Client VPN
Windows Enterprise 6.87

Guide de l'administrateur

Dernière mise à jour : 22 février 2022
Référence de document : 20220222_AG_VPE_6.8_FR_1.9

Table des matières

1 Présentation

1.1 Introduction

Ce guide est destiné aux administrateurs du Client VPN Windows Enterprise.
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 sur le site TheGreenBow.

1.2 Informations importantes

1.2.1 Fichiers de configuration de versions antérieures

Les fichiers de configuration VPN des versions antérieures au Client VPN Windows Enterprise 6.8 ne peuvent pas être importés dans le Panneau de Configuration.

S'il s'agit d'une mise à jour, l'installeur effectuera la conversion de la configuration existante avant de l'importer automatiquement dans le Panneau de Configuration.

1.2.2 Vérification du certificat de la passerelle

Par défaut, le certificat de la passerelle est systématiquement vérifié à l'ouverture d'un tunnel. Il peut être nécessaire d'importer la chaîne complète des CA (autorités de certification) de la passerelle, soit dans le magasin Windows, soit dans le fichier de configuration VPN.

Il est également possible (mais non recommandé) de modifier ce comportement par défaut (Menu Options -> Options PKI).

1.2.3 Fin de prise en charge des algorithmes « faibles »

Pour des raisons de sécurité, cette version ne prend plus en charge les algorithmes suivants : DES, 3DES, MD-5, SHA-1, DH 1-2, DH 5. Si une configuration antérieure comporte l'un de ces algorithmes, l'installeur les convertira en « auto » (négociation automatique avec la passerelle).

Dans le cas où la passerelle prend uniquement en charge ces algorithmes, la connexion avec cette version du Client VPN sera impossible.

1.3 Nouveautés de la version 6.8

1.3.1 Interface TrustedConnect

- Nouvelle interface utilisateur TrustedConnect, offrant une signalétique simple et intuitive
- Fonctionnalité TND (Trusted Network Detection), qui permet d'ouvrir automatiquement un tunnel si le poste est à l'extérieur du réseau de confiance, en se basant sur les suffixes DNS et l'identification de balises
- Fonctionnalité Always-On, qui assure le maintien de la connexion sécurisée à chaque changement d'interface réseau, par exemple, entre Ethernet, Wi-Fi et 4G

1.3.2 Installation, configuration et déploiement

- Utilisation de Microsoft Windows Installer (MSI) pour simplifier le déploiement et la mise à jour du logiciel avec GPO, offrant de nombreuses options d'installation pour répondre à tous types de besoins d'intégration (interface graphique, certificats, cartes à puce, tokens…)
- Le logiciel est intégralement compilé en 64 bits pour Windows 10 & 11, afin d'optimiser les performances et la sécurité
- Possibilité de réserver l'accès à la configuration VPN à l'administrateur Windows

1.3.3 Cryptographie

- Prise en charge des RFC 4304 Extended Sequence Number (ESN) et RFC 6023 (Childless IKE Initiation) pour une sécurité accrue
- Prise en charge des algorithmes de signature numérique suivants pour l'authentification forte des certificats :
    - méthode 9 : ECDSA "secp256r1" with SHA-256 on the P-256 curve [RFC4754]
    - méthode 10: ECDSA "secp384r1" with SHA-384 on the P-384 curve [RFC4754]
    - méthode 11: ECDSA "secp521r1" with SHA-512 on the P-521 curve [RFC4754
    - méthode 14 : Digital Signature Authentication PKCS1-v1.5 [RFC7427]
- Les algorithmes suivants, réputés vulnérables, ne sont plus pris en charge à partir de la version 6.8 : DES, 3DES, SHA, DH 1-2, DH 5
- Renforcement du chiffrement et de l'intégrité de la configuration VPN

1.3.4 Carte à puce et token

- Prise en charge de l'API Microsoft CNG (Cryptography API: Next Generation) permettant l'utilisation de la dernière génération de cartes à puce et de tokens
- Microsoft a rendu obsolète l'API CSP (Cryptographic Service Providers), elle n'est plus prise en charge en IKEv2 à partir de la version 6.8

1.3.5 SSL / TLS

- Prise en charge de la compression Lz4

2 Installation

2.1 Introduction

L'installation du Client VPN Windows Enterprise s'effectue en exécutant le programme téléchargeable sur le site web TheGreenBow.

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 » disponible sur le site web TheGreenBow.

☞ Se reporter à la section 2.2 Procédure d'installation.

2.1.1 Conditions d'installation

Le Client VPN Windows Enterprise fonctionne sur la version 64 bits de Windows 10 & 11.

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

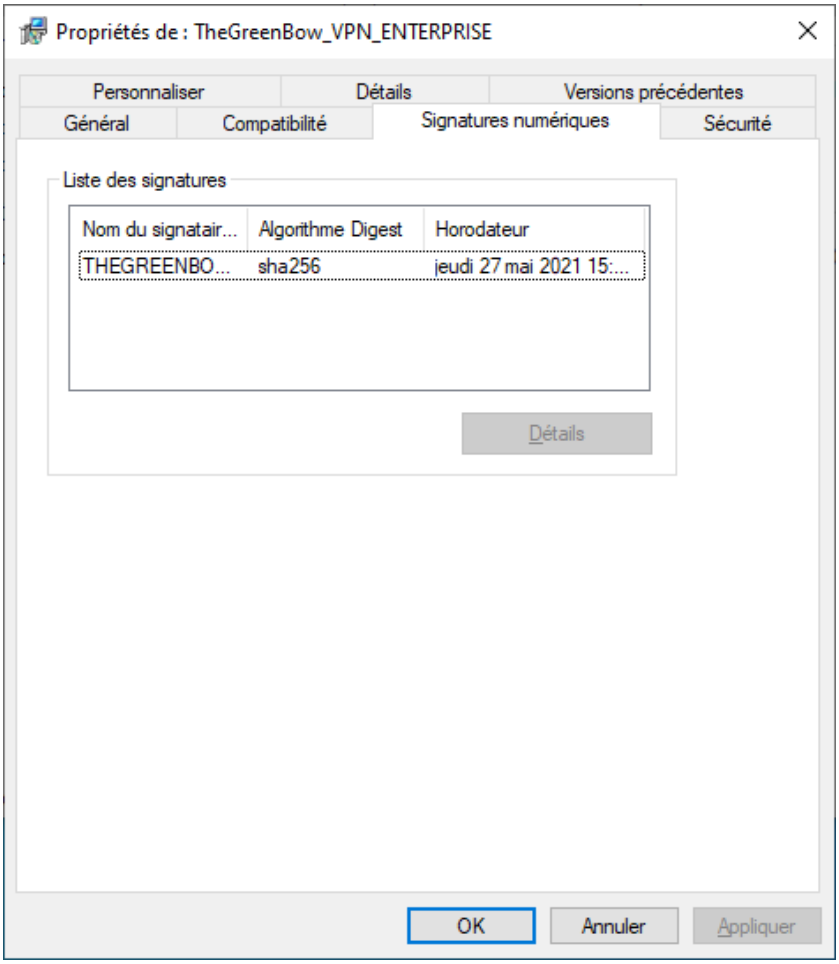
- Processeur : processeur 1 gigahertz (GHz) ou plus rapide
- RAM : 2 Go
- Espace disponible sur le disque dur : 40 Mo

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.

2.1.2 Signature numérique et version

Le logiciel installeur du Client VPN Windows Enterprise est signé par le certificat « THEGREENBOW SA ». Ceci permet à l'installateur ou à l'utilisateur de vérifier à tout moment 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 du Client VPN Windows Enterprise peut être vérifiée par l'utilisateur dans la fenêtre « À propos... » du logiciel.

