA associés, après confirmation par l'utilisateur. Ce menu est désactivé tant qu'un des tunnels de l'IKE Auth concerné est ouvert.
Nouveau Child SA	Ajoute un nouveau Child SA à l'IKE Auth sélectionné.
Coller Child SA	Ajoute à l'IKE Auth le Child SA copié dans le presse-papiers.

Child SA ou TLS

Un clic droit sur Child SA ou une TLS affiche le menu contextuel suivant :



Menu tunnel fermé



Menu tunnel ouvert

Ouvre Tunnel…	S'affiche si le tunnel VPN est fermé. Ouvre le tunnel (Child SA ou TLS) sélectionné.
Fermer le tunnel	S'affiche si le tunnel VPN est ouvert. Ferme le tunnel (Child SA ou TLS) sélectionné.

Export	Exporte le Child SA / TLS sélectionné. Cette fonction permet d'exporter le tunnel complet, c'est-à-dire le Child SA et son IKE Auth associé, ou le TLS, et de créer ainsi une configuration VPN mono-tunnel complètement opérationnelle (qui peut par exemple être importée en étant immédiatement fonctionnelle).
Copier	Copie le Child SA / TLS sélectionné.
Renommer	Renomme le Child SA /TLS sélectionné. Ce menu est désactivé tant que le tunnel est ouvert.
Supprimer	Supprime le Child SA / TLS sélectionné après confirmation par l'utilisateur. Ce menu est désactivé tant que le tunnel est ouvert.

Raccourcis

Pour la gestion de l'arborescence, les raccourcis suivants sont disponibles :

F2	Permet d'éditer le nom de la phase sélectionnée.
Del	Si une phase est sélectionnée, la supprime après confirmation de l'utilisateur. Si la configuration VPN est sélectionnée (racine de l'arborescence), propose l'effacement (reset) de la configuration complète.
Ctrl+O	Si un Child SA / TLS est sélectionné, ouvre le tunnel VPN correspondant.
Ctrl+W	Si un Child SA / TLS est sélectionné, ferme le tunnel VPN correspondant.
Ctrl+C	Copie la phase sélectionnée dans le presse-papiers.
Ctrl+V	Colle (ajoute) la phase copiée dans le presse-papiers.
Ctrl+N	Crée un nouvel IKE Auth, si la configuration VPN est sélectionnée, ou crée un nouveau Child SA / TLS pour l'IKE Auth sélectionné.
Ctrl+S	Sauvegarde la configuration VPN.

Panneau TrustedConnect

Introduction

Le **Panneau TrustedConnect** permet de garder en permanence une connexion sécurisée au réseau de confiance, grâce aux deux fonctionnalités suivantes :

- **TND (Trusted Network Detection)** : permet de déterminer si le poste est à l'intérieur du réseau de confiance en se basant sur des suffixes DNS et l'identification de balises.
- **Always-On** : assure le maintien de la sécurité de la connexion à chaque changement d'interface réseau, par exemple, entre Ethernet, Wi-Fi et 4G/5G.

NOTE
Depuis la version 7.5 de SN VPN Client Exclusive, le comportement du **Panneau TrustedConnect** s'adapte en fonction du niveau de conformité détecté par le Secure Connection Agent (SCA), qui détermine si un poste doit être autorisé à accéder au réseau de l'entreprise (voir la section Sélection du tunnel à ouvrir en fonction du niveau de conformité).

Interface

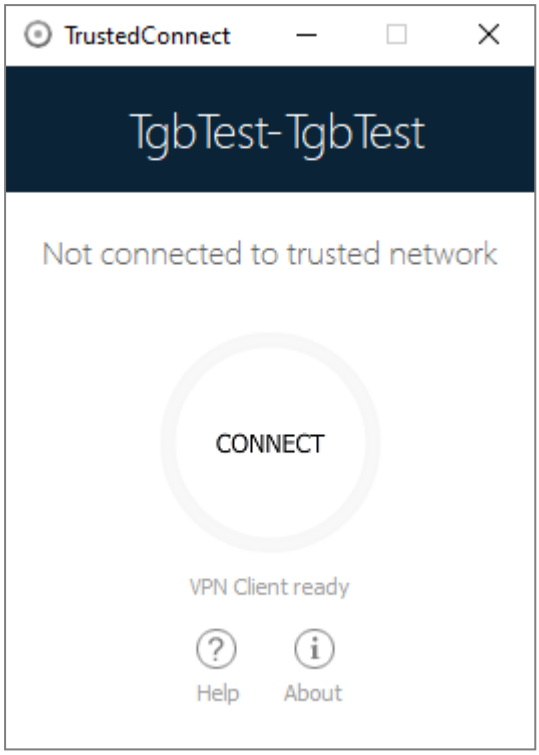
Lors de la première utilisation, le **Panneau TrustedConnect** est affiché au centre de l'écran.

Lors des utilisations suivantes, le **Panneau TrustedConnect** mémorise l'endroit où l'utilisateur l'aura déplacé.

L'interface du **Panneau TrustedConnect** est composée des éléments suivants :

- un titre qui identifie le nom de la connexion qui est gérée ;
- un texte d'information sur l'état de la connexion ;
- un bouton de connexion ;
- un texte qui indique dans quel état se trouve le logiciel et affiche éventuellement des codes d'erreur ;
- un bouton d'aide qui donne accès à un document d'aide pour l'utilisateur ;
- un bouton d'information qui affiche les principales informations du logiciel ;
- un jeu d'icônes dont la couleur représente l'état de la connexion.

NOTE
Depuis la version 7.4 de SN VPN Client Exclusive, vous pouvez activer une option permettant de sélectionner la connexion en cliquant sur le bandeau de titre (voir la section Choix de la connexion).



À tout moment, le **Panneau TrustedConnect** peut être minimisé soit en barre des tâches en cliquant sur le bouton **Minimiser** de la barre de titre, soit dans la zone de notification en cliquant sur le bouton **Fermer** de la barre de titre.

Réciproquement, le **Panneau TrustedConnect** peut être affiché à tout moment en cliquant sur l'icône **TrustedConnect** en barre des tâches ou en zone de notification.

Pour quitter le logiciel, cliquez avec le bouton droit de la souris sur l'icône **TrustedConnect** dans la zone de notification, puis sélectionnez **Quitter**.

NOTE
L'administrateur peut désactiver le bouton de déconnexion. Dans ce cas, il n'est plus possible de fermer un tunnel dès qu'il est ouvert. Pour plus de détails, voir la section Désactivation du bouton de déconnexion.

Icône en barre des tâches et codes couleurs

L'icône en barre des tâches de l'application du **Panneau TrustedConnect** est légèrement distincte de celle du **Panneau de Configuration** / **Panneau des Connexions** de SN VPN Client Exclusive.

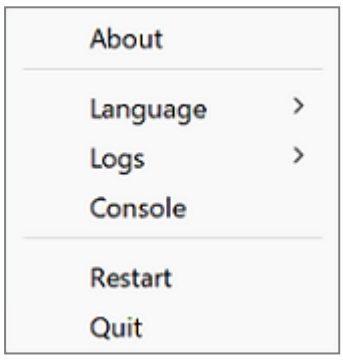
Signification des codes couleurs des différentes icônes du **Panneau TrustedConnect** :

	Cet état signifie que **Panneau TrustedConnect** ne gère aucune connexion sur le poste de travail. En général, cet état sera rencontré lorsque l'utilisateur demande explicitement la fermeture de sa connexion VPN.
	Cet état signifie que le poste de travail est connecté directement au réseau de l'entreprise, considéré comme réseau de confiance.

	Cet état signifie que le poste de travail est connecté au réseau de l'entreprise via une connexion VPN. Le poste de travail est donc physiquement sur un réseau non considéré de confiance.
	Cet état signifie que la connexion VPN n'a pas pu être établie.

Menu contextuel

Un clic droit sur l'icône du **Panneau TrustedConnect** en barre des tâches affiche le menu contextuel associé à l'icône :



Les options du menu contextuel sont les suivantes :

À propos…	Ouvre la fenêtre **À propos…** du logiciel.
Langue	Permet de basculer entre le français et l'anglais.
Journaux	Démarre la journalisation. Une fois la journalisation démarrée, deux options supplémentaires s'affichent pour afficher les journaux et arrêter la journalisation.
Console	Ouvre la fenêtre **Console** de logs VPN.
Redémarrer	Redémarre le tunnel.
Quitter	Ferme le tunnel VPN et quitte le logiciel.

NOTE
L'administrateur peut désactiver le menu ou une partie des options. Pour plus de détails, voir la section Suppression des éléments de menu.

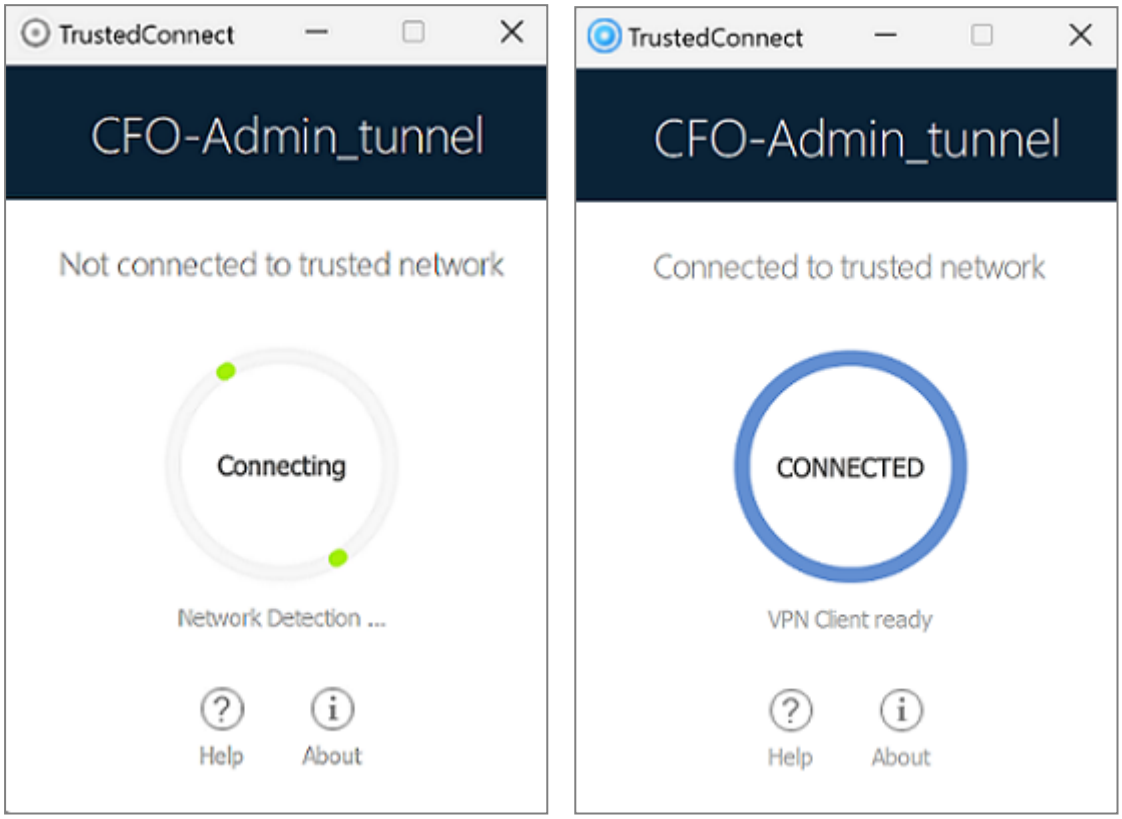
Utilisation

Deux cas d'usage existent selon que le poste est déjà connecté au réseau de l'entreprise ou non.

NOTE
Depuis la version 7.3 de SN VPN Client Exclusive, vous pouvez désactiver la fonction TND pour ouvrir un tunnel même lorsque le poste se trouve sur le réseau de confiance, reportez-vous à la section Désactivation de TND.

Poste connecté au réseau de l'entreprise

Le **Panneau TrustedConnect** passe dans l'état **CONNECTÉ** après avoir effectué la détection des réseaux de confiance :



Ensuite, la fenêtre du **Panneau TrustedConnect** se minimise automatiquement, en barre des tâches ou dans la zone de notification en fonction du comportement configuré par l'administrateur.

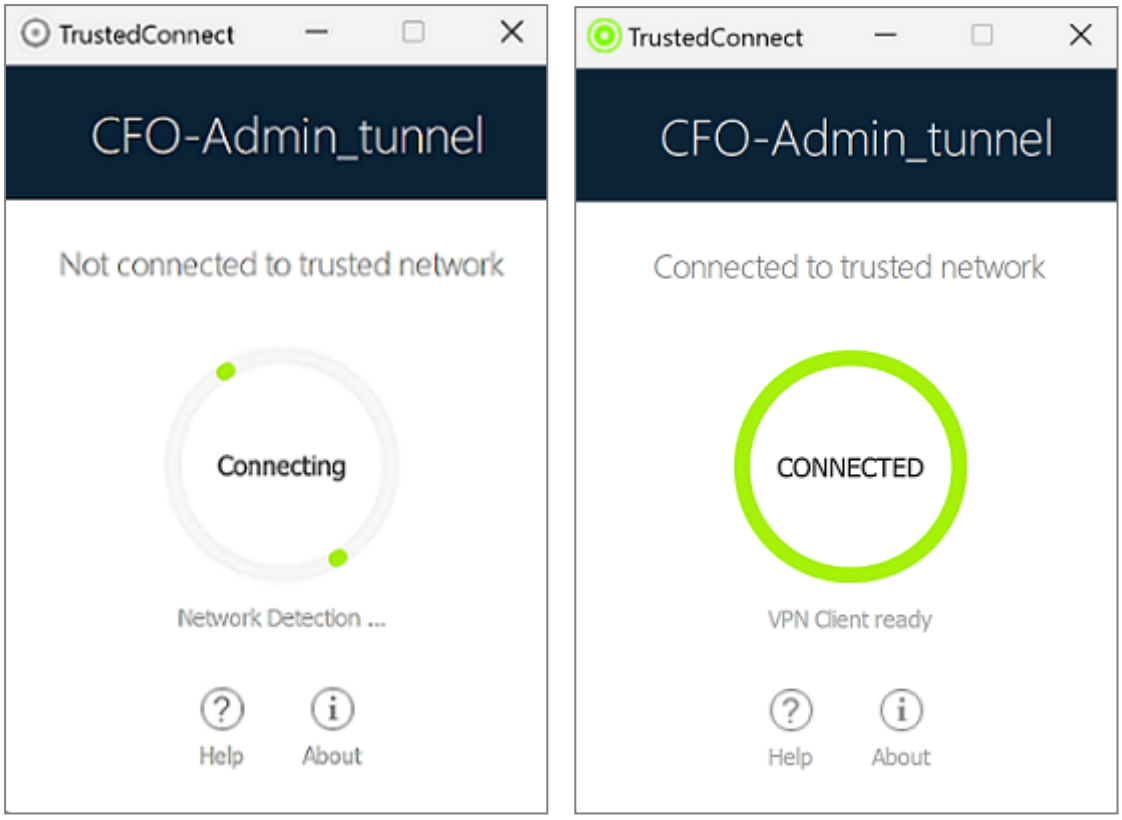
Voir le « Guide de déploiement ».

La fenêtre réapparait en sélectionnant l'application depuis la barre des tâches, et dans cet état, il n'y aucune action possible sur l'état de la connexion pour l'utilisateur.

Poste non connecté au réseau de l'entreprise

Lors du passage sur un réseau non considéré comme de confiance, le **Panneau TrustedConnect** va ouvrir automatiquement le tunnel VPN.

L'animation du bouton identifie la progression de l'établissement de la connexion, jusqu'à ce qu'elle soit établie.

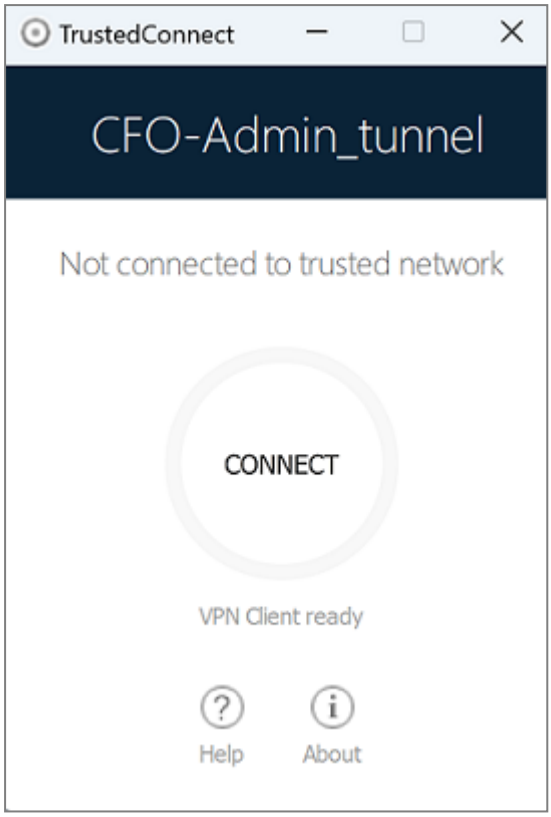


Lorsque la connexion est établie, la fenêtre du **Panneau TrustedConnect** se minimise automatiquement, en barre des tâches ou dans la zone de notification en fonction du comportement configuré par l'administrateur.

La connexion peut ne pas s'établir pour différentes raisons. Le texte d'information en dessous du bouton donne un premier niveau d'information. La section suivante détaille les cas de non-fonctionnement possibles.

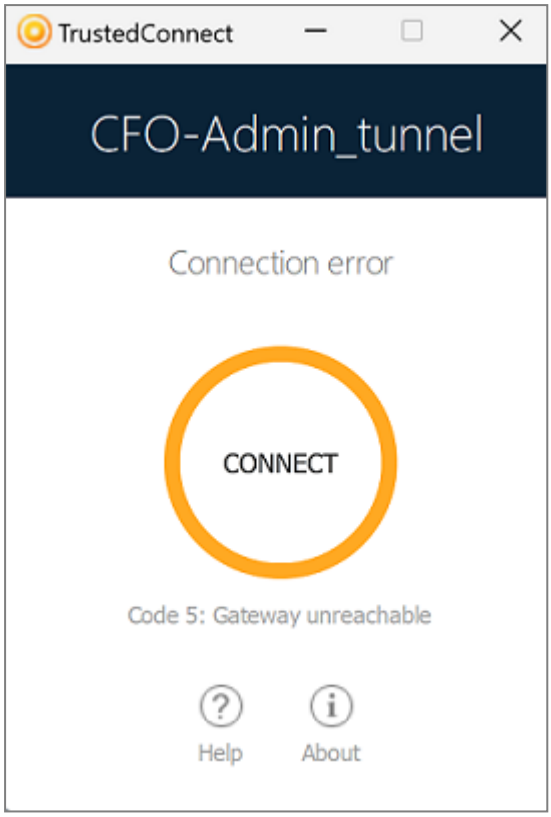
Quand le tunnel est monté et que le poste apparait comme étant sur le réseau de l'entreprise, vous pouvez cliquer à l'intérieur de l'anneau indicateur de l'état de connexion pour arrêter le tunnel.

L'application passe alors dans un état **Non connecté**, et il est possible d'appuyer sur le bouton pour ouvrir à nouveau le tunnel manuellement :



Cas d'erreur

Les principaux cas d'erreur sont identifiés sur l'interface du **Panneau TrustedConnect** par le bouton de connexion en couleur orange, par un code d'erreur et un texte succinct décrivant l'erreur.



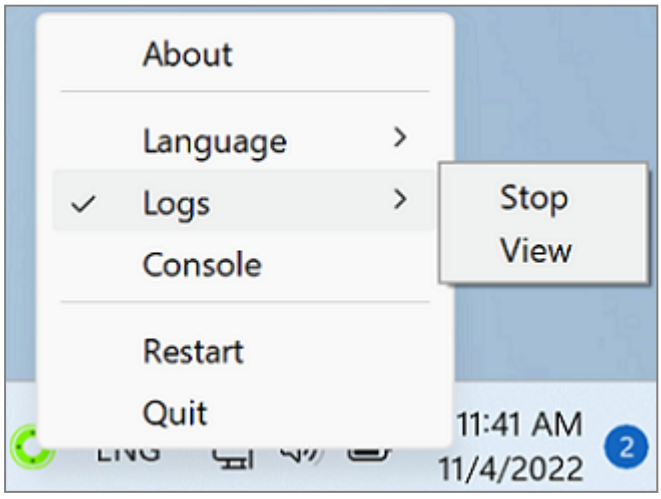
L'administrateur réseau peut être contacté pour résoudre le problème. En fonction du code d'erreur indiqué, il peut fournir des indications ou des explications sur le problème rencontré. Si l'administrateur demande des logs, reportez-vous à la procédure décrite dans la section suivante.

La liste des codes d'erreurs est fournie en annexe de ce document (cf. section Diagnostics du Panneau TrustedConnect).

Génération de journaux et Console

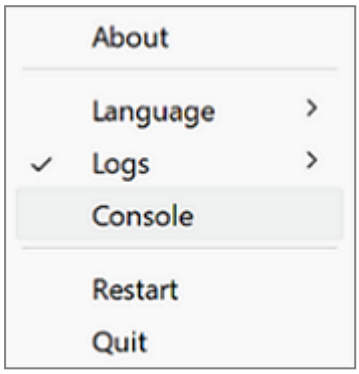
Le **Panneau TrustedConnect** permet de créer et de consulter des journaux.

Pour initier la création des journaux, depuis l'icône **TrustedConnect** de la zone de notification, sélectionner l'option **Journaux**, une coche à gauche de cette option indique ensuite que les journaux sont actifs :



Pour les consulter, aller dans le menu système et sélectionner l'option **Accéder aux journaux**. Une fenêtre avec le dossier des journaux apparait alors avec un certain nombre de fichiers. Ces fichiers peuvent être envoyés à l'administrateur en cas de problème.

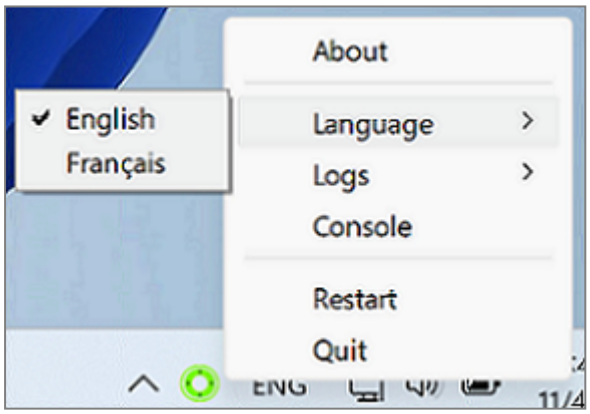
Vous pouvez désormais également afficher la **Console** de logs VPN à partir du menu contextuel du **Panneau TrustedConnect**.



Pour plus de détails sur le fonctionnement de la **Console**, reportez-vous à la section Console.

Sélection de la langue

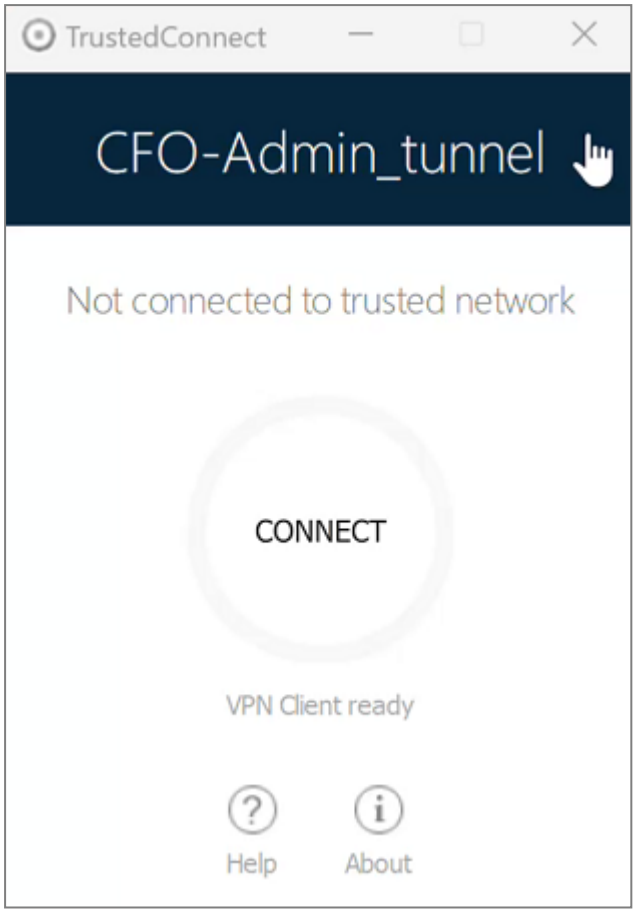
Le **Panneau TrustedConnect** permet de sélectionner la langue du logiciel : français ou anglais. Pour sélectionner la langue, aller dans le menu et sélectionner l'option **Langues**. Dans le sous-menu choisir **English** ou **Français** :



Choix de la connexion

Si vous avez activé cette option à l'aide de la propriété MSI `DIALERBEHAVIOR` lors de l'installation du Client VPN (cf. « Guide de déploiement »), à partir de la version 7.4 de SN VPN Client Exclusive, l'utilisateur peut choisir entre les connexions disponibles dans la configuration VPN, si elle en contient deux ou plus.

Lorsque l'option est activée, l'utilisateur voit le pointeur de la souris se transformer en main lorsqu'il le passe sur le nom de la connexion dans le bandeau de titre du **Panneau TrustedConnect** après avoir arrêté le tunnel.



IMPORTANT
Le pointeur en forme de main ne s'affiche pas et il n'est pas possible de changer de connexion active tant qu'une connexion est ouverte ou en cours d'initialisation ou de fermeture.

Pour changer de connexion, procédez comme suit :

1. Si le **Panneau TrustedConnect** n'est pas affiché à l'écran, cliquez sur son icône dans la barre des tâches pour l'afficher.
2. Si une connexion est en cours, cliquez sur le bouton **CONNECTÉ** pour fermer le tunnel. L'anneau indicateur de l'état de connexion devient gris et le libellé du bouton change en **CONNECTER**.
3. Cliquez sur le nom de la connexion dans le bandeau de titre bleu. Le nom de la connexion suivante disponible dans la configuration s'affiche. Continuez à cliquer pour faire défiler tous les noms des connexions disponibles dans la configuration jusqu'à atteindre celle que vous souhaitez activer.
4. Cliquez sur le bouton **CONNECTER**. Le client VPN tente d'établir la connexion. Lorsque la connexion a réussi, l'anneau indicateur de l'état de connexion devient vert et le libellé du bouton change en **CONNECTÉ**. Le **Panneau TrustedConnect** est ensuite minimisé dans la barre des tâches.

NOTE
Le **Panneau TrustedConnect** garde en mémoire la dernière connexion activée. Si vous quittez le **Panneau TrustedConnect**, celle-ci s'ouvre automatiquement lors du prochain lancement.

NOTE
Lorsque le **Panneau TrustedConnect** est configuré avec plusieurs connexions dont au moins une en mode GINA, il convient de tenir compte des précisions du paragraphe **Cas d'usage particulier** à la section Présentation.

Pour les cas d'erreur, reportez-vous à la section Cas d'erreur.

Limitations actuelles

Le **Panneau TrustedConnect** (lancé à partir de l'exécutable *VpnDialer.exe*) ne peut être lancé en même temps que le **Panneau de Configuration** ou le **Panneau des Connexions** (tous deux lancés à partir de l'exécutable *VpnConf.exe*, du raccourci sur le Bureau ou du menu **Démarrer** de Windows).

Lorsque *VpnConf.exe* est en cours d'exécution et que vous lancez *VpnDialer.exe*, tous les tunnels ouverts dans *VpnConf.exe* seront fermés et *VpnDialer.exe* (TrustedConnect) tentera de lancer automatiquement le tunnel configuré.

En revanche, lorsque *VpnDialer.exe* (TrustedConnect) est en cours d'exécution, il n'est pas possible de lancer *VpnConf.exe*. Vous devez d'abord quitter *VpnDialer.exe* avant de pouvoir lancer *VpnConf.exe*.

Le **Panneau TrustedConnect** (*VpnDialer.exe*) est actuellement uniquement disponible en français et en anglais.

Fenêtre « À propos… »

La fenêtre **À propos…** est accessible :

- par le menu **?** > **À propos…** du **Panneau de Configuration**,
- par le menu système du **Panneau de Configuration**,
- par le bouton **[?]** du **Panneau des Connexions**,
- par le bouton **[?]** du **Panneau TrustedConnect**.

La fenêtre **À propos…** donne les informations suivantes :

- le nom et la version du logiciel ;
- lorsque le logiciel est activé, le numéro de licence et l'adresse e-mail utilisés pour l'activation ;
- lorsque le logiciel est en période d'évaluation, le nombre de jours restants pour l'évaluation ;

- les versions de tous les composants du logiciel.

  Il est possible de sélectionner tout le contenu de la liste des versions (clic droit dans la liste et choisir **Tout sélectionner**), puis de le copier, par exemple pour transmettre l'information à des fins d'analyse. Lorsque la fenêtre **À propos…** est ouverte, si SN VPN Client Exclusive n'est pas activé, le logiciel tente de se connecter au serveur d'activation pour valider la licence.

Importer et exporter la configuration VPN

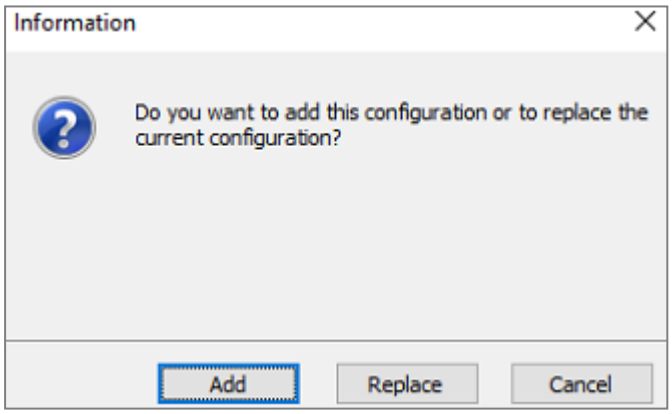
Importer une configuration VPN

SN VPN Client Exclusive permet d'importer une configuration VPN de différentes façons :

- par l'option **Importer** du menu **Configuration** > **Importer** du **Panneau de Configuration** (interface principale) ;
- par ligne de commande en utilisant l'option */import*. L'utilisation des options de ligne de commande du logiciel est détaillée dans le document « Guide de déploiement ». Y sont en particulier détaillées toutes les options disponibles pour l'importation d'une configuration VPN : */import*, */add*, */replace* ou */importonce*.

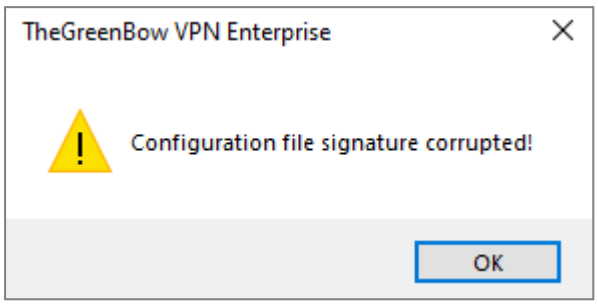
NOTE
Le SN VPN Client Exclusive peut gérer l'intégrité du fichier de configuration VPN (voir propriété MSI *SIGNFILE* dans le « Guide de déploiement »). Dans ce cas, une signature est générée lors de l'exportation et l'intégrité du fichier est vérifiée lors de l'importation.

Lors de l'importation d'une configuration VPN, il est demandé à l'utilisateur s'il veut ajouter la nouvelle configuration VPN à la configuration courante, ou s'il veut remplacer (écraser) la configuration courante par la nouvelle configuration VPN :

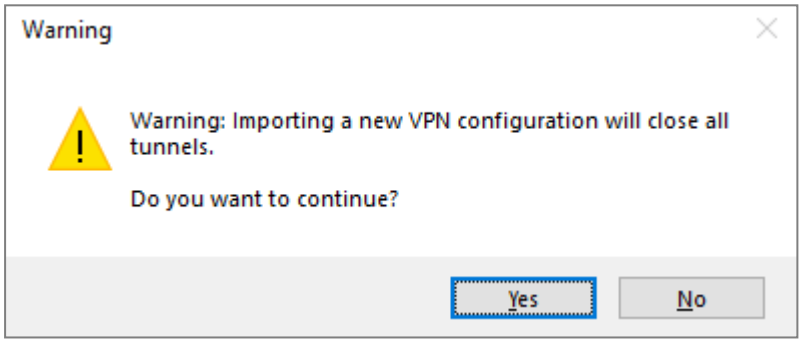


Si la configuration VPN importée a été exportée avec une protection par mot de passe (cf. section Exporter une configuration VPN), le mot de passe est demandé à l'utilisateur.

Si la configuration VPN a été exportée avec contrôle d'intégrité (cf. section Exporter une configuration VPN ci-dessous) et qu'elle a été corrompue, un message alerte l'utilisateur, et le logiciel n'importe pas la configuration.



Si un ou plusieurs tunnels sont ouverts au moment de l'importation, la fenêtre d'information suivante s'affiche pour vous indiquer que l'importation va fermer tous les tunnels :



Une fois ce message confirmé et l'importation effectuée, il conviendra de rouvrir les tunnels.

NOTE
Si des tunnels VPN ajoutés ont le même nom que des tunnels VPN de la configuration courante, ils sont automatiquement renommés au cours de l'importation (ajout d'un incrément entre parenthèse).

Exporter une configuration VPN

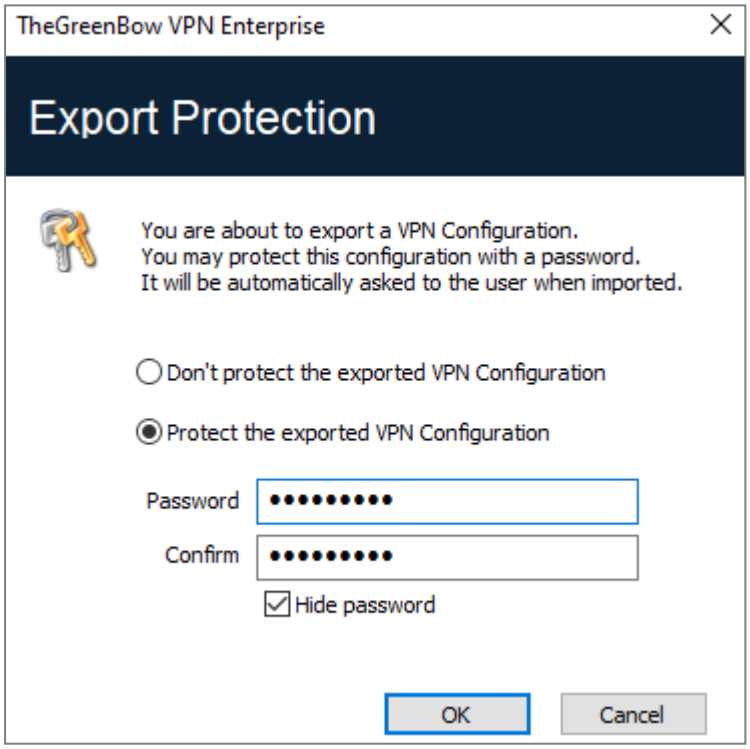
Le SN VPN Client Exclusive permet d'exporter une configuration VPN de différentes façons :

1. Menu **Configuration** > **Exporter** : la configuration VPN complète est exportée.
2. Menu contextuel associé à la racine de l'**arborescence de la configuration VPN** > **Export** : la configuration VPN complète est exportée.
3. Menu contextuel associé à un **IKE Auth** > **Export** : tout l'IKE Auth (incluant les Child SA qu'il contient) est exporté.
4. Menu contextuel associé à un **Child SA** > **Export** : le Child SA est exporté, avec l'IKE Auth auquel il est associé.
5. Menu Contextuel associé à un **TLS** > **Export** : le TLS est exporté.

6. Par ligne de commande en utilisant l'option */export*.
   L'utilisation des options de ligne de commande du logiciel est détaillée dans le document « Guide de déploiement ». Y sont en particulier détaillées toutes les options disponibles pour l'exportation d'une configuration VPN : */export* ou */exportonce*. Quelle que soit la méthode employée, l'opération d'exportation débute par le choix de la protection pour la configuration VPN exportée : elle peut être exportée protégée (chiffrée) par un mot de passe, ou exportée « en clair ». Quand il est configuré, le mot de passe est demandé à l'utilisateur au moment de l'importation

NOTE
Les fichiers de configuration VPN exportés portent par défaut l'extension *.tgb*.

NOTE
Qu'elle soit exportée chiffrée ou « en clair », la configuration VPN exportée peut être protégée en intégrité (comportement par défaut).
La protection en intégrité de la configuration VPN exportée est une fonction désactivable via une propriété de l'installeur MSI. Cette fonction est détaillée dans le « Guide de Déploiement ».



Il est recommandé de toujours exporter la configuration VPN protégée par un mot de passe (chiffrée).

NOTE
À partir de la version 7.3, le mot de passe doit suivre les recommandations de l'ANSSI, c'est-à-dire contenir au moins 16 caractères et utiliser un alphabet de 90 caractères, dont au moins une majuscule, une minuscule et un caractère spécial.

Lorsqu'une configuration VPN exportée est protégée en intégrité, et par la suite corrompue, un message d'alerte prévient l'utilisateur au moment de l'importation, et le logiciel n'importe pas cette configuration (cf. section Importer une configuration VPN ci-dessus).

Fusionner des configurations VPN

Il est possible de fusionner plusieurs configurations VPN en une seule, en important successivement les configurations VPN, et en choisissant **Ajouter** à chaque importation (cf. section Importer une configuration VPN ci-dessus).

Scinder une configuration VPN

En utilisant les différentes options d'exportation (exportation d'un IKE Auth / TLS avec tous les Child SA / TLS associés, ou exportation d'un tunnel simple), il est possible de scinder une configuration VPN en autant de « sous-configurations » que désiré (cf. section Exporter une configuration VPN ci-dessus).

Cette technique peut être utilisée pour déployer les configurations VPN d'un parc informatique : dériver d'une configuration VPN commune les configurations VPN associées chacune à un poste, avant de les diffuser à chaque utilisateur pour importation.

Configurer un tunnel VPN

VPN SSL ou IPsec IKEv2

SN VPN Client Exclusive permet de créer et de configurer plusieurs types de tunnels VPN.

Il permet aussi, le cas échéant, de les ouvrir simultanément.

SN VPN Client Exclusive permet de configurer des tunnels

- IPsec IKEv2
- SSL

La méthode pour créer un nouveau tunnel VPN est décrite dans les sections précédentes : Assistant de Configuration et Arborescence de la configuration VPN > Menus contextuels.

ASTUCE
Il est recommandé de configurer des tunnels IKEv2 avec certificat. Reportez-vous au chapitre Recommandations de sécurité.

Modification et sauvegarde de la configuration VPN

SN VPN Client Exclusive permet d'effectuer des modifications dans les tunnels VPN, et de tester « à la volée » ces modifications, ceci sans avoir besoin de sauvegarder la configuration VPN.

Toute modification dans la configuration VPN est illustrée dans l'arborescence par le passage en caractères gras du nom de l'élément modifié.