2.1.3 Vulnérabilités

Par ailleurs, un utilisateur du Client VPN Windows Enterprise peut être averti des vulnérabilités identifiées dans le logiciel et des moyens pour y remédier (nouvelle version, mise à jour, patchs disponibles, conseils de contournement…) en envoyant ses coordonnées à l'adresse mail referent@thegreenbow.com.

Voir aussi les recommandations de sécurité.

2.2 Procédure d'installation

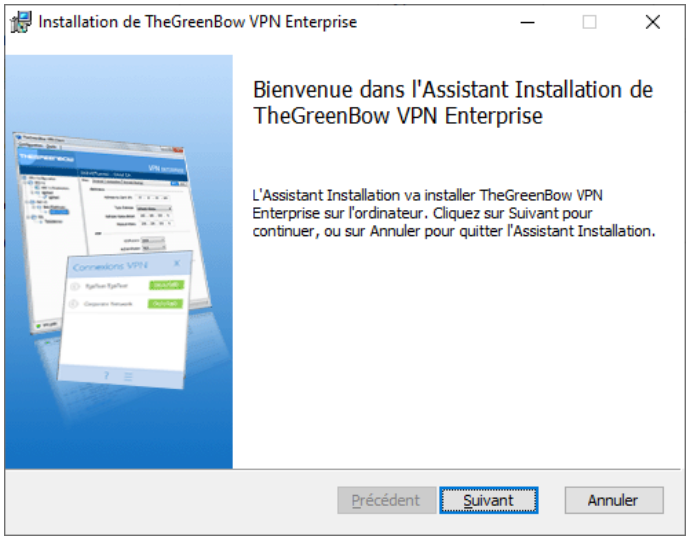
Après avoir téléchargé le programme d'installation du Client VPN Windows Enterprise et vérifié son authenticité (voir section 2.1.2 Signature numérique et version ci-dessus), vous pouvez procéder à son installation en suivant les étapes décrites ci-dessous.

⚠ La mise à jour du logiciel ne peut se faire que si votre abonnement est toujours en cours (cf. section 4.1 Comment obtenir une mise à jour).

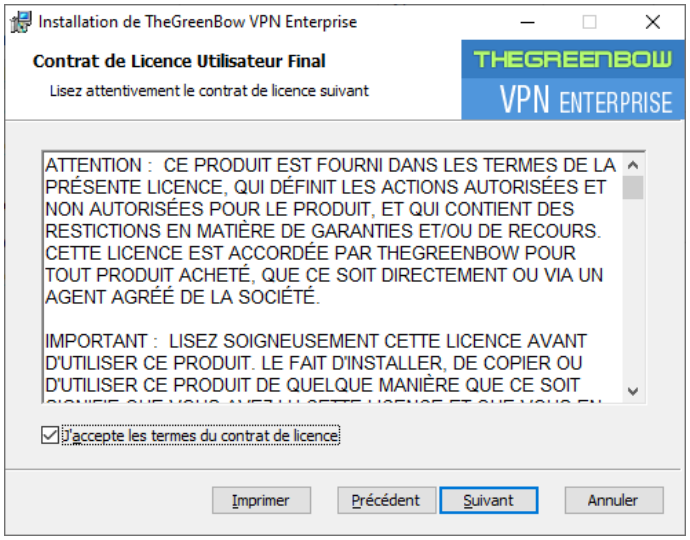
La procédure d'installation est identique qu'il s'agisse d'une première installation ou d'une mise à jour (cf. chapitre 4 Mise à jour). Lors d'une mise à jour, les paramètres du logiciel, la configuration VPN existante et la licence sont conservés.

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 ».

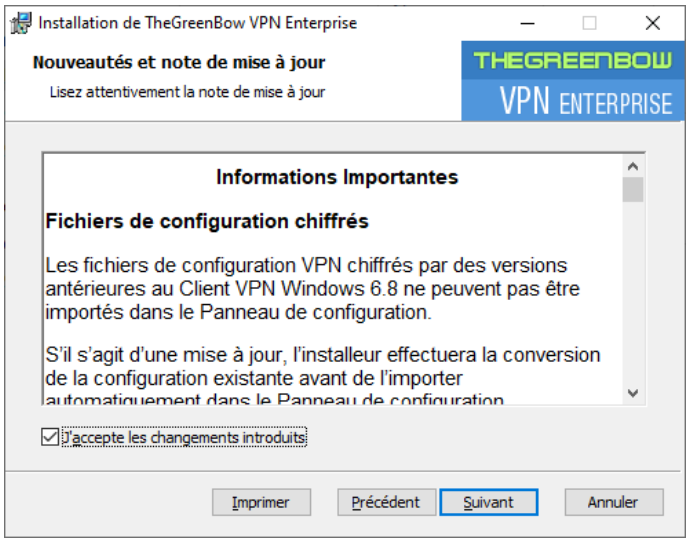
1/ Double-cliquez sur le programme d'installation que vous avez téléchargé. La fenêtre suivante s'affiche :



2/ Cliquez sur « Suivant ». La fenêtre suivante s'affiche :



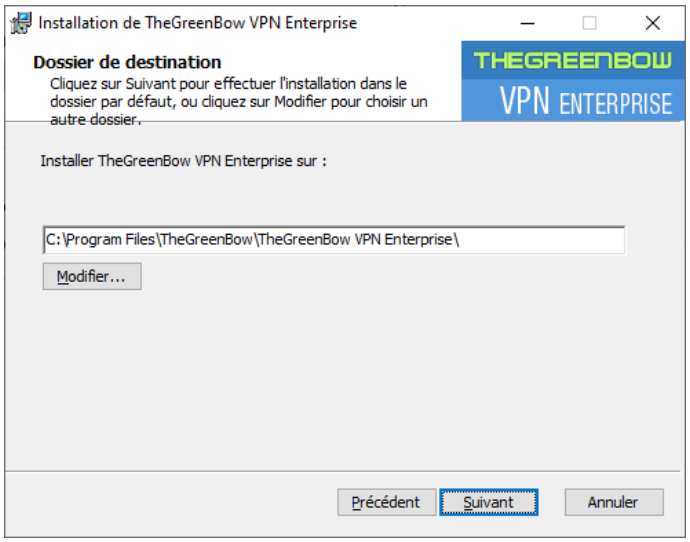
3/ Lisez attentivement le Contrat de licence de l'utilisateur final (CLUF). Si vous acceptez tous les termes du contrat, cochez la case « J'accepte les termes du contrat de licence », puis cliquez sur « Suivant ». Dans le cas contraire, vous ne pourrez pas poursuivre l'installation du Client VPN Windows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



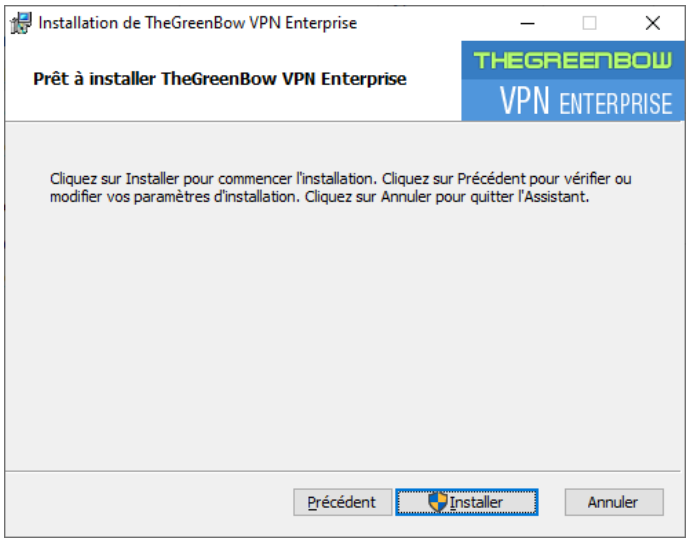
4/ Lisez attentivement les informations relatives aux nouveautés et la note de mise à jour concernant la conversion de la configuration VPN existante.

> ⚠ 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.

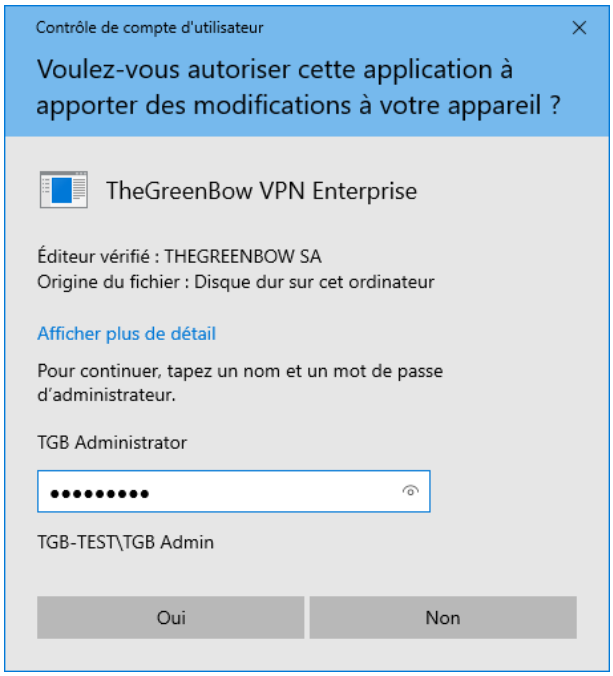
Si vous acceptez les changements introduits, cochez la case « J'accepte les changements introduits », puis cliquez sur « Suivant ». La fenêtre suivante s'affiche :



5/ Si vous souhaitez installer le Client VPN Windows Enterprise 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 :



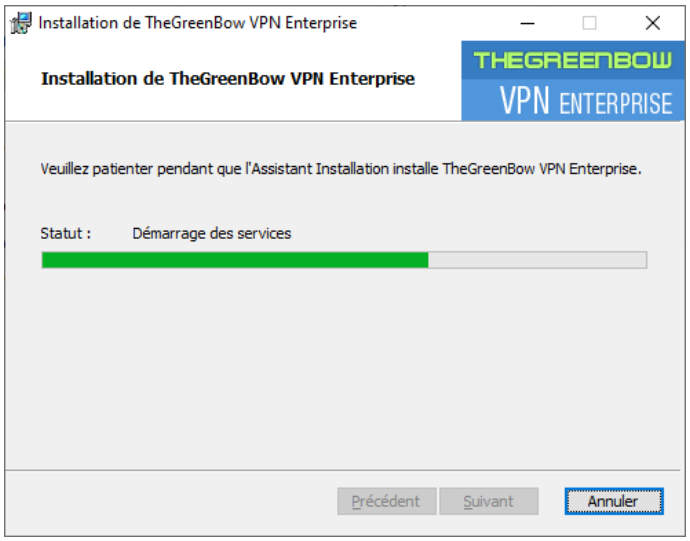
6/ Le programme est prêt à installer. Si vous souhaitez revenir en arrière pour vérifier ou modifier vos paramètres d'installation, cliquez sur « Précédent ». Sinon, cliquez sur « Installer ». Si vous effectuez l'installation à partir d'un compte qui ne dispose pas des droits d'administration, la fenêtre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



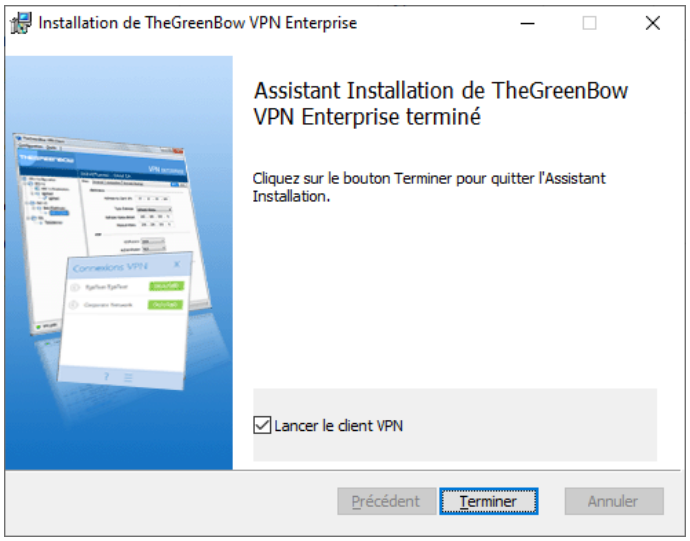
7/ Pour poursuivre l'installation, vous devez entrer un nom et mot de passe d'administrateur pour autoriser le programme d'installation d'apporter des modifications à votre ordinateur. Dans le cas contraire, le logiciel ne sera pas installé.

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 :



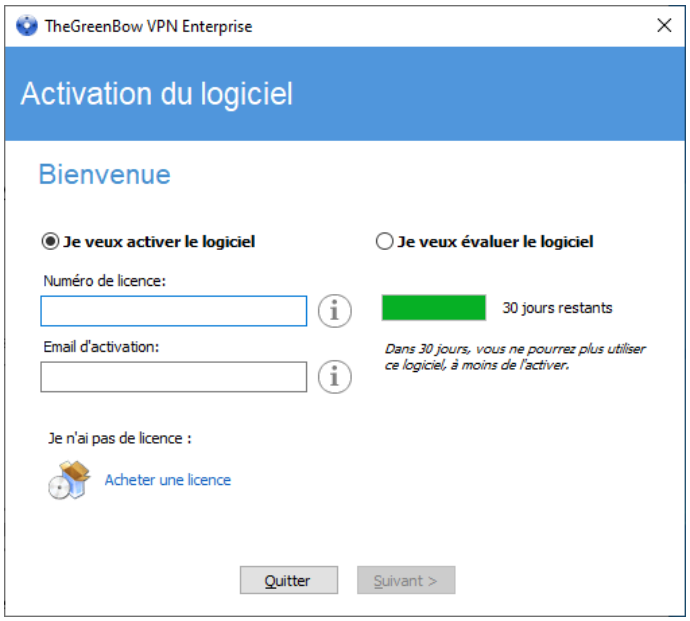
9/ Attendez la fin de la l'installation de l'ensemble des composants du Client VPN Windows Enterprise. Lorsque l'installation a réussi, la fenêtre suivante s'affiche :



10/ Si vous ne souhaitez pas lancer le Client VPN immédiatement, décochez la case correspondante. Pour quitter l'assistant d'installation, cliquez sur « Terminer ».

Si vous avez effectué une mise à jour, le logiciel est lancé directement dans la barre des tâches. Vous pouvez tester votre installation en lançant le tunnel de test (cf. section 6.3 Ouvrir un tunnel VPN de test avec le Panneau des Connexions).

Sinon, l'écran d'activation du logiciel s'affiche :



11/ Le Client VPN Windows Enterprise est désormais installé sur votre poste de travail.

Si vous possédez déjà une licence pour le Client VPN Windows Enterprise :

- sélectionnez « Je veux activer le logiciel »,
- entrez le numéro de licence et l'email d'activation,
- puis cliquez sur « Suivant > ».

Pour en savoir davantage sur la procédure d'activation, reportez-vous au chapitre 3 Activation.

Si vous souhaitez évaluer le Client VPN Windows Enterprise :

- 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 2.4 Période d'évaluation.