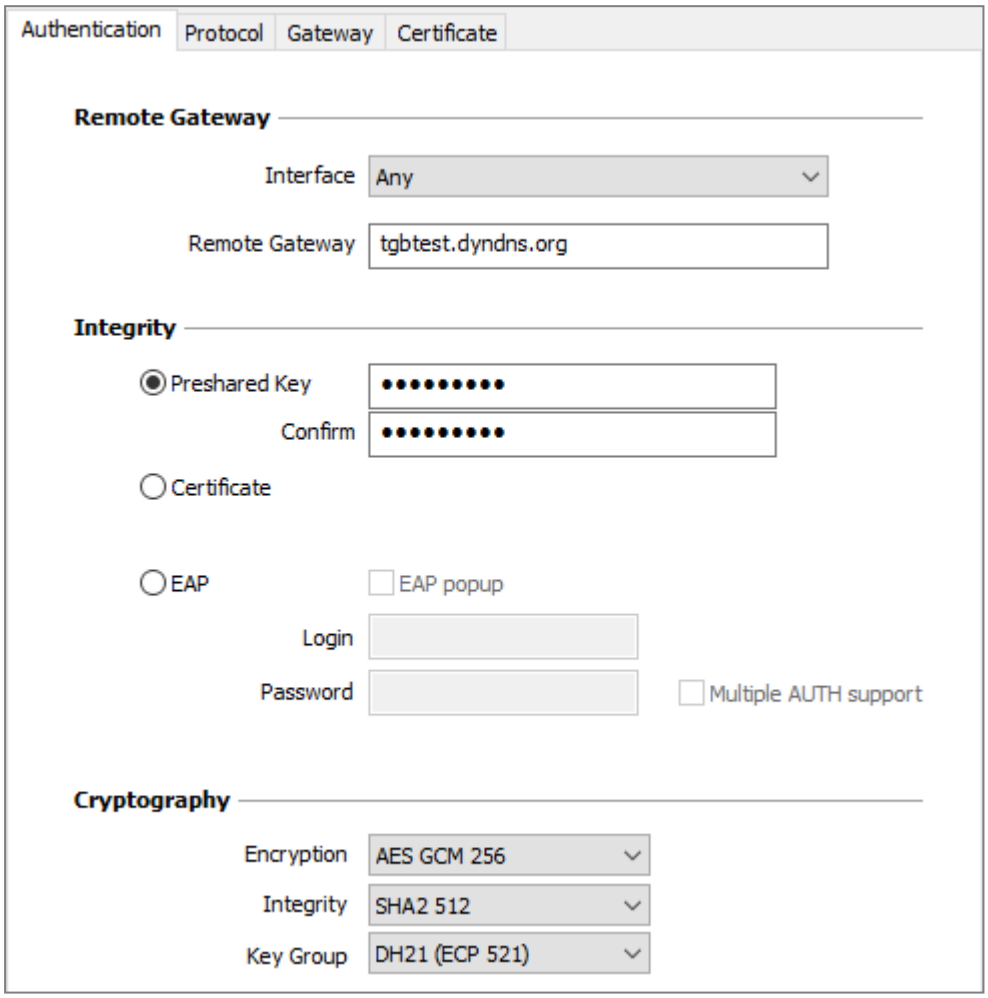
À tout moment, la configuration VPN peut être sauvegardée :

- par Ctrl+S,
- via le menu **Configuration** > **Sauver**.

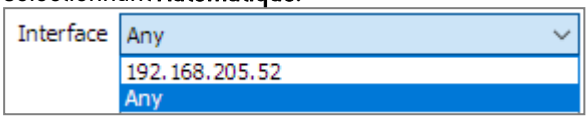
Si une configuration VPN est modifiée et que l'utilisateur quitte l'application sans l'avoir sauvegardée, il est alerté.

Configurer un tunnel IPsec IKEv2

IKE Auth : Authentification



Adresses

Interface	Nom de l'interface réseau sur laquelle la connexion VPN est ouverte. Il est possible de laisser au logiciel le soin de déterminer cette interface, en sélectionnant **Automatique**.  Privilégier ce choix lorsque le tunnel en cours de configuration est destiné à être déployé sur un autre poste par exemple. **NOTE** Lorsque l'interface réseau possède plusieurs adresses IP, vous pouvez spécifier l'adresse à l'aide du paramètre dynamique *local_subnet* (voir section Général, paragraphe Afficher plus de paramètres). Seules les adresses IPv4 sont prises en charge. Le format de l'adresse à renseigner comme valeur du paramètre dynamique est le suivant : *aaa.bbb.ccc.ddd/xx*. Si le masque de sous-réseau est omis en ne renseignant que *aaa.bbb.ccc.ddd*, l'adresse correspondra à *aaa.bbb.ccc.ddd/32*.
Adresse routeur distant	Adresse IP (IPv6 ou IPv4) ou adresse DNS de la passerelle VPN distante. Ce champ doit être obligatoirement renseigné.

Authentification

Clé partagée	Mot de passe ou clé partagée par la passerelle distante. **NOTE** La clé partagée (preshared key) est un moyen simple de configurer un tunnel VPN. Il apporte toutefois moins de souplesse dans la gestion de la sécurité que l'utilisation de certificats. Voir le chapitre Recommandations de sécurité.
Certificat	Utilisation d'un certificat pour l'authentification de la connexion VPN. **NOTE** L'utilisation de l'option **Certificat** apporte une plus grande sécurité dans la gestion des connexions VPN (authentification mutuelle, vérification des durées de vie, révocation, etc.). Voir le chapitre Recommandations de sécurité. Voir le chapitre dédié : Gestion des certificats.
EAP	Le mode EAP (Extensible Authentication Protocol) permet d'authentifier l'utilisateur grâce à un couple login/mot de passe. Quand le mode EAP est sélectionné, une fenêtre demande à l'utilisateur de saisir son login/mot de passe à chaque ouverture du tunnel. Lorsque le mode EAP est sélectionné, il est possible de choisir entre le fait que le login/mot de passe EAP soient demandés à chaque ouverture de tunnel (via la case **EAP popup**), ou qu'ils soient mémorisés dans la configuration VPN en les configurant dans les champs **Login** et **Mot de passe**. Ce dernier mode n'est pas recommandé (cf. chapitre Recommandations de sécurité).

Multiple AUTH Support	Active la combinaison des deux authentifications par certificat puis par EAP. Le Client VPN prend en charge la double authentification « certificat puis EAP ». Le Client VPN ne prend pas en charge la double authentification « EAP puis certificat ».

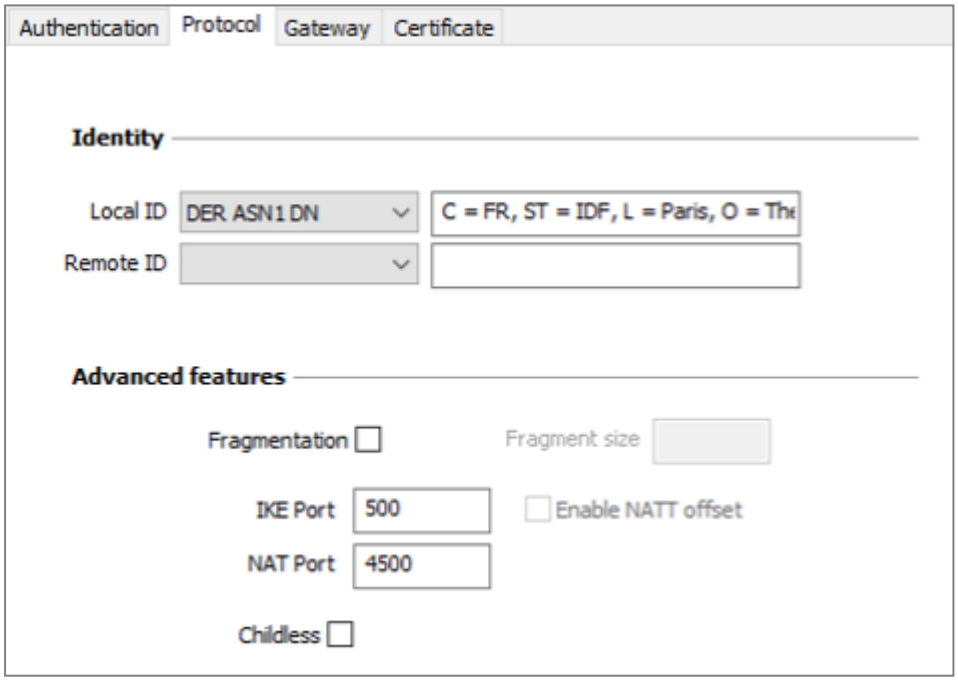
Cryptographie

Chiffrement	Algorithme de chiffrement négocié au cours de la phase d'authentification : Auto, AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Intégrité	Algorithme d'intégrité négocié au cours de la phase d'authentification : Auto, SHA2 256, SHA2 384, SHA2 512.
Groupe de clé	Longueur de la clé Diffie-Hellman : Auto, DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521) DH28 (BrainpoolP256r1).

Reportez-vous au chapitre Recommandations de sécurité pour le choix de l'algorithme.

Auto signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.

IKE Auth : Protocole



NOTE

Si vous utilisez une passerelle IPsec DR, il convient d'ajouter le paramètre dynamique *nonce_size* (voir section Afficher plus de paramètres) et de le définir à la valeur 16. En effet, ces passerelles ne prennent pas en charge de nonce avec une taille différente.

Identité

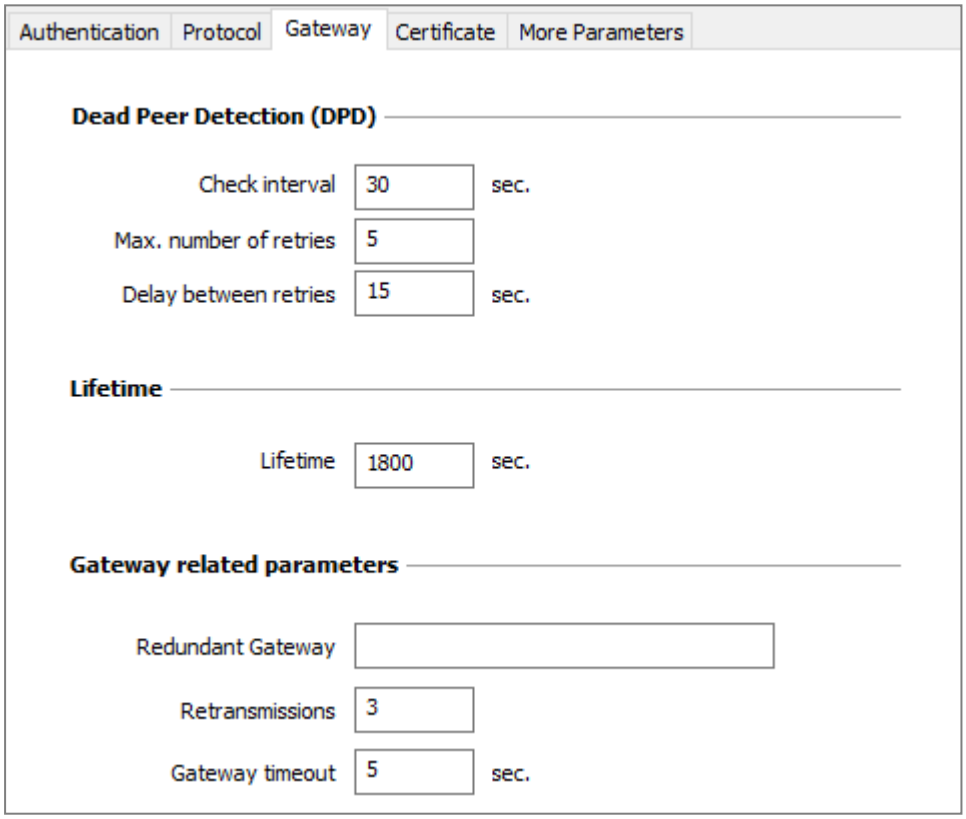
Local ID	Le « Local ID » est l'identifiant de la phase d'authentification que le Client VPN envoie à la passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : • Adresse IPv4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 195.100.205.101 • DNS : un nom de domaine (type = FQDN), p. ex. gw.mondomaine.net • KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123456 • Adresse IPv6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3 • Email : une adresse email (type = USER FQDN), • DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) ; ce champ est automatiquement renseigné avec le sujet d'un certificat X.509 lorsque le tunnel est associé à un certificat utilisateur (cf. chapitre Gestion des certificats) Quand ce paramètre n'est pas renseigné, c'est l'adresse IP du Client VPN qui est utilisée par défaut.
Remote ID	Le « Remote ID » est l'identifiant de la phase d'authentification que le Client VPN s'attend à recevoir de la passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : • Adresse IPv4 : une adresse IPv4 (type = IPV4 ADDR), p. ex. 80.2.3.4 • DNS : un nom de domaine (type = FQDN), p. ex. routeur.mondomaine.com • Email : une adresse email (type = USER FQDN), p. ex. admin@mondomaine.com • Adresse IPv6 : une adresse IPv6 (type = IPV6 ADDR), p. ex. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3 • DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) • KEY ID : une chaîne de caractères (type = KEY ID), p. ex. 123456

Fonctions avancées

Fragmentation IKEv2	Active la fragmentation des paquets IKEv2 conformément à la RFC 7383. Cette fonction permet d'éviter que les paquets IKEv2 ne soient fragmentés par le réseau IP traversé. En général, il convient de spécifier une taille de fragment inférieure de 200 octets à la MTU de l'interface physique, par exemple 1300 octets dans le cas d'une MTU classique de 1500 octets.
Port IKE	Les échanges IKE Init (pendant la phase d'authentification IKE) s'effectuent sur le protocole UDP, en utilisant par défaut le port 500. Le paramétrage du port IKE permet de passer les équipements réseau (pare-feux, routeurs) qui filtrent ce port 500. **NOTE** La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Auth sur un port différent de 500.

Port NAT	Les échanges IKE Auth, les échanges IKE Child SA et le trafic IPsec s'effectuent sur le protocole UDP, en utilisant par défaut le port 4500. Le paramétrage du port NAT permet de passer les équipements réseau (pare-feux, routeurs) qui filtrent ce port 4500. **NOTE** La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Child SA sur un port différent de 4500.
Activer l'offset NATT	Lorsque le port IKE est différent de 500, il peut être nécessaire de cocher cette option pour que la passerelle accepte la connexion.
Childless	Lorsque ce mode est activé, le Client VPN tentera d'effectuer l'initiation des échanges IKE sans création de Child SA, conformément au RFC 6023. Ce mode est recommandé.

IKE Auth : Passerelle



Dead Peer Detection (DPD)

Période de vérification	La fonction DPD (Dead Peer Detection) permet au Client VPN de détecter que la passerelle VPN devient inaccessible ou inactive. La période de vérification est la période entre deux envois de messages de vérification DPD, exprimée en secondes. La fonction de DPD est active à l'ouverture du tunnel (après la phase d'authentification). Associé à une passerelle redondante, le DPD permet au Client VPN de basculer automatiquement d'une passerelle à l'autre sur indisponibilité de l'une ou l'autre.
Nombre d'essais	Nombre d'essais infructueux consécutifs avant de déclarer que la passerelle VPN est injoignable.

Durée entre essais	Intervalle entre les messages DPD lorsqu'aucune réponse n'est reçue de la passerelle VPN, exprimé en secondes.

IMPORTANT
Lorsque la fonction DPD n'est pas opérationnelle après avoir monté un tunnel, une cause possible est que l'adresse IP de la passerelle appartient au réseau distant, soit en raison d'une configuration locale ou parce que cette adresse a été envoyée par la passerelle. Dans un tel cas, tous les paquets IKE à destination de la passerelle sont acheminés à travers le tunnel, au lieu d'être envoyés en dehors de celui-ci. C'est ce qui provoque le problème.
Il convient, par conséquent, de vérifier ce point et de le corriger, le cas échéant.

Durée de vie

Durée de vie	Durée de vie de la phase IKE Authentication. La durée de vie est exprimée en secondes. Sa valeur par défaut est de 14 400 secondes (4 h).

Paramètres relatifs à la passerelle

Passerelle redondante	Permet de définir l'adresse d'une passerelle VPN de secours sur laquelle le Client VPN bascule lorsque la passerelle VPN initiale est indisponible ou inaccessible. L'adresse de la passerelle VPN redondante peut être une adresse IP ou DNS. **IMPORTANT** La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction **Tunnel de repli**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé. Voir le chapitre Passerelle redondante.
Retransmissions	Nombre de retransmissions de messages protocolaires IKE avant échec.
Délai passerelle	Délai entre chaque retransmission.

IKE Auth : Certificat

Voir le chapitre : Gestion des certificats.

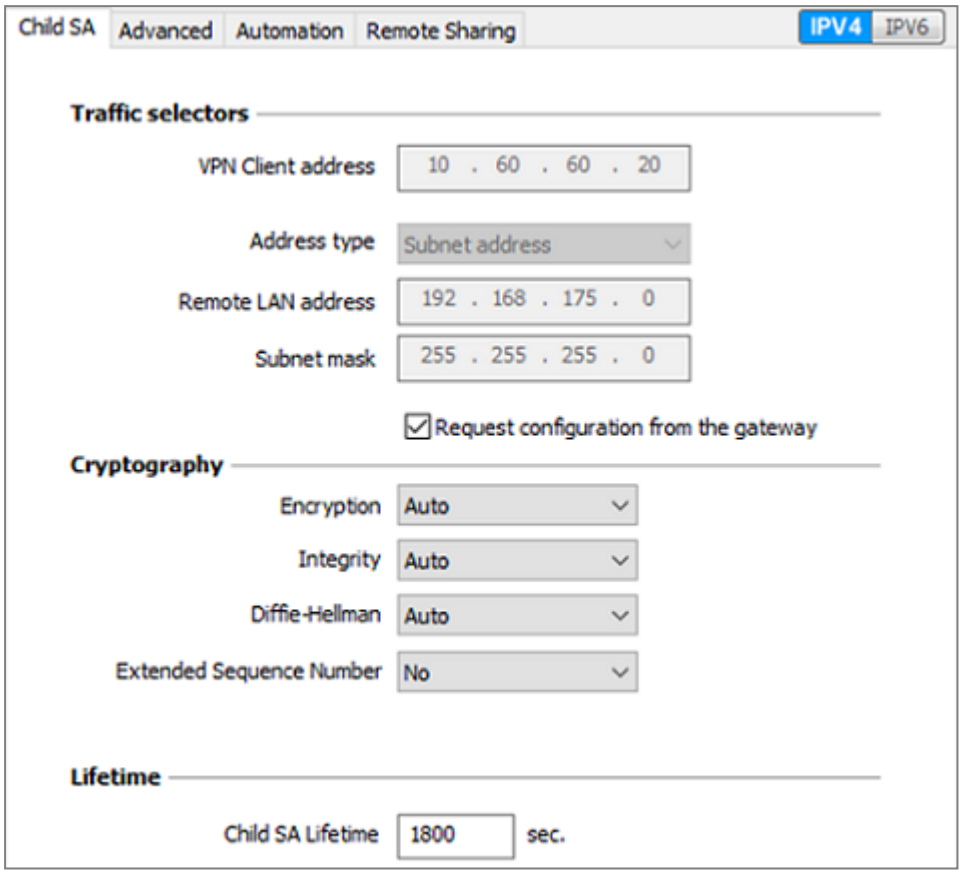
Child SA : Généralités

Le « Child SA » (Security Association IPsec) d'un tunnel VPN sert à la négociation des paramètres de sécurité qui seront appliqués aux données transmises dans le tunnel VPN.

Pour configurer les paramètres d'un Child SA, sélectionnez ce Child SA dans l'arborescence de la configuration VPN. Les paramètres se configurent dans les onglets de la partie droite du **Panneau de Configuration**.

Après modification, le tunnel concerné passe en caractères gras dans l'arborescence de la configuration VPN. Il n'est pas nécessaire de sauvegarder la configuration VPN pour que celle-ci soit prise en compte : le tunnel peut être testé immédiatement avec la configuration modifiée.

Child SA : Child SA



Trafic sélecteurs

Adresse du Client VPN	Adresse IP « virtuelle » du poste, tel qu'il sera « vu » sur le réseau distant. Techniquement, c'est l'adresse IP source des paquets IP transportés dans le tunnel IPsec. **NOTE** La taille par défaut du réseau local virtuel est 24. Pour utiliser un réseau local d'une autre taille (p. ex. 32), il convient d'ajouter le paramètre dynamique `local_virtual_network_size` défini à la valeur souhaitée (valeurs possibles : 1 à 32 ; voir section Afficher plus de paramètres).
Type d'adresse	L'extrémité du tunnel peut être un réseau ou un poste distant. Voir la section Configuration du type d'adresse ci-dessous.

Obtenir la configuration depuis la passerelle	Cette option (aussi appelée « Configuration Payload » ou encore « Mode CP ») permet au Client VPN de récupérer depuis la passerelle VPN toutes les informations utiles à la connexion VPN : adresse du Client VPN, adresse réseau distant, masque réseau et adresses DNS. Lorsque cette option est cochée, tous ces champs sont grisés (désactivés). Ils sont renseignés dynamiquement au cours de l'ouverture du tunnel, avec les valeurs envoyées par la passerelle VPN dans l'échange Mode CP. **NOTE** Le Mode CP permet à la passerelle de configurer jusqu'à 16 sous-réseaux. Dans ce cas, seul le premier sous-réseau sera renseigné dans la partie **Trafic Sélecteurs**. L'ensemble des sous-réseaux configurés par la passerelle sera renseigné dans la **Console**. **NOTE** Si plus de 16 sous-réseaux sont configurés par la passerelle, seuls les 16 premiers seront pris en compte.

Cryptographie

Chiffrement	Algorithme de chiffrement négocié au cours de la phase IPsec : Auto, AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Intégrité	Algorithme d'intégrité négocié au cours de la phase IPsec : Auto, SHA2 256, SHA2 384, SHA2 512.
Diffie-Hellman	Longueur de la clé Diffie-Hellman : Auto, DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521), DH28 (BrainpoolP256r1).
Extended Sequence Number	Permet l'usage de numéros de séquence étendus de taille 64 bits (cf. RFC 4304) : Auto, Non, Oui. Il est recommandé d'activer le mode ESN.

Reportez-vous au chapitre Recommandations de sécurité pour le choix de l'algorithme.

Auto signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle.

NOTE
Si l'adresse IP du poste Client VPN fait partie du plan d'adressage du réseau distant (p.ex. @IP poste = 192.168.10.2 et @réseau distant = 192.168.10.x), l'ouverture du tunnel empêche le poste de communiquer avec son réseau local. En effet, toutes les communications sont orientées dans le tunnel VPN.

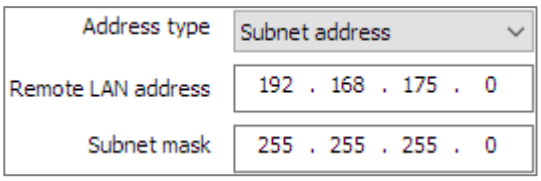
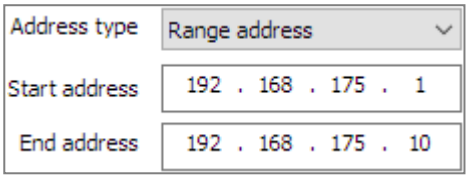
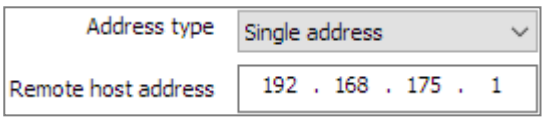
Durée de vie

Durée de vie Child SA	Durée en secondes entre deux renégociations. La valeur par défaut pour la durée de vie Child SA est de 1 800 s (30 min).

IPv4 / IPv6

IPv4 / IPv6	Voir le chapitre IPv4 et IPv6.

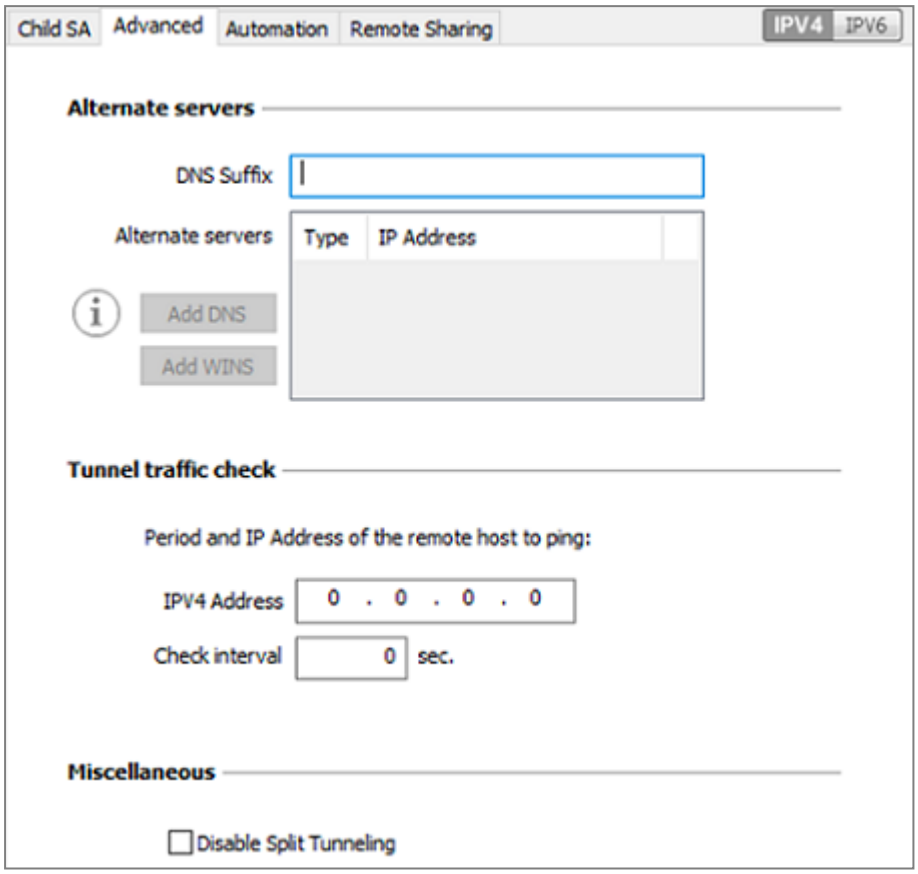
Configuration du type d'adresse

Si l'extrémité du tunnel est un réseau, choisir le type **Adresse réseau** puis définir l'**Adresse** et le **Masque du réseau distant** :	
Ou choisir **Plage d'adresses** et définir l'**Adresse de début** et l'**Adresse de fin** :	
Si l'extrémité du tunnel est un poste, choisir **Adresse Poste** et définir l'**Adresse du poste distant** :	

NOTES

- La fonction **Ouverture automatiquement sur détection de trafic** permet d'ouvrir automatiquement un tunnel sur détection de trafic vers l'une des adresses de la plage d'adresses spécifiée (moyennant le fait que cette plage d'adresses soit aussi autorisée dans la configuration de la passerelle VPN).
- **Configuration « tout le trafic dans le tunnel VPN »**
  Il est possible de configurer le Client VPN pour que l'intégralité du trafic sortant du poste passe dans le tunnel VPN. Pour réaliser cette fonction, sélectionnez le type d'adresse **Adresse réseau** et indiquer comme adresse et masque réseau 0.0.0.0.

Child SA : Avancé



Serveurs alternatifs

Suffixe DNS	Suffixe de domaine à ajouter à chaque nom de machine. Ce paramètre est optionnel. Lorsqu'il est spécifié, le Client VPN essaye de traduire l'adresse de la machine sans ajouter le suffixe DNS. Puis, si la traduction échoue, il ajoute le suffixe DNS et essaye à nouveau de traduire l'adresse.
Serveurs alternatifs	Table des adresses IP des serveurs DNS (2 maximum) et WINS (2 maximum) accessibles sur le réseau distant. Les adresses IP seront des adresses IPv4 ou IPv6 suivant le type de réseau choisi dans l'onglet **Child SA**. **NOTE** Si le Mode CP est activé (voir le paramètre **Obtenir la configuration depuis la passerelle** dans l'onglet **Child SA**), ces champs sont grisés (non disponibles à la saisie). Ils sont en effet automatiquement renseignés au cours de l'ouverture du tunnel, avec les valeurs envoyées par la passerelle VPN dans l'échange Mode CP.

Test de trafic dans le tunnel

Vérification trafic après ouverture	Il est possible de configurer le Client VPN pour vérifier régulièrement la connectivité au réseau distant. Si la connectivité est perdue, le Client VPN ferme automatiquement le tunnel puis tente de le rouvrir. Le champ **IPV4/IPV6** est l'adresse d'une machine située sur le réseau distant, censée répondre aux « ping » envoyés par le Client VPN. S'il n'y a pas de réponse au « ping », la connectivité est considérée comme perdue. **NOTE** Si le tunnel est configuré en IPv4 (bouton en haut à droite de l'onglet), c'est le champ IPv4 qui est présenté. Si le tunnel est configuré en IPv6, c'est le champ IPv6 qui est présenté.
Fréquence de test	Le champ **Fréquence de test** indique la période, exprimée en secondes, entre chaque « ping » émis par le Client VPN à destination de la machine dont l'adresse IP est spécifiée au-dessus.

Autres

Bloquer les flux non chiffrés	Lorsque cette option est cochée, seul le trafic passant dans le tunnel est autorisé. L'option de configuration **Bloquer les flux non chiffrés** accroît « l'étanchéité » du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction permet d'éviter les risques de flux entrants qui pourraient transiter hors du tunnel VPN. Associée à la configuration **Passer tout le trafic dans le tunnel** (voir la section Configuration du type d'adresse), cette option permet de garantir une étanchéité totale du poste, dès lors que le tunnel VPN est ouvert. Ce mode est recommandé.

Child SA : Automatisation

Voir le chapitre Automatisation.

Child SA : Bureau distant

Voir le chapitre Partage de bureau distant.

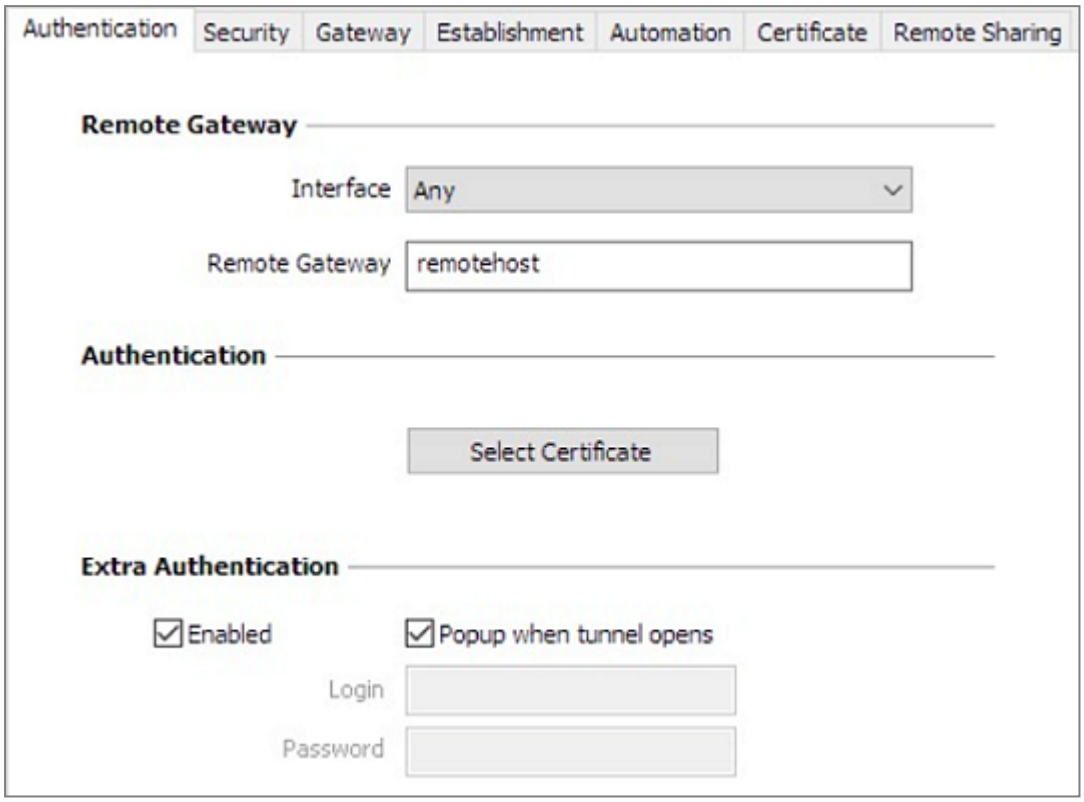
Configurer un tunnel SSL / OpenVPN

Introduction

SN VPN Client Exclusive permet d'ouvrir des tunnels VPN SSL.

Les tunnels VPN SSL de SN VPN Client Exclusive sont compatibles OpenVPN et permettent d'établir des connexions sécurisées avec toutes les passerelles qui implémentent ce protocole.

SSL : Authentification



Adresse routeur distant

Interface	Nom de l'interface réseau sur laquelle la connexion VPN est ouverte. Il est possible de laisser au logiciel le soin de déterminer cette interface, en sélectionnant **Automatique**.  Privilégier ce choix lorsque le tunnel en cours de configuration est destiné à être déployé sur un autre poste par exemple.
Adresse routeur distant	Adresse IP (IPv6 ou IPv4) ou adresse DNS de la passerelle VPN distante. Ce champ doit être obligatoirement renseigné.

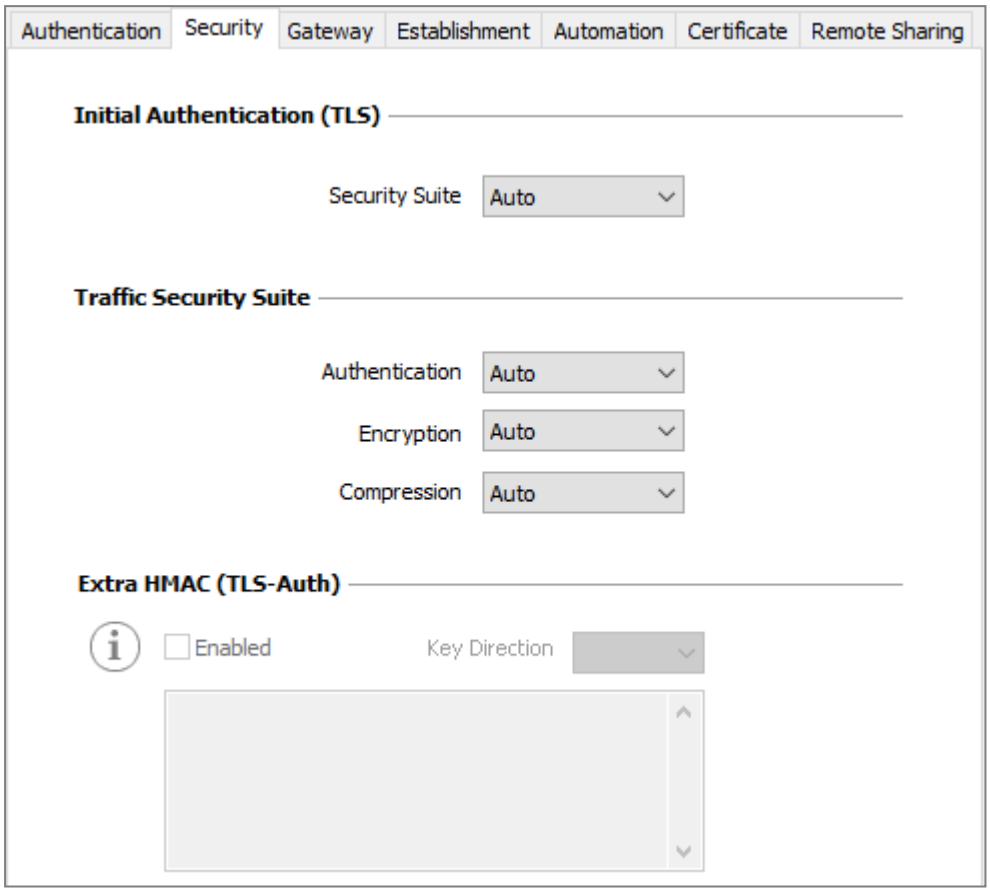
Authentification

Sélectionner un certificat	Sélection du Certificat pour l'authentification de la connexion VPN. Voir le chapitre dédié : Gestion des certificats.

Extra Authentification

Extra Authentification	Cette option apporte un niveau de sécurité supplémentaire en demandant à l'utilisateur la saisie d'un login / mot de passe à chaque ouverture du tunnel. Lorsque la case **Popup quand le tunnel s'ouvre** est cochée, le login et le mot de passe sera demandé à l'utilisateur à chaque ouverture du tunnel. Lorsqu'elle est décochée, le login et le mot de passe doivent être saisis ici de manière permanente. L'utilisateur n'aura alors pas besoin de les saisir à chaque ouverture du tunnel.

SSL : Sécurité



Authentification initiale (TLS)

Suite de Sécurité	Ce paramètre est utilisé pour configurer le niveau de sécurité de la phase d'authentification dans l'échange SSL. • **Automatique** : toutes les suites cryptographiques (sauf nulle) sont proposées à la passerelle qui décide de la meilleure suite à utiliser. • **TLS v1.2 — Medium** : seules les suites cryptographiques « moyennes » sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement de 128 bits. • **TLS v1.2 — High** : seules les suites cryptographiques fortes sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement supérieurs ou égaux à 128 bits. • **TLS v1.3** : suite TLS 1.3 négociée avec la passerelle, incluant : ◦ TLS_AES_128_GCM_SHA256 ◦ TLS_AES_256_GCM_SHA384 ◦ TLS_CHACHA20_POLY1305_SHA256 ◦ TLS_AES_128_CCM_SHA256 ◦ TLS_AES_128_CCM_8_SHA256 Pour plus d'informations : https://www.openssl.org/docs/man1.1.1/man1/ciphers.html

Suite de Sécurité pour le Trafic

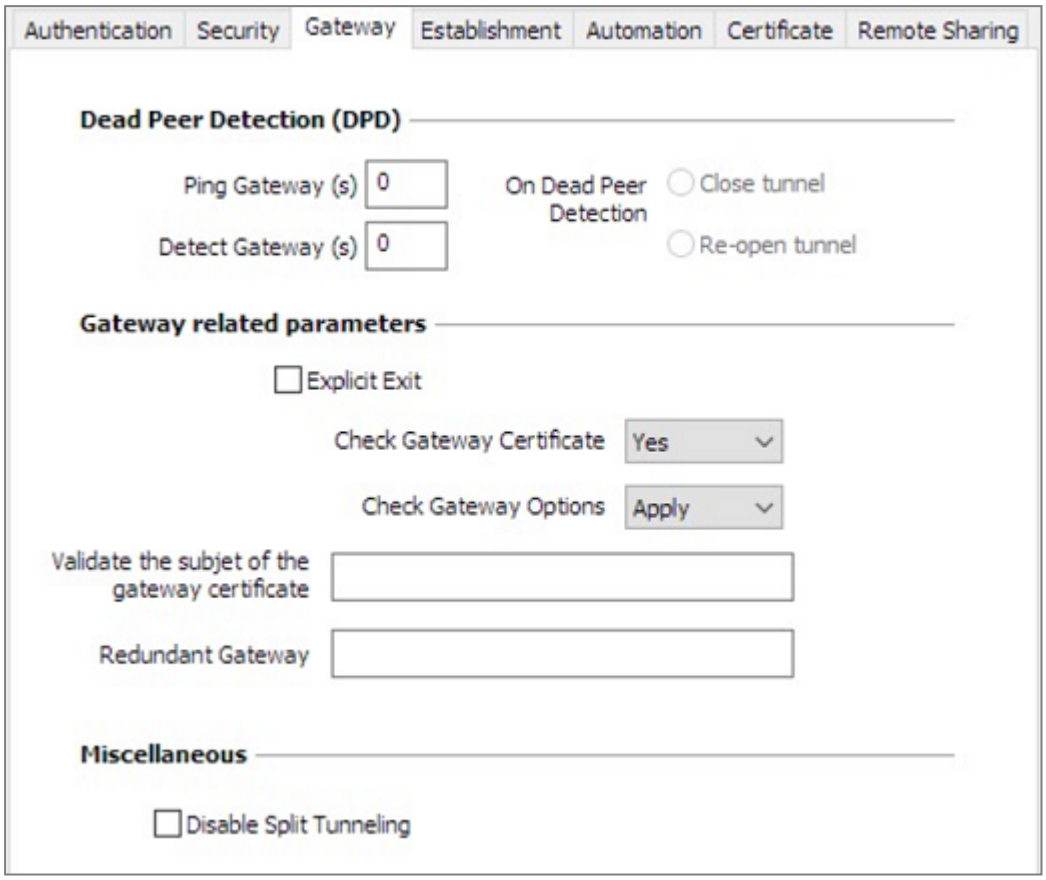
Authentification	Algorithme d'authentification négocié pour le trafic : Automatique, SHA-224, SHA-256, SHA-384, SHA-512. **NOTE** Si l'option **Extra HMAC** est activée (cf. ci-dessous), l'algorithme d'authentification ne peut être **Automatique**. Il doit être configuré explicitement, et doit être identique à celui choisi côté passerelle.
Chiffrement	Algorithme de chiffrement du trafic : Automatique, AES-128-CBC, AES-192-CBC, AES-256-CBC.
Compression	Compression du trafic : Auto, LZO, Non, LZ4.