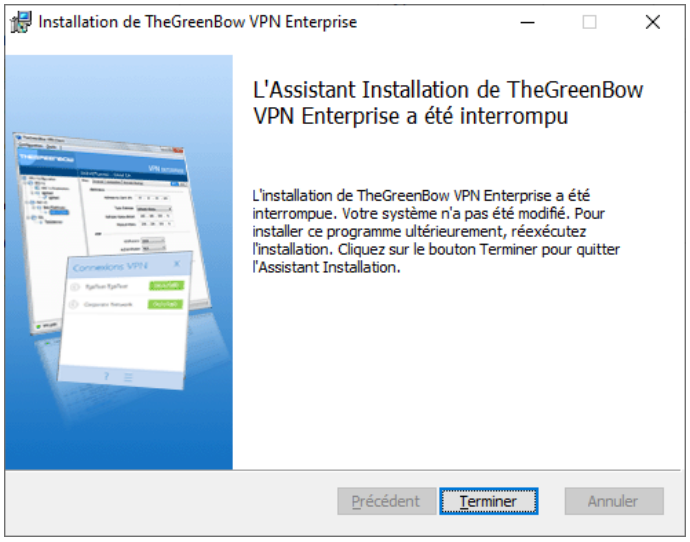
Si vous n'avez pas de licence et que vous souhaitez en acquérir une, cliquez sur « Acheter une licence ». La boutique en ligne TheGreenBow s'affiche dans une fenêtre de navigateur. Vous pouvez y acheter une ou plusieurs licences. Pour en savoir davantage sur la procédure d'activation, reportez-vous au chapitre 3 Activation.

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

- Pour commencer à utiliser le Client VPN Windows Enterprise immédiatement, reportez-vous au chapitre 6 Prise en main du logiciel.
- Pour utiliser l'assistant de configuration pour créer une connexion VPN rapidement, reportez-vous au chapitre 7 Assistant de configuration.
- Pour importer une configuration VPN TheGreenBow compatible avec cette version du logiciel, reportez-vous à la section 12.1 Importer une configuration VPN.
- Pour une présentation détaillée des interfaces disponibles, reportez-vous aux chapitres 8 Panneau des Connexions, 9 Panneau de Configuration et 10 Panneau TrustedConnect.
- Pour une explication complète de l'ensemble des options de configuration d'un tunnel VPN, reportez-vous au chapitre 13 Configurer un tunnel VPN.
- Pour désinstaller le Client VPN Windows Enterprise, reportez-vous au chapitre 5 Désinstallation.

2.3 Interruption de l'installation

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

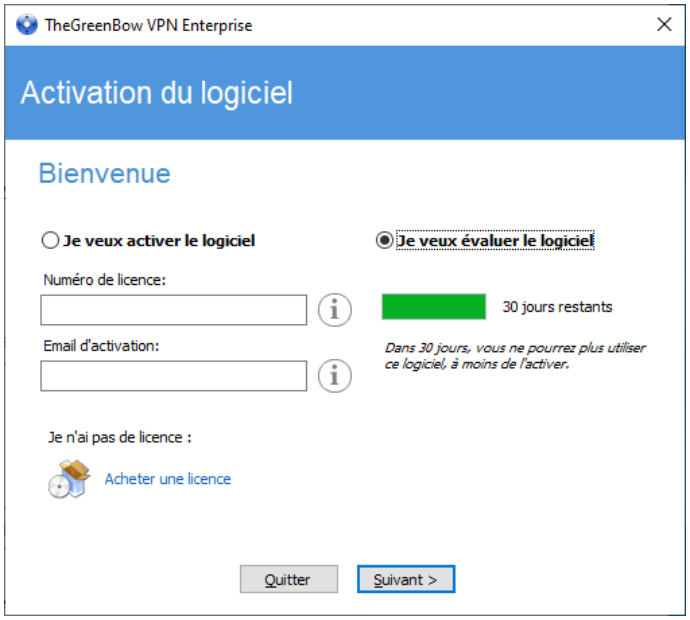


Votre système n'a pas été modifié et vous pouvez reprendre l'installation ultérieurement.

2.4 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.

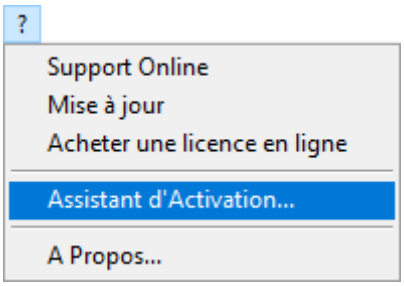
Pendant la période d'évaluation, la fenêtre d'activation est affichée à chaque démarrage du logiciel. Elle indique le nombre de jours d'évaluation restants.



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

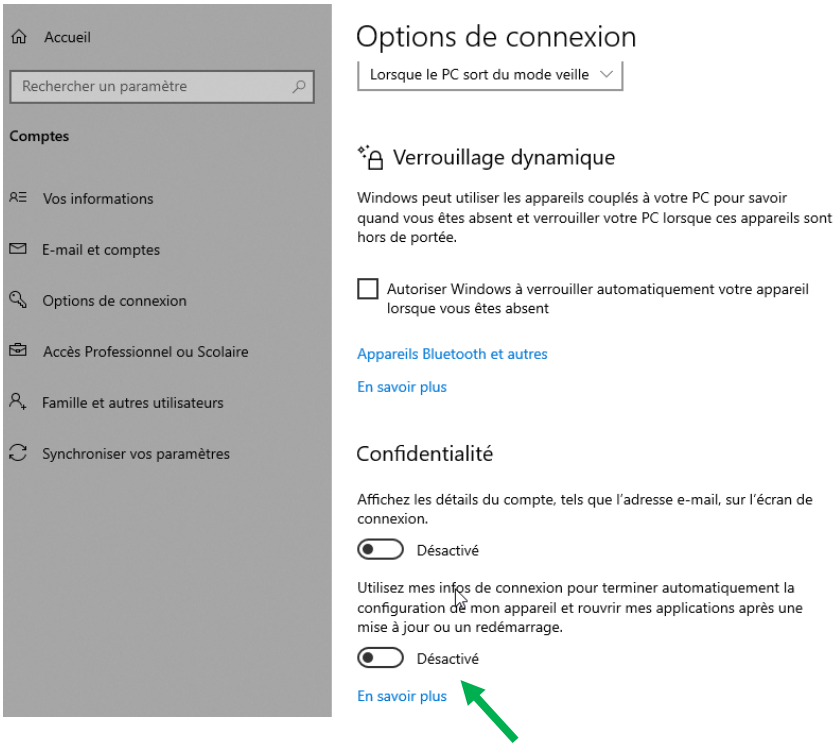
Pendant la période d'évaluation, la fenêtre « À propos… » affiche le nombre de jours d'évaluation restants.

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).



2.5 Configuration de Windows

Une fois l'installation terminée, il convient de s'assurer de la désactivation du paramètre de confidentialité Windows « 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 », qui se trouve dans les « Options de Connexion » du Panneau de configuration, comme indiqué dans la capture d'écran des réglages de Windows 10 ci-dessous :



La même option est disponible dans les réglages de Windows 11.

3 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.