Automatique signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle

Extra HMAC (TLS-Auth)

Extra HMAC	Cette option ajoute un niveau d'authentification aux paquets échangés entre le Client VPN et la passerelle VPN. Pour être opérationnelle, cette option doit aussi être configurée sur la passerelle (sur une passerelle, cette option est souvent appelée « TLS-Auth ») Quand cette option est sélectionnée, une clé doit être saisie dans le champ situé en dessous de la case cochée. Cette clé doit être saisie à l'identique sur la passerelle. C'est une suite de caractères hexadécimaux, dont le format est : *-----BEGIN Static key-----* *362722d4fbff4075853fbe6991689c36* *b371f99aa7df0852ec70352122aee7be* *…* *515354236503e382937d1b59618e5a4a* *cb488b5dd8ce9733055a3bdc17fb3d2d-----END Static key-----* La **Direction de la clé** doit être choisie : • **BiDir** : La clé spécifiée est utilisée dans les deux sens (mode par défaut). • **Client** : La direction de la clé à configurer sur la passerelle doit être **Serveur**. • **Serveur** : La direction de la clé à configurer sur la passerelle doit être **Client**.

SSL : Passerelle



Dead Peer Detection (DPD)

La fonction DPD (Dead Peer Detection) permet aux deux extrémités du tunnel de vérifier mutuellement leur présence.

La fonction de DPD est active une fois le tunnel ouvert. Associé à une passerelle redondante, le DPD permet au Client VPN de basculer automatiquement d'une passerelle à l'autre sur indisponibilité de l'une ou l'autre.

Ping passerelle (s)	Période exprimée en seconde d'envoi par le Client VPN d'un « ping » vers la passerelle. Cet envoi permet à la passerelle de déterminer que le Client VPN est toujours présent.
Détection de la passerelle (s)	Durée en secondes à l'issue de laquelle, si aucun « ping » n'a été reçu de la passerelle, celle-ci est considérée comme indisponible.
Sur détection d'inactivité	Lorsque la passerelle est détectée comme indisponible (c'est-à-dire à la fin de la durée **Détection de la passerelle**), le tunnel peut être fermé ou le Client VPN peut tenter de le rouvrir.

Paramètres relatifs à la passerelle

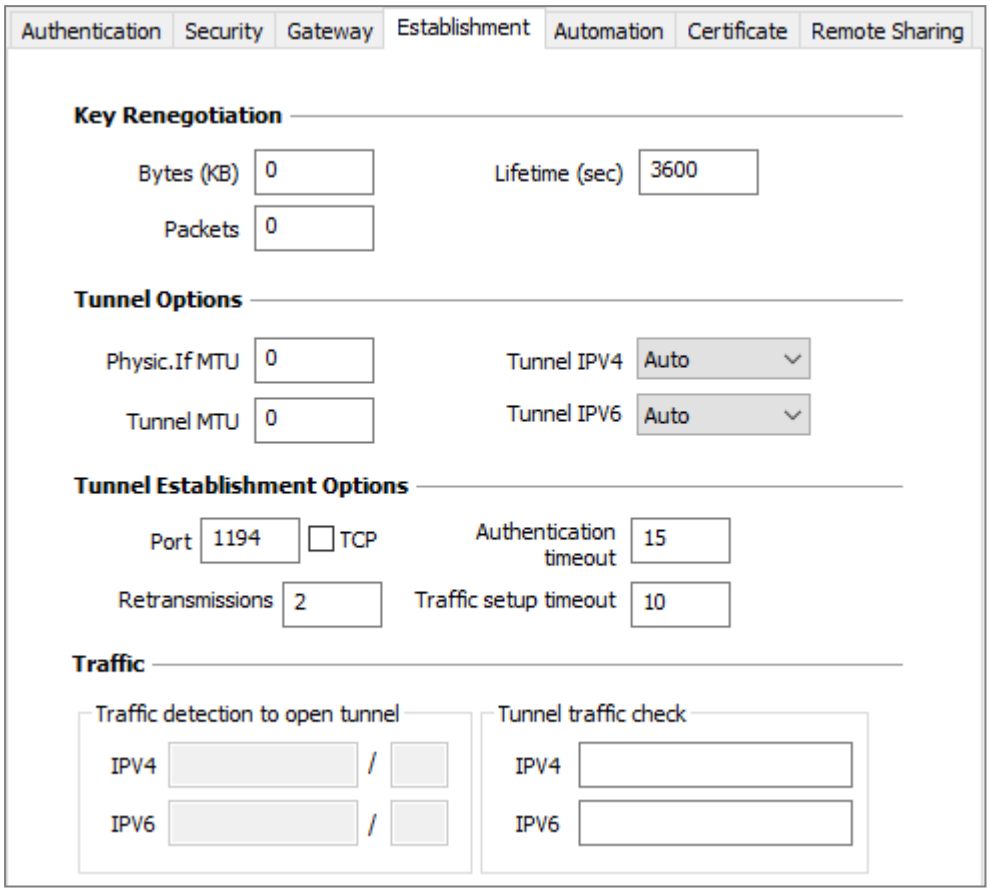
Explicit exit	Ce paramètre configure le Client VPN pour envoyer une trame spécifique de clôture du tunnel VPN à la passerelle, quand on ferme le tunnel. Si cette option n'est pas cochée, la passerelle utilise le DPD pour fermer le tunnel de son côté, ce qui est moins performant.

Vérification du certificat de la passerelle	Spécifie le niveau de contrôle appliqué au certificat de la passerelle. Dans la version actuelle, deux niveaux sont disponibles : • **Oui** (la validité du certificat est vérifiée) ; • **Non** (la validité du certificat n'est pas vérifiée). Le choix **Simple** est réservé pour un usage futur. Il est équivalent au choix **Oui** dans cette version. Si l'option **Vérifier la signature du certificat de la passerelle** est activée dans les **Options PKI** (cf. section Options PKI), la présente option de l'onglet **Passerelle** est grisée et le choix est fixé à **Oui**.
Vérification des options de la passerelle	Permet de définir le niveau de cohérence entre les paramètres du tunnel VPN et ceux de la passerelle (algorithmes de chiffrement, compression, etc.). • **Oui** : La cohérence est vérifiée sur l'ensemble des paramètres VPN. Le tunnel VPN ne peut s'ouvrir si un paramètre diffère. • **Non** : La cohérence n'est pas vérifiée avant ouverture du tunnel. Le tunnel VPN tente de s'ouvrir, quitte à ce qu'aucun trafic ne puisse passer parce que certains paramètres sont incohérents. • **Simple** : La cohérence entre le Client VPN et la passerelle n'est vérifiée que sur les paramètres essentiels. • **Appliquer** : Les paramètres de la passerelle sont appliqués.
Valider le sujet du certificat de la passerelle	Si ce champ est rempli, le Client VPN vérifie que le sujet du certificat reçu de la passerelle est bien celui spécifié.
Passerelle redondante	Définit l'adresse d'une passerelle VPN de secours sur laquelle le Client VPN bascule lorsque la passerelle VPN initiale est indisponible ou inaccessible. L'adresse de la passerelle VPN redondante peut être une adresse IP ou DNS. **IMPORTANT** La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction **Tunnel de repli**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé. Voir le chapitre Passerelle redondante.

Autres

Bloquer les flux non chiffrés	Lorsque cette option est cochée, seul le trafic passant dans le tunnel est autorisé. L'option de configuration **Bloquer les flux non chiffrés** accroît « l'étanchéité » du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction permet d'éviter les risques de flux entrants qui pourraient transiter hors du tunnel VPN.

SSL : Établissement



Renégociation des clés

Octets (Ko), Paquets, Durée de vie (sec)	Les clés peuvent être renégociées sur échéance de 3 critères (qui peuvent être combinés) : • Quantité de trafic, exprimée en Ko • Quantité de paquets, exprimée en nombre de paquets • Durée de vie, exprimée en seconde Si plusieurs critères sont configurés, les clés sont renégociées sur échéance du premier critère vérifié.

Options du tunnel

MTU interface physique	Taille maximale des paquets OpenVPN. Permet de spécifier une taille de paquet de telle sorte que les trames OpenVPN ne soient pas fragmentées au niveau réseau. Par défaut, la MTU spécifiée est à 0, ce qui signifie que le logiciel prend la valeur de la MTU de l'interface physique.
MTU du tunnel	MTU de l'interface virtuelle. Lorsqu'elles sont renseignées, il est recommandé de configurer une valeur pour la MTU du tunnel inférieure à celle de la MTU de l'interface physique. Par défaut, la MTU spécifiée est à 0, ce qui signifie que le logiciel prend la valeur de la MTU de l'interface physique.

Tunnel IPv4	Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv4 : • **Automatique** : Accepte ce qui est envoyé par la passerelle • **Oui** : Vérifie que ce qui est envoyé par la passerelle correspond au comportement configuré. Si ce n'est pas le cas, un message d'alerte est affiché dans la **Console** et le tunnel ne se monte pas. • **Non** : Ignore **NOTE** Vérifier que les deux choix **Tunnel IPv4** et **Tunnel IPv6** ne sont pas tous deux à **Non**.
Tunnel IPv6	Définit le comportement du Client VPN lorsqu'il reçoit de la part de la passerelle une configuration IPv6 : • **Automatique** : Accepte ce qui est envoyé par la passerelle • **Oui** : Vérifie que ce qui est envoyé par la passerelle correspond au comportement configuré. Si ce n'est pas le cas, un message d'alerte est affiché dans la **Console** et le tunnel ne se monte pas. • **Non** : Ignore **NOTE** Vérifier que les deux choix **Tunnel IPv4** et **Tunnel IPv6** ne sont pas tous deux à **Non**.

Option d'établissement de tunnel

Port / TCP	Numéro du port utilisé pour l'établissement du tunnel. Par défaut, le port est configuré à 1194. Par défaut, le tunnel utilise UDP. L'option **TCP** permet de transporter le tunnel sur TCP.
Timeout authentification	Délai d'établissement de la phase d'authentification au bout duquel on considère que le tunnel ne s'ouvrira pas. À échéance de ce timeout, le tunnel est fermé.
Retransmissions	Nombre de retransmission d'un message protocolaire. Sur absence de réponse au bout de ce nombre de retransmission du message, le tunnel est fermé.
Timeout d'init. du trafic	Phase d'établissement du tunnel : délai au bout duquel, si toutes les étapes n'ont pas été établies, le tunnel est fermé.

Trafic

Détection de trafic pour ouvrir le tunnel	Les caractéristiques du réseau distant ne sont pas configurées en OpenVPN (elles sont récupérées automatiquement dans l'échange d'ouverture du tunnel avec la passerelle). Pour mettre en œuvre la fonction de détection de trafic en OpenVPN, il est donc nécessaire de spécifier explicitement ces caractéristiques du réseau distant. C'est l'objet des champs **IPv4** et **IPv6**. Il n'est pas obligatoire de renseigner les deux champs. Le champ **IP** est une adresse de sous réseau, configurée sous forme d'une adresse IP et d'une longueur de préfixe. Exemple : IP = 192.168.1.0 / 24 : les 24 premiers bits de l'adresse IP sont pris en compte, soit le réseau : 192.168.1.x **NOTE** Ces paramètres sont liés à la fonction de détection de trafic. Pour que les champs IPv4 et IPv6 soient activés, la case **Ouvrir automatiquement sur détection de trafic** de l'onglet Automatisation doit être cochée.
Test de trafic dans le tunnel	Si ces champs sont renseignés, le Client VPN tente de faire un « ping » sur ces adresses après ouverture du tunnel VPN. L'état de la connexion (réponse au ping ou absence de réponse au ping) est affiché dans la **Console**. Il n'est pas obligatoire de renseigner les deux champs. **NOTE** Aucune action particulière n'est faite s'il n'y a pas de réponse au « ping ».

SSL : Automatisation

Voir le chapitre Automatisation.

SSL : Certificat

Voir le chapitre Gestion des certificats.

SSL : Bureau distant

Voir le chapitre Partage de bureau distant.

Passerelle redondante

SN VPN Client Exclusive permet la gestion d'une passerelle VPN redondante.

Associée au paramétrage du DPD (Dead Peer Detection), cette fonction permet au Client VPN de basculer automatiquement sur la passerelle redondante dès que la passerelle principale est détectée comme étant injoignable ou indisponible.

En effet, sur perte d'un pair, si une passerelle redondante est configurée, le tunnel tente de se rouvrir automatiquement. Il est possible de configurer une passerelle redondante identique à la passerelle principale pour profiter de ce mode de réouverture automatique sans avoir réellement deux passerelles.

L'algorithme de prise en compte de la passerelle redondante est le suivant :

- Le Client VPN contacte la passerelle initiale pour ouvrir le tunnel VPN.
- Si le tunnel ne peut être ouvert au bout de N tentatives, le Client VPN contacte la passerelle redondante.

Le même algorithme s'applique à la passerelle redondante :

- Si la passerelle redondante est indisponible, le Client VPN tente d'ouvrir le tunnel VPN avec la passerelle initiale.

NOTES

- Le Client VPN n'essaye pas de contacter la passerelle redondante si la passerelle initiale est accessible mais qu'il y a des incidents d'ouverture du tunnel.
- Le Client VPN n'essaye pas de contacter la passerelle redondante si la passerelle initiale est inaccessible à cause d'un problème de résolution DNS.

IMPORTANT

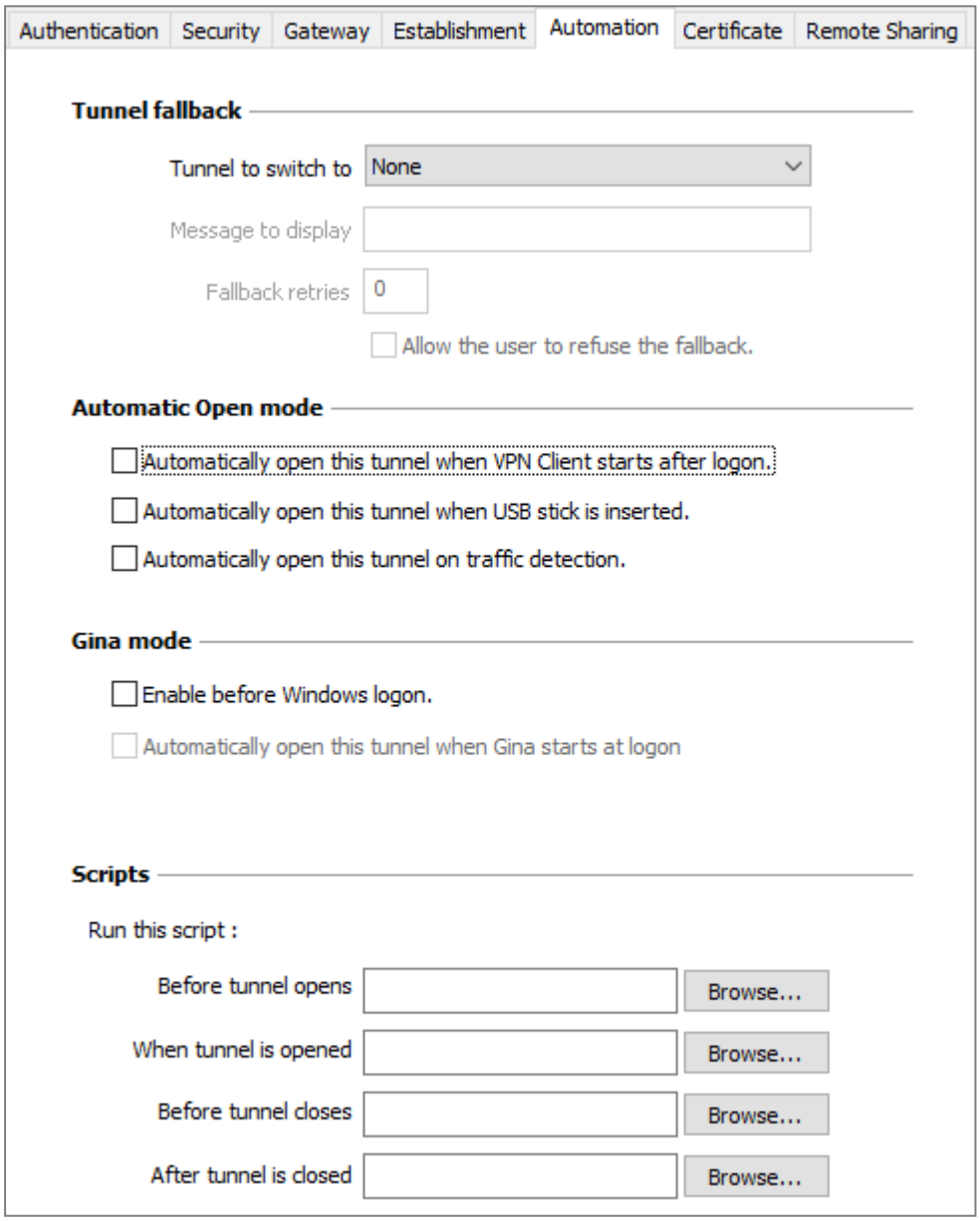
La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction **Tunnel de repli**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé.

Automatisation

SN VPN Client Exclusive permet d'associer des automatismes à chaque tunnel VPN : bascule vers un tunnel de repli (fallback tunnel), ouverture automatique du tunnel suivant différents critères, exécution de batches ou de scripts à différentes étapes de l'ouverture ou de la fermeture du tunnel, etc.

Ces automatismes sont disponibles pour tout type de tunnel : IKEv2 et SSL.

Pour chaque type de tunnel, le paramétrage des automatisations s'effectue dans l'onglet **Automatisation** du tunnel : Child SA (IKEv2) ou TLS (SSL).



Tunnel de repli (fallback)

IMPORTANT
La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction

Tunnel de repli. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé.

Voir le chapitre Tunnel de repli.

Mode d'ouverture automatique

Ouvrir automatiquement ce tunnel lorsque le Client VPN démarre	Le tunnel s'ouvre automatiquement au démarrage du Client VPN
Ouvrir automatiquement ce tunnel lorsqu'une clé USB est insérée	Si le tunnel est configuré avec un certificat contenu sur une carte à puce ou un token, il est ouvert automatiquement sur insertion de cette carte à puce ou token.
Ouvrir automatiquement ce tunnel sur détection de trafic	Le tunnel s'ouvre automatiquement sur détection de trafic à destination d'une adresse IP faisant partie du réseau distant.

Mode GINA

Peut être ouvert avant le logon Windows	Cette option indique que la connexion VPN peut être ouverte avant l'ouverture de session Windows : elle apparaît dans la fenêtre des connexions GINA (voir le chapitre Mode GINA ci-dessous).
Ouvrir automatiquement le tunnel par la Gina au logon	Quand cette option est cochée, le tunnel s'ouvre automatiquement avant l'ouverture de session Windows. Cette option est active si l'option **Peut être ouvert avant le logon Windows** est sélectionnée.

Scripts

Avant ouverture du tunnel	La ligne de commande spécifiée est exécutée avant que le tunnel ne s'ouvre.
Après ouverture du tunnel	La ligne de commande spécifiée est exécutée dès que le tunnel est ouvert.
Avant fermeture du tunnel	La ligne de commande spécifiée est exécutée avant que le tunnel ne se ferme.
Après fermeture du tunnel	La ligne de commande est exécutée dès que le tunnel est fermé.

Les lignes de commande peuvent être :

- l'appel à un fichier « batch », par exemple : *C:\vpn\batch\script.bat*
- l'exécution d'un programme, par exemple : *C:\Windows\notepad.exe*
- l'ouverture d'une page web, par exemple : *https://mon.site*
- etc.

Les applications sont nombreuses :

- création d'un fichier sémaphore lorsque le tunnel est ouvert, de telle sorte qu'une application tierce puisse détecter le moment où le tunnel est ouvert ;
- ouverture automatique d'un serveur intranet de l'entreprise, une fois le tunnel ouvert ;
- nettoyage ou vérification d'une configuration avant l'ouverture du tunnel ;

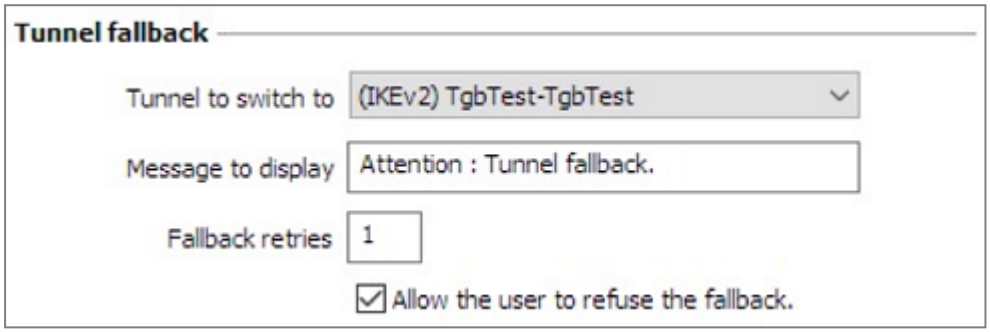
- vérification du poste (anti-virus mis à jour, versions correctes des applications, etc.) avant l'ouverture du tunnel ;
- nettoyage automatique (suppression des fichiers) d'une zone de travail sur le poste avant fermeture du tunnel ;
- application de comptabilisation des ouvertures, fermetures et durées des tunnels VPN ;
- modification de la configuration réseau, une fois le tunnel ouvert, puis restauration de la configuration réseau initiale après fermeture du tunnel ;
- etc.

NOTE
Les scripts ne sont pas configurables pour un tunnel configuré en mode GINA. Les champs de saisie sont désactivés.

Tunnel de repli

Le SN VPN Client Exclusive implémente une fonction de tunnel de repli (tunnel fallback) qui permet de tenter automatiquement l'ouverture d'un tunnel alternatif lorsque l'ouverture du premier tunnel échoue.

Cette fonction se configure dans l'onglet **Automatisation** de chaque tunnel (IKEv2 ou SSL).



IMPORTANT
La fonction **Passerelle redondante** ne doit pas être configurée conjointement avec la fonction **Tunnel de repli**. Il convient de choisir soit l'une ou l'autre, faute de quoi le Client VPN pourrait adopter un comportement non déterminé.

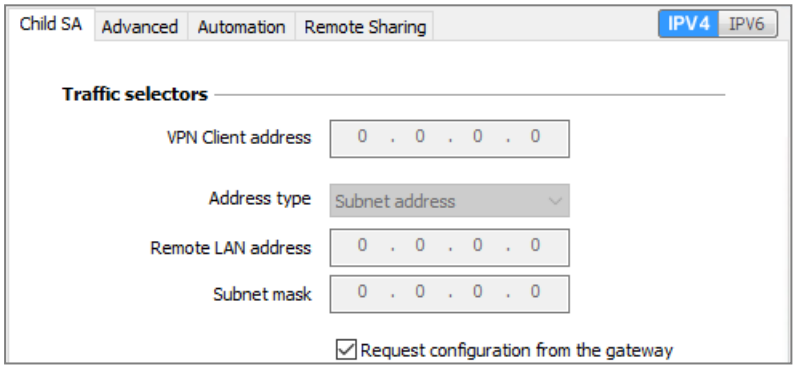
Repli vers le tunnel	Le champ présente la liste des tunnels vers lequel le logiciel peut basculer automatiquement si le tunnel en cours d'édition est indisponible.
Message à afficher	Comme cette fonction peut passer automatiquement d'un tunnel à un autre, le second étant par exemple moins sécurisé que le premier, il est possible de saisir un message d'avertissement à l'utilisateur, qui lui sera délivré à chaque bascule vers le tunnel de repli.
Nombre d'essais	Le nombre d'essais est enregistré de façon à éviter les boucles de bascules sans fin (un tunnel 1 qui se replie sur un tunnel 2 qui se replie sur un tunnel 1).
Autoriser l'utilisateur à refuser ce repli	Permet de configurer la fonction de repli de sorte que ce soit l'utilisateur qui décide de passer d'un tunnel à l'autre.

IPv4 et IPv6

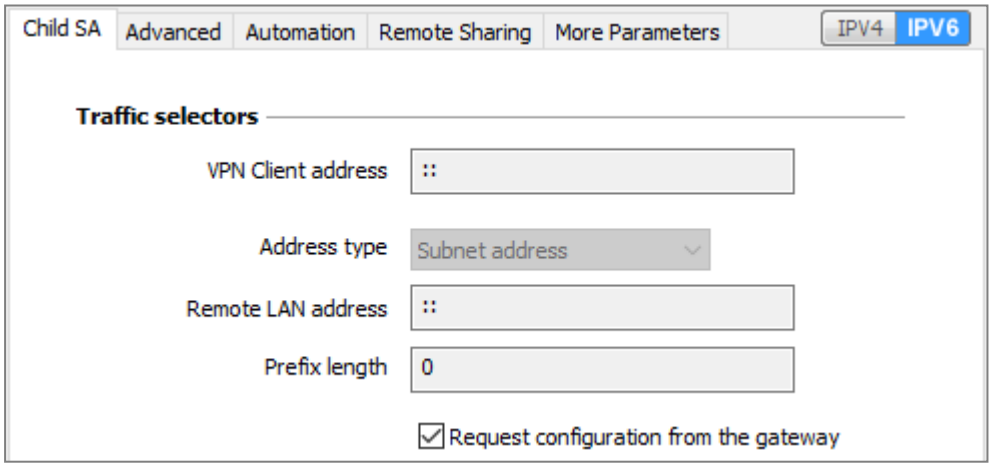
SN VPN Client Exclusive supporte les protocoles IPv4 et IPv6, que ce soit pour la communication avec la passerelle ou pour la communication sur le réseau distant. Le Client VPN permet de combiner l'utilisation d'IPv4 et IPv6, par exemple pour établir une connexion IPv4 sécurisée dans un tunnel VPN transporté sur IPv6.

Le choix IPv4/IPv6 se fait soit d'après l'adresse IP si elle est numérique, soit d'après la résolution DNS. Dans ce dernier cas, la résolution du nom de la passerelle fournit soit une adresse IP soit IPv4, soit IPv6, soit les deux. Si les deux adresses sont fournies, l'adresse IPv4 est privilégiée.

Pour les tunnels VPN IKEv2, la configuration du protocole IPv4 ou IPv6 est accessible en haut à droite de l'onglet **Child SA**.



Le protocole IP configuré par le bouton **IPv4/IPv6** est exactement le protocole utilisé sur le réseau distant.



NOTE

Le choix IPv4 ou IPv6 a un impact sur les paramètres des autres onglets de configuration du tunnel. Ainsi, pour ces autres onglets, le bouton de choix IPv4/IPv6 est rappelé en haut à droite mais est désactivé.

Gestion des certificats

Introduction

SN VPN Client Exclusive offre un ensemble de fonctions permettant l'exploitation de certificats de toute nature, issus de PKI / IGC de tout type et stockés sur des supports de toute nature : carte à puce, token, magasin de certificats, fichier de configuration.

SN VPN Client Exclusive implémente en particulier les facilités suivantes :

- sélection automatique du support à utiliser parmi plusieurs ;
- accès aux cartes à puce et aux tokens en PKCS#11 et CNG ;
- sélection multicritère des certificats à utiliser en fonction du sujet et du key usage ;
- gestion des certificats côté utilisateur (côté client VPN), comme des certificats de la passerelle VPN, incluant la gestion des dates de validité, des chaînes de certification, des certificats racines, intermédiaires et des CRL ;
- gestion des autorités de certification (Certificate Authority : CA) ;
- possibilité de préconfigurer tous les paramètres PKI / IGC pour une prise en compte automatique lors de l'installation.

SN VPN Client Exclusive apporte des fonctions de sécurité supplémentaires sur la gestion des PKI / IGC comme l'ouverture et la fermeture automatique du tunnel sur insertion et extraction de carte à puce et de token, ou encore la possibilité de configurer l'interface PKI / IGC dans l'installeur du logiciel de façon à automatiser le déploiement.

La liste des cartes à puce et des tokens compatibles avec SN VPN Client Exclusive est disponible sur le site TheGreenBow à l'adresse : https://thegreenbow.com/fr/support/guides-dintegration/tokens-vpn-compatibles/.

La configuration et la caractérisation des certificats peut être effectuée dans :

1. l'onglet **Certificat** du tunnel concerné : IKE Auth (IKEv2) ou TLS (SSL) ;
2. l'onglet **Options PKI** de la fenêtre **Outils** > **Options** du **Panneau de Configuration** ;
3. un fichier de configuration des lecteurs de cartes à puce et tokens appelé *vpnconf.ini* (cf. « Guide de déploiement »).

Les types de certificat suivants sont pris en charge :

- RSASSA-PKCS1-v1.5 avec SHA-2 (uniquement si le paramètre dynamique correspondant est configuré, cf. section Méthodes d'authentification des certificats),
- RSASSA-PSS avec SHA-2 (uniquement si le paramètre dynamique correspondant est configuré, cf. section Méthodes d'authentification des certificats),
- ECDSA « secp256r1 » avec SHA-2 (256 bits),
- ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits).

Pour en savoir davantage sur les méthodes d'authentification et la cryptographie utilisées dans SN VPN Client Exclusive, consultez la section Notions élémentaires de cryptographie dans l'annexe.

Certificat utilisateur

Généralités

Le certificat utilisateur est envoyé par le Client VPN à la passerelle pour qu'elle puisse authentifier l'utilisateur.

Il doit se conformer aux contraintes suivantes (recommandations de sécurité de l'ANSSI) :

- L'extension Key Usage doit être présente, marquée comme critique, et contenir uniquement la valeur *digitalSignature*.
- L'extension Extended Key Usage doit être présente, marquée comme non-critique, et uniquement contenir la valeur *id-kp-clientAuth*.

Si ces contraintes ne sont pas respectées, le Client VPN affichera un avertissement dans la **Console** mais n'empêchera pas la communication avec la passerelle. Celle-ci devrait néanmoins refuser l'authentification du Client VPN.

Paramètres dynamiques

Depuis la version 7.4 de SN VPN Client Exclusive, deux paramètres dynamiques viennent remplacer les propriétés MSI correspondantes. Ils sont définis au niveau de la charge utile d'authentification IKE_AUTH et s'appliquent à un tunnel donné, alors que les propriétés MSI s'appliquent à l'ensemble des tunnels.

user_cert_dnpattern

Le paramètre dynamique `user_cert_dnpattern` permet de caractériser le certificat à utiliser. Lorsqu'il est défini, SN VPN Client Exclusive recherche, sur token, carte à puce et dans le magasin de certificats Windows, le certificat dont le sujet contient `[texte]`.

user_cert_keyusage

Le paramètre dynamique `user_cert_keyusage` permet de sélectionner un certificat en fonction de son champ « key usage » :

- 0 ou non défini : Pas de sélection du certificat par le champ « key usage ».
- 1 : Sélection du certificat par le champ « key usage » dont la valeur de l'attribut `digitalSignature=1`.
- 2 : Sélection du certificat par le champ « key usage » dont la valeur des attributs `digitalSignature=1` et `keyEncipherment=1`.

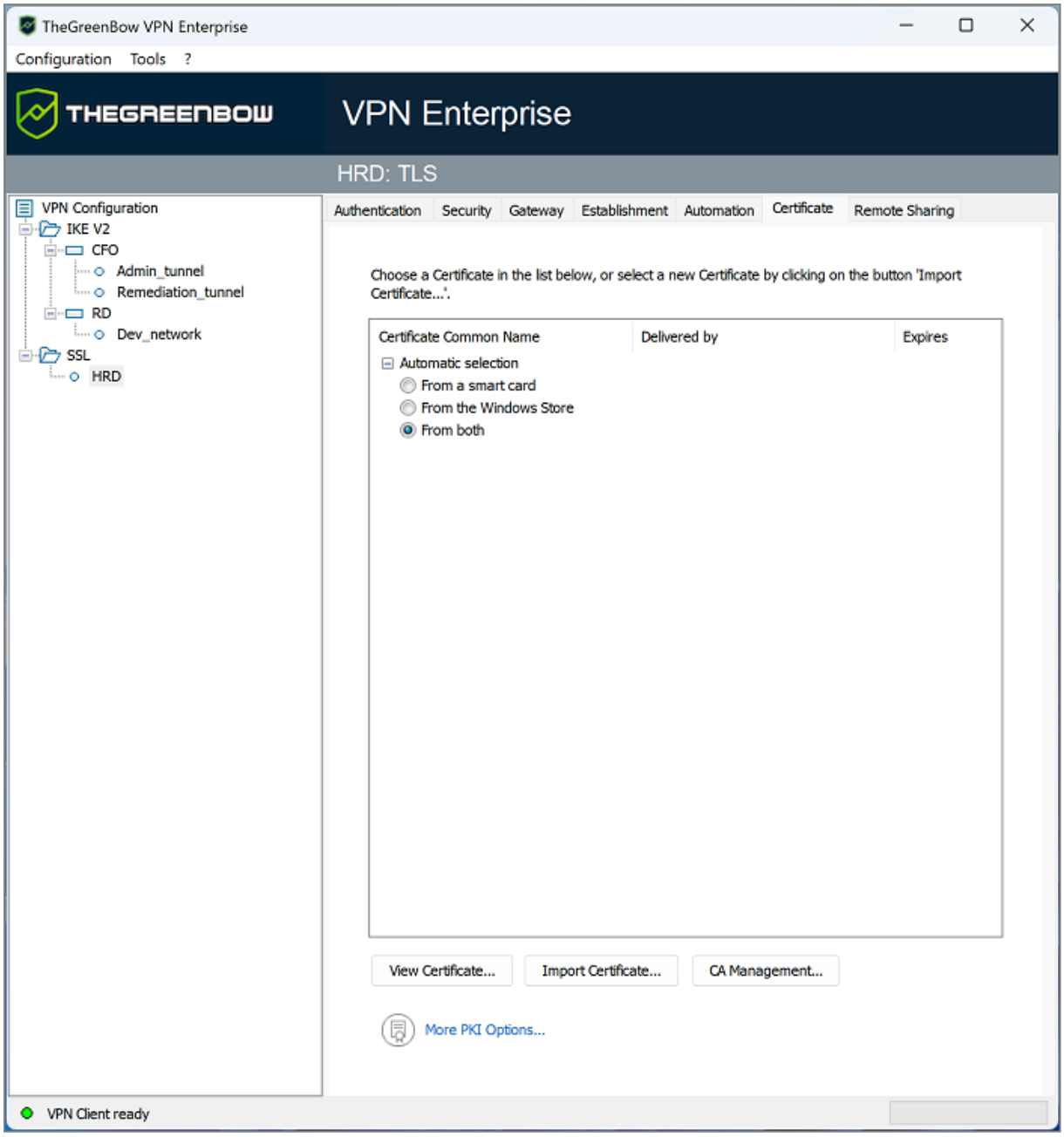
> **NOTE**
> Lorsque la valeur du paramètre dynamique `user_cert_keyusage` est définie sur 2, la case à cocher **Utiliser seulement les certificats de type authentification** de l'onglet **Options PKI** est grisée (cf. section Options PKI).

Sélection automatique

Depuis la version 7.4 de SN VPN Client Exclusive, une option permet de sélectionner automatiquement le certificat utilisateur depuis un token /une carte à puce, le magasin de certificats Windows ou les deux.

L'onglet **Certificat** de la connexion IKE ou SSL présente une entrée **Sélection automatique** avec les options suivantes :

- Depuis une carte à puce
- Depuis le magasin Windows
- Depuis les deux

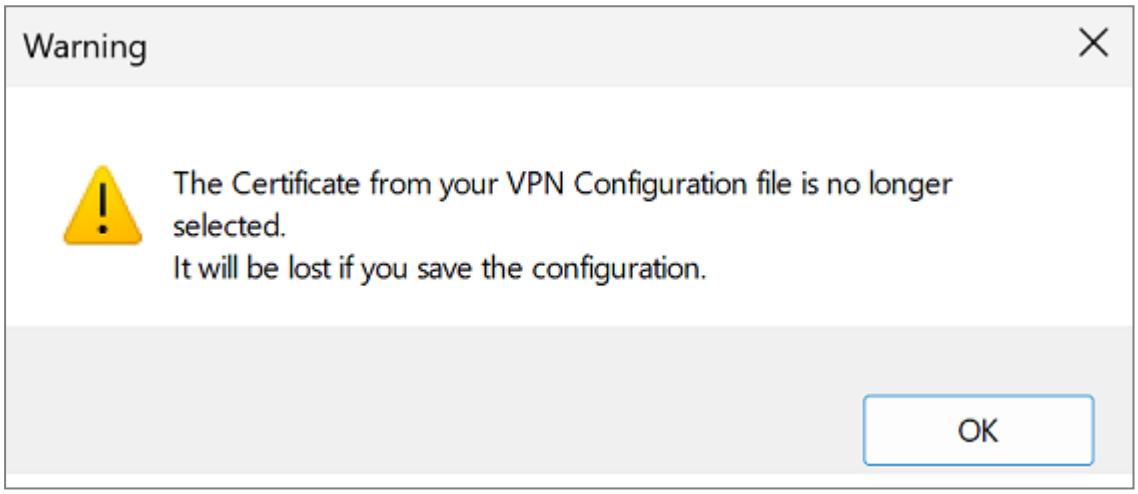


Si vous choisissez la dernière option, le logiciel va d'abord chercher le certificat utilisateur sur un token / une carte à puce. S'il n'en trouve pas, il va poursuivre la recherche dans le magasin de certificats Windows.

Pour les options **Depuis une carte à puce** et **Depuis les deux**, si vous utilisez plusieurs lecteurs de tokens / cartes à puce vous devez configurer le paramètre dynamique `reader_pattern` pour spécifier le lecteur à partir duquel le certificat doit être sélectionné (voir section Afficher plus de paramètres). Comme valeur du paramètre, indiquez le nom du lecteur (p. ex. *NEOWAVE*) ou *Virtual* s'il s'agit d'un module de plateforme sécurisée (TPM ou *Trusted Platform Module*).

NOTE
Depuis la version 7.5 de SN VPN Client Exclusive, en présence de plusieurs cartes à puce du même fabricant utilisant des lecteurs identiques, le paramètre dynamique `user_smartcard_tip` peut être défini au niveau IKE Auth à une valeur au choix, qui sera affichée lors de la demande du mot de passe pour identifier de manière univoque chaque carte à puce (voir section Afficher plus de paramètres).

Si vous avez précédemment importé un certificat dans la configuration et que vous décidez de choisir la sélection automatique, un avertissement s'affiche pour vous indiquer que le certificat sera supprimé de la configuration lorsque vous la sauvegarderez.



Sélectionner un certificat (onglet Certificat)

Le Client VPN permet d'affecter un certificat utilisateur à un tunnel VPN.

Il ne peut y avoir qu'un seul certificat par tunnel, mais chaque tunnel peut avoir son propre certificat.

Le Client VPN permet de choisir un certificat stocké :

- dans le fichier de configuration VPN (voir ci-dessous Importer un certificat dans la configuration VPN) ;
- sur une carte à puce ou dans un token (voir ci-dessous Utiliser un certificat sur carte à puce ou sur token) ;
- dans le magasin de certificats Windows (voir ci-dessous Utiliser un certificat du magasin de certificats Windows) ;

L'onglet **Certificat** du tunnel concerné énumère tous les supports accessibles sur le poste, qui contiennent des certificats, dès lors que :

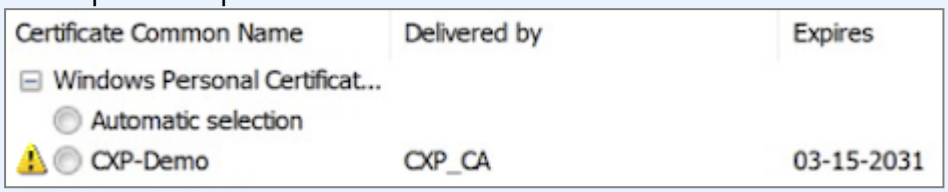
- la carte à puce ou le token est compatible CNG ou PKCS#11 ;
- le middleware de la carte à puce ou du token est correctement installé sur l'ordinateur ;
- le cas échéant, la carte à puce est correctement insérée dans le lecteur associé.

Si un support ne contient pas de certificat, il n'est pas affiché dans la liste (p.ex. si le fichier de configuration VPN ne contient pas de certificat, il n'apparaît pas dans la liste).

En cliquant sur le support désiré, la liste des certificats qu'il contient est affichée.

NOTE

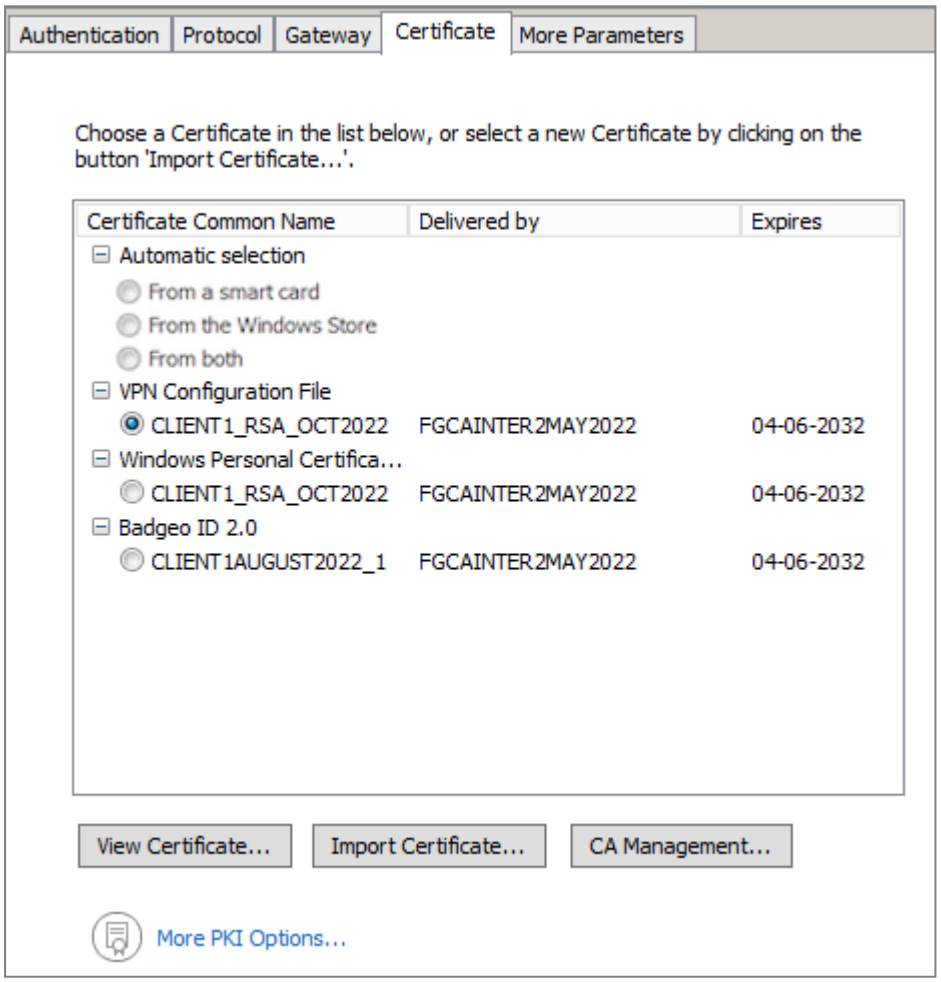
Dans le cas d'un lecteur de cartes à puce, le lecteur s'affiche précédé d'une icône d'alerte si la carte à puce n'est pas insérée.



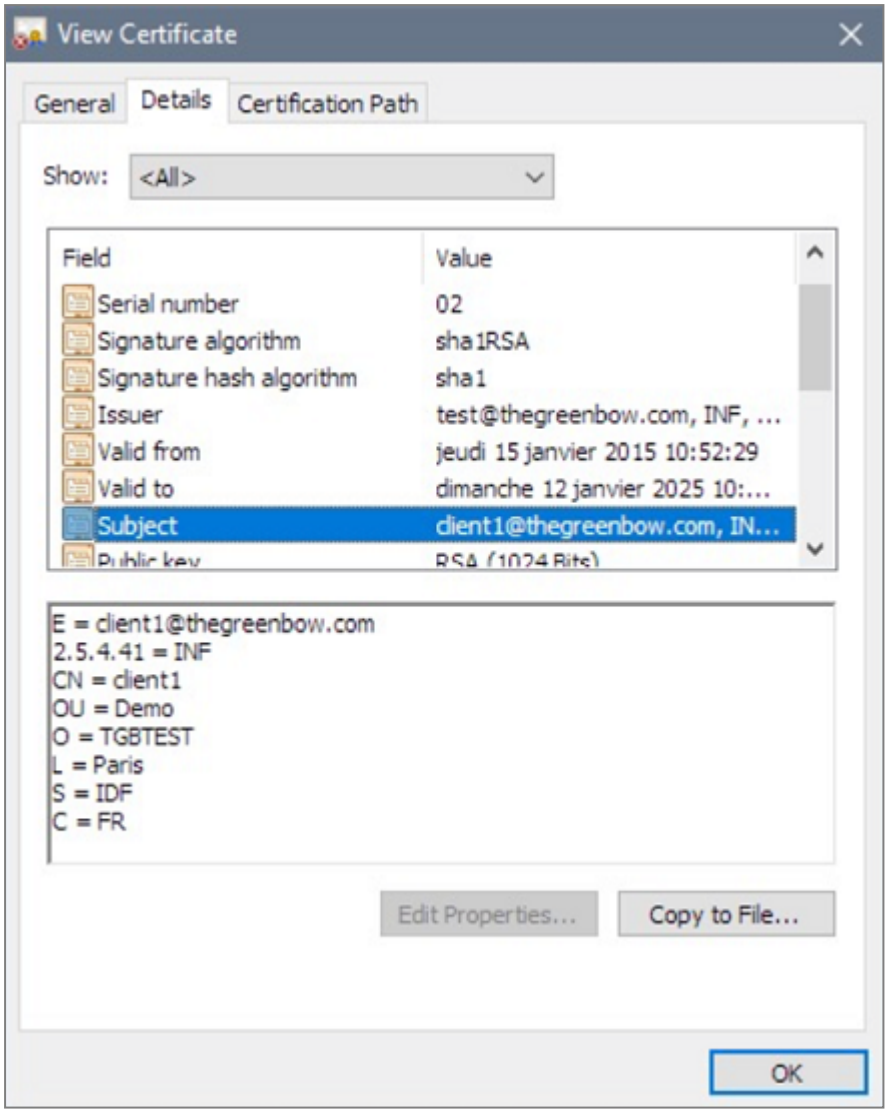
Cliquez sur le certificat souhaité pour l'affecter au tunnel VPN.

NOTE

Seuls les certificats présents qui ne sont pas expirés sont affichés.

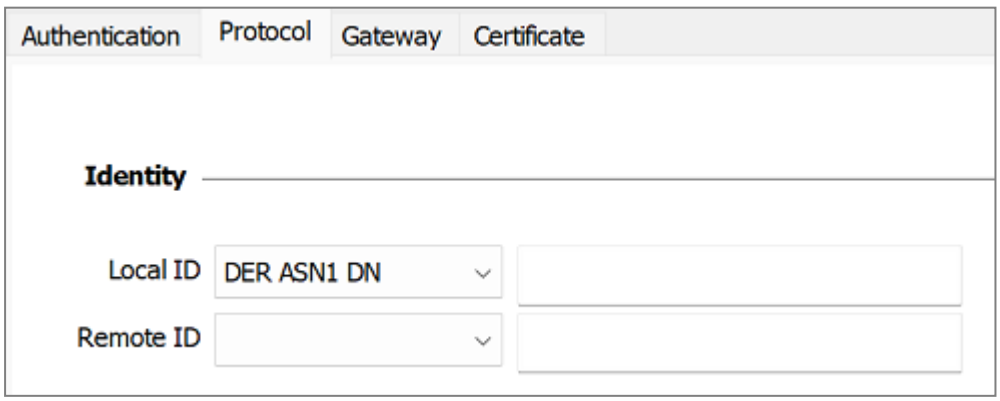


Une fois le certificat sélectionné, le bouton **Voir le certificat** permet d'afficher le détail du certificat.



NOTE

Une fois le certificat sélectionné, le type de Local ID du tunnel passe automatiquement à **DER ASN1 DN**, et le sujet du certificat est utilisé par défaut comme valeur de ce **Local ID**. Voir ci-dessous pour renseigner automatiquement une valeur de DNS ou d'e-mail issue du certificat.



Depuis la version 7.3 de SN VPN Client Exclusive, vous pouvez sélectionner le type **DNS** ou **Email** dans la liste déroulante **Local ID**, afin d'affecter automatiquement au Local ID une valeur de DNS ou d'e-mail récupérée du certificat.

Si vous choisissez le type **DNS**, la valeur du Local ID prendra automatiquement la valeur du champ *dNSName* du nom alternatif du sujet du certificat (*SubjAltName*). Si ce champ n'est pas renseigné (absence de *SubjAltName* dans le certificat ou absence de *dNSName* dans le *SubjAltName*), c'est la valeur CN du sujet du certificat qui est reprise. Si cette dernière valeur n'est pas non plus présente, aucun certificat n'est admissible pour configurer le tunnel et la montée du tunnel échoue.

Si vous choisissez le type **Email**, la valeur du Local ID prendra automatiquement la valeur du champ *rfc822Name* du nom alternatif du sujet du certificat (*SubjAltName*). Si ce champ n'est pas renseigné (absence de *SubjAltName* dans le certificat ou absence de *rfc822Name* dans le *SubjAltName*), c'est la valeur *Email* du sujet du certificat qui est reprise. Si cette dernière valeur n'est pas non plus présente, aucun certificat n'est admissible pour configurer le tunnel et la montée du tunnel échoue.

NOTE
Depuis la version 7.4 de SN VPN Client Exclusive, une option permet de sélectionner automatiquement le certificat utilisateur depuis un token /une carte à puce, le magasin de certificats Windows ou les deux (voir la section Sélection automatique).

Importer un certificat dans la configuration VPN

SN VPN Client Exclusive permet d'importer dans la configuration VPN des certificats au format PEM/PFX ou PKCS#12. L'intérêt de cette solution, moins sécurisée que l'utilisation du magasin de certificats Windows, d'une carte à puce ou d'un token, est de faciliter le transport des certificats.

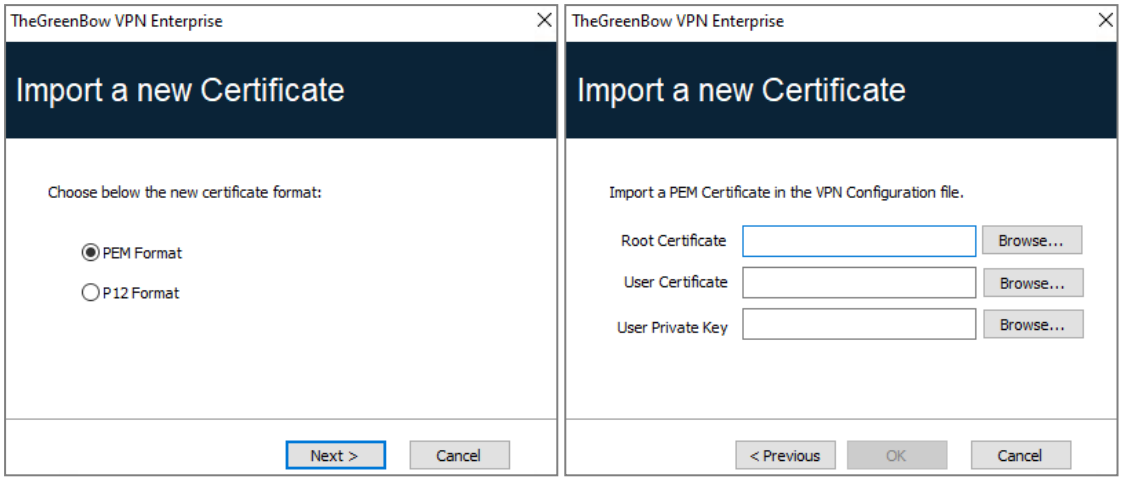
Cette solution présente l'avantage de regrouper le certificat (propre à un utilisateur) et la configuration VPN (a priori générique) dans un fichier unique, facile à transmettre vers le poste utilisateur et à importer dans le Client VPN.

Néanmoins, l'inconvénient de transporter les certificats dans une configuration VPN est que chaque configuration devient alors propre à chaque utilisateur. Cette solution, n'est donc pas préconisée pour un déploiement conséquent.

IMPORTANT
Dès lors qu'un certificat est importé dans une configuration VPN, il est fortement recommandé lors de l'exportation du fichier de configuration, de le protéger par un mot de passe (cf. section Exporter une configuration VPN), pour éviter que le certificat ne soit visible en clair.

Importer un certificat au format PEM/PFX

1. Dans l'onglet **Certificat** d'un IKE Auth, cliquez sur **Importer un Certificat…**.
2. Choisissez **Format PEM**.
3. Cliquez sur **Parcourir** pour sélectionner le **Certificat Racine**, le **Certificat (Utilisateur)** et la **Clé privée** à importer.
4. Cliquez sur **OK** pour valider.



Le certificat apparaît et est sélectionné dans la liste des certificats de l'onglet **Certificat**.

Sauvegarder la configuration VPN : le certificat est sauvegardé dans la configuration VPN.

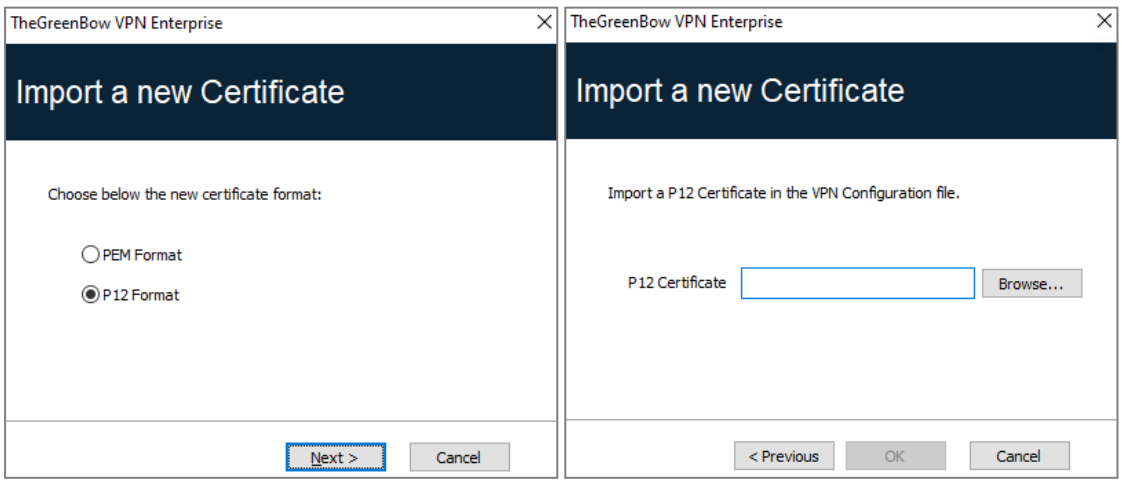
NOTE
Le fichier avec la clé privée ne doit pas être chiffré.

Importer un certificat au format PKCS#12

1. Dans l'onglet **Certificat** d'un Child SA, cliquez sur **Importer un Certificat...**.
2. Choisissez **Format P12**.
3. Cliquez sur **Parcourir** pour sélectionner le certificat PKCS#12 à importer.

IMPORTANT
Pour des raisons de sécurité, à partir de la version 7.5 de SN VPN Client Exclusive, les certificats PKCS#12 chiffrés avec l'algorithme RC2 ne sont plus pris en charge et ne peuvent plus être importés.

4. S'il est protégé par mot de passe, saisissez le mot de passe et cliquez sur **OK** pour valider.



Le certificat est ajouté à la liste des certificats de l'onglet **Certificat** et y est sélectionné.

Sauvegarder la configuration VPN : le certificat est sauvegardé dans la configuration VPN.

NOTE
Toutes les CA au format PKCS#12 présentes dans le fichier seront également importées dans la configuration VPN.

Utiliser un certificat sur carte à puce ou sur token

Lorsqu'un tunnel VPN est configuré pour exploiter un certificat stocké sur carte à puce ou sur token, le code PIN d'accès à cette carte à puce ou token est demandé à l'utilisateur à chaque ouverture du tunnel.

Si la carte à puce n'est pas insérée, ou si le token n'est pas accessible, le tunnel ne s'ouvre pas.

Si le certificat trouvé ne remplit pas les conditions configurées (cf. section Importer un certificat en fonction du type de magasin ci-dessous), le tunnel ne s'ouvre pas.

Si le code PIN présenté est erroné, SN VPN Client Exclusive avertit l'utilisateur, qui a habituellement trois essais consécutifs avant blocage de la carte à puce ou du token.

SN VPN Client Exclusive implémente un mécanisme de détection automatique de l'insertion d'une carte à puce.

Ainsi, les tunnels associés au certificat contenu sur la carte à puce sont montés automatiquement à l'insertion de cette carte à puce. Réciproquement, l'extraction de la carte à puce ferme automatiquement tous les tunnels associés.

Pour mettre en œuvre cette fonction, cocher **Ouvrir ce tunnel automatiquement lorsqu'une clé USB est insérée** (cf. chapitre Automatisation).

NOTE
Depuis la version 7.4 de SN VPN Client Exclusive, une option permet de sélectionner automatiquement le certificat utilisateur depuis un token /une carte à puce, le magasin de certificats Windows ou les deux (voir la section Sélection automatique).

NOTE
Depuis la version 7.5 de SN VPN Client Exclusive,en présence de plusieurs cartes à puce identiques utilisant des lecteurs identiques, le paramètre dynamique `user_smartcard_tip` peut être défini à une valeur au choix permettant d'identifier de manière univoque chaque carte à puce (voir section Afficher plus de paramètres).

Utiliser un certificat du magasin de certificats Windows

Caractéristiques requises

NOTE
En vue d'offrir une granularité plus fine dans la configuration du choix de magasin de certificats à utiliser, depuis la version 7.5 de SN VPN Client Exclusive, ce choix n'est plus opéré au niveau du poste, mais à celui du tunnel.

Pour qu'un certificat du magasin de certificats Windows soit identifié par le SN VPN Client Exclusive, il doit respecter les caractéristiques suivantes :

- Le certificat doit être certifié par une autorité de certification (ce qui exclut les certificats auto-signés),
- Par défaut, le certificat doit être situé dans le magasin de certificats « Personnel » (il représente l'identité personnelle de l'utilisateur qui veut ouvrir un tunnel VPN vers son réseau d'entreprise). Pour utiliser le magasin de certificats machine de Windows, il convient d'ajouter le paramètre dynamique `MachineStore` défini à la valeur `true` (voir section Afficher plus de paramètres).

NOTE
Pour gérer les certificats dans le magasin de certificats Windows, Microsoft propose en standard l'outil de gestion *certmgr.msc*. Pour exécuter cet outil, aller dans le menu **Démarrer** de Windows, puis dans le champ **Rechercher les programmes et fichiers**, entrer *certmgr.msc*.

Importer un certificat en fonction du type de magasin

Lors de l'importation de certificats, il convient de spécifier le type de magasin utilisé (utilisateur ou machine) dans la ligne de commande. Ci-dessous, vous trouverez des exemples de ligne de commande avec les options à préciser.

- Magasin utilisateur :

```
certutil -csp KSP -user -importpfx CertFileName.p12
```

- Magasin machine :

```
certutil -csp KSP -importpfx CertFileName.p12
```

NOTE
Dans les lignes de commande, l'option **-user** de la commande *certutil* sert à spécifier le magasin utilisateur. Lorsqu'elle est omise, le magasin machine est utilisé par défaut.

NOTE
Depuis la version 7.4 de SN VPN Client Exclusive, une option permet de sélectionner automatiquement le certificat utilisateur depuis un token /une carte à puce, le magasin de certificats Windows ou les deux (voir la section Sélection automatique).

Options PKI : caractériser le certificat et son support

SN VPN Client Exclusive offre plusieurs possibilités pour caractériser le certificat à utiliser, ainsi que pour sélectionner le lecteur de cartes à puce ou le token qui contient le certificat.

Cette fonctionnalité est disponible via le lien Plus d'options PKI en bas de l'onglet **Certificat**, et dans l'onglet **Options PKI** de la fenêtre de configuration des **Options**.

Certificat de la passerelle VPN

Il est recommandé de forcer SN VPN Client Exclusive à vérifier la chaîne de certification du certificat reçu de la passerelle VPN (comportement par défaut).

Voir section Vérification des certificats.

Cela nécessite d'importer le certificat racine et tous les certificats de la chaîne de certification (l'autorité de certification racine et les autorités de certification intermédiaires) dans le fichier de configuration.

Si l'option est cochée, le Client VPN utilisera aussi la liste des certificats révoqués(CRL ou *Certificate Revocation List* en anglais) des différentes autorités de certification.

Si ces CRL sont absentes du magasin de certificats, ou si ces CRL ne sont pas téléchargeables à l'ouverture du tunnel VPN, le Client VPN ne sera pas en mesure de valider le certificat de la passerelle.

La vérification de chaque élément de la chaîne implique :

- la vérification de la date d'expiration du certificat,
- la vérification de la date de début de validité du certificat,
- la vérification des signatures de tous les certificats de la chaîne de certificats (y compris le certificat racine, certificats intermédiaires et le certificat du serveur),
- la vérification des CRL de tous les émetteurs de certificats de la chaine de confiance.

NOTE
Depuis la version 7.5 de SN VPN Client Exclusive, il est possible de vérifier la révocation du certificat de la passerelle à l'aide du protocole de vérification de certificat en ligne en mode agrafage (OCSP ou *Online Certificate Status Protocol* en anglais). Pour cela, il convient d'ajouter le paramètre dynamique `enable_OCSP` défini à la valeur `true` (voir section Afficher plus de paramètres).

Empêcher ou limiter le téléchargement des CRL

Introduction

Une liste de révocation de certificats (*Certificate Revocation List* ou CRL) contient l'ensemble des certificats qui ne sont plus valables (date de validité expirée, perte ou compromission de la clé privée associée au certificat, changement d'un champ relatif au titulaire, etc.) et qui ne sont donc plus dignes de confiance.

Les CRL sont définies dans les normes RFC 5280 et RFC 6818.

Les CRL sont publiées par les autorités de certification (CA) et les infrastructures de gestion de clés (IGC ou *Public Key Infrastructure* – PKI).

Dans certains cas, ces listes peuvent être relativement volumineuses (plusieurs Mo). Leur téléchargement peut donc prendre du temps et par conséquent ralentir le temps d'ouverture d'un tunnel lorsqu'un grand nombre d'utilisateurs contacte le serveur HTTP en même temps.

SN VPN Client Exclusive met à disposition deux paramètres dynamiques décrits ci-dessous pour accélérer le temps d'ouverture d'un tunnel. Ces paramètres fonctionnent de manière indépendante et peuvent être associés.

Le premier paramètre dynamique, nommé `check_user_crl`, empêche le téléchargement de la CRL de validation du certificat utilisateur. Le second, nommé `crl_cache_duration`, limite le téléchargement de la CRL de validation du certificat passerelle.

Empêcher le téléchargement de la CRL de validation du certificat utilisateur

Par défaut, lorsque le Client VPN vérifie le certificat utilisateur (p. ex. parce qu'il dépend d'une CA connue), il vérifie également la CRL pour savoir si ce certificat est toujours valide. Si le

certificat n'est pas valide, un simple avertissement est consigné dans la **Console**. En fin de compte, c'est la passerelle qui va décider si le certificat utilisateur peut être accepté ou non.

Afin d'empêcher le téléchargement de la CRL et donc accélérer le temps d'ouverture d'un tunnel, vous pouvez ajouter le paramètre dynamique *check_user_crl* défini à la valeur *false* (voir section Afficher plus de paramètres). Dans ce cas, la vérification de la CRL n'est pas effectuée pour le certificat utilisateur. C'est la passerelle qui se charge d'effectuer cette vérification.

Limiter le téléchargement de la CRL de validation du certificat utilisateur

Si vous souhaitez limiter le nombre de fois qu'une CRL est téléchargée pour la validation du certificat de la passerelle sans pour autant empêcher son téléchargement – toujours en vue d'accélérer le temps d'ouverture d'un tunnel –, vous pouvez ajouter le paramètre dynamique *crl_cache_duration* défini à une valeur *true* correspondant au nombre d'heures pendant lequel la CRL est mise en cache (voir section Afficher plus de paramètres).

Lorsque la valeur du paramètre est égale à zéro, la mise en mémoire cache de la CRL est désactivée. La durée de la mise en cache est limitée à sept jours, soit 168 heures. Toute valeur supérieure à 168 sera considérée comme égale au maximum de sept jours.

Lorsque le paramètre dynamique est configuré avec une valeur différente de zéro, la CRL est stockée dans une mémoire cache et un délai d'expiration correspondant au nombre d'heures configuré est fixé pour cette CRL. Tant que le délai n'est pas écoulé, la CRL dans la mémoire cache est utilisée et aucun téléchargement n'est effectué. Lorsque le délai est écoulé, la CRL est téléchargée et mise à jour dans la mémoire cache.

Contraintes relatives à l'extension Key Usage

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Key Usage. Elle doit :

- être présente,
- être marquée comme non-critique et
- contenir uniquement les valeurs *digitalSignature* et/ou *nonRepudation*.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le paramètre dynamique *allow_server_and_client_auth* défini à la valeur *true* (voir section Afficher plus de paramètres).

Dans cette configuration, le certificat sera également validé si l'extension Key Usage contient l'une des combinaisons de valeurs suivantes :

- digitalSignature + keyEncipherment + keyAgreement
- digitalSignature + keyAgreement
- nonRepudiation + keyEncipherment
- nonRepudiation + keyEncipherment + keyAgreement
- nonRepudiation + keyAgreement
- keyEncipherment
- keyEncipherment + keyAgreement

De plus, dans cette configuration l'extension Key Usage peut être marquée comme non critique.

NOTE
Conformément aux exigences de sécurité, la valeur `keyEncipherment` de l'extension Key

Usage a été rendue obsolète et remplacée par la valeur `nonRepudiation`, qui est désormais acceptée par défaut. Cependant, la version 7.5 de SN VPN Client Exclusive continue d'accepter la valeur keyEncipherment sans l'utilisation du paramètre dynamique `allow_extra_keyusage`.

ASTUCE
Il est recommandé de préférer la valeur `nonRepudiation` de l'extension Key Usage à la valeur `keyEncipherment`.

Contraintes relatives à l'extension Extended Key Usage

Le certificat de la passerelle doit se conformer aux contraintes suivantes relatives à l'extension Extended Key Usage. Cette dernière peut être absente ou présente. Si elle est présente, elle doit :

- être marquée comme non-critique et
- uniquement contenir les valeurs suivantes :
  - *id-kp-serverAuth* ou
  - *id-kp-serverAuth* + *id-kp-ipsecIKE*.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage mentionnées ci-dessus, il est possible de configurer le Client VPN pour valider le certificat malgré tout, en ajoutant le paramètre dynamique *allow_server_and_client_auth* défini à la valeur *true* (voir section Afficher plus de paramètres).

Dans cette configuration, le certificat sera également validé si l'extension Extended Key Usage contient l'une des combinaisons de valeurs suivantes :

- *id-kp-ServerAuth* + *id-kp-ClientAuth* ou
- *id-kp-ServerAuth* + *id-kp-ClientAuth* + *id-kp-ipsecIKE*.

Gestion des autorités de certification

Généralités

Lorsque SN VPN Client Exclusive est configuré pour vérifier les certificats passerelle, les autorités de certification doivent être également accessibles.

La CA racine de la passerelle doit obligatoirement être importée dans la configuration.

Si la passerelle n'est pas configurée pour envoyer les CA, alors il est également nécessaire d'importer les CA intermédiaires dans la configuration.

NOTE
Depuis la version 7.3 de SN VPN Client Exclusive, il est possible de créer des configurations avec plus de trois autorités de certification (CA).

Les types de CA intermédiaires prises en charge sont :

- RSASSA-PKCS1-v1.5 avec SHA-2,
- RSASSA-PSS avec SHA-2,

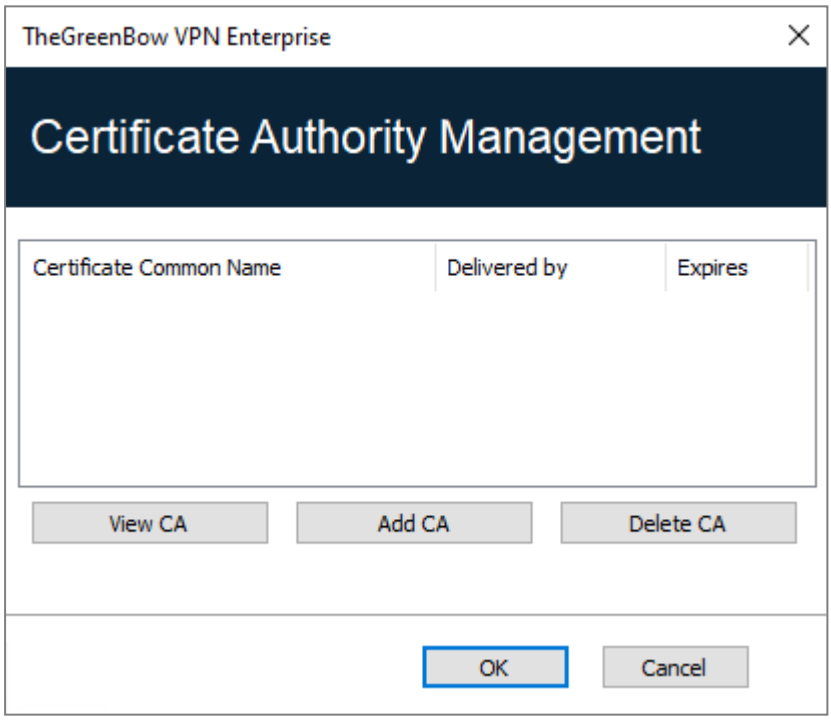
- ECDSA « secp256r1 » avec SHA-2,
- ECDSA « BrainpoolP256r1 » avec SHA-2.

Les types de CA racine prises en charge sont :

- RSASSA-PKCS1-v1.5 avec SHA-2,
- RSASSA-PSS avec SHA-2,
- ECDSA « secp256r1 » avec SHA-2,
- ECDSA « BrainpoolP256r1 » avec SHA-2.

NOTE
Pour des raisons de sécurité, l'utilisation du magasin de certificats Windows pour accéder aux CA n'est pas autorisé.

Importer une autorité de certification



1. Dans la fenêtre **Gestion des CA**, cliquez sur **Ajouter CA**.
2. Choisissez le format de CA souhaité (PEM ou DER).
3. Cliquez sur **Parcourir** pour sélectionner le CA à importer.

Mode IPsec DR

Pour pouvoir utiliser SN VPN Client Exclusive en mode IPsec DR, l'une des exigences du référentiel IPsec DR de l'ANSSI est que la valeur *Certification Auhtority* dans la charge utile de demande de certificat (CERTREQ payload) est une liste concaténée de condensats SHA-2 des clés publiques des autorités de certification de confiance.

Depuis la version 7.5 de SN VPN Client Exclusive, le Client VPN détecte automatiquement le format (SHA-1 ou SHA-2) en fonction de la longueur de la charge utile de demande de certificat

[CERTREQ] qu'il reçoit de la passerelle. Cette sélection automatique est uniquement effectuée si le paramètre dynamique `sha2_in_cert_req` n'est pas présent.

Si vous souhaitez sélectionner le format manuellement, vous pouvez ajouter le paramètre dynamique `sha2_in_cert_req` défini à la valeur `true` pour SHA-2 ou à la valeur `false` pour SHA-1 (voir section Afficher plus de paramètres).

NOTE

Si la longueur ne permet pas de déterminer le format, SHA-1 est privilégié. Face à une passerelle configurée en mode IPsec DR, il convient donc d'utiliser le paramètre dynamique `sha2_in_cert_req` pour exclure toute ambiguïté.

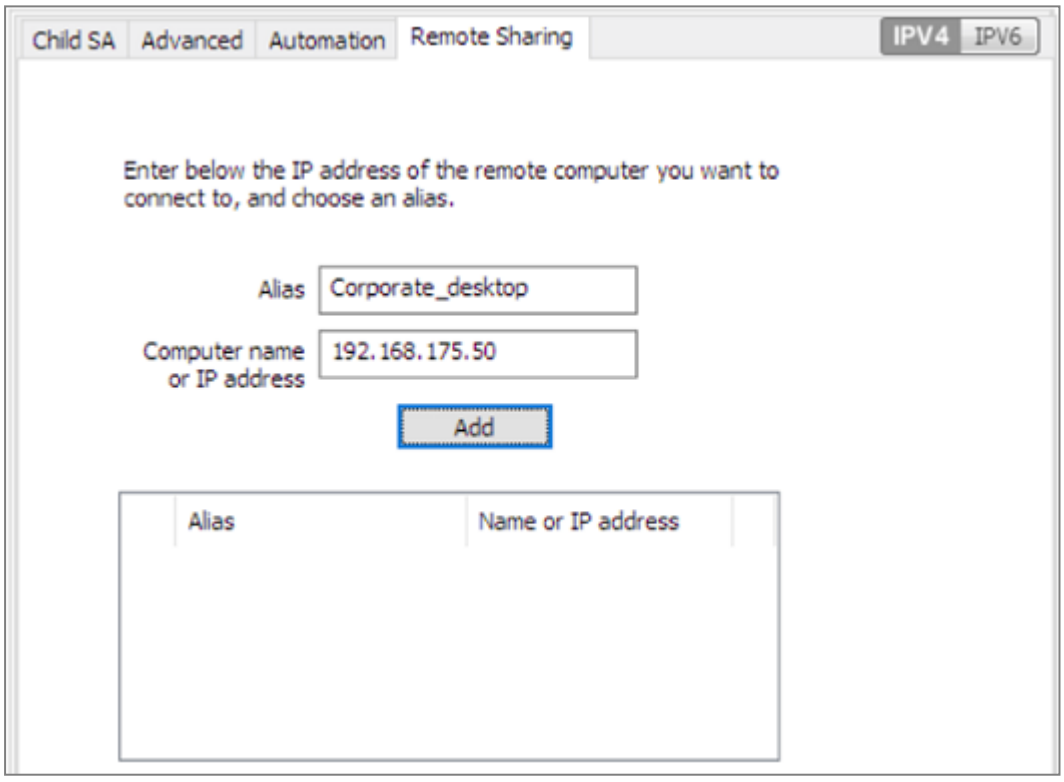
Partage de bureau distant

L'ouverture d'une session « Remote Desktop » (partage de bureau distant) au travers d'internet sur un ordinateur Windows distant nécessite habituellement l'établissement d'une connexion sécurisée, ainsi que la saisie des paramètres de connexions (adresse de l'ordinateur distant, etc.).

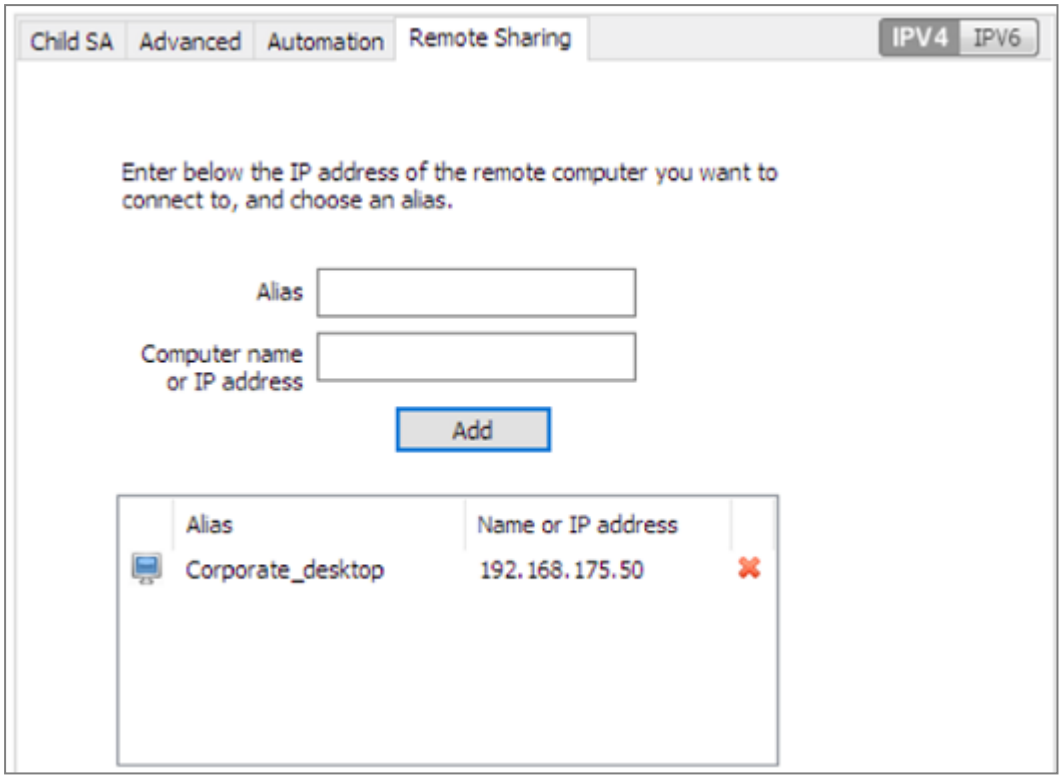
SN VPN Client Exclusive permet de simplifier et de sécuriser automatiquement l'ouverture d'une session « Remote Desktop » : en un seul clic, la connexion VPN s'établit avec le poste distant et la session RDP (Remote Desktop Protocol) est automatiquement ouverte sur ce poste distant.