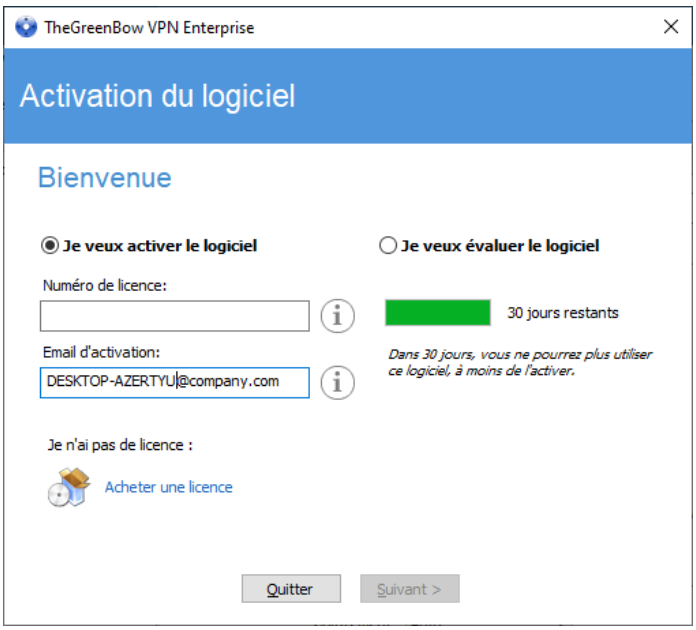
3.1 Étape 1

Si vous n'avez pas encore de licence, cliquez sur « Acheter une licence ». La boutique en ligne TheGreenBow s'affiche dans une fenêtre de navigateur. Suivez les instructions pour acheter une ou plusieurs licences.

Dans le champ « Numéro de licence », entrez le numéro de licence reçu par email.

Le numéro de licence peut être copié-collé depuis l'email 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 email permettant d'identifier votre activation. Cette information permet de retrouver, en cas de perte, les informations sur votre activation.



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.

3.2 Étape 2

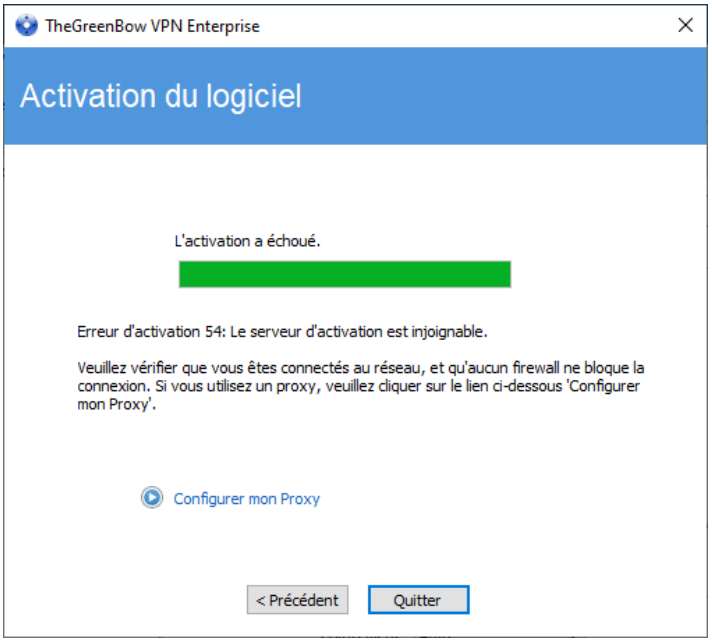
Cliquez sur « Suivant > », le processus d'activation en ligne s'exécute automatiquement.

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

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.

3.3 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.



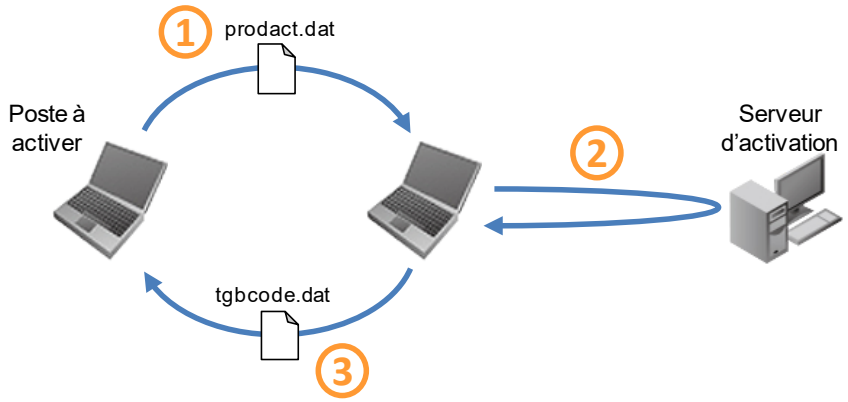
TheGreenBow indique sur son site web toutes les erreurs d'activation ainsi que les procédures de résolution des problèmes d'activation.

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 TheGreenBow
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 un proxy. Le cas échéant, configurer le firewall pour laisser passer la communication, ou le proxy pour la rediriger correctement.

3.4 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 :

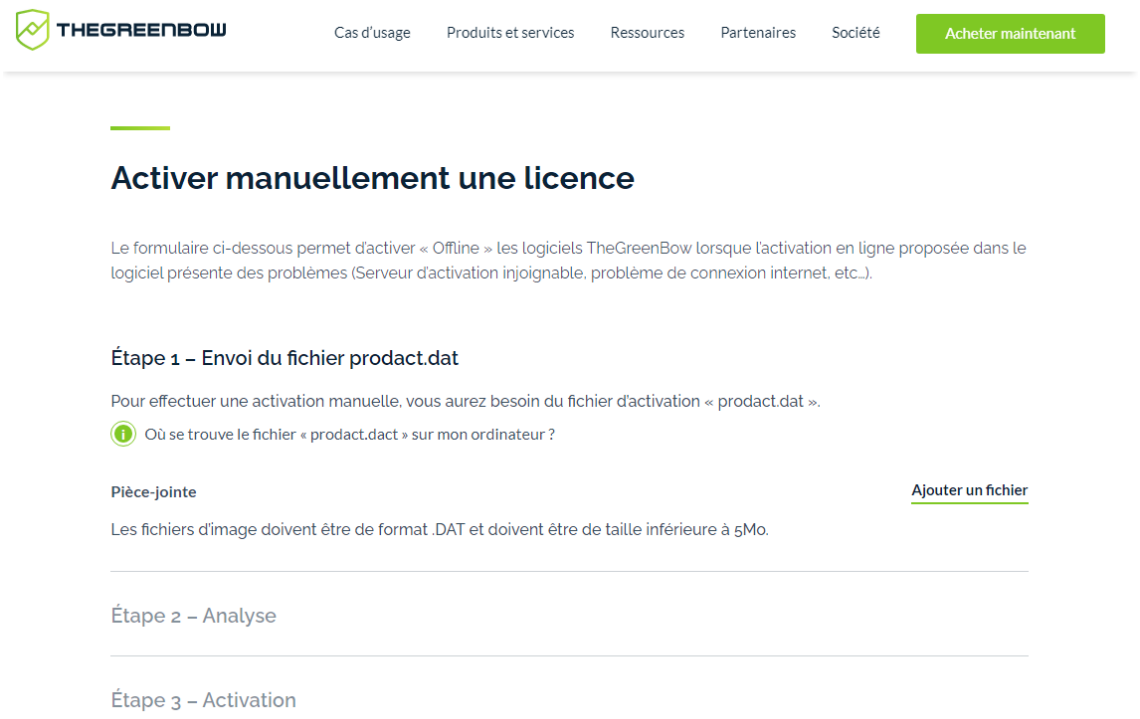


1	Fichier `prodact.dat`	Sur le poste à activer, récupérer le fichier `prodact.dat` situé dans le répertoire Windows « Mes Documents ». (1)
2	Activation	Sur un poste connecté au serveur d'activation (2), ouvrir la page d'activation manuelle (3), y poster le fichier `prodact.dat` et récupérer le fichier `tgbcode` créé automatiquement par le serveur.
3	Fichier `tgbcode`	Copier ce fichier `tgbcode` dans le répertoire Windows « Mes documents » du poste à activer. Lancer le logiciel : il est activé.