Pour configurer le partage de bureau distant, procédez comme suit :

1. Sélectionnez le tunnel VPN (Child SA ou TLS) dans lequel sera ouverte la session « Remote Desktop ».
2. Sélectionnez l'onglet **Bureau distant**.
3. Entrez un alias pour la connexion (ce nom est utilisé pour identifier la connexion dans les différents menus du logiciel) et l'adresse IP ou le nom Windows du poste distant.



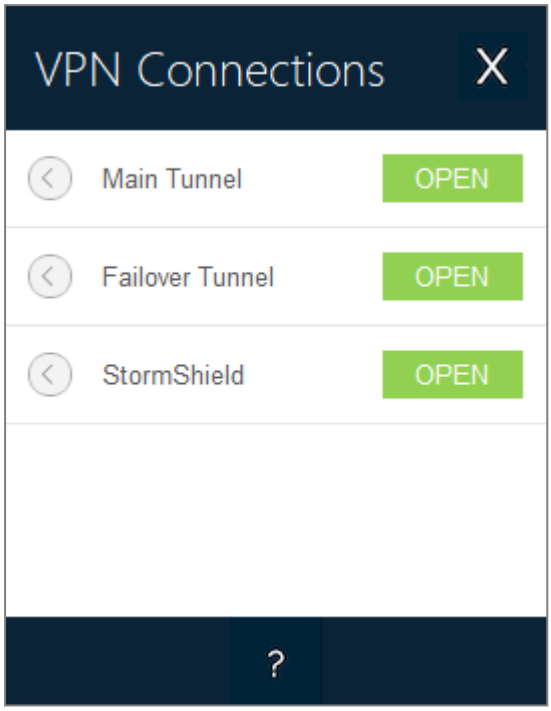
4. Cliquez sur **Ajouter** : la session de partage de bureau distant (RDP) est ajoutée à la liste des sessions.



Pour ouvrir cette connexion RDP en un seul clic, il est recommandé de la faire apparaître spécifiquement dans le **Panneau des Connexions**, en utilisant la fonction de Configuration des connexions détaillée dans le chapitre suivant.

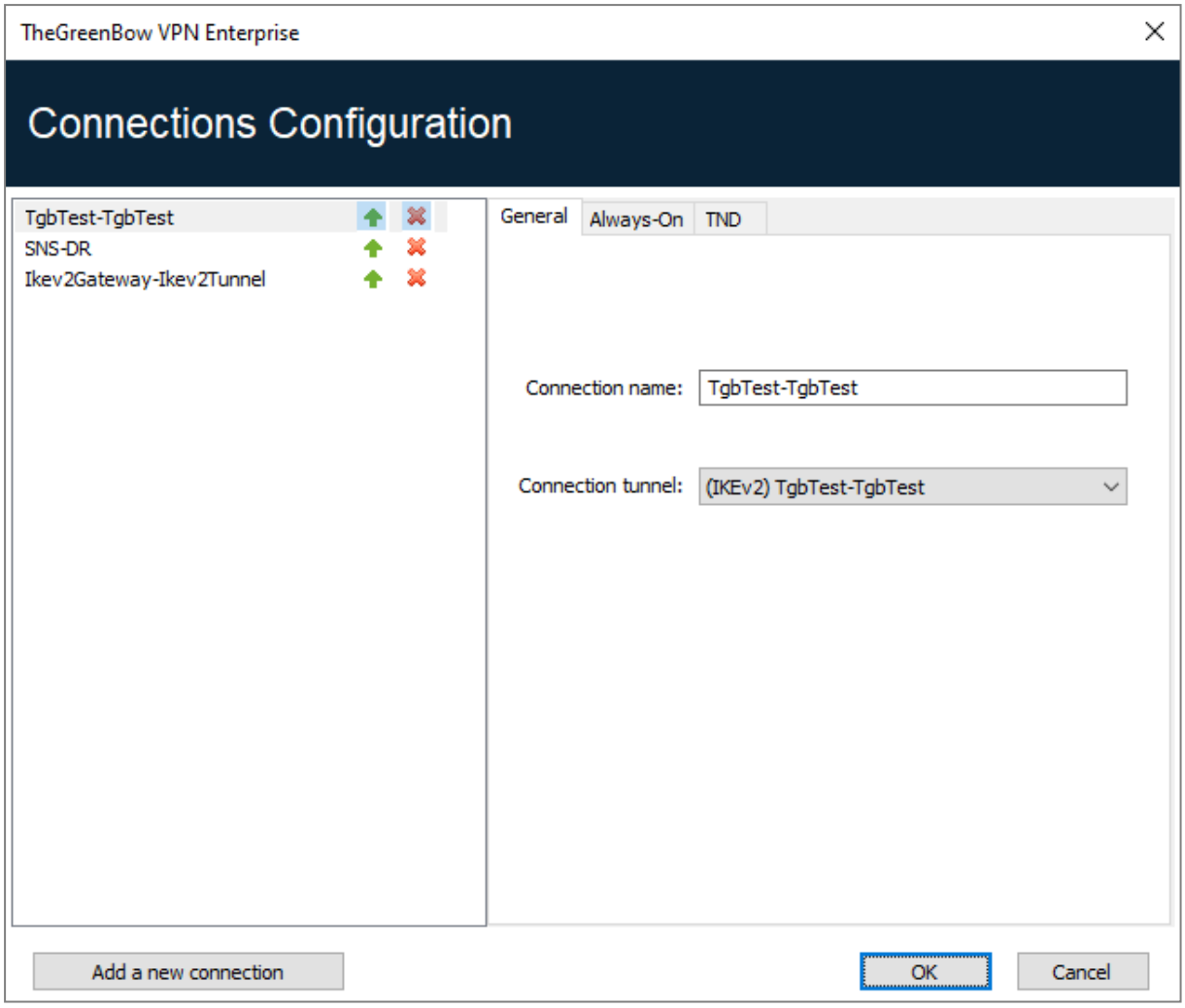
Gestion du Panneau des Connexions

Le **Panneau des Connexions** de SN VPN Client Exclusive est entièrement configurable.



Une connexion VPN est soit un tunnel VPN, soit une connexion **Bureau distant**, c'est-à-dire un tunnel VPN dont la fonction **Bureau distant** est renseignée.

Une fenêtre, accessible dans le menu **Outils** > **Configuration des connexions** permet la gestion des connexions VPN dans le **Panneau des Connexions** : création, nommage, ordonnancement.



La fenêtre de **Configuration des connexions** permet de :

- choisir les connexions VPN qui apparaissent ou pas dans le **Panneau des Connexions** ;
- créer et ordonner les connexions VPN ;
- renommer les connexions VPN ;
- configurer **Always-On** dans le **Panneau TrustedConnect** ;
- configurer **TND** (Détection de réseau de confiance) dans le **Panneau TrustedConnect**.

La partie gauche de la fenêtre illustre la liste des connexions telles qu'elles apparaissent dans le **Panneau des Connexions**.

La partie droite comporte trois onglets :

- **Général**
- **Always-On**
- **TND**

Dans l'onglet **Général**, sont indiquées les paramètres de chaque connexion : son nom, le tunnel VPN associé et l'éventuelle connexion RDP (Remote Desktop Sharing) configurée.

Pour créer une nouvelle connexion VPN, cliquez sur le bouton **Ajouter une connexion**, choisissez un nom et choisissez le tunnel VPN associé. Si une connexion Remote Desktop Sharing est configurée, la possibilité de la choisir apparaît automatiquement en dessous du tunnel choisi. Une fois validées, les modifications faites dans la fenêtre de gestion du **Panneau de Connexions** apparaissent immédiatement dans le **Panneau des Connexions**.

Les onglets **Always-On** et **TND** sont décrits dans le chapitre Gestion du Panneau des Connexions ci-dessous.

NOTE
La configuration du **Panneau des Connexions** est mémorisée dans le fichier de configuration VPN. Elle peut donc être exportée dans les fichiers *.tgb*, ce qui est utile pour déployer un **Panneau de Connexion** identique sur tous les postes.

Gestion du Panneau TrustedConnect

Le **Panneau TrustedConnect** est décrit dans le chapitre Panneau TrustedConnect. Il permet d'ouvrir une connexion VPN de manière automatisée en dehors du réseau de confiance et de garder la connexion ouverte en cas de changement d'interface réseau.

Pour être prise en compte, cette connexion VPN doit respecter les conditions suivantes :

1. La connexion VPN doit être la première connexion VPN définie dans le **Panneau des Connexions**. Pour configurer cette première connexion, reportez-vous au chapitre Gestion du Panneau des Connexions ci-dessus.
2. La connexion VPN doit être configurée en IKEv2.

Les fonctions suivantes du **Panneau TrustedConnect** sont configurables :

- Exclusion d'interfaces réseau d'Always-On
- Détection du réseau de confiance (TND)
- Gestion de l'extraction des tokens ou des cartes à puce
- Gestion des scripts liés au tunnel VPN
- Minimisation de l'IHM
- Purge des fichiers de logs

Always-On

Principe et fonctionnement

La fonctionnalité **Always-On**, toujours active avec le **Panneau TrustedConnect**, assure le maintien de la sécurité de la connexion à chaque changement d'interface réseau.

Les type d'interfaces réseaux pris en charge sont les suivants :

- Adaptateur virtuel (ex : vmware)
- Wi-Fi
- Ethernet
- Modem USB (type smartphone)
- Modem Bluetooth (type smartphone)

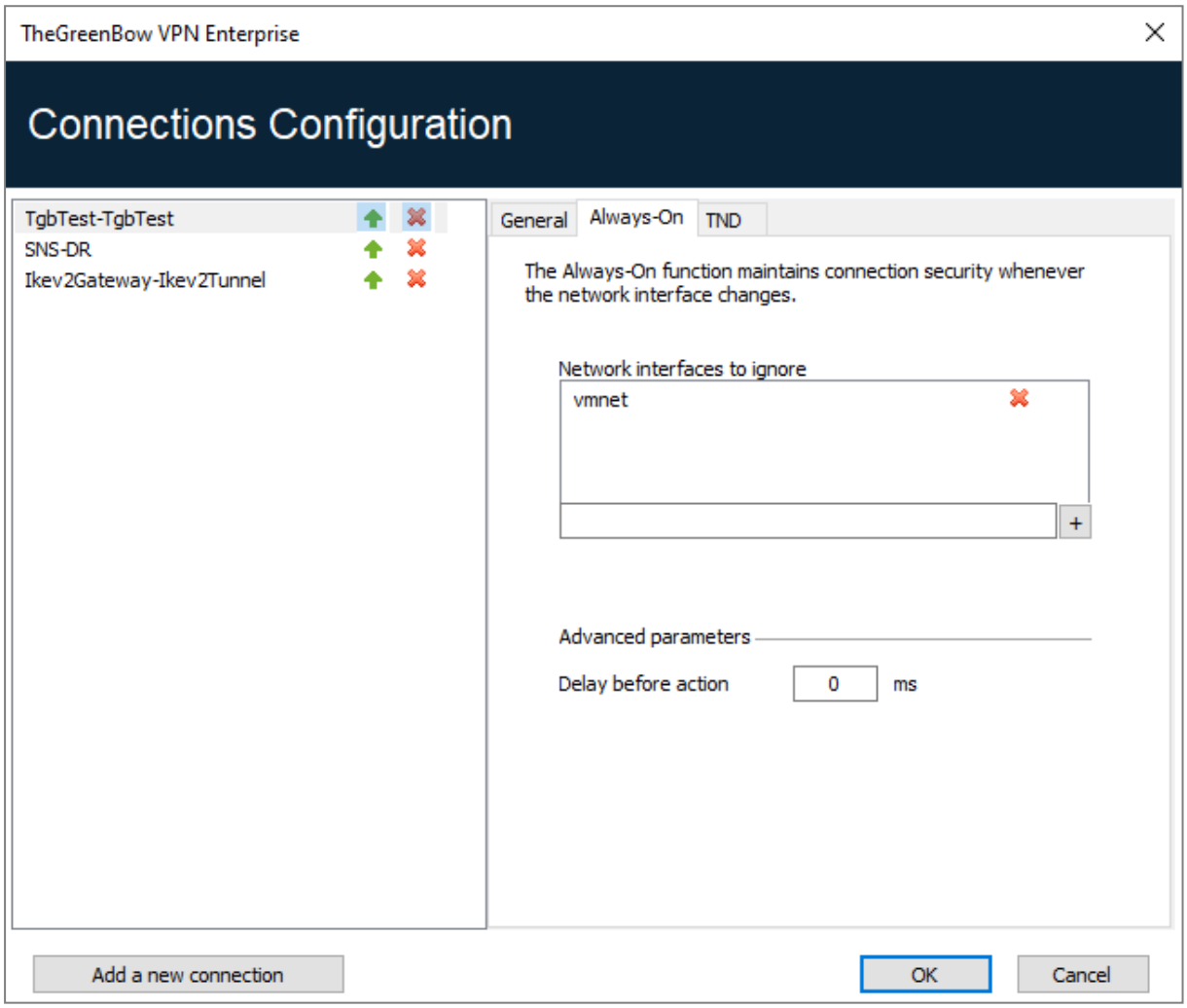
Les évènements réseau déclenchant la reconnexion automatique du tunnel (et la détection du réseau de confiance, le cas échéant), sauf exclusion explicite (voir section Configuration de Always-On) sont les suivants :

- Connexion à un réseau (adresses APIPA ignorées)
- Déconnexion d'un réseau
- Un adaptateur change d'adresse IP ou passage DHCP à statique et vice versa
- ipconfig /release
- ipconfig /renew
- Passage en mode avion

Configuration de Always-On

La fonctionnalité **Always-On** est activée dès lors que le **Panneau TrustedConnect** est utilisé pour ouvrir un tunnel VPN. Elle peut être configurée pour exclure certaines interfaces réseau de la reconnexion automatique du tunnel VPN.

L'onglet **Always-On** de la fenêtre de **Configuration des connexions** permet de configurer les paramètres de la fonctionnalité **Always-On**.



Interfaces réseau à ignorer	Il est possible d'exclure des interfaces réseaux du monitoring de Always-On. L'exclusion d'une interface se fait sur la base de sa propriété **description** (visible par ipconfig /all). La valeur de ce paramètre doit contenir une partie ou la totalité du champ **description** de l'interface réseau à exclure. Si la valeur est partielle, alors toute interface dont le champ **description** contient la valeur définie, sera exclue du monitoring. Les valeurs de ce paramètre ne sont pas sensibles à la casse (toutes les chaînes de caractères sont converties en minuscules avant la comparaison). Vous pouvez spécifier plusieurs interfaces réseau à exclure. Pour cela, entrez le nom de l'interface réseau à exclure, puis cliquez sur le bouton + à droit du champ de saisie. The nom de l'interface réseau est ajouté à liste d'exclusion. Répétez l'opération autant de fois que nécessaire.

Délai de prise en compte	Le temps de prise en compte d'une nouvelle interface réseau varie suivant les systèmes. S'il est trop long, il peut interférer avec le mécanisme TND, ce qui peut aboutir au fait que le Client VPN essaye d'établir une connexion VPN alors que le poste est connecté au réseau de confiance. Pour éviter ce problème, ce paramètre permet de retarder le déclenchement du mécanisme TND (voir section suivante). Il est exprimé en millisecondes. Si la valeur par défaut doit être modifiée, il est recommandé de spécifier une valeur supérieure ou égale à 3000 ms. Par défaut, la valeur vaut 0 et le mécanisme TND est lancé immédiatement, ce qui convient dans la majorité des cas observés.

Détection du réseau de confiance (TND)

Principe et fonctionnement

Généralités

Cette fonctionnalité consiste à détecter si le poste est connecté au réseau de l'entreprise (réseau de confiance) ou non.

Lorsque le Client VPN détecte que le poste n'est pas sur le réseau de l'entreprise, le tunnel prédéfini est ouvert automatiquement. Ce document fait référence à cette fonctionnalité sous le terme TND (Trusted Network Detection).

Le **Panneau TrustedConnect** utilise l'une des deux méthodes suivantes pour détecter si le poste se trouve sur un réseau de confiance ou non par l'association de la détection :

1. d'un suffixe DNS de confiance et de la vérification de l'accès à un serveur web de confiance ainsi que de la validité de son certificat (cf. section Méthode HTTPS) ;
2. d'un serveur Active Directory (AD) et la présence d'un nom de domaine dans une liste de domaines de confiance (cf. section Méthode AD).

Méthode HTTPS

La méthode HTTPS existante est conservée. Elle se déroule en deux étapes :

1. Vérification que l'un des suffixes DNS des interfaces réseau présentes sur le poste fait partie de la liste des suffixes DNS de confiance (liste configurée dans le logiciel, cf. ci-dessous).
2. Accès automatique en HTTPS à un serveur web de confiance, et vérification de la validité de son certificat.

Les deux étapes sont obligatoires et doivent être associées pour détecter que le poste se trouve sur un réseau de confiance. Pour cela, le Client VPN teste en premier lieu la présence d'un suffixe DNS de confiance :

- s'il n'en trouve pas, le Client VPN ne poursuit pas le test, et conclut que le poste n'est pas connecté au réseau de confiance ;
- s'il en trouve un, il poursuit la séquence de test en vérifiant l'accès au serveur de confiance et la validité de son certificat.

Au premier serveur de confiance accessible dont le certificat est valide, le Client VPN conclut que le poste est connecté au réseau de confiance.

Dans tous les autres cas énumérés ci-dessous, le Client VPN conclut que le poste n'est pas connecté au réseau de confiance, et tente alors automatiquement d'ouvrir la connexion VPN configurée :

- aucun suffixe DNS trouvé dans la liste des suffixes DNS de confiance,
- liste des suffixes DNS de confiance vide,
- liste d'URL de serveurs de confiance vide,
- aucun serveur de confiance accessible, ou aucun n'ayant de certificat valide,

Pour activer la fonctionnalité de détection du réseau de confiance (TND), les paramètres suivants doivent donc être configurés :

- une liste de suffixes DNS,
- une liste d'URL de serveurs de confiance.

NOTE
Sur certains postes, lors de l'apparition d'une interface réseau, un délai de quelques secondes est nécessaire avant que l'interface ne soit prête à émettre. Pour pallier ce délai, le paramètre **Délai de prise en compte** est disponible dans l'onglet **Always-On** (voir section précédente).

Méthode AD

Cette méthode de détection de réseaux de confiance (TND), introduite avec la version 7.5 de SN VPN Client Exclusive, permet d'exploiter la connexion à Active Directory (AD) pour déterminer si le poste se trouve sur un réseau de confiance. Cette méthode se décline en trois variantes :

- **AD seul** : vérifie si le poste est intégré à un domaine et, si c'est le cas, le nom du domaine est vérifié par rapport à une liste de noms de domaines de confiance (si la liste est vide, tout domaine est accepté) ;
- **LDAP** : comme **AD seul**, plus validation par la connexion à un service d'annuaire LDAP ;
- **LDAPS** : comme **AD seul**, plus validation sécurisée par la connexion à un service d'annuaire LDAPS.

NOTE
En mode GINA, le poste sera déclaré comme n'étant pas sur un réseau de confiance tant qu'il n'a pas ouvert de session Windows.

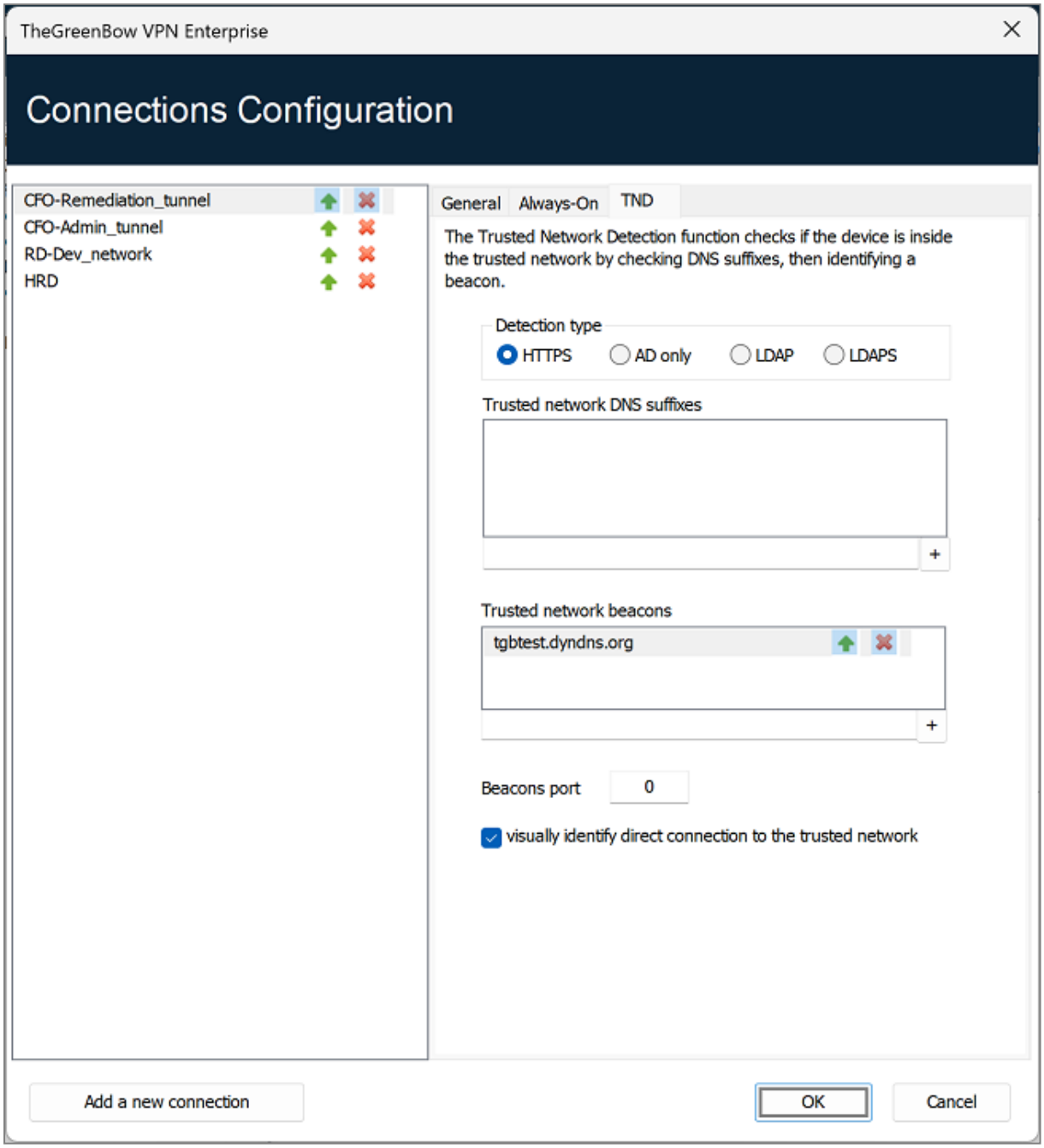
Configuration de TND

L'onglet **TND** de la fenêtre de **Configuration des connexions** permet de configurer les paramètres de la fonctionnalité **Trusted Network Detection**.

Quatre boutons radio permettent de sélectionner le type de détection :

- HTTPS
- AD seul
- LDAP
- LDAPS

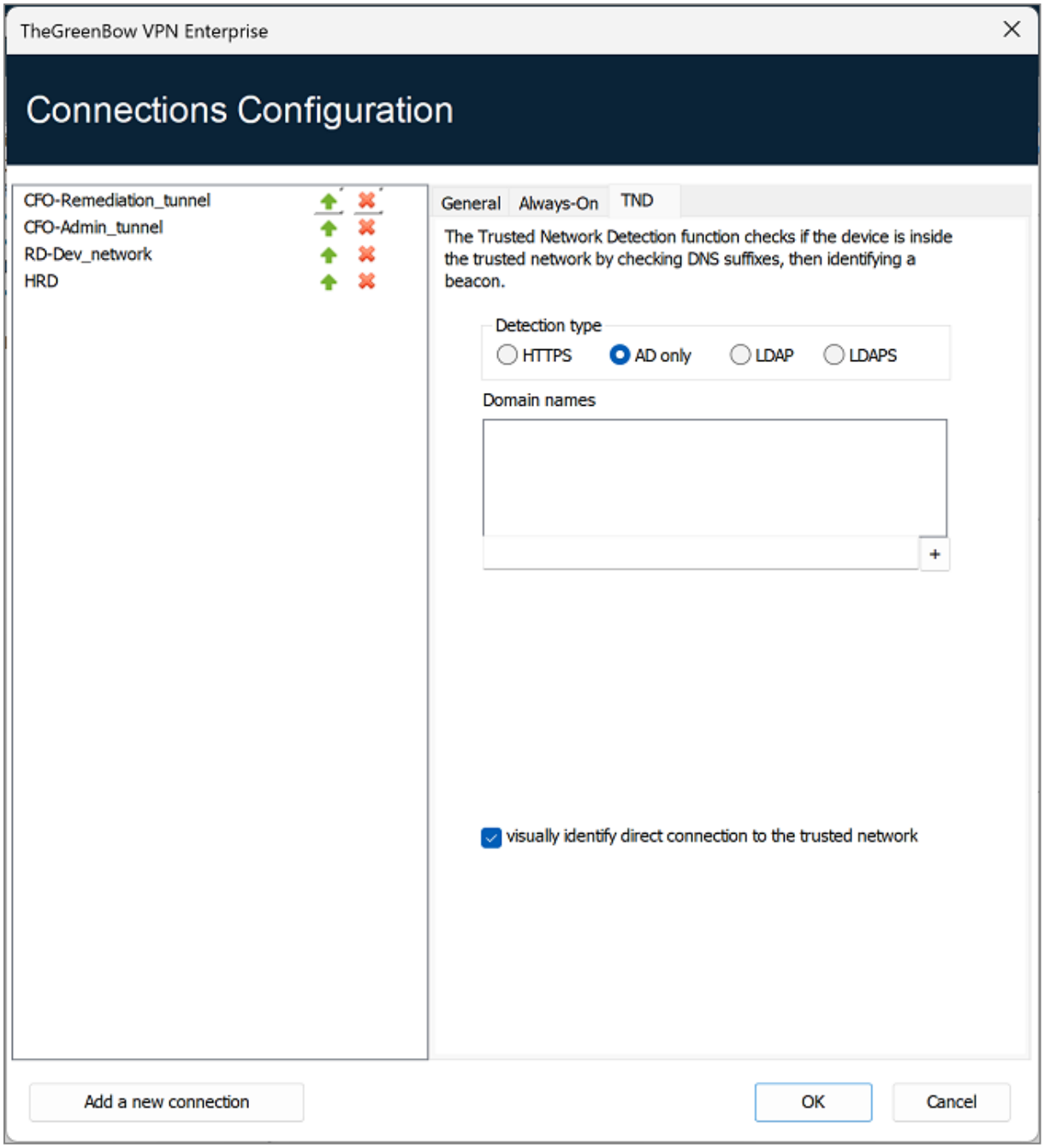
Voici les options pour le type de détection **HTTPS** :



Suffixes DNS du réseau de confiance	Ce paramètre définit la liste des suffixes DNS de confiance. Il peut contenir plusieurs suffixes DNS. Pour cela, entrez le nom du suffixe à ajouter, puis cliquez sur le bouton **+** à droit du champ de saisie. Répétez l'opération autant de fois que nécessaire.

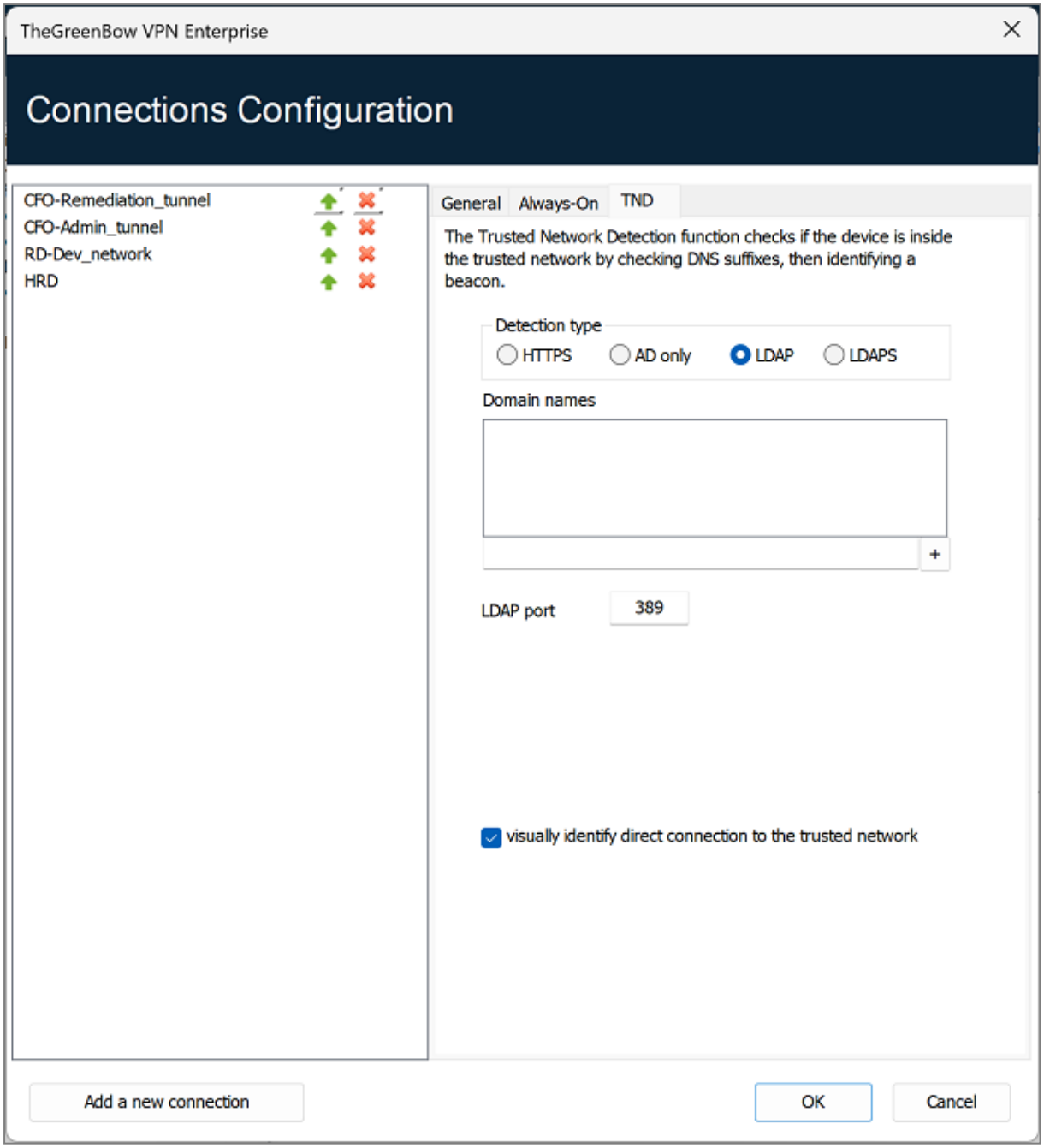
Balises du réseau de confiance	Ce paramètre définit la liste des adresses IP (ou noms DNS) des serveurs de confiance à utiliser. Cette liste peut contenir plusieurs adresses IP (ou noms DNS) de serveurs de confiance. Le Client VPN teste alors successivement toutes les adresses IP (ou noms DNS) et tous les certificats associés à chaque serveur, jusqu'à en trouver un accessible et valide. Les adresses IP (ou noms DNS) de la liste doivent être séparées par une virgule, sans espace. Il n'est pas nécessaire de faire précéder l'adresse IP (ou le nom DNS) du préfixe *https://*. **IMPORTANT** Par défaut, le **Panneau TrustedConnect** tente de se connecter à la page */index.html*. Si celle-ci n'existe pas sur le serveur, celui-ci ne peut pas servir de balise.
Port des balises	Ce paramètre définit le port à utiliser pour joindre les serveurs de confiance. Il n'est possible de configurer qu'un seul port, qui sera utilisé pour toutes les adresses IP (ou noms DNS). Si ce paramètre n'est pas configuré, le Client VPN utilise par défaut le port 443.
Identifier visuellement la connexion directe au réseau de confiance	Cette option ajoute un repère visuel au **Panneau TrustedConnect** pour indiquer que le Client VPN est connecté au réseau de confiance. Si la case est cochée, l'icône en barre des tâches et la couleur du rond dans le panneau est bleue lorsque la machine est connectée au réseau de confiance et verte lorsqu'un tunnel est ouvert. Si la case est décochée, l'icône en barre des tâches et le rond dans le panneau reste vert dans les deux cas. Aucune distinction n'est faite entre le réseau de confiance et un tunnel ouvert.

Voici les options pour le type de détection **AD seul** :



Noms de domaines	Ce paramètre définit la liste des noms de domaines de confiance. Il peut contenir plusieurs noms de domaines. Pour cela, entrez le nom du domaine à ajouter, puis cliquez sur le bouton **+** à droit du champ de saisie. Répétez l'opération autant de fois que nécessaire. Les noms de domaines sont insensibles à la casse.
Identifier visuellement la connexion directe au réseau de confiance	Cette option ajoute un repère visuel au **Panneau TrustedConnect** pour indiquer que le Client VPN est connecté au réseau de confiance. Si la case est cochée, l'icône en barre des tâches et la couleur du rond dans le panneau est bleue lorsque la machine est connectée au réseau de confiance et verte lorsqu'un tunnel est ouvert. Si la case est décochée, l'icône en barre des tâches et le rond dans le panneau reste vert dans les deux cas. Aucune distinction n'est faite entre le réseau de confiance et un tunnel ouvert.

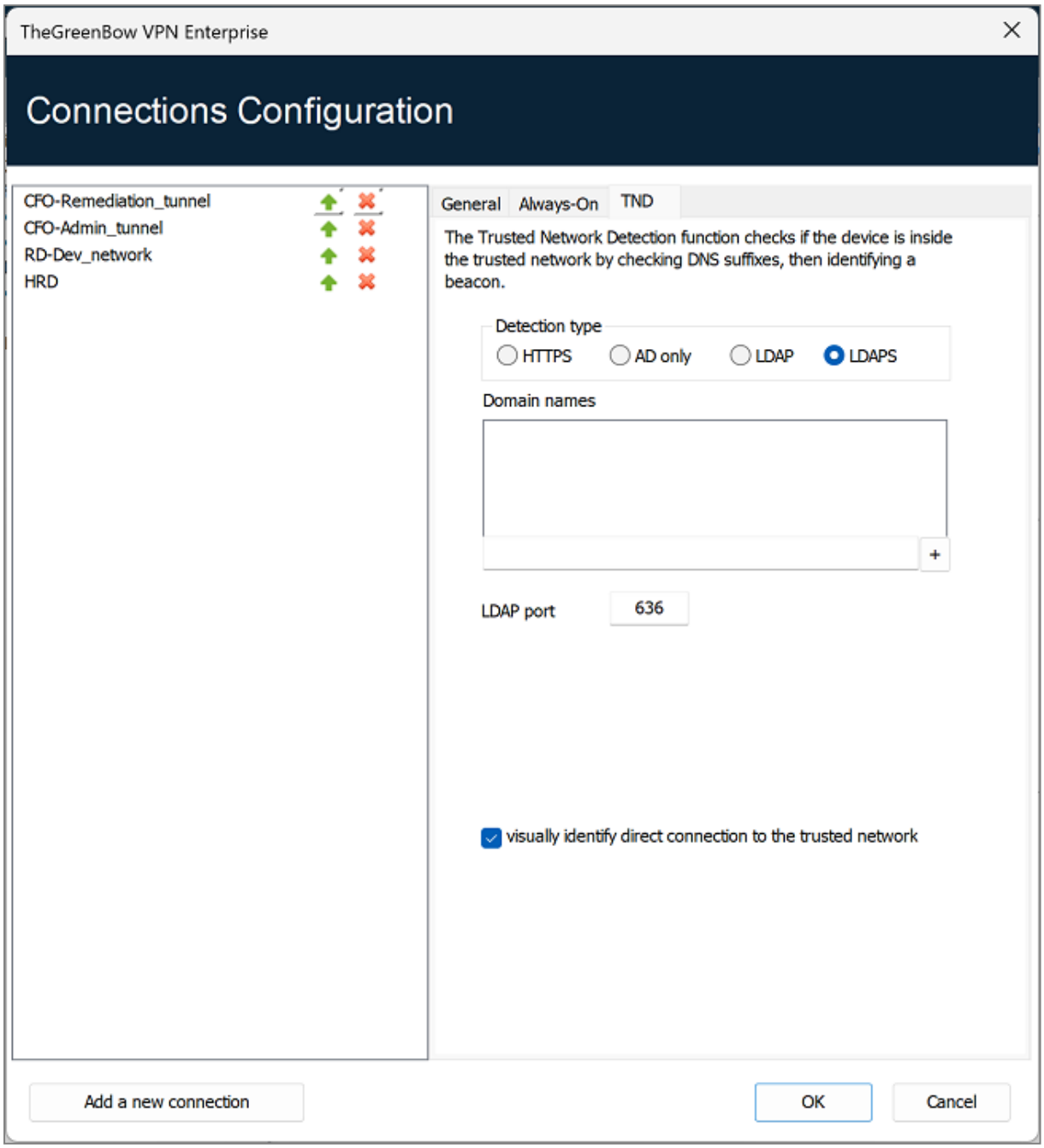
Voici les options pour le type de détection **LDAP** :



Noms de domaines	Ce paramètre définit la liste des noms de domaines de confiance. Il peut contenir plusieurs noms de domaines. Pour cela, entrez le nom du domaine à ajouter, puis cliquez sur le bouton + à droit du champ de saisie. Répétez l'opération autant de fois que nécessaire. Les noms de domaines sont insensibles à la casse.
Port LDAP	Ce paramètre définit le port à utiliser pour joindre le serveur LDAP. Il n'est possible de configurer qu'un seul port, qui sera utilisé pour tous les noms de domaines. La valeur par défaut est 389.

Identifier visuellement la connexion directe au réseau de confiance	Cette option ajoute un repère visuel au **Panneau TrustedConnect** pour indiquer que le Client VPN est connecté au réseau de confiance. Si la case est cochée, l'icône en barre des tâches et la couleur du rond dans le panneau est bleue lorsque la machine est connectée au réseau de confiance et verte lorsqu'un tunnel est ouvert. Si la case est décochée, l'icône en barre des tâches et le rond dans le panneau reste vert dans les deux cas. Aucune distinction n'est faite entre le réseau de confiance et un tunnel ouvert.