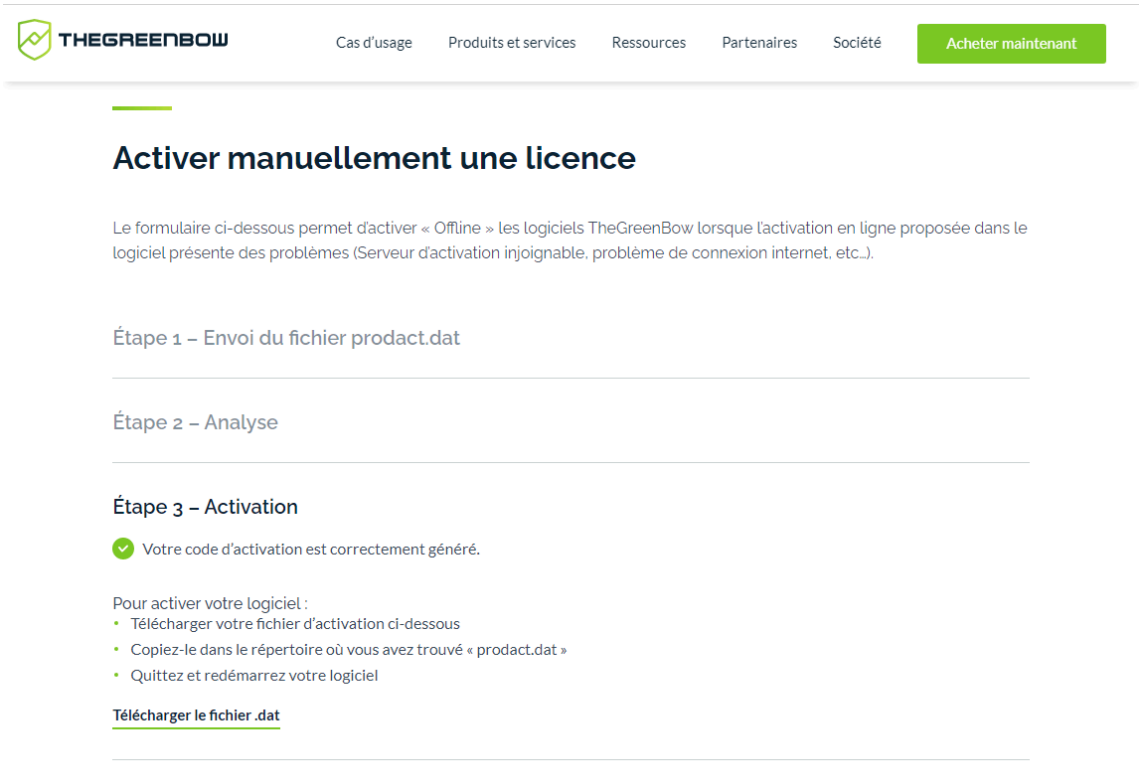
(1) Le fichier `prodact.dat` est un fichier texte qui contient les éléments du poste utilisés pour l'activation. Si ce fichier n'existe pas dans le répertoire « Mes documents », effectuer sur le poste une activation : même si elle échoue, elle a pour effet de créer ce fichier.
(2) Le serveur d'activation est le serveur TheGreenBow, accessible sur Internet.
(3) Se reporter à la procédure détaillée ci-dessous.

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.



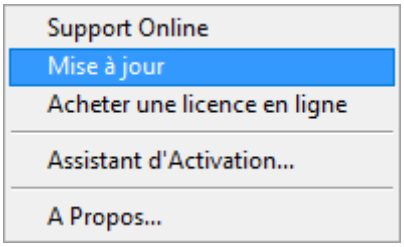
Ce fichier a un nom de la forme : `tgbcode_[date]_[code].dat` (par exemple : `tgbcode__20210615_1029.dat`).

3.5 Licence et logiciel activé

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

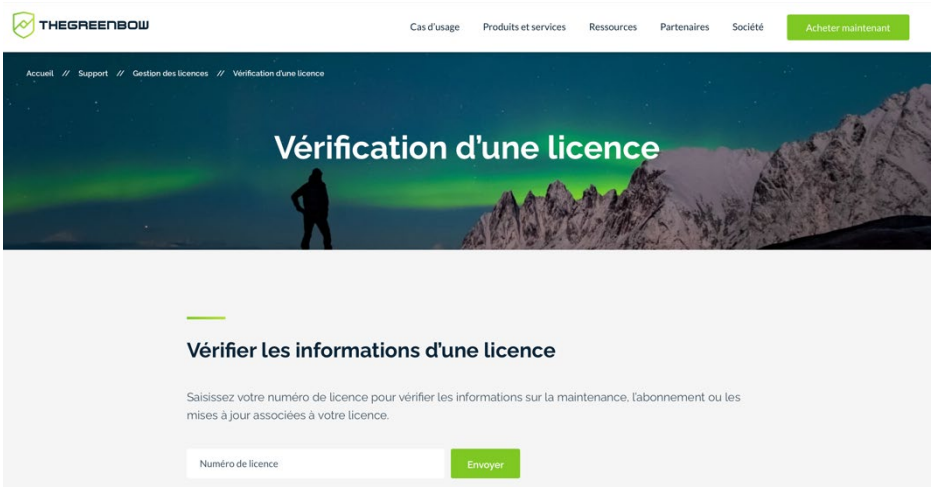
4 Mise à jour

Le logiciel permet de vérifier à tout moment si une mise à jour est disponible, via le menu de l'interface principale : « ? > Mise à jour ».



Ce menu ouvre la page web de vérification de mise à jour, qui indique si une mise à jour est disponible et activable, suivant le type de licence achetée, et suivant le type de maintenance ou d'abonnement souscrit. Pour obtenir ces information, il convient de rentrer le numéro de licence dans le champ correspondant de la page de vérification, également consultable directement par le lien suivant : https://www.thegreenbow.com/fr/support/gestion-des-licences/verification-dune-licence/.

Exemple :



4.1 Comment obtenir une mise à jour

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

En cours d'abonnement (1)	Je peux installer toute mise à jour
Hors période d'abonnement	Je ne peux utiliser le logiciel ni faire de mise à jour

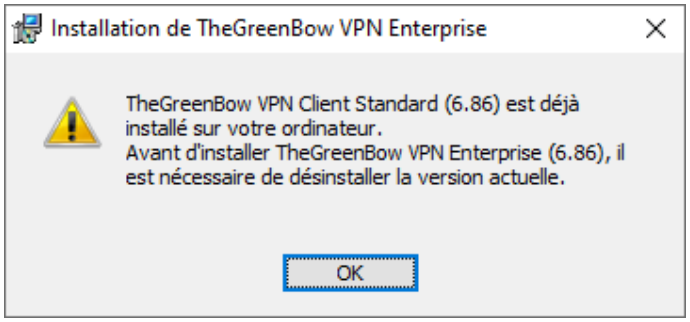
(1) L'abonnement démarre à la date d'achat du logiciel.

⚠ La mise à jour d'une édition Standard vers une édition Enterprise et vice-versa n'est pas autorisée. En revanche la mise à jour à partir de toute version antérieure du Client VPN Enterprise (y compris Premium et Certifié) est possible.