Voici les options pour le type de détection **LDAPS** :

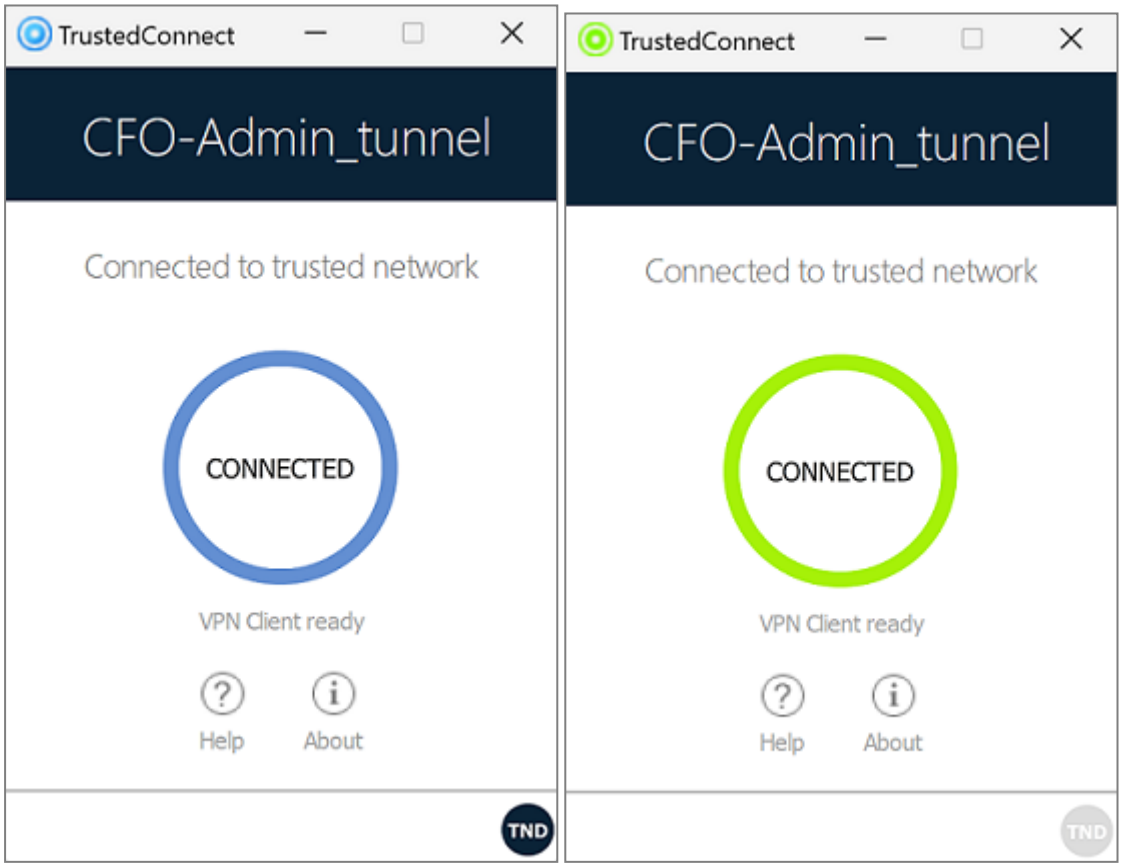


Noms de domaines	Ce paramètre définit la liste des noms de domaines de confiance. Il peut contenir plusieurs noms de domaines. Pour cela, entrez le nom du domaine à ajouter, puis cliquez sur le bouton + à droit du champ de saisie. Répétez l'opération autant de fois que nécessaire. Les noms de domaines sont insensibles à la casse.
Port LDAPS	Ce paramètre définit le port à utiliser pour joindre le serveur LDAP sécurisé. Il n'est possible de configurer qu'un seul port, qui sera utilisé pour tous les noms de domaines. La valeur par défaut est 636.
Identifier visuellement la connexion directe au réseau de confiance	Cette option ajoute un repère visuel au **Panneau TrustedConnect** pour indiquer que le Client VPN est connecté au réseau de confiance. Si la case est cochée, l'icône en barre des tâches et la couleur du rond dans le panneau est bleue lorsque la machine est connectée au réseau de confiance et verte lorsqu'un tunnel est ouvert. Si la case est décochée, l'icône en barre des tâches et le rond dans le panneau reste vert dans les deux cas. Aucune distinction n'est faite entre le réseau de confiance et un tunnel ouvert.

Désactivation de TND

Dans certains cas, il peut s'avérer utile de pouvoir ouvrir un tunnel pour accéder à certaines ressources, même lorsque le réseau de confiance a été détecté.

La propriété MSI *DIALERBEHAVIOR*, à configurer lors de l'installation, ajoute une option dans la barre d'état permettant de désactiver et de réactiver la fonction TND.



Lorsque la fonction TND est désactivée (icône TND grisée), le tunnel est monté systématiquement. Lorsqu'elle est activée (icône TND bleue), il n'est pas possible de monter de tunnel lorsqu'un réseau de confiance a été détecté (comportement par défaut).

Reportez-vous au « Guide de déploiement » pour les instructions correspondantes.

Scripts

Le **Panneau TrustedConnect** exécute les scripts liés à l'ouverture et à la fermeture d'un tunnel. Pour configurer cette fonctionnalité, reportez-vous au chapitre Automatisation.

Minimisation du Panneau

Par défaut, le **Panneau TrustedConnect** est minimisé automatiquement dans la zone de notification (systray) au bout de deux secondes, lorsque le poste a été détecté comme étant connecté au réseau de confiance (soit physiquement, soit au travers du tunnel VPN).

Il est possible de configurer le délai avant que l'IHM du Client VPN ne soit minimisée, ainsi que le type de minimisation. Le **Panneau TrustedConnect** peut être minimisé en barre des tâches ou dans la zone de notification (systray, par défaut).

NOTE
Délai et type de minimisation ne sont applicables qu'à la minimisation automatique du **Panneau TrustedConnect**, sur détection de connexion au réseau de confiance.

Ces configurations doivent être effectuées à l'aide des propriétés de l'installeur du Client VPN.

Reportez-vous au « Guide de déploiement » pour les instructions correspondantes.

Désactivation du bouton de déconnexion

Afin de garantir une meilleure protection du poste de travail, l'administrateur peut désactiver le bouton de déconnexion dès que la connexion est en cours (contrôle TND, ouverture d'un tunnel, etc.). Pour cela, il convient d'utiliser la propriété MSI *BTNBEHAVIORTC* ou le paramètre correspondant dans le fichier *vpnsetup.ini* lors de l'installation.

Lorsque cette option est activée, tout clic sur le bouton **En cours…** ou **Connecté** dans le **Panneau TrustedConnect** sera sans effet. Il est impossible de fermer le tunnel.

Reportez-vous au « Guide de déploiement » pour les instructions correspondantes.

Suppression des éléments de menu

Afin de garantir une meilleure protection du poste de travail, l'administrateur peut désactiver toutes ou une partie des options du menu. Pour cela, il convient d'utiliser la propriété MSI *MENUITEMTC* ou le paramètre correspondant dans le fichier *vpnsetup.ini* lors de l'installation.

Lorsque cette option est activée, l'utilisateur n'aura pas accès à certaines options du menu (accès aux logs, quitter l'interface, etc.), voire n'aura pas du tout accès au menu.

Reportez-vous au « Guide de déploiement » pour les instructions correspondantes.

Redémarrage automatique du Panneau TrustedConnect

Afin de garantir une meilleure protection du poste de travail, l'administrateur peut forcer le redémarrage automatique du **Panneau TrustedConnect** lorsqu'il est arrêté. Pour cela, il convient d'utiliser la propriété MSI RESTARTGUITC ou le paramètre correspondant dans le fichier vpnsetup.ini lors de l'installation.

Lorsque cette option est activée, le **Panneau TrustedConnect** sera redémarré automatiquement lorsque l'utilisateur quitte le logiciel ou si ce dernier s'est arrêté de manière inopinée.

Reportez-vous au « Guide de déploiement » pour les instructions correspondantes.

Purge des logs

Il est possible de configurer le nombre de jours pendant lequel conserver les fichiers de logs. La valeur par défaut est de 10 jours.

Cette configuration doit être effectuée à l'aide de la propriété *VPNLOGPURGE* de l'installeur du Client VPN.

Reportez-vous au « Guide de déploiement » pour les instructions correspondantes.

Retrait de carte à puce ou de token

Il est possible de configurer le comportement du **Panneau TrustedConnect** lorsque la carte à puce ou le token est extrait du lecteur, alors qu'un tunnel VPN est ouvert.

Cette configuration doit être effectuée à l'aide des propriétés de l'installeur du Client VPN.

Reportez-vous au « Guide de déploiement » pour les instructions correspondantes.

Mode GINA

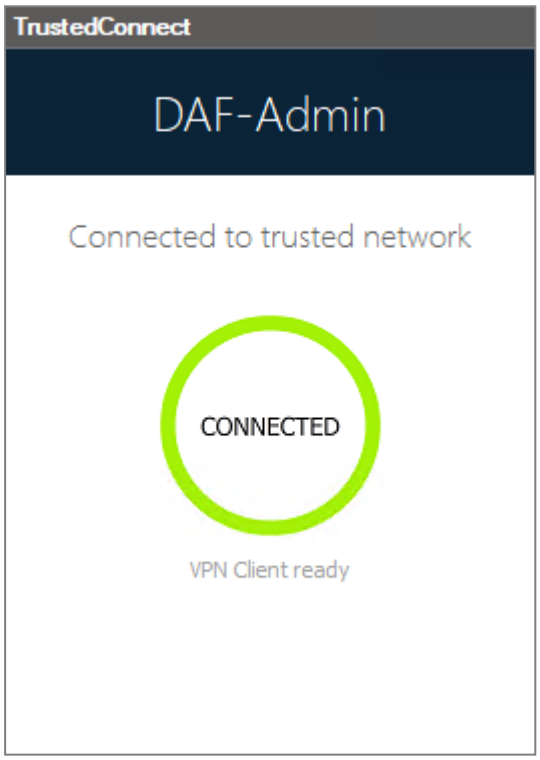
Présentation

Le mode GINA permet d'ouvrir des connexions VPN avant l'ouverture d'une session Windows.

Cette fonction permet par exemple d'établir une connexion sécurisée vers un serveur de gestion des droits d'accès de façon à obtenir les droits d'accès au poste utilisateur avant l'ouverture de la session utilisateur.

Lorsqu'un tunnel est configuré « en mode GINA », deux cas se présentent :

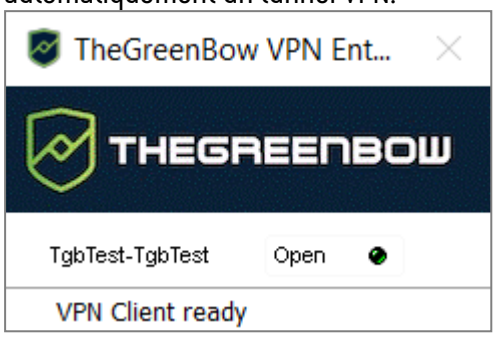
1. Si le mode de démarrage du Client VPN est configuré en mode **TrustedConnect** (voir section Général), alors le **Panneau TrustedConnect** est affiché sur l'écran d'ouverture de session Windows et le Client VPN tente de se connecter automatiquement au réseau de confiance.



NOTE

À partir de la version 7.4 de SN VPN Client Exclusive, si l'option permettant de choisir la connexion dans le **Panneau TrustedConnect** a été activée à l'aide de la propriété MSI `DIALERBEHAVIOR` lors de l'installation du Client VPN (cf. « Guide de déploiement »), l'utilisateur peut choisir la connexion avant l'ouverture de la session Windows (cf. section Choix de la connexion).

2. Sinon, une fenêtre d'ouverture de tunnel similaire au **Panneau des Connexions** est affichée sur l'écran d'ouverture de session Windows. Elle permet d'ouvrir manuellement ou automatiquement un tunnel VPN.



NOTE
Depuis la version 7.5 de SN VPN Client Exclusive, le comportement du mode GINA s'adapte en fonction du niveau de conformité détecté par le Secure Connection Agent (SCA), qui détermine si un poste doit être autorisé à accéder au réseau de l'entreprise (voir la section En mode GINA).

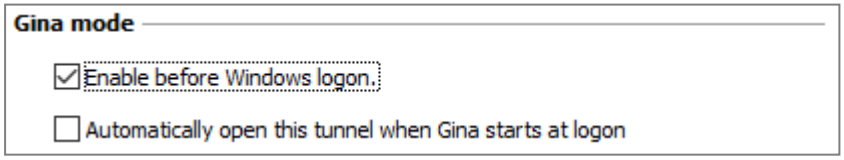
Cas d'usage particulier

Si vous souhaitez utiliser plusieurs tunnels, dont un pour le mode GINA et un autre pour la connexion de l'utilisateur en mode TrustedConnect après l'ouverture de la session Windows, le tunnel utilisateur doit être le premier de la liste des connexions.

Ainsi, le tunnel GINA sera ouvert au démarrage du poste, puis une transition vers le tunnel utilisateur sera opérée lors de l'ouverture de la session Windows. De même, une transition du tunnel utilisateur vers le tunnel GINA sera effectuée lorsque l'utilisateur ferme sa session Windows.

Configurer le mode GINA

La configuration d'une connexion VPN en mode GINA s'effectue dans l'onglet **Automatisation** du tunnel concerné.



Voir le chapitre Automatisation.

Utiliser le mode GINA

Lorsque le tunnel VPN est configuré en mode GINA, la fenêtre d'ouverture des tunnels GINA est affichée sur l'écran d'ouverture de session Windows. Le tunnel VPN s'ouvre automatiquement s'il est configuré dans ce sens.

Un tunnel VPN en mode GINA peut parfaitement mettre en œuvre une authentification EAP (l'utilisateur doit alors entrer son login / mot de passe), ou une authentification par certificat (l'utilisateur doit alors entrer le code PIN d'accès à la carte à puce).

Considération de sécurité

Un tunnel configuré en mode GINA peut être ouvert avant l'ouverture de la session Windows, donc par n'importe quel utilisateur du poste. Il est donc fortement recommandé de configurer une authentification forte par certificat, et si possible sur support amovible.

NOTE

Pour que l'option **Ouvrir automatiquement sur détection de trafic** soit opérationnelle après ouverture de la session Windows, l'option **Peut être ouvert avant le logon Windows** ne doit pas être cochée.

IMPORTANT

- Limitation : Les scripts ne sont pas disponibles pour les tunnels VPN en mode GINA.
- Un tunnel VPN configuré avec un certificat mémorisé dans le magasin de certificats Windows ne fonctionne pas en mode GINA. En effet, le mode GINA est exécuté avant qu'un utilisateur Windows ne soit identifié (hors de toute session utilisateur). Le logiciel ne peut donc pas identifier, dans le magasin de certificats Windows, le magasin utilisateur qui doit être utilisé.

Mode filtrant

SN VPN Client Exclusive contient des fonctionnalités avancées appelées Mode filtrant et Détection de portail captif (ou CPD pour *Captive Portal Detection*) prévues pour un usage spécifique et qu'il convient d'ajouter lors de l'installation du logiciel avant de pouvoir les utiliser.

Le Mode filtrant du Client VPN est une fonction de filtrage des flux entrants et sortants du poste. Il est activé dès lors que le Client VPN ne se trouve pas sur le réseau de confiance. Par conséquent, il est uniquement disponible avec le **Panneau TrustedConnect**.

Le temps accordé à l'utilisateur pour se connecter au portail captif est paramétrable dans l'onglet **CPD** de la fenêtre de **Configuration des connexions**. La valeur par défaut est 180 s (3 min).

Secure Connection Agent

Présentation

Depuis la version 7.5 de SN VPN Client Exclusive, le Client VPN est en mesure de communiquer avec un module complémentaire fourni séparément appelé Secure Connection Agent (SCA). Il fait partie de l'offre de produits élargie et sert de lien entre les Clients VPN et le Connection Management Center (CMC).

Le SCA assure les deux fonctions suivantes :

1. Surveillance de la conformité des postes : le SCA vérifie si le poste doit être autorisé à accéder au réseau de l'entreprise. Le Client VPN adaptera son comportement en fonction du niveau de conformité détecté.
2. Transfert des traces d'audit du Client VPN au CMC.

Surveillance de la conformité des postes

Introduction

La fonction de conformité du poste vérifie la disponibilité et l'état du pare-feu Windows et du logiciel antivirus renseigné au niveau du Centre de sécurité Windows.

À ce jour, trois niveaux de conformité sont définis et le Client VPN agira de façon différente pour chacun de ces niveaux, comme décrit dans la table de vérité ci-dessous.

Protection contre les virus et les menaces		Pare-feu et protection du réseau		Résultat
0	+	0	=	 Aucun tunnel ne peut être ouvert
1	+	0	=	 Passage par une zone de remédiation
0	+	1	=	
1	+	1	=	 Accès au réseau sensible

Une connexion VPN de remédiation doit être considérée comme un tunnel VPN à accès restreint. Elle pourrait, par exemple, permettre à un administrateur système de prendre le contrôle du PC à partir du réseau de l'entreprise.

NOTE
Après l'ouverture d'une session Windows, le Secure Connection Agent utilisera le dernier niveau de conformité connu jusqu'au démarrage du service du Centre de sécurité Windows.

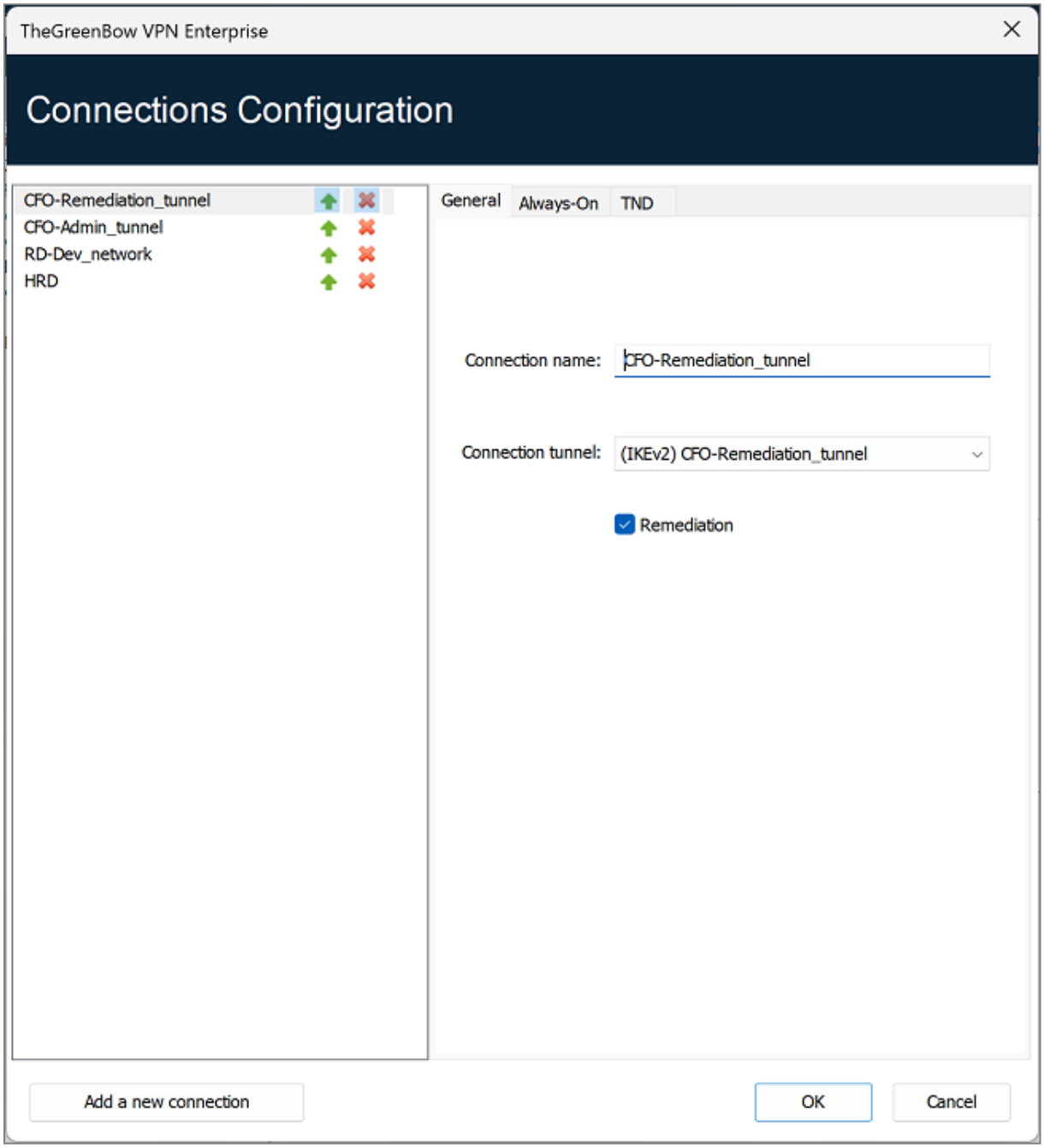
Configuration du Client VPN

Lorsque le Secure Connection Agent (SCA) détecte une quasi-conformité, une connexion de remédiation sera ouverte si elle a été configurée.

Pour configurer une connexion de remédiation, procédez comme suit :

1. Accédez au **Panneau de Configuration** de SN VPN Client Exclusive.
2. Dans le menu **Outils**, sélectionnez **Configuration des connexions** pour ouvrir la fenêtre de **Configuration des connexions**.
3. Sur l'onglet **Général**, cochez la case **Remédiation** pour la connexion que vous souhaitez utiliser en tant que connexion de remédiation.

NOTE
Cette information est stockée dans le fichier de configuration.



IMPORTANT
La case **Remédiation** ne doit être cochée que pour une seule connexion. Si la case **Remédiation** est cochée pour plusieurs connexions, il est impossible de savoir quelle connexion sera utilisée.

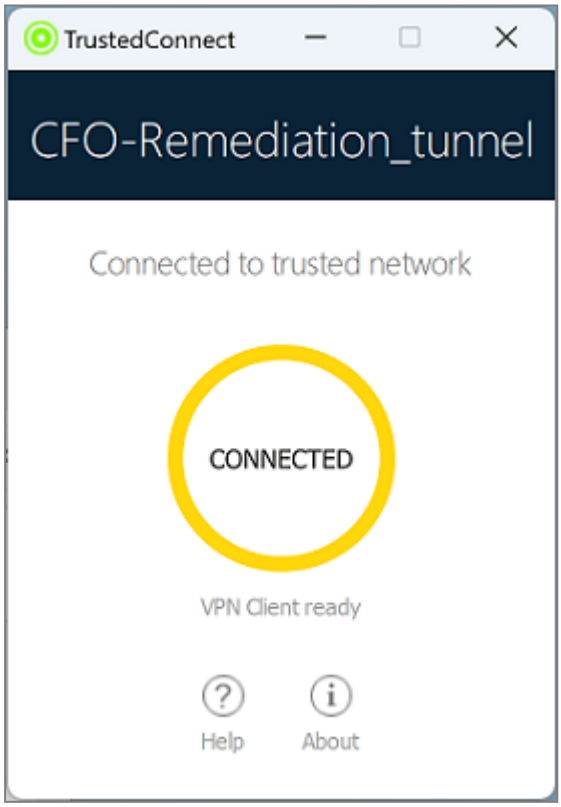
Sélection du tunnel à ouvrir en fonction du niveau de conformité

Dans le Panneau TrustedConnect

Le niveau de conformité est utilisé par le **Panneau TrustedConnect** lors de la sélection du tunnel.

Lorsque le contrôle de conformité échoue, le message suivant s'affiche :

Lorsque le poste doit passer par une zone de remédiation et qu'un tunnel de remédiation a été configuré, le message suivant s'affiche :



Le **Panneau TrustedConnect** prend en compte les changements de conformité à la volée. Le comportement du **Panneau TrustedConnect** peut être configuré à l'aide de la propriété MSI

`DIALERBEHAVIOR` (cf. « Guide de déploiement ») afin de provoquer un basculement automatique vers :

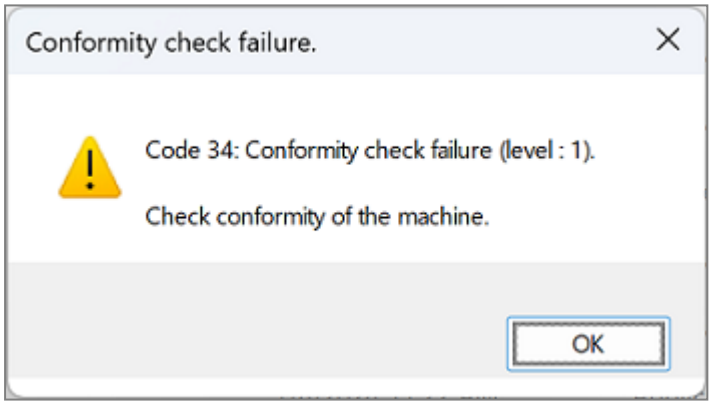
- une erreur de conformité ou un tunnel de remédiation lorsque le niveau de conformité devient non conforme ;
- un tunnel normal lorsque le niveau de conformité devient conforme ;
- le tunnel de remédiation lorsque le niveau de conformité exige un passage en zone de remédiation.

Dans le Panneau des Connexions

Le contrôle de conformité peut être réalisé dans le **Panneau des Connexions** de manière similaire au fonctionnement dans le **Panneau TrustedConnect** (cf. section Dans le Panneau TrustedConnect).

La principale différence avec le **Panneau TrustedConnect** réside dans le fait qu'il n'y a pas de mécanisme d'automatisation dans le **Panneau des Connexions**. C'est uniquement au moment de l'ouverture du tunnel que la vérification est faite pour savoir si en fonction de la conformité le tunnel doit s'ouvrir ou non.

Lorsque le tunnel ne doit pas s'ouvrir, une erreur s'affiche à l'écran et un message est consigné dans la **Console** :



Si un tunnel de remédiation est configuré, l'utilisateur pourra l'ouvrir en vue de mettre en conformité le poste.

Lorsque le SCA n'est pas installé et que, par conséquent, le contrôle de conformité n'est pas activé, quelle que soit la connexion, le tunnel lié à la connexion peut être ouvert.

IMPORTANT
Le niveau de conformité est uniquement disponible au niveau connexion et non au niveau tunnel. Par conséquent, le contrôle de conformité est uniquement géré en mode **Panneau des Connexions**.
Un utilisateur ayant accès au **Panneau de Configuration** du Client VPN peut monter n'importe quel tunnel indépendamment du niveau de conformité.

En mode GINA

L'information permettant de basculer vers un tunnel de remédiation n'étant pas disponible avant l'ouverture de la session Windows, l'ouverture d'un tunnel de remédiation n'est pas possible en mode GINA. En revanche, l'ouverture de tout tunnel sera bloquée si le poste ne respecte aucun critère de conformité.

Transfert des traces d'audit du Client VPN au CMC

Introduction

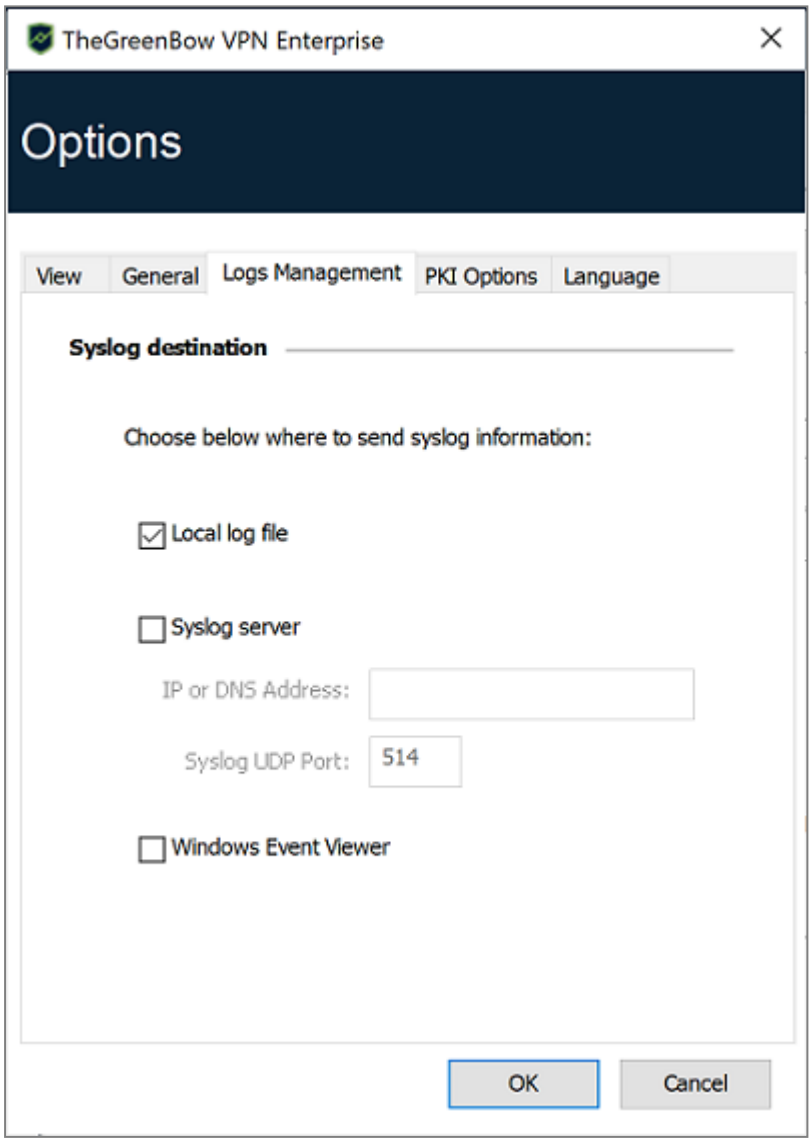
Le transfert des traces d'audit a pour objectif de collecter les traces d'audit générées par le Client VPN (stockées dans le sous-dossier *LogFiles\System*) et de les transmettre au Connection Management Center (CMC).

Configuration du Client VPN

Pour que des traces d'audit puissent être transférées, il faut déjà que le Client VPN en génère !

Pour activer les traces d'audit, procédez de la manière suivante :

1. Accédez au **Panneau de Configuration** de SN VPN Client Exclusive.
2. Dans le menu **Outils**, sélectionnez **Options...**.
3. Sélectionnez l'onglet **Gestion des logs**.
4. Cochez la case **Fichier local**.
5. Cliquez sur **OK**.



Reportez-vous au chapitre **Logs administrateur, Console et traces** pour une description complète des différents types de logs disponibles.

Options

Affichage

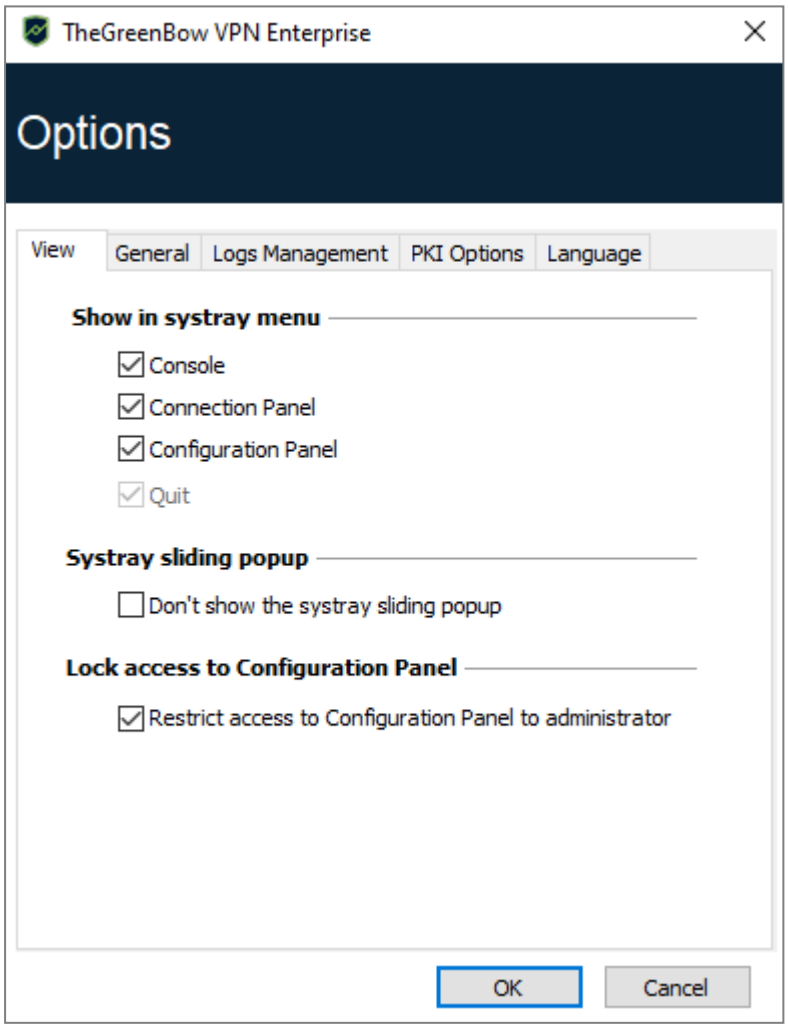
Les options de l'onglet **Affichage** de la fenêtre **Options** permettent de masquer pratiquement toutes les interfaces du logiciel :

- options du menu en barre des tâches,
- popup glissante en barre des tâches,
- accès au **Panneau de Configuration**.

Visualisation des options de menu en barre des tâches

Les options **Console**, **Panneau de Configuration** et **Panneau des Connexions** du menu en barre des tâches peuvent être masquées. Le menu peut ainsi se réduire à l'option **Quitter**.

L'option **Quitter** du menu en barre des tâches ne peut être supprimée à partir du logiciel. Elle peut toutefois être supprimée en utilisant les options d'installation (cf. « Guide de déploiement »).



Affichage de la popup glissante en barre des tâches

Lorsque l'option **Ne pas afficher la popup de barre des tâches** est désactivée, une fenêtre popup glissante apparaît au-dessus de l'icône du Client VPN en barre des tâches à l'ouverture et à la fermeture d'un tunnel VPN.

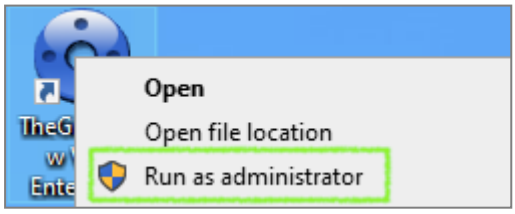
Cette fenêtre identifie l'état du tunnel au cours de son ouverture ou de sa fermeture, et disparaît automatiquement, à moins que la souris ne soit dessus :

Tunnel ouvert	
Tunnel fermé	
Incident d'ouverture du tunnel : la fenêtre affiche l'explication succincte de l'incident, et un lien cliquable vers plus d'informations sur cet incident.	

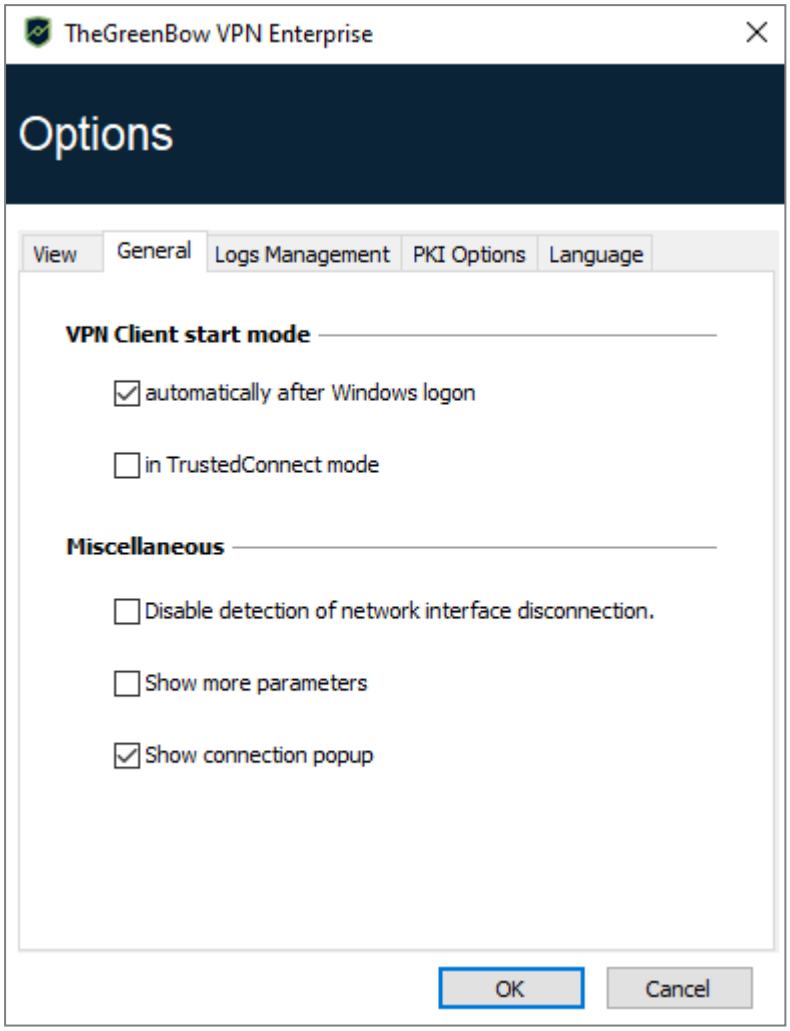
Restreindre l'accès au Panneau de Configuration

Dans SN VPN Client Exclusive, l'interface du **Panneau de Configuration** est par défaut restreinte aux administrateurs. Pour rendre le **Panneau de Configuration** accessible aux utilisateurs, décochez l'option **Restreindre l'accès du panneau de configuration aux administrateurs**.

Pour lancer le Client VPN en mode administrateur, cliquez sur l'icône **SN VPN Client Exclusive** avec le bouton droit de la souris, puis sélectionnez l'option de menu **Exécuter en tant qu'administrateur**.



Général



Mode de démarrage du Client VPN

Lorsque l'option **automatiquement après le logon Windows** est cochée, le Client VPN démarre automatiquement à l'ouverture de la session utilisateur.

Si l'option est décochée, l'utilisateur devra lancer manuellement le Client VPN, soit par double-clic sur l'icône du bureau, soit en sélectionnant le menu de lancement du logiciel dans le menu **Démarrer** de Windows.

Reportez-vous à la section Démarrer le logiciel pour plus de détails.

Si l'option **en mode TrustedConnect** est également cochée, le Client VPN démarre avec le **Panneau TrustedConnect**. Sinon, le Client VPN démarre avec le **Panneau des Connexions**.

Désactiver la détection de déconnexion

Dans son comportement standard, le Client VPN ferme le tunnel VPN (de son côté), dès lors qu'il constate un problème de communication avec la passerelle VPN distante.

Pour des réseaux physiques peu fiables, sujets à des micro-déconnexions fréquentes, cette fonction peut présenter des inconvénients (qui peuvent aller jusqu'à l'impossibilité d'ouvrir un tunnel VPN).

En cochant la case **Désactiver la détection de déconnexion**, le Client VPN évite de fermer les tunnels dès qu'une déconnexion est constatée. Cela permet de garantir une excellente stabilité du tunnel VPN, y compris sur des réseaux physiques peu fiables, typiquement les réseaux sans fil de type Wi-Fi, 4G, 5G, ou satellite.

Afficher la popup de connexion

Une fenêtre de connexion est automatiquement affichée à chaque connexion VPN établie.