4.2 Procédure de mise à jour

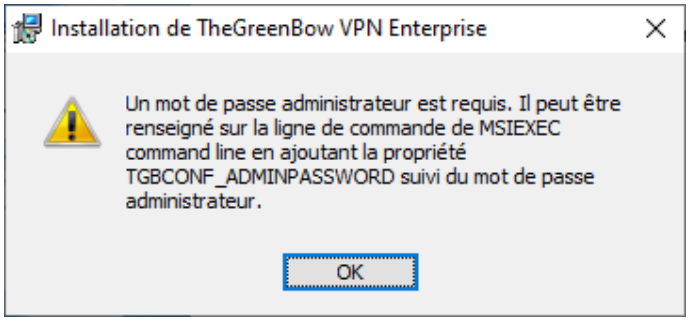
La mise à jour du Client VPN Windows Enterprise permet de passer à une version plus récente du logiciel tout en conservant les paramètres, la configuration VPN et la licence. Elle s'effectue comme une installation normale (cf. section 2.2 Procédure d'installation) à deux exceptions près :

1/ Si la licence du produit installé n'est pas compatible avec le Client VPN Windows Enterprise 6.8, 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 :



La protection par mot de passe de l'accès au Panneau de Configuration a été remplacée dans la version 6.8 du Client VPN Windows Enterprise par un mécanisme plus sécurisé. Celui-ci consiste à limiter l'accès au Panneau de Configuration aux seuls administrateurs Windows. Cette option est activée par défaut, mais peut être désactivée comme indiqué dans la section 24.1 Affichage de l'interface (masquage), option « Restreindre l'accès du panneau de configuration aux administrateurs ».

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 ».

4.3 Mise à jour de la configuration VPN

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

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.

4.4 Automatisation

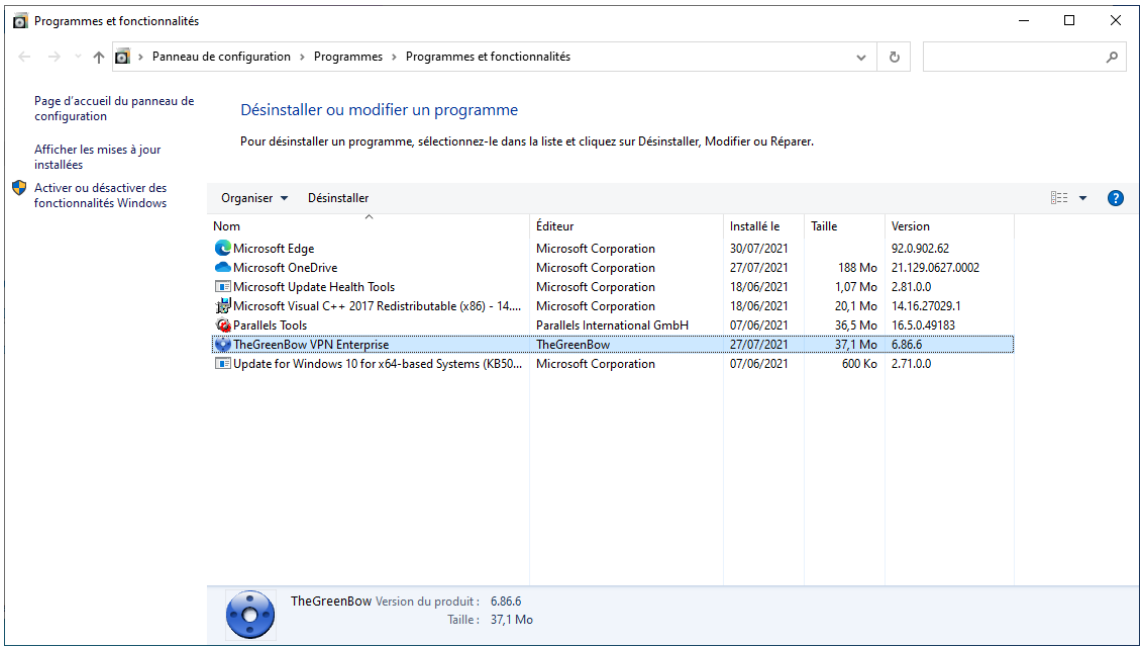
L'exécution d'une mise à jour est configurable, en utilisant une liste d'options de ligne de commande, ou en utilisant un fichier d'initialisation.

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

5 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 « TheGreenBow VPN Enterprise » dans la liste de programmes.
4/ Cliquez sur « Désinstaller » et suivre les instructions pour désinstaller le programme.



Ou

1/ Ouvrez le menu Windows « Démarrer ».
2/ Cliquez avec le bouton droit de la souris sur le programme « TheGreenBow VPN Enterprise », puis sélectionnez « Désinstaller ».

3/ Le Panneau de configuration Windows s'affiche. Sélectionnez « TheGreenBow VPN Enterprise » dans la liste de programmes.
4/ Cliquez sur « Désinstaller » et suivez les instructions pour désinstaller le programme.

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

6 Prise en main du logiciel

6.1 Introduction

L'interface graphique du Client VPN Windows Enterprise 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 des tunnels 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.

6.2 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 3 Activation). Lorsque le logiciel est activé ou que vous avez choisi de l'évaluer, le Client VPN Windows Enterprise se lance minimisé et l'icône TheGreenBow VPN Enterprise 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, ou que vous souhaitez utiliser le tunnel de test après l'installation ou la mise à jour du logiciel, pour lancer le Client VPN Windows Enterprise, 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.

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.

Le Client VPN Windows Enterprise peut être lancé directement en double-cliquant sur cette icône.

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

Démarrer le Client VPN à partir du menu Démarrer

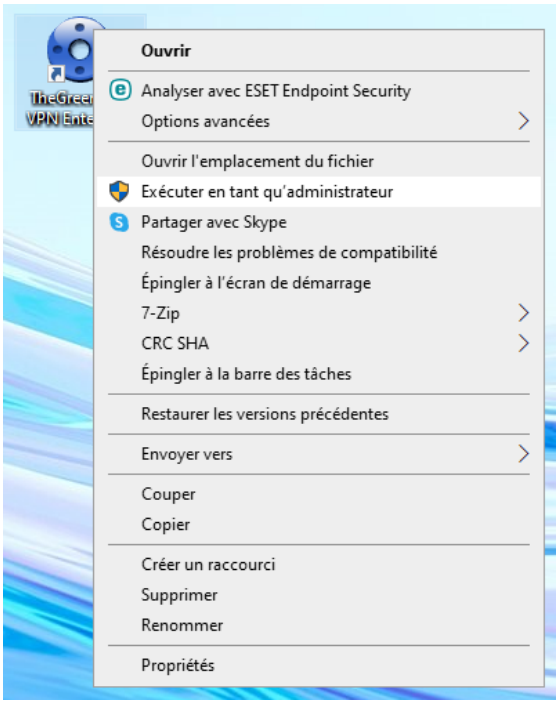
À l'issue de l'installation, le Client VPN Windows Enterprise peut être lancé depuis le menu « Démarrer » de Windows en cliquant sur le programme TheGreenBow VPN Enterprise.

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

Démarrer le Client VPN en tant qu'administrateur

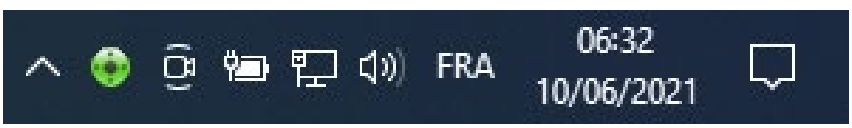
Par défaut, l'accès au Panneau de Configuration du Client VPN est réservé aux seuls administrateurs Windows.