Il est possible ici de désactiver l'affichage de cette fenêtre en décochant la case **Afficher la popup de connexion**.

Afficher plus de paramètres

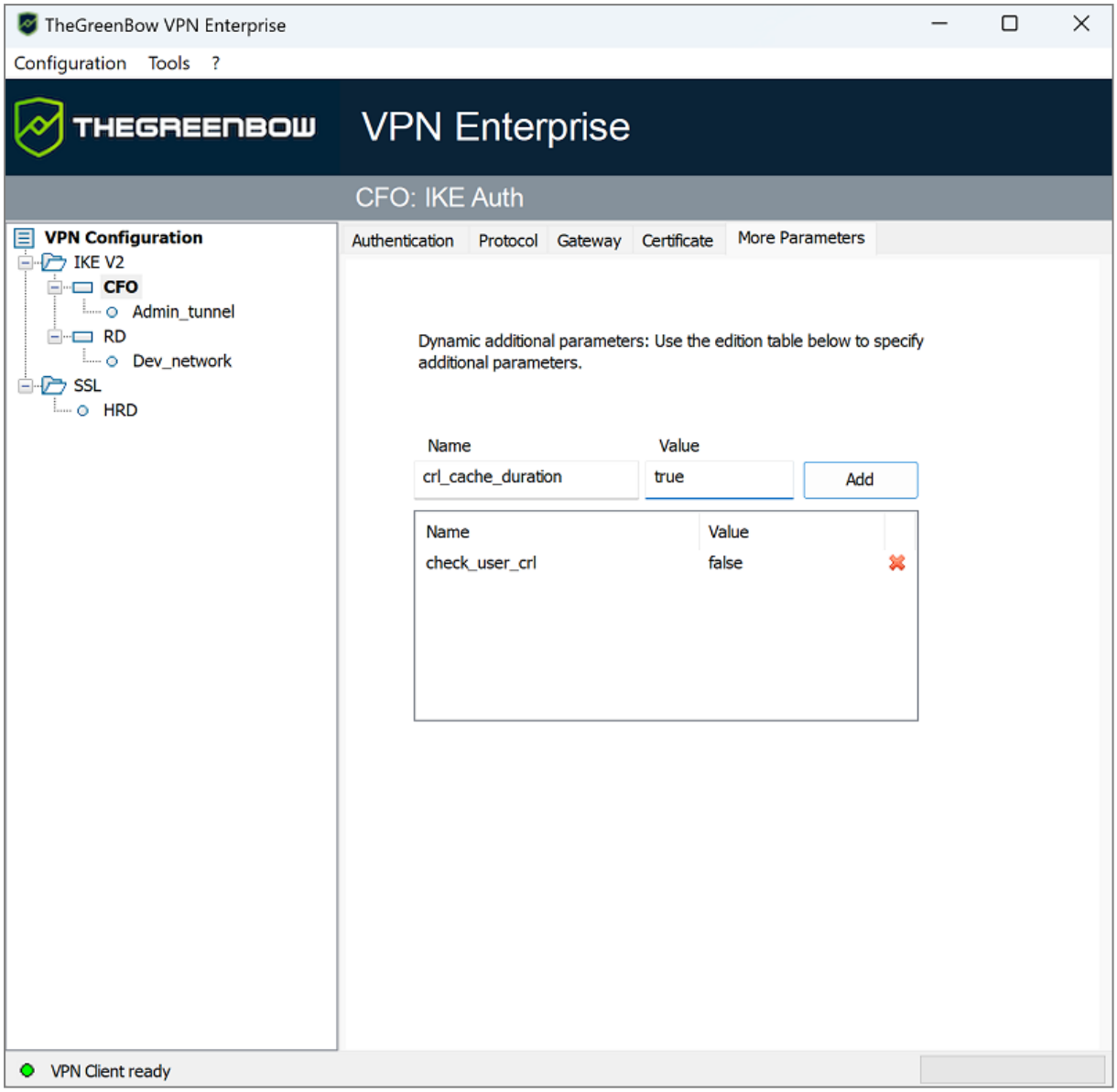
SN VPN Client Exclusive permet si besoin de configurer des paramètres dynamiques additionnels, au niveau de la configuration IKE Auth, dont seuls les suivants sont documentés dans le présent guide :

- Spécifier l'adresse IP de l'interface réseau
  - *local_subnet* (cf. section Adresses)
- Spécifier la taille du nonce pour les passerelles IPsec DR
  - *nonce_size* (cf. section IKE Auth : Protocole)
- Spécifier la taille du réseau local virtuel
  - *local_virtual_network_size* (cf. section Trafic sélecteurs)
- Sélectionner un certificat en fonction de son sujet
  - *user_cert_dnpattern* (cf. section user_cert_dnpattern)
- Sélectionner un certificat en fonction de son champ « key usage »
  - *user_cert_keyusage* (cf. section user_cert_keyusage)
- Sélectionner le lecteur de tokens / cartes à puce à utiliser pour la sélection automatique du certificat utilisateur
  - *reader_pattern* (cf. section Paramètres dynamiques)
- Définir le magasin de certificats à utiliser au niveau tunnel
  - *MachineStore* (cf. section Caractéristiques requises)
- Activer le protocole de vérification de certificat en ligne (OCSP ou *Online Certificate Status Protocol* en anglais)
  - *enable_OCSP* (cf. section Certificat de la passerelle VPN)
- Empêcher ou limiter le chargement de la CRL
  - *check_user_crl* (cf. section Empêcher ou limiter le téléchargement des CRL)
  - *crl_cache_duration* (cf. section Empêcher ou limiter le téléchargement des CRL)
- Valider le certificat même s'il ne se conforme pas aux contraintes relatives à l'extension Key Usage
  - *allow_server_extra_keyusage* (cf. section Contraintes relatives à l'extension Key Usage)
- Valider le certificat même s'il ne se conforme pas aux contraintes relatives à l'extension Extended Key Usage
  - *allow_server_and_client_auth* (cf. section Contraintes relatives à l'extension Extended Key Usage)

- Utiliser l'algorithme de hachage SHA-2 dans la charge utile de demande de certificat
  - *sha2_in_cert_req* (cf. section Mode IPsec DR)
- Employer d'autres méthodes d'authentification des certificats
  - *Method14_RSASSA_PKCS1* (cf. section Méthodes d'authentification des certificats)
  - *Method1_PKCS1v15_Scheme* (cf. section Méthodes d'authentification des certificats)
- Employer la méthode 214 ou la méthode 14 pour l'authentification des certificats utilisateurs Brainpool
  - *use_method_214* (cf. section Méthodes d'authentification des certificats)
- Afficher un message personnalisé dans la fenêtre popup de demande du code PIN
  - *user_smartcard_tip* (cf. section Utiliser un certificat sur carte à puce ou sur token)

Dans certaines circonstances, le support Stormshield peut vous proposer d'ajouter d'autres paramètres dynamiques (Nom, Valeur), non documentés dans le présent guide, qui permettront de gérer des cas d'usage particuliers, soit sur la version du logiciel installée, soit sur des patches qui vous seront fournis.

Pour activer l'onglet **Plus de paramètres** sur la fenêtre de configuration des tunnels VPN comme ci-dessous, cochez l'option **Afficher plus de paramètres** dans l'onglet **Général** de la fenêtre **Options**.



Gestion des logs

Voir la section Logs administrateur.

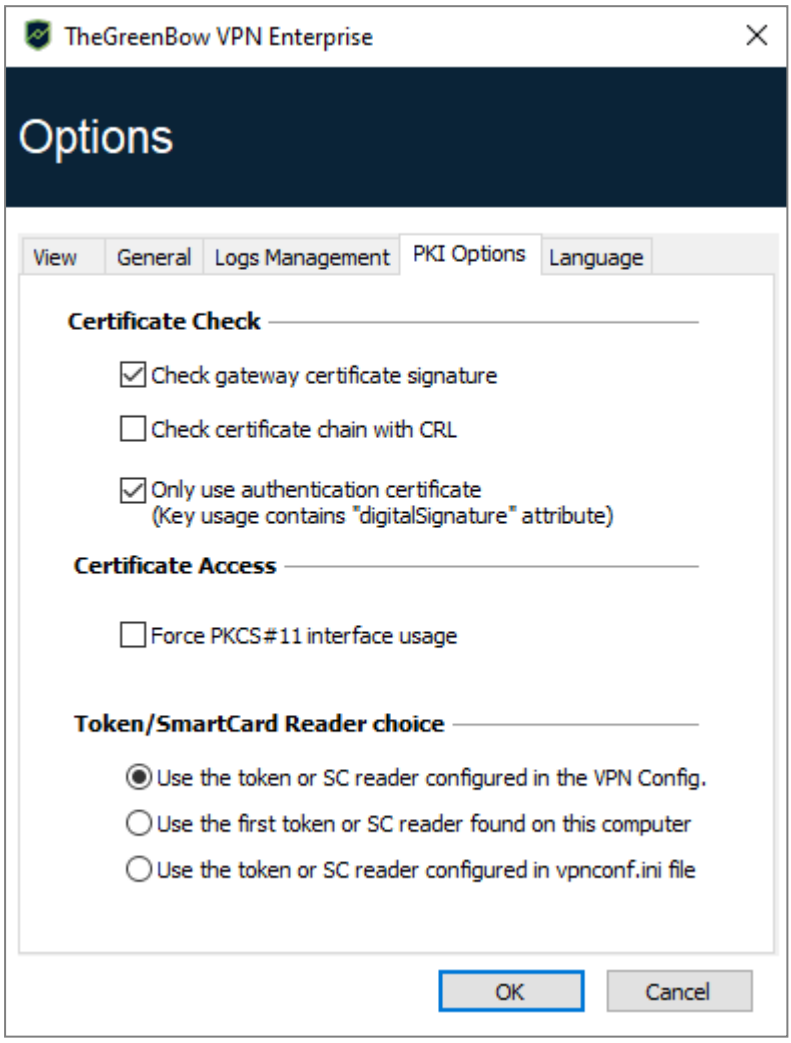
Options PKI

L'onglet **Options PKI** permet d'affiner la gestion des cartes à puce et des tokens et de caractériser précisément l'accès aux certificats.

Les options PKI comprennent :

- la configuration de règles pour la vérification du certificat de la passerelle (validité, CRL, key usage) ;
- la caractérisation du certificat que le Client VPN doit utiliser pour ouvrir un tunnel VPN ;
- la définition du lecteur de cartes à puce ou du token à utiliser sur le poste utilisateur.

NOTE
Dans le cadre du déploiement du logiciel, toutes ces options peuvent être préconfigurées au cours de l'installation du logiciel SN VPN Client Exclusive. Ce mécanisme est décrit dans le document « Guide de déploiement ».



Vérification des certificats

Vérifier la signature du certificat de la passerelle	Lorsque cette option est sélectionnée, le certificat de la passerelle VPN est vérifié (incluant sa date de validité), ainsi que chaque certificat de la chaîne de certification jusqu'au certificat racine. **ASTUCE** Lorsque cette option est sélectionnée, il est nécessaire de renseigner le Remote ID du tunnel concerné avec le sujet du certificat de la passerelle, pour éviter une exploitation de la vulnérabilité 2018_7293.

Vérifier la chaîne de certification avec CRL	Lorsque cette option est sélectionnée, le Client VPN vérifie la liste des certificats révoqués (CRL ou *Certificate Revocation List* en anglais) du certificat de la passerelle VPN, ainsi que celle de chaque certificat de la chaîne de certification jusqu'au certificat racine. Le certificat racine et les certificats intermédiaires doivent être importés dans la configuration ou accessibles dans le magasin de certificats Windows. De même, les CRL doivent être accessibles, soit dans le magasin de certificats Windows, soit téléchargeables. **NOTE** Depuis la version 7.5 de SN VPN Client Exclusive, il est possible de vérifier la révocation du certificat de la passerelle à l'aide du protocole de vérification de certificat en ligne en mode agrafage (OCSP ou *Online Certificate Status Protocol* en anglais). Pour cela, il convient d'ajouter le paramètre dynamique *enable_OCSP* défini à la valeur true (voir section Afficher plus de paramètres).
Certificats Passerelle et Client VPN issus de CA différentes	Si le Client VPN et la passerelle VPN utilisent des certificats issus d'une autorité de certification différente, cette case doit être cochée.
Utiliser seulement les certificats de type Authentification	Lorsque cette option est cochée, seuls les certificats de type **Authentification** (c'est-à-dire dont l'extension *Key Usage* contient l'attribut *digitalSignature*) sont pris en compte par le Client VPN. Cette fonction permet de sélectionner automatiquement un certificat parmi plusieurs stockés sur la même carte à puce ou le même token. La case à cocher est grisée lorsque la propriété MSI *KEYUSAGE* est définie sur la valeur 2 ou 3 lors de l'installation (cf. « Guide de déploiement »).

Accès aux certificats

Forcer l'utilisation de PKCS#11	Le Client VPN sait gérer les API PKCS#11 et CNG pour accéder au certificat des cartes à puce ou des tokens. Lorsque cette option est cochée, le Client VPN ne prend en compte que l'API PKCS#11 pour accéder au certificat des cartes à puce et des tokens.
Utiliser le premier certificat trouvé	Lorsque cette option est cochée, le Client VPN utilise le premier certificat trouvé sur le lecteur de cartes à puce ou le token spécifié.

Choix du token/lecteur de cartes à puce

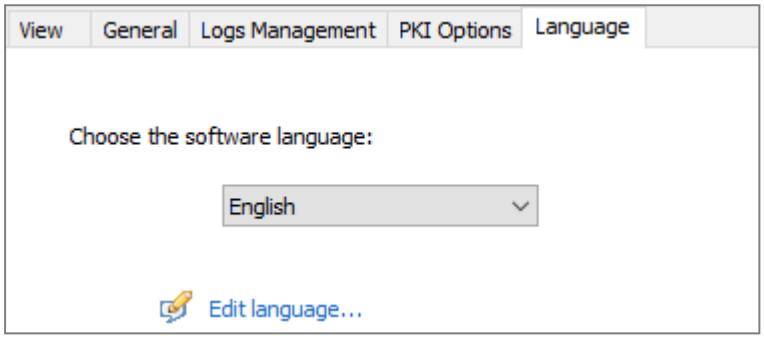
Utiliser le token/lecteur CàP spécifié dans la config. VPN	Le Client VPN utilise le lecteur ou le token spécifié dans le fichier de configuration VPN pour y chercher un certificat.
Utiliser le premier token/lecteur CàP trouvé	Le Client VPN utilise la première carte à puce ou le premier token trouvé sur le poste pour y chercher un certificat.
Utiliser le token/lecteur CàP spécifié dans vpnconf.ini	Le Client VPN utilise le fichier de configuration vpnconf.ini pour identifier les lecteurs de cartes à puce ou les tokens à utiliser pour y chercher un certificat. Voir le « Guide de déploiement ». **NOTE** Comme l'utilisation du fichier *vpnconf.ini* ne s'applique qu'à l'interface PKCS#11, cette option requiert que l'option **Forcer l'utilisation de PKCS#11** soit sélectionnée.

Gestion des langues

Choix d'une langue

SN VPN Client Exclusive peut être exécuté en plusieurs langues. Il est possible de changer de langue en cours d'exécution du logiciel.

Pour choisir une autre langue, ouvrez le menu **Outils** > **Options**, puis sélectionnez l'onglet **Langue**. Choisissez la langue souhaitée dans la liste déroulante proposée :

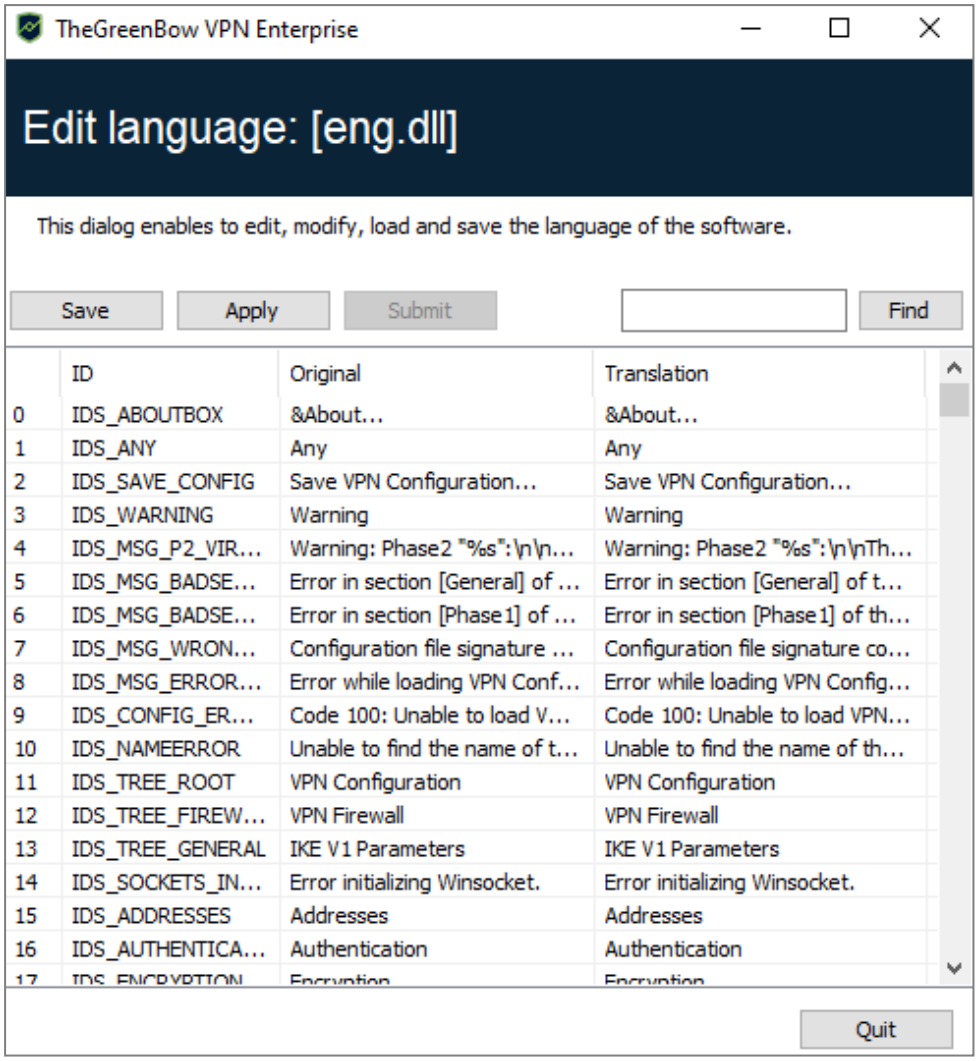


La liste des langues disponibles en standard dans le logiciel est donnée en annexe à la section Caractéristiques techniques de SN VPN Client Exclusive.

Modification ou création d'une langue

SN VPN Client Exclusive permet aussi de créer une nouvelle traduction ou d'effectuer des modifications sur la langue utilisée, puis de tester ces modifications dynamiquement, via un outil de traduction intégré.

Dans l'onglet **Langue**, cliquez sur le lien **Éditer la langue...**, la fenêtre de traduction s'affiche :



La fenêtre de traduction est partagée en 4 colonnes qui indiquent respectivement le numéro de la chaîne de caractère, son identifiant, sa traduction dans la langue d'origine, et sa traduction dans la langue choisie.

La fenêtre de traduction permet :

- de traduire chaque chaîne de caractère en cliquant sur la ligne correspondante ;
- de rechercher une chaîne de caractères donnée dans n'importe quelle colonne du tableau (champ de saisie **Chercher**, puis utiliser la touche **F3** pour parcourir toutes les occurrences de la chaîne de caractères recherchée) ;
- de sauvegarder les modifications (bouton **Sauver**).

IMPORTANT

Les caractères ou suites de caractères suivantes ne doivent pas être modifiées au cours de la traduction :
%s sera remplacé par le logiciel par une chaîne de caractères
%d sera remplacé par le logiciel par un nombre
\n indique un retour chariot
& indique que le caractère suivant doit être souligné
%m-%d-%Y indique un format de date (ici le format américain : mois-jour-année). Ne modifier ce champ qu'en connaissance du format dans la langue traduite.
La chaîne **IDS_SC_P11_3** doit être reprise sans modification.

Logs administrateur, Console et traces

SN VPN Client Exclusive propose trois types de logs :

1. Les logs administrateur sont spécifiquement dédiés au rapport d'activité et d'utilisation du logiciel.
2. La **Console** détaille les informations et les étapes des ouvertures et fermeture des tunnels. Elle est principalement constituée des messages IKE et apporte une information de haut niveau sur l'établissement du tunnel VPN. Elle est destinée à l'administrateur, pour l'aider à identifier d'éventuels incidents de connexions VPN.
3. Le mode traçant fait produire par chaque composant du logiciel le log de son fonctionnement interne. Ce mode est destiné au support Stormshield pour le diagnostic d'incident logiciels.

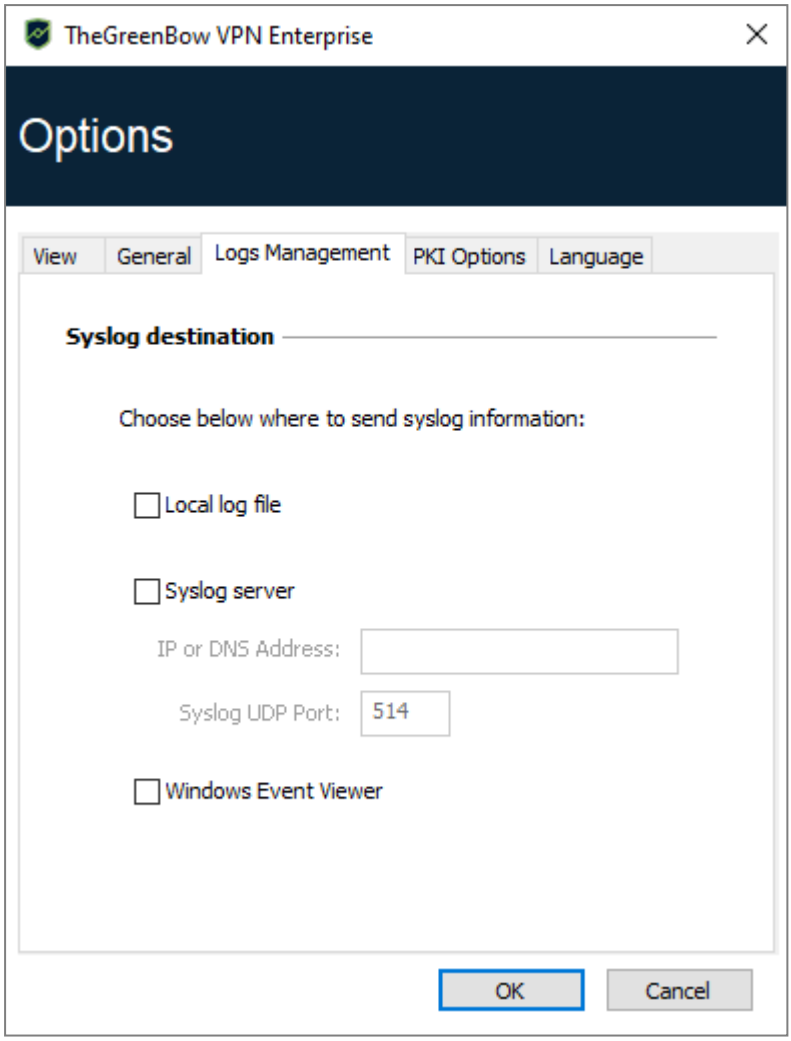
Logs administrateur

SN VPN Client Exclusive permet de collecter des logs de type administrateur : ouverture de tunnel, certificat expiré, durée de connexion, login/mot de passe erroné, modification de la configuration VPN, import ou export de cette configuration, etc. Les logs administrateur offrent en particulier un premier niveau d'analyse sur les problèmes rencontrés.

Les logs collectés peuvent être au choix et/ou simultanément :

- stockés dans un fichier local,
- journalisés dans le journal d'évènements Windows,
- envoyés à un serveur syslog.

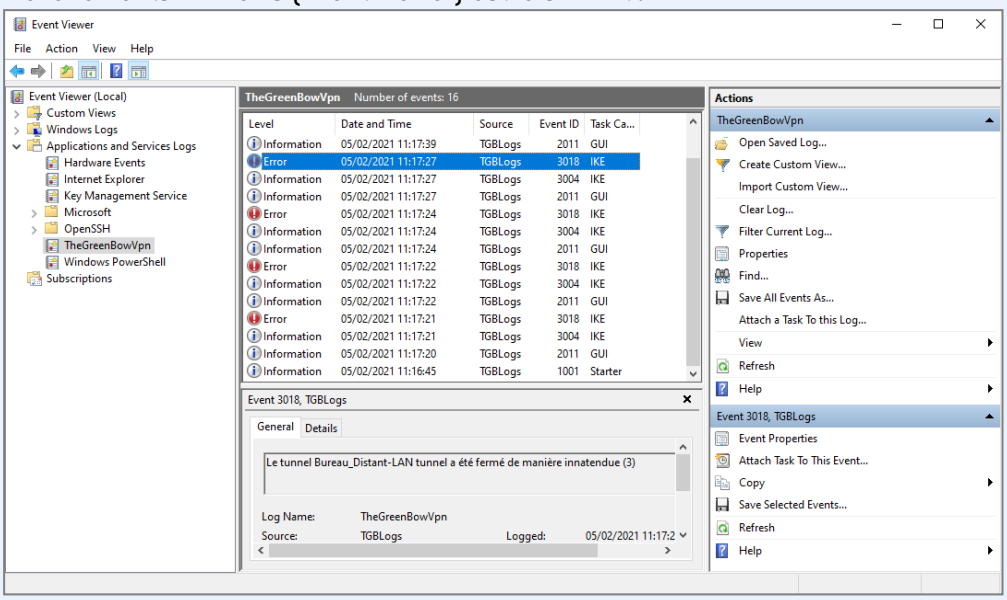
Le paramétrage des log administrateur s'effectue dans la fenêtre **Outils** > **Options...**, dans l'onglet **Gestion des logs**.



NOTES

- Les logs administrateur sont listés à la section Logs administrateur dans les annexes.
- Les logs administrateur sont uniquement disponibles en anglais. Ils ne sont pas localisés dans d'autres langues.
- Lorsque les logs administrateur sont stockés dans un fichier local, le chemin de ces logs est le sous-répertoire **System** du répertoire des logs : *C:\ProgramData\Stormshield\Network VPN Client Exclusive\LogFiles\System*.
  Ce répertoire peut être lu dans tous les modes, mais n'est accessible en écriture qu'en mode Administrateur.

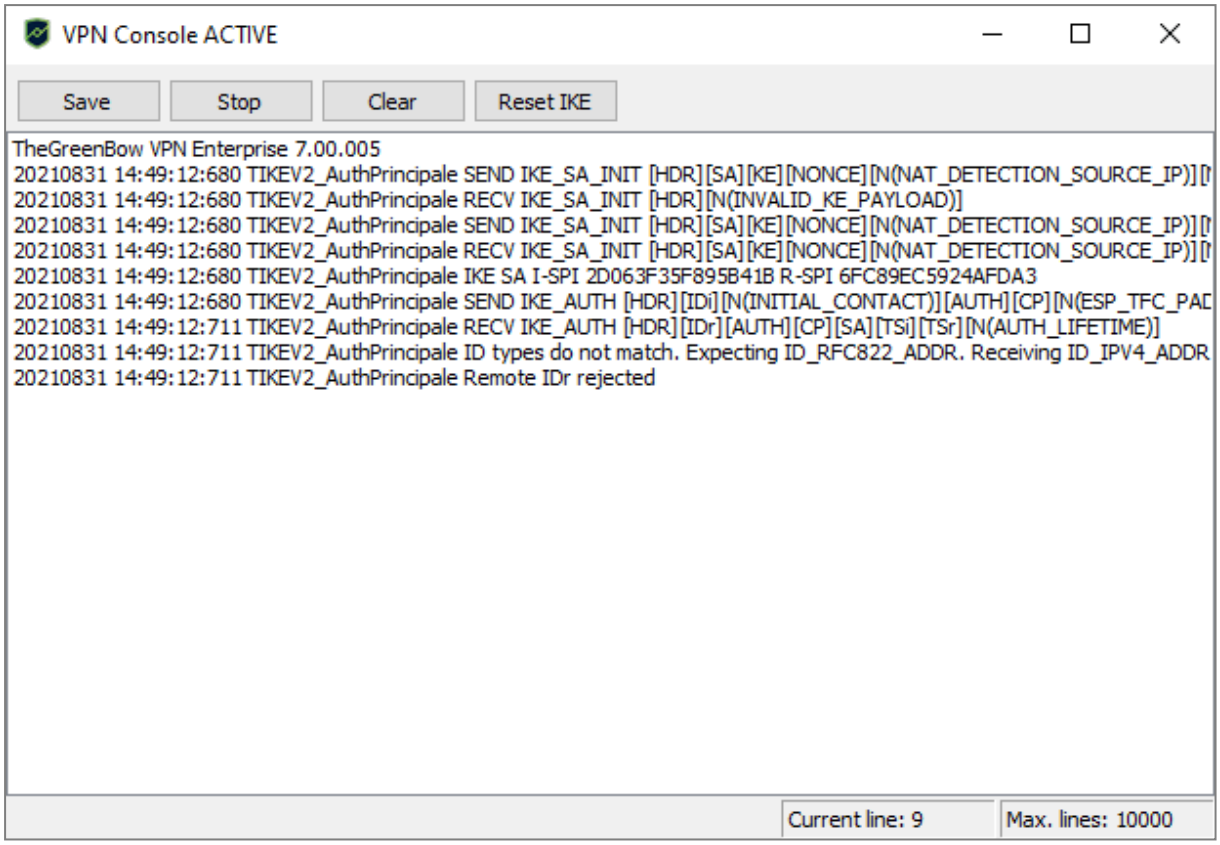
- Le chemin d'accès aux logs de SN VPN Client Exclusive dans le gestionnaire d'évènements Windows (Event Viewer) est le suivant :



Console

La **Console** peut être affichée par les moyens suivants :

- menu **Outils** > **Console** du **Panneau de Configuration** (interface principale) ;
- menu contextuel > **Console** du **Panneau TrustedConnect** ;
- raccourci Ctrl+D lorsque le **Panneau de Configuration** est ouvert ;
- dans le menu du logiciel en barre des tâches, sélectionnez **Console**.



Les fonctions de la **Console** sont les suivantes :

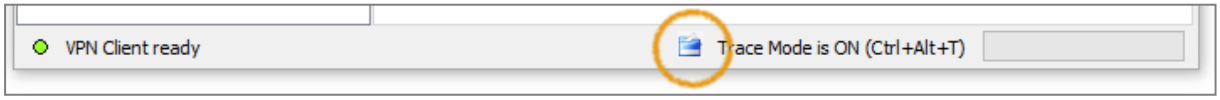
- **Sauver** : Sauvegarde dans un fichier la totalité des traces affichées dans la fenêtre.
- **Start** / **Stop** : Démarre / arrête la capture des traces.
- **Effacer** : Efface le contenu de la fenêtre.
- **Reset IKE** : Redémarre le service IKE.

Mode traçant

Le mode traçant est activé par le raccourci : Ctrl+Alt+T.

Le passage en mode traçant ne nécessite pas de redémarrer le logiciel.

Lorsque le mode traçant est activé, chaque composant de SN VPN Client Exclusive génère les logs de son activité. Les logs générés sont mémorisés dans un dossier accessible en cliquant sur l'icône **Dossier** bleue dans la barre d'état du **Panneau de Configuration** (interface principale).



NOTES

- L'activation des logs traçant ne peut se faire que depuis le **Panneau de Configuration**, dont l'accès peut être strictement réservé à l'administrateur.

- Même si les logs ne contiennent pas d'information sensible, il est recommandé que, lorsqu'ils sont activés par l'administrateur, celui-ci veille à ce qu'ils soient désactivés, et si possible supprimés, lorsqu'il quitte le logiciel.
- Les fichiers de logs sont générés chaque jour et conservés 10 jours par défaut. Au-delà de cette période, le logiciel purge automatiquement les fichiers plus anciens. La durée de conservation des logs peut être configurée à l'aide de la propriété *VPNLOGPURGE* de l'installeur du Client VPN (voir « Guide de déploiement »).
- Les logs administrateur mémorisés dans un fichier local ne sont pas purgés (cf. section Logs administrateur).

Recommandations de sécurité

Hypothèses

Afin de garantir un niveau de sécurité approprié, les conditions de mise en œuvre et d'utilisation suivantes doivent être respectées.

Profil et responsabilités des administrateurs

L'administrateur système et réseau et l'administrateur sécurité chargés respectivement de l'installation du logiciel et de la définition des politiques de sécurité VPN sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et les procédures d'administration.

L'administrateur sécurité s'assure régulièrement que la configuration du produit est conforme à celle qu'il a mise en place et effectue les mises à jour requises le cas échéant.

La fonction de journalisation du produit est activée et correctement configurée. Les administrateurs sont responsables de la consultation régulière des journaux.

Profil et responsabilités de l'utilisateur

L'utilisateur du logiciel est une personne non hostile et formée à son utilisation. En particulier, l'utilisateur exécute les opérations dont il a la charge pour le bon fonctionnement du produit et ne divulgue pas les informations utilisées pour son authentification auprès de la passerelle VPN.

Respect des règles de gestion des éléments cryptographiques

Les bi-clés et les certificats utilisés pour ouvrir le tunnel VPN sont gérés (génération, révocation) par une autorité de certification de confiance qui garantit le respect des règles dans la gestion de ces éléments cryptographiques et plus particulièrement les recommandations issues de [RGS_B1] et [RGS_B2].

Poste de l'utilisateur

La machine sur laquelle est installé et exécuté le logiciel SN VPN Client Exclusive doit être saine et correctement administrée. En particulier :

- Elle dispose d'un anti-virus dont la base de données est régulièrement mise à jour.
- Elle est protégée par un pare-feu qui permet de maîtriser (cloisonner ou filtrer) les communications entrantes et sortantes du poste qui ne passent pas par le Client VPN.
- Son système d'exploitation est à jour des différents correctifs.
- Sa configuration permet d'éviter les attaques menées localement (analyse de la mémoire, patch ou corruption de binaire).

Des recommandations de configuration pour durcir le poste de travail sont disponibles sur le site de l'ANSSI, par exemple (sans que cette liste ne soit exhaustive) :

- Guide d'hygiène informatique
- Guide de configuration
- Mot de passe

Administration du Client VPN

SN VPN Client Exclusive est conçu pour être installé et configuré avec les droits « administrateur », et ensuite être utilisé avec des droits « utilisateur ».

Il est recommandé de protéger l'accès à la configuration VPN par un mot de passe et de limiter la visibilité du logiciel à l'utilisateur final (comportement par défaut de SN VPN Client Exclusive), comme détaillé à la section Restreindre l'accès au Panneau de Configuration.

Il est recommandé d'activer la vérification du hachage d'intégrité du fichier de configuration VPN en utilisant la propriété MSI *SIGNFILE* avec la valeur 1 à l'installation du logiciel (voir propriété MSI *SIGNFILE* dans le « Guide de déploiement »). La valeur par défaut, si la propriété n'est pas indiquée à l'installation, est 0 (désactivé).

Le logiciel doit par conséquent être lancé en mode administrateur pour pouvoir accéder au **Panneau de Configuration**.

Il est recommandé de conserver le mode **Démarrage du Client VPN avec la session Windows** (après l'ouverture de session Windows), qui est le mode d'installation par défaut.

Enfin, il est à noter que SN VPN Client Exclusive présente la même configuration VPN à tous les utilisateurs d'un poste multi-utilisateurs. Il est donc recommandé de mettre en œuvre le logiciel sur un poste dédié (en conservant par exemple un compte administrateur et un compte utilisateur, comme indiqué précédemment).

Configuration VPN

Données sensibles dans la configuration VPN

Il est recommandé de ne mémoriser aucune donnée sensible dans le fichier de configuration VPN.

À ce titre, il est recommandé de ne pas utiliser les facilités suivantes offertes par le logiciel :

- Ne pas utiliser le mode EAP (mot de passe / login) seul, mais uniquement en combinaison avec un certificat,
- Dans le cas où EAP est utilisé, ne pas mémoriser le login / mot de passe EAP dans la configuration VPN (fonction décrite à la section Authentification),
- Ne pas importer de certificat dans la configuration VPN (fonction décrite à la section Importer un certificat dans la configuration VPN), et privilégier l'utilisation de certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows,
- Ne pas utiliser le mode « Clé partagée » (fonction décrite à la section IKE Auth : Authentification) et privilégier le mode « Certificat » avec des certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows,
- Ne pas exporter la configuration VPN en clair, c'est-à-dire non protégée par un mot de passe (fonction décrite à la section Exporter une configuration VPN).

Authentification de l'utilisateur

Les fonctions d'authentification de l'utilisateur proposées par SN VPN Client Exclusive sont décrites ci-dessous, de la plus faible à la plus forte.

En particulier, il est à noter qu'une authentification par clé partagée (preshared key), si elle est facile à mettre en œuvre, permet néanmoins à tout utilisateur ayant accès au poste, de monter un tunnel, sans vérification d'authentification.

Type d'authentification de l'utilisateur	Force
Clé partagée	faible
EAP	
EAP popup	
Certificat mémorisé dans la configuration VPN	
Certificat dans le magasin de certificats Windows	
Certificat sur carte à puce ou sur token	forte

Authentification de la passerelle VPN

Il est recommandé de mettre en œuvre la vérification du certificat de la passerelle VPN, tel que décrit à la section Options PKI.

Il est recommandé de ne pas configurer le Client VPN pour valider les certificats non conformes aux contraintes relatives aux extensions Extended Key Usage et Key Usage (ne pas utiliser les paramètres dynamiques *allow_server_and_client_auth* et *allow_server_extra_keyusage*).

Protocole

Il est recommandé de ne configurer que des tunnels IPsec / IKEv2 (et pas SSL / OpenVPN).

Mode « tout dans le tunnel » et « split tunneling »

Il est recommandé de configurer le tunnel VPN en mode « tout le trafic dans le tunnel » avec le mode « bloquer les flux non chiffrés » (split tunneling) activé.

Voir les sections Configuration du type d'adresse et Autres.

Mode GINA

Il est recommandé d'associer une authentification forte à tout tunnel en mode GINA.

Recommandations de l'ANSSI

Les recommandations décrites ci-dessus peuvent être complétées par le document de configuration IPsec rédigé par l'ANSSI : Recommandations de sécurité relatives à IPsec pour la protection des flux réseau.

Annexes

Raccourcis

Panneau des Connexions

Esc	Ferme la fenêtre.
Ctrl+Entrée	Ouvre le **Panneau de Configuration** (interface principale).
Flèches	Les flèches haut et bas permettent de sélectionner une connexion VPN.
Ctrl+O	Ouvre la connexion VPN sélectionnée.
Ctrl+W	Ferme la connexion VPN sélectionnée.

Arborescence de la configuration VPN

F2	Permet d'éditer le nom de la phase sélectionnée
Del	Si une phase est sélectionnée, la supprime après confirmation de l'utilisateur. Si la configuration est sélectionnée (racine de l'arborescence), propose l'effacement (reset) de la configuration complète.
Ctrl+O	Si un Child SA est sélectionné, ouvre le tunnel VPN correspondant.
Ctrl+W	Si un Child SA est sélectionné, ferme le tunnel VPN correspondant.
Ctrl+C	Copie la phase sélectionnée dans le presse-papiers.
Ctrl+V	Colle (ajoute) la phase copiée dans le presse-papiers.
Ctrl+N	Crée un nouvel IKE Auth, si la configuration VPN est sélectionnée, ou crée un nouveau Child SA pour l'IKE Auth sélectionné.
Ctrl+S	Sauvegarde la configuration VPN.

Panneau de Configuration

Ctrl+Entrée	Permet de basculer au **Panneau des Connexions**.
Ctrl+D	Ouvre la fenêtre **Console** de traces VPN.
Ctrl+Alt+R	Redémarrage du service IKE.
Ctrl+Alt+T	Activation du mode traçant (génération de logs).
Ctrl+S	Sauvegarde la configuration VPN.

Logs administrateur

ID Log define	ID Log value	Severity	Log string
LOGID_STARTERINIT	1001	Notice	Starter service is started.
LOGID_VPNCONFSTARTING	2001	Notice	GUI is starting.
LOGID_VPNCONFSTOPPED	2002	Notice	GUI has closed.
LOGID_TGBIKESTARTED	3001	Notice	IKE has started (status %d).
LOGID_TGBIKESTOPPED	3002	Notice	IKE has stopped.
LOGID_TUNNELOPEN	3004	Info	Tunnel %s is asked to open.
LOGID_VPNCONFCRASHED	2003	Notice	GUI crashed (state %d).
LOGID_TGBIKECRASHED	3003	Notice	IKE crashed (state %d).
LOGID_STARTERSTOP	1002	Notice	Starter service is stopped.
LOGID_RESETIKE	2007	Warning	IKE is asked to reset.
LOGID_VPNCONFSTARTED	2008	Notice	GUI has started from user %s.
LOGID_VPNCONFSTOPPING	2009	Notice	GUI is stopping from user %s.
LOGID_VPNCONFLOADERROR	2010	Error	Configuration couldn't load (reason: %s).
LOGID_ VPNCONFOPENTUNNEL	2011	Info	GUI opens tunnel (source: %s).
LOGID_ VPNCONFCLOSETUNNEL	2012	Info	GUI closes tunnel (source: %s).
LOGID_VPNCONFSAVE	2013	Notice	New configuration is saved.
LOGID_VPNCONFIMPORT	2014	Info	%s has been imported.
LOGID_VPNCONFIMPORTERR	2015	Error	%s could not be imported (status %d).
LOGID_VPNCONFEXPORT	2016	Info	%s has been exported.
LOGID_TOKENINSERT	2017	Info	Token %s has been inserted.
LOGID_TOKENEXTRACT	2018	Info	Token %s has been extracted.
LOGID_USBINSERT	2019	Info	USB Key has been inserted
LOGID_USBEXTRACT	2020	Info	USB Key has been extracted
LOGID_INSTALLATION	2021	Info	VPN running for the 1st time.
LOGID_UPDATE	2022	Info	VPN software has been updated to version %s.
LOGID_VERSION	2023	Info	VPN Version is %s.
LOGID_GINASTARTED	4001	Notice	GINA has started.
LOGID_GINASTOPPING	4002	Notice	GINA is stopping.

ID Log define	ID Log value	Severity	Log string
LOGID_GINAOPENTUNNEL	4003	Info	GINA opens tunnel (source: %s).
LOGID_GINACLOSETUNNEL	4004	Info	GINA closes tunnel (source: %s).
LOGID_TUNNELAUTH_OK	3005	Info	Tunnel authentication Ok (%s).
LOGID_TUNNELTRAFIC_OK	3006	Info	Tunnel %s Ok
LOGID_TUNNELAUTH_NOK	3007	Error	Tunnel authentication failed (reason %d).
LOGID_TUNNELTRAFIC_NOK	3008	Error	Tunnel %s Failed (reason %d).
LOGID_AUTHREKEYING	3009	Info	Tunnel %s initiated rekey (source %d).
LOGID_AUTHREKEYED	3010	Info	Tunnel %s rekeyed.
LOGID_TUNNELREKEYING	3011	Info	Tunnel %s initiated rekey (source %d).
LOGID_TUNNELREKEYED	3012	Info	Tunnel %s rekeyed.
LOGID_PINCODE	3013	Notice/Error	Pin code is entered (status %d).
LOGID_DRIVERNOK	3014	Critical	Driver could not be loaded (status %d).
LOGID_IKEEXT_STOP	1003	Warning	IKEEXT service is stopped.
LOGID_IKEEXT_RESTART	1004	Notice	IKEEXT service is restarted.
LOGID_IKEEXT_ERROR	1005	Critical	IKEEXT could not be stopped (status %d).
SYSTEMLOGID_VIRTIFOK	3015	Info	Virtual interface created successfully (instance %d).
SYSTEMLOGID_VIRTIFNOK	3016	Error	Virtual interface could not be created (error %d).
LOGID_TUNNELCLOSED	3017	Notice	%s tunnel successfully closed (%d min).
LOGID_TUNNELCLOSED_ERR	3018	Error	%s tunnel closed unexpectedly (%d).
LOGID_CERTERROR	3019	Error	Error %d when handling certificate %s.

Diagnostics du Panneau TrustedConnect

Le **Panneau TrustedConnect** informe l'utilisateur des problèmes d'établissement de la connexion VPN via l'affichage d'un code d'erreur.

Ces codes erreurs, leur diagnostic et leur solution éventuelle sont détaillés ci-dessous. Cette liste permet à l'administrateur, sur avertissement de l'utilisateur, d'étudier une réponse au problème rencontré.

Code	Diagnostic	Solution
0	Problème de configuration VPN La connexion VPN n'a pas été trouvée dans la configuration.	• Vérifier la présence du fichier *tgbvpn.conf* dans le répertoire d'installation du Client VPN.

Code	Diagnostic	Solution
1	Problème de certificat La configuration VPN utilise un certificat dont la clé privée est introuvable.	• Vérifier la configuration du client VPN ainsi que les éventuels périphériques d'authentification associés (lecteur de cartes à puce, token ou magasin de certificats Windows). • Réimporter la configuration VPN puis réimporter le certificat concerné. • Créer un ticket sur votre espace MyStormshield en joignant l'ensemble des fichiers de log.
3	Problème de configuration Le message **No proposal chosen** a été reçu lors d'un échange avec IKE : la suite d'algorithmes cryptographique configurée pour la séquence IKE_SA_INIT ne correspond pas à celle configurée sur la passerelle.	• Vérifier que la suite d'algorithmes cryptographiques pour la séquence IKE_SA_INIT de la connexion VPN correspond à celui de la passerelle (reportez-vous au IKE Auth dans le **Panneau de Configuration**).
4	Problème de configuration Le message « No proposal chosen » a été reçu lors d'un échange avec IKE : la suite d'algorithmes cryptographique du protocole ESP ne correspond pas à celui configuré sur la passerelle.	• Vérifier que la suite d'algorithmes cryptographique protocole ESP (reportez-vous au Child SA dans le **Panneau de Configuration**) correspond à celui de la passerelle.
5	Passerelle non accessible L'adresse de la passerelle (« Adresse routeur distant ») indiquée dans la configuration VPN n'est pas joignable. Si c'est une adresse IP, elle est introuvable ou injoignable. Si c'est une adresse DNS elle peut être inaccessible, indéfinie ou ne peut être résolue.	• Vérifier l'adresse de la passerelle/poste distant. Par exemple, essayer de « pinguer » cette adresse.
6	Problème de configuration Le message **Remote ID other than expected** a été reçu. Cela signifie que la valeur du **Remote ID** ne correspond pas à la valeur attendue par la passerelle VPN distante.	• Vérifier que le paramètre **Local ID** de l'onglet **Protocole** du client VPN correspond au Remote ID de la passerelle (ou du poste) distant(e). Attention : le Remote ID sur le routeur est le Local ID sur le Client VPN et inversement !

Code	Diagnostic	Solution
7	Certificat passerelle La vérification de la chaîne de certification du certificat reçu de la passerelle VPN est active. La chaîne de certification du certificat de la passerelle n'a pas pu être validée.	• Vérifier la date d'expiration du certificat de la passerelle. • Vérifier la date de début de validité du certificat de la passerelle. • Vérifier les signatures de tous les certificats de la chaîne de certification (y compris le certificat racine, les certificats intermédiaires et le certificat de la passerelle). • Vérifier la mise à jour des CRL de tous les émetteurs de certificats de la chaîne de certification. • Vérifier l'absence de révocation de certificats concernés dans les listes de CRL correspondante. • Vérifier que le certificat racine et tous les certificats de la chaîne de certification (l'autorité de certification racine et les autorités de certification intermédiaires) sont présents dans le magasin de certificats Windows du poste de travail. • Vérifier que les CRL des différentes autorités de certification sont présentes dans le magasin de certificats Windows, ou que ces CRL sont téléchargeables à l'ouverture de la connexion VPN.
9	Pas de réponse passerelle Le Client VPN a abandonné la connexion, le plus souvent après plusieurs tentatives de connexion.	• Vérifier si la passerelle est toujours accessible depuis le poste de travail.
10	Problème d'authentification La passerelle a refusé les éléments d'authentification de l'utilisateur.	• Vérifier le certificat utilisateur. • Vérifier dans l'onglet **Protocole** du **Panneau de Configuration** que le Local ID correspond à la valeur et au type définis sur la passerelle. Attention : le Local ID sur le Client VPN est le Remote ID sur le routeur et inversement ! • Vérifier les logs de la passerelle distante pour obtenir plus d'informations sur ce problème.
13	Problème de configuration Une erreur est survenue lors de l'établissement de la connexion VPN. L'établissement de la connexion VPN a été abandonnée.	• Récupérer les fichiers de logs de l'utilisateur, leur analyse est nécessaire. • Créer un ticket sur votre espace MyStormshield en joignant l'ensemble des fichiers de log.

Code	Diagnostic	Solution
14	Configuration réseau Une erreur est survenue lors de la création de l'interface virtuelle utilisée pour la connexion VPN.	• Récupérer les fichiers de logs de l'utilisateur, leur analyse est nécessaire. • Créer un ticket sur votre espace MyStormshield en joignant l'ensemble des fichiers de log.
15	Configuration réseau L'adresse IP virtuelle affectée lors de la connexion VPN est déjà existante sur l'une des interfaces du poste de travail.	• Changer l'adresse IP virtuelle (Paramètre **Adresse du client VPN**) indiquée dans la configuration du client VPN. • Changer l'adresse IP fournie par la passerelle au client VPN.
16	Configuration réseau Une erreur est survenue lors de la création de l'interface virtuelle utilisée pour la connexion VPN.	• Récupérer les fichiers de logs de l'utilisateur, leur analyse est nécessaire. • Créer un ticket sur votre espace MyStormshield en joignant l'ensemble des fichiers de log.
24	Problème de configuration La suite d'algorithmes cryptographique proposée par le client VPN n'a pas été acceptée par la passerelle.	• Vérifier que les suites d'algorithmes cryptographique du Client VPN correspondent à celles de la passerelle. • Vérifier le Local ID et le Remote ID. Avertissement : le Local ID sur le routeur est le Remote ID sur le Client VPN et inversement !
25	Problème de configuration Le réseau distant configuré dans le client VPN, ou l'adresse IP Virtuelle proposée par le client VPN n'ont pas été acceptés par la passerelle.	• Vérifier que l'adresse IP virtuelle (paramètre **Adresse du client VPN**) indiquée dans la configuration du client VPN est acceptable côté passerelle. • Vérifier que le réseau distant (paramètre **Adresse réseau distant**) indiqué dans la configuration du client VPN est acceptable côté passerelle.
26	Problème de configuration Le client VPN propose ses propres trafic selectors, alors que la passerelle est configurée pour les lui fournir.	• Cocher le paramètre **Obtenir la configuration depuis la passerelle** dans l'onglet **Child SA**.
27	Erreur passerelle La passerelle a reporté une erreur non prise en charge par le client VPN.	• Analyser les logs côté passerelle. • Récupérer les fichiers de logs de l'utilisateur, leur analyse est nécessaire. • Créer un ticket sur votre espace MyStormshield en joignant l'ensemble des fichiers de log.
28	Erreur login/mot de passe La passerelle a rejeté l'authentification EAP lors de l'établissement de la connexion VPN.	• Vérifier les paramètres d'authentification EAP dans la configuration du client VPN. • Vérifier que l'utilisateur connaît ses identifiants s'il en a besoin lors de l'établissement de la connexion.

Code	Diagnostic	Solution
30	Erreur carte à puce ou token Impossible d'accéder au certificat stocké sur la carte à puce ou le token.	• Vérifier que le lecteur de cartes à puce ou le token est correctement configuré sur le poste de travail, et accessible depuis le client VPN.
31	Délai d'authentification portail captif expiré Aucune session n'a été ouverte sur le portail captif. Le poste ne dispose donc pas d'une connectivité internet.	• Cliquer sur le bouton connecter pour pouvoir vous authentifier sur le portail captif.
100	Impossible de charger la configuration VPN Aucune connexion VPN n'a été trouvée dans le fichier de configuration.	• Vérifier qu'au moins un tunnel est configuré pour le **Panneau des Connexions**. Aller dans **Outils** > **Configuration du panneau des connexions**, puis ajouter un tunnel et sauvegarder la configuration.
101	Erreur de configuration GINA Un tunnel est actif avant logon, mais n'a pas été configuré pour être utilisé par le **Panneau TrustedConnect**.	• Vérifier que le tunnel actif avant logon est également configuré pour le **Panneau des Connexions**. Aller dans **Outils** > **Configuration du panneau des connexions**, puis ajouter un tunnel et sauvegarder la configuration.
102	Erreur d'initialisation IKE Une erreur s'est produite pendant l'initialisation du daemon IKE.	• Récupérer les fichiers de logs de l'utilisateur. • Créer un ticket sur votre espace MyStormshield en joignant l'ensemble des fichiers de log.
103	Erreur DNS Un nom DNS n'a pas pu être résolu dans le jeu de règles du mode filtrant.	• Vérifier que le poste a accès à internet. • Vérifier que le mode filtrant ne bloque pas lui-même l'accès aux requêtes DNS. • Remplacer les noms DNS par des adresses IP.
200	Activation du logiciel Le logiciel n'est pas activé et la période d'essai terminée.	• Récupérer les fichiers de logs de l'utilisateur. • Vérifier l'activation du logiciel.

Notions élémentaires de cryptographie

Algorithmes SHA, RSA, ECDSA et ECSDSA

Les signatures numériques font généralement intervenir deux algorithmes différents :

- un algorithme de hachage (SHA ou *secure hash algorithm*) et
- un algorithme de signature (RSA : initiales des trois inventeurs, ECDSA : *elliptic curve digital signature algorithm* ou ECSDSA : *elliptic curve Schnorr digital signature algorithm*).

La force du chiffrement RSA dépend de la taille de la clé utilisée. Dès lors que la taille est doublée, l'opération de déchiffrage va demander une puissance de traitement six à sept fois supérieure.

Selon l'ANSSI et le NIST, la taille de clé minimale recommandée est de 2048 bits.

Les algorithmes de hachage peuvent subir deux types d'attaques :

- la collision et
- la pré-image.

Une collision a lieu lorsque deux fichiers différents produisent le même condensat et qu'il est donc possible de substituer l'un pour l'autre.

La pré-image consiste à déterminer la valeur d'un fichier à partir de son condensat. Une pré-image secondaire consiste à produire à partir du condensat une valeur différente que celle à l'origine du hachage.

Selon l'ANSSI, la famille de fonctions de hachage SHA-1 n'est plus conforme à son référentiel général de sécurité et il convient par conséquent d'utiliser la famille SHA-2. Le NIST encourage de la même manière les agences fédérales étatsuniennes d'abandonner le SHA-1 au profit du SHA-2.

Les règles appliquées par SN VPN Client Exclusive suivent les recommandations de l'ANSSI et du NIST. Toutefois, si la PKI implémentée ne répond pas à ces exigences, il est possible de débrider le logiciel à l'aide de paramètres dynamiques.

NOTE
On trouve plusieurs notations pour les algorithmes de la famille SHA-2. Par exemple, SHA-2 (256 bits) s'écrit aussi SHA-256, SHA-2 (384 bits) s'écrit aussi SHA-384 et ainsi de suite.
Il en va de même pour les courbes elliptiques. Par exemple, pour secp256r1 on parle aussi de « courbe P-256 », pour secp384r1 de « courbe P-384 » et pour secp521r1 de « courbe P-521 ».

Accès aux certificats

CSP, CNG et PKCS#11 : quelles différences ?

La gestion des certificats sous Windows fait intervenir différents logiciels et normes pour leur stockage, que ce soit dans un magasin de certificats, sur un token ou sur une carte à puce.

NOTE
Les certificats stockés sur des cartes à puce ou tokens sont généralement copiés dans le magasin de certificats de l'utilisateur actuel, lorsque la carte est insérée dans le lecteur ou que le token est connecté à l'ordinateur.

CSP, CNG et PKCS#11 sont des notions connexes qui font toutes appel à des interfaces de programmation d'application (API) pour la gestion des certificats, mais la technologie mise en œuvre est différente dans chaque cas.

CSP et KSP

Sous Windows, la gestion des certificats faisait traditionnellement appel à des fournisseurs de services cryptographiques ou *Cryptographic Service Providers* (CSP) en anglais. Les CSP servent notamment à créer, stocker et accéder aux clés cryptographiques.

Aujourd'hui, il existe une nouvelle génération de modules logiciels indépendants appelés fournisseurs de stockage de clés ou *Key Storage Providers* (KSP) en anglais. Un KSP sert à créer, supprimer, exporter, importer, ouvrir et stocker des clés.

CAPI et CNG

L'évolution des normes de sécurité a conduit Microsoft à rendre obsolète l'API associée à ces CSP, appelée Cryptography API (CryptoAPI ou CAPI). Celle-ci a été remplacée par Cryptography API: Next Generation (CNG), dans laquelle les fournisseurs cryptographiques sont dissociés des fournisseurs de clés.

C'est pourquoi les versions 7.2 et supérieures de SN VPN Client Exclusive ne prennent pas en charge les CSP et que seule l'API CNG est prise en charge par cette version. Il convient donc de s'assurer que le certificat est importé dans le magasin de certificats Windows avec la bonne bibliothèque (cf. section Déterminer le type de conteneur d'un certificat ci-dessous).

Magasin machine et magasin utilisateur

Par ailleurs, il convient de savoir qu'il existe deux magasins de certificats sous Windows :

- le magasin machine, disponible pour tous les utilisateurs d'une machine, et
- le magasin utilisateur, uniquement disponible pour l'utilisateur actuel d'une machine.

> **NOTE**
> Dans les lignes de commande, l'option **-user** de la commande *certutil* sert à spécifier le magasin utilisateur. Lorsqu'elle est omise, le magasin machine est utilisé par défaut.

PKCS#11

Enfin, en cryptographie, il existe des normes de cryptographie à clé publique ou *Public Key Cryptography Standard*s (PKCS) en anglais. Il s'agit d'un ensemble de spécifications conçues par la société RSA Security.

La norme PKCS#11 fournit des applications avec une méthode d'accès aux périphériques matériels (cartes à puce ou tokens), indépendamment du type d'appareil. Elle comporte donc une API servant d'interface générique à un pilote de périphérique prenant en charge la norme PKCS #11. Cette API est prise en charge par la version 7.x de SN VPN Client Exclusive dès lors qu'un middleware correspondant est installé.

Synthèse

En résumé, il existe donc plusieurs types de middleware d'accès aux certificats stockés sur token, sur carte à puce et dans un magasin de certificats (certmgr.msc) :

- **CSP** pour **C**ryptographic **S**ervice **P**rovider (déprécié au profit de CNG) : non pris en charge par les versions 7.x.
- **CNG** pour **C**ryptography API: **N**ext **G**eneration : seule API prise en charge dans les versions 7.x. Dans le cas présent, il est nécessaire d'importer le certificat dans le magasin Windows avec la bonne bibliothèque.
- **PKCS#11** pour **P**ublic-**K**ey **C**ryptography **S**tandards : pris en charge par les versions 7.x.

Déterminer le type de conteneur d'un certificat

CSP et CNG sont des middlewares Microsoft. Sous Windows, les certificats sont stockés dans des conteneurs de type CNG ou de type CSP.

Pour connaître le conteneur des certificats dans le magasin de certificats, le token ou la carte à puce, vous pouvez lister les certificats contenus dans le magasin (utilisateur ou machine). Les informations retournées indiquent le type de fournisseur à partir duquel vous pouvez déduire le type de conteneur (CSP ou CNG). Ce dernier vous permet ensuite de déterminer la compatibilité du certificat avec les versions 7.2 et supérieures de SN VPN Client Exclusive.

- Pour lister les certificats contenus dans le magasin utilisateur, exécutez la commande suivante :

```
certutil -verifystore -user My
```

- Pour lister les certificats contenus dans le magasin machine, exécutez la commande suivante :

```
certutil -verifystore My
```

À partir des informations retournées, vous pouvez déterminer le type de conteneur de la manière suivante. Si le fournisseur est :

- Microsoft Smart Card Key Storage Provider, le conteneur est de type CNG (compatible avec les versions 7.2 et supérieures) ;
- Microsoft Base Smart Card Crypto Provider, le conteneur est de type CSP (non compatible avec les versions 7.2 et supérieures).

Format des certificats

À partir de la version 7 de SN VPN Client Exclusive, le format des certificats doit respecter une taille de clé et un algorithme de hachage précis.

Obligatoire

- Longueur de clé (en bits) : dans le cas des certificats RSA, la taille doit être de 2048 ou plus
- Algorithme de prise d'empreinte (ou *digest algorithm*) : doit être SHA 256, SHA-384 ou SHA-512

Optionnel

La vérification de la CRL du certificat utilisateur.

> **NOTE**
> Depuis la version 7.5 de SN VPN Client Exclusive, il est possible de vérifier la révocation du certificat de la passerelle à l'aide du protocole de vérification de certificat en ligne en mode agrafage (OCSP ou *Online Certificate Status Protocol* en anglais). Pour cela, il convient d'ajouter le paramètre dynamique enable_OCSP défini à la valeur true (voir section Afficher plus de paramètres).

Certificat passerelle

Partie Key Usage extension

- doit être présente,
- doit être marquée comme critique et
- ne doit contenir que les valeurs *digitalSignature* et/ou *nonRepudiation*.

Si ce n'est pas le cas, référez-vous au paramètre dynamique allow_server_extra_keyusage décrit à la section Contraintes relatives à l'extension Key Usage.

> **NOTE**
> Conformément aux exigences de sécurité, la valeur *keyEncipherment* de l'extension Key Usage a été abandonnée au profit de la valeur *nonRepudiation*. Cependant, la version 7.5 de SN VPN Client Exclusive continue d'accepter la valeur *keyEncipherment* sans l'utilisation du paramètre dynamique *allow_extra_keyusage*.

ASTUCE
Il est recommandé de préférer la valeur *nonRepudiation* de l'extension Key Usage à la valeur *keyEncipherment*.

Partie Extended Key Usage extension

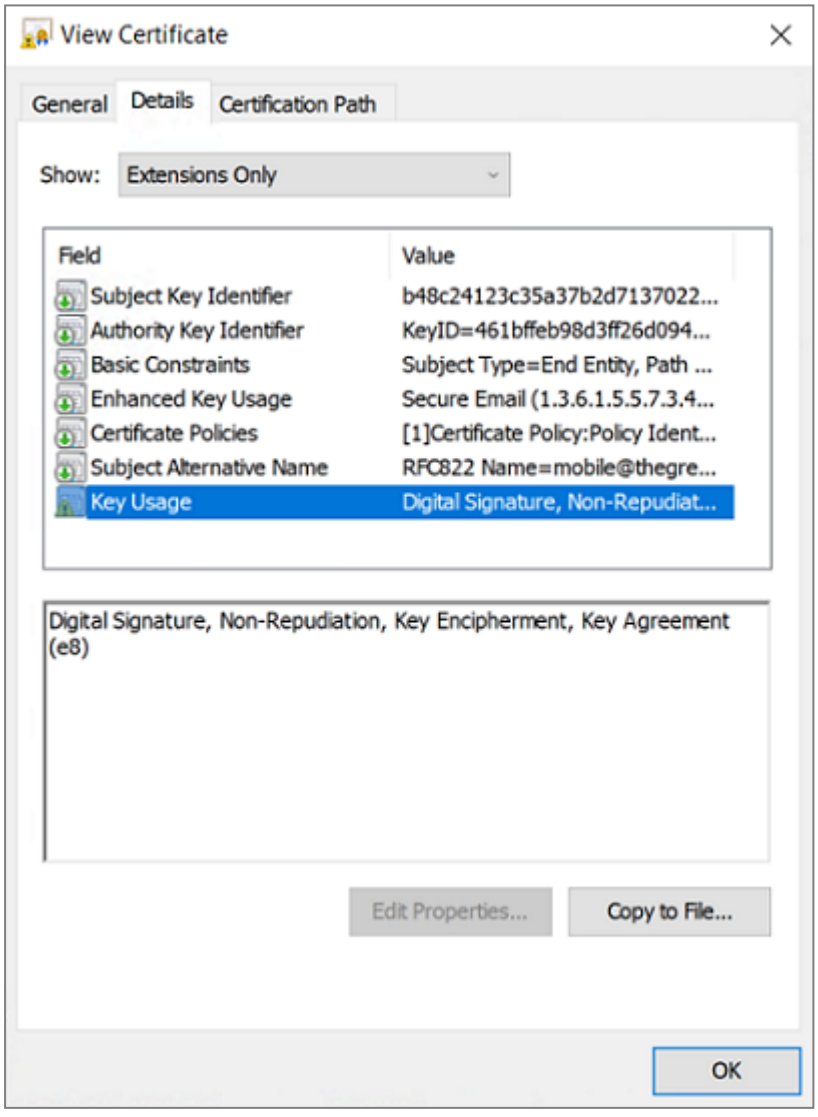
- peut être absente ou présente,
- si elle est présente, elle doit :
  - doit être marquée comme non-critique et
  - uniquement contenir les valeurs suivantes :
    id-kp-serverAuth ou
    id-kp-serverAuth et *id-kp-ipsecIKE*.

Si ce n'est pas le cas, référez-vous au paramètre dynamique allow_server_and_client_auth décrit à la section Contraintes relatives à l'extension Extended Key Usage.

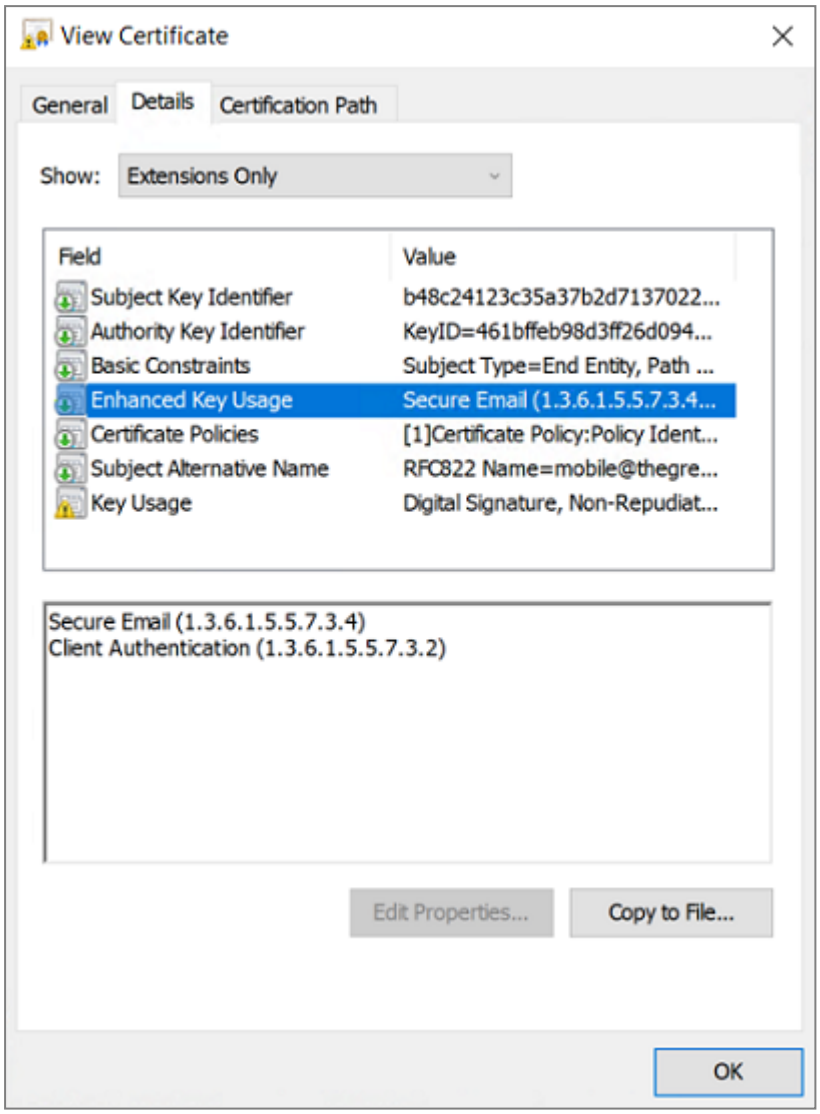
Exemple de certificat sous Windows

Dans une PKI Windows, voici la relation entre un certificat et les extensions :

- Extended Key Usage :



- Key Usage :



Exemple de log d'un certificat

Les extensions sont présentes dans un log de certificat (fichier *tgbikeng.log*) :

```
20220826 17:20:23:953 Local0.Info [11204] X509v3 extensions
20220826 17:20:23:956 Local0.Info [11204] Basic constraints :
20220826 17:20:23:960 Local0.Info [11204] CA:FALSE
20220826 17:20:23:965 Local0.Info [11204] Netscape Certificate comment :
20220826 17:20:23:968 Local0.Info [11204] TheGreenBow PKI generated server
certificate
20220826 17:20:23:971 Local0.Info [11204] Subject key identifier :
20220826 17:20:23:974 Local0.Info [11204]
FB:D6:5A:EF:FE:1B:DC:68:90:66:B9:D7:47:45:EA:B5:86:97:4A:B3
20220826 17:20:23:978 Local0.Info [11204] Authority key identifier :
20220826 17:20:23:981 Local0.Info [11204] keyIdentifier:
6F:6D:B8:A5:0B:EA:64:82:2E:B4:5F:0A:35:53:8B:80:05:4C:7B:0E
20220826 17:20:23:984 Local0.Info [11204] authorityCertIssuer: C = FR, ST
= Ile-de-France, L = Paris, O = TheGreenBow, OU = QA40, CN = Root CA
20220826 17:20:23:988 Local0.Info [11204] authorityCertSerialNumber: 10:00
20220826 17:20:23:990 Local0.Info [11204] Key usage : critical
20220826 17:20:23:995 Local0.Info [11204] Digital signature
20220826 17:20:24:000 Local0.Info [11204] Extended key usage :
20220826 17:20:24:003 Local0.Info [11204] Server authentication
```

Certificat utilisateur

Dans le cas d'un certificat utilisateur, il peut il y avoir des avertissements, mais il n'est pas nécessaire de débrider le Client VPN. Les messages sont affichés dans la **Console**.

Méthodes d'authentification des certificats

SN VPN Client Exclusive prend en charge les méthodes d'authentification des certificats suivantes :

- Méthode 1 : signature numérique RSA avec SHA-2 [RFC 7296]
- Méthode 9 : ECDSA « secp256r1 » avec SHA-2 (256 bits) sur la courbe P-256 [RFC 4754]
- Méthode 10 : ECDSA « secp384r1 » avec SHA-2 (384 bits) sur la courbe P-384 [RFC 4754]
- Méthode 11 : ECDSA « secp521r1 » avec SHA-2 (512 bits) sur la courbe P-521 [RFC 4754]
- Méthode 14 : signature numérique RSASSA-PSS, RSASSA PKCS1 v1_5 et Brainpool avec SHA-2 (256/384/512 bits) [RFC 7427]
- Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) sur la courbe BrainpoolP256r1 (uniquement disponible avec des passerelles prenant en charge cette méthode)

Par défaut, la méthode d'authentification utilisée pour les certificats de type RSA (RSASSA-PSS ou RSASSA-PKCS1-v1_5) est la méthode 14 avec signature RSASSA-PSS. Si la passerelle / le pare-feu utilise la méthode 14 avec la signature RSASSA-PKCS1-v1.5, le Client VPN va rejeter le certificat, avec le message suivant dans la **Console** :

```
RSASSA-PKCS1-v1_5 signature scheme not supported with authentication
method 14
```

Dans le cas où la passerelle ne prend pas en charge la méthode 14 avec la signature RSASSA-PSS, il est possible de configurer le Client VPN pour employer la méthode 14 avec la signature *RSASSA-PKCS1-v1_5*, en ajoutant le paramètre dynamique *Method14_RSASSA_PKCS1* défini à la valeur *true* ou *yes* (voir section Afficher plus de paramètres).

Dans le cas où la passerelle ne prend pas non plus en charge la méthode 14 avec la signature *RSASSA-PKCS1-v1_5*, il est possible de configurer le Client VPN pour employer la méthode 1 avec signature numérique RSA et SHA-2, en ajoutant le paramètre dynamique *Method1_PKCS1v15_Scheme* défini à la valeur *04* (SHA-256), *05* (SHA-384) ou *06* (SHA-512) (voir section Afficher plus de paramètres). Toute autre valeur sera rejetée par le Client VPN.

La méthode d'authentification utilisée pour les certificats de type ECDSA (courbes elliptiques) dépend de la courbe elliptique utilisée dans le certificat : ECDSA avec SHA-256 sur la courbe P-256, ECDSA avec SHA-384 sur le courbe P-384, ECDSA avec SHA-512 sur la courbe P-521 ou ECDSA avec SHA-256 sur la courbe BrainpoolP256r1.

Lorsque le Client VPN doit créer une signature pour un certificat utilisateur de type Brainpool, la méthode d'authentification 14 est utilisée par défaut, ce qui convient pour une passerelle ne fonctionnant pas en mode DR. Si ce type de certificat doit être utilisé avec une passerelle fonctionnant en mode DR, il convient d'ajouter le paramètre dynamique *use_method_214* défini à la valeur true (voir section Afficher plus de paramètres). L'algorithme d'empreinte numérique NID_sha256, NID_sha384 ou NID_sha512 est utilisé pour signer selon la taille de la clef.

NOTES

- L'utilisation de l'algorithme SHA-1 dans les signatures numériques n'est pas possible.
- Les certificats RSA avec une clé de taille inférieure à 2048 bits seront refusés par SN VPN Client Exclusive.
- Les certificats ECDSA avec une clé de taille inférieure à 256 bits seront refusés par SN VPN Client Exclusive.

Caractéristiques techniques de SN VPN Client Exclusive

Général

Version Windows	Windows 11 64 bits Windows 10 64 bits
Langues	Allemand, anglais, arabe, chinois (simplifié), coréen, espagnol, danois, persan, finnois, français, grec, hindi, hongrois, italien, japonais, néerlandais, norvégien, polonais, portugais, russe, serbe, slovène, tchèque, thaï, turc

Mode d'utilisation

Mode invisible	Ouverture automatique du tunnel sur détection de trafic Contrôle d'accès aux configurations VPN Possibilité de masquer tout ou partie des interfaces
Gina	Ouverture d'un tunnel avant le logon Windows par : GINA / Credential providers sur Windows 10
Scripts	Exécution de scripts configurable sur ouverture et fermeture du tunnel VPN
Partage de bureau à distance	Ouverture en un seul clic d'un ordinateur distant via RDP et le tunnel VPN
Panneau TrustedConnect	Ouverture automatique du tunnel avec Always-on et détection de réseau de confiance (TND)

Connexion / Tunnel

Mode de connexion	Peer-to-gateway
Réseaux	IPv4 et IPv6
Protocoles	IPsec / IKEv2 SSL / OpenVPN
Mode CP	Récupération automatique des paramètres réseaux depuis la passerelle VPN

Cryptographie et authentification

Chiffrement, Groupes de clé, Hachage (IKEv2)	Symétrique : AES CBC/CTR/GCM 128/192/256 bits Diffie-Hellman : DH 14 (MODP 2048), DH 15 (MODP 3072), DH 16 (MODP 4096), DH 17 (MODP 6144), DH 18 (MODP 8192), DH 19 (ECP 256), DH 20 (ECP 384), DH 21 (ECP 521), DH 28 (BrainpoolP256r1) Hachage : SHA-2 (256/384/512 bits)
Suites de sécurité TLS (OpenVPN)	TLS 1.2 – Medium TLS 1.2 – High TLS 1.3 : • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256
Chiffrement, Hachage (OpenVPN)	Symétrique : AES-128-CBC, AES-192-CBC, AES-256-CBC Hachage : SHA-2 (224/256/384/512 bits)
Authentification	• Clé partagée • EAP-MSCHAPv2 • Certificats X.509 • Multiple Auth
Méthodes d'authentification des certificats	• Méthode 1 : signature numérique RSA avec SHA-2 [RFC 7296] • Méthode 9 : ECDSA « secp256r1 » avec SHA-2 (256 bits)sur la courbe P 256 [RFC 4754] • Méthode 10 : ECDSA « secp384r1 » avec SHA-2 (384 bits) sur la courbe P-384 [RFC 4754] • Méthode 11 : ECDSA « secp521r1 » avec SHA-2 (512 bits) sur la courbe P-521 [RFC 4754] • Méthode 14 : signature numérique RSASSA-PSS, RSASSA-PKCS1-v1_5 et Brainpool avec SHA-2 (256/384/512 bits) [RFC 7427] • Méthode 214 : ECDSA « BrainpoolP256r1 » avec SHA-2 (256 bits) sur la courbe BrainpoolP256r1 (uniquement disponible avec des passerelles prenant en charge cette méthode)
IGC / PKI	• Prise en charge des certificats X.509 • Import de certificats au format PKCS#12, PEM/PFX • Multi-support : magasin de certificats Windows, carte à puce, token, fichier de configuration • Prise en charge de la liste des certificats révoqués (CRL) et de l'agrafage OCSP • Détection automatique du lecteur de cartes à puce ou du token en fonction de critères • Accès aux cartes à puce et aux tokens en PKCS#11 et CNG • Vérification complète de la chaîne des certificats « utilisateur » et « passerelle »

Divers

NAT / NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 et RFC 3947, IP address emulation, inclut le support de : NAT_OA, NAT keepalive, NAT-T mode agressif, NAT-T en mode forcé, automatique ou désactivé
DPD	RFC 3706. Détection des extrémités IKE non actives.
Passerelle redondante	Gestion d'une passerelle de secours (passerelle redondante), automatiquement sélectionnée sur déclenchement du DPD (passerelle inactive)

Administration

Déploiement	Installation silencieuse via Microsoft Installer (MSI)
Gestion des configurations VPN	Options d'importation et d'exportation des configurations VPN Sécurisation des importations / exportations par mot de passe, chiffrement et contrôle d'intégrité
Automatisation	Possibilité d'ouvrir, fermer et superviser un tunnel en ligne de commande (batch et scripts) Possibilité de démarrer et arrêter le logiciel par batch
Logs et traces	**Console** de logs IKE/IPsec et SSL/OpenVPN et mode traçant activable Logs administrateur : fichier local, journal d'évènements Windows, serveur syslog
Mises à jour	Vérification des mises à jour depuis le logiciel
Licence et activation	Licences par abonnement, activation manuelle / automatique / silencieuse

STORMSHIELD