Pour lancer le Client VPN en mode administrateur, afin de pouvoir accéder au Panneau de Configuration, cliquez sur l'icône TheGreenBow VPN Enterprise 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 du Client VPN Windows Enterprise 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

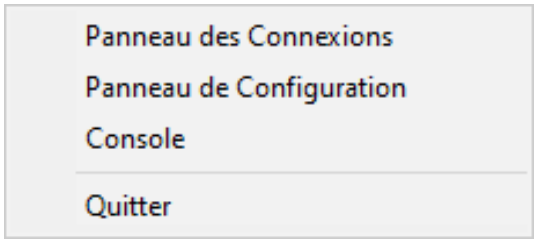
Icône verte : au moins un tunnel VPN est ouvert

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

- « VPN Tunnel ouvert » si un ou plusieurs tunnels sont ouverts ;
- « TheGreenBow VPN Enterprise » 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 24.1 Affichage de l'interface (masquage)). Par défaut, les options du menu contextuel sont les suivantes :

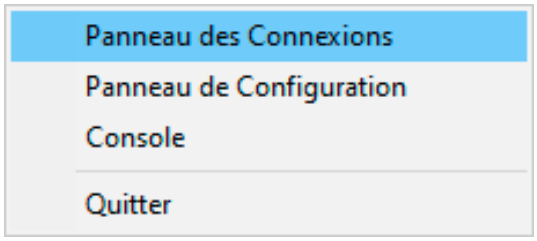
1/ Panneau des Connexions : ouvre le Panneau des Connexions.
2/ Panneau de Configuration : ouvre le Panneau de Configuration.
3/ Console : ouvre la fenêtre des traces VPN.
4/ Quitter : ferme les tunnels VPN ouverts et quitte le logiciel.

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).

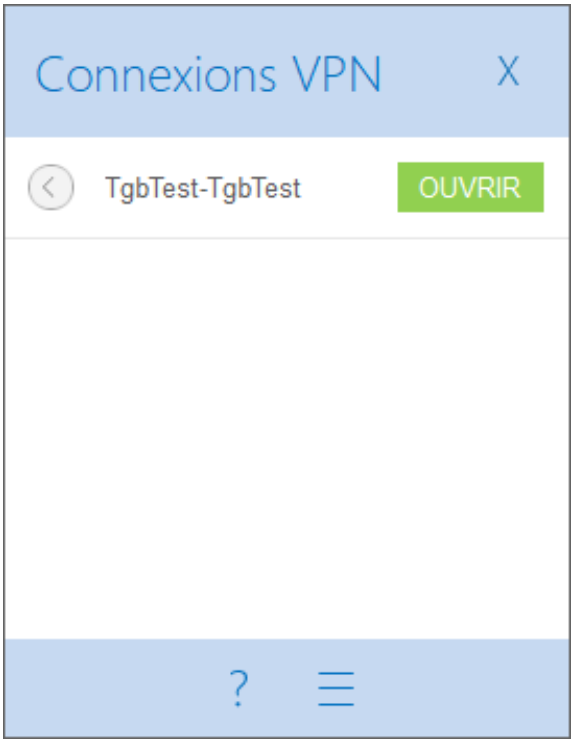
6.3 Ouvrir un tunnel VPN de test avec le Panneau des Connexions

Le Client VPN Windows Enterprise est fourni en standard avec une configuration VPN contenant un tunnel VPN de test nommé « TgbTest-TgbTest ».

Pour ouvrir le Panneau des Connexions, 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 des Connexions ». Le Panneau des Connexions est décrit en détail dans le chapitre 8 Panneau des Connexions.

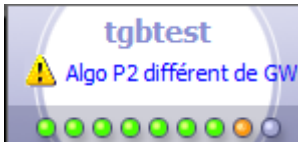


Dans le Panneau des Connexions, cliquez sur le bouton « OUVRIR » du tunnel VPN de test « TgbTest-TgbTest ».



Lorsque le logiciel n'est pas démarré en tant qu'administrateur et que l'option « Restreindre l'accès du panneau de configuration aux administrateurs » n'est pas désactivée, le bouton à trois barres, situé à droite du point d'interrogation, donnant accès au Panneau de Configuration n'est pas affiché.

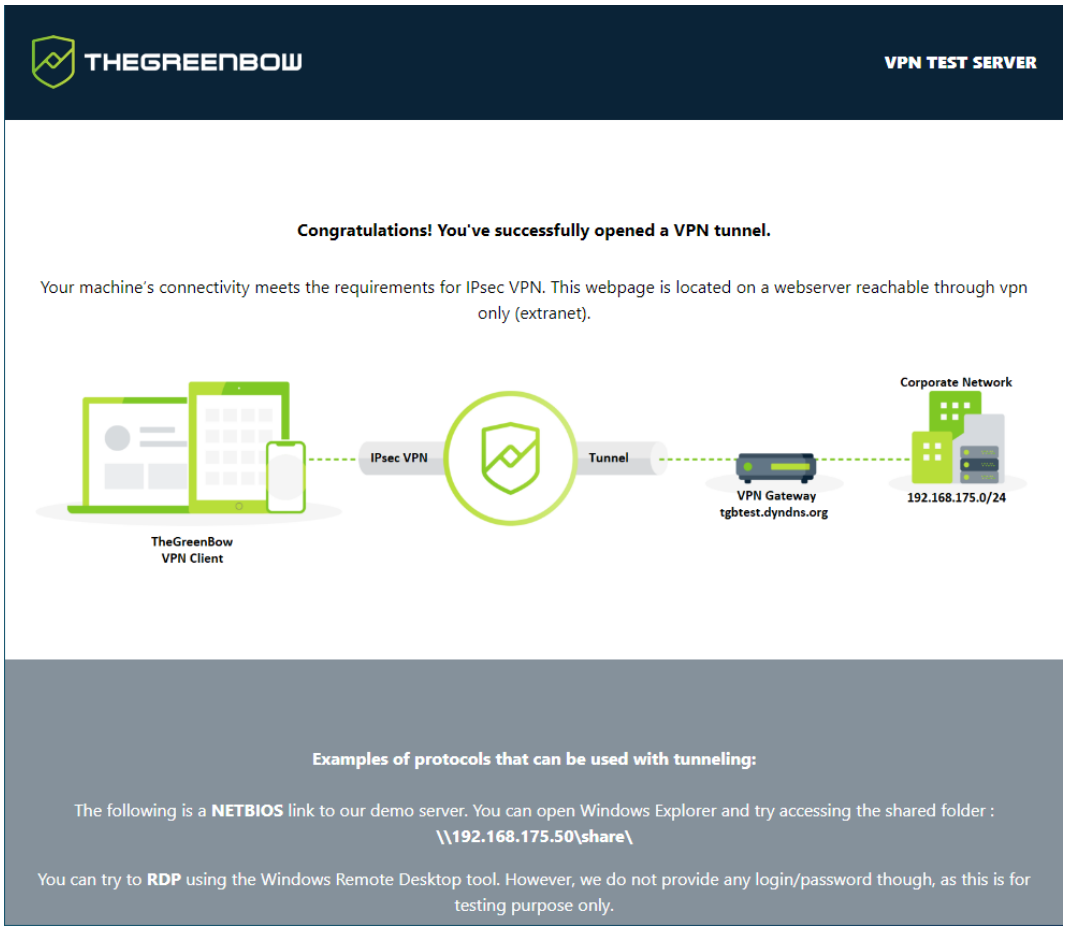
Au moment de l'ouverture ou de la fermeture d'un tunnel VPN, une fenêtre popup glissante apparaît au-dessus de l'icône du Client VPN en barre des tâches. Cette fenêtre identifie l'état du tunnel au cours de son ouverture ou de sa fermeture, et disparaît automatiquement, à moins que la souris ne soit dessus :

Tunnel en cours d'ouverture	
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.	

L'affichage de la fenêtre glissante peut être désactivé, dans le menu « Outils > Options », onglet « Affichage », option « Ne pas afficher la popup de barre des tâches ».

Le tunnel s'ouvre et la fenêtre de confirmation suivante s'affiche brièvement :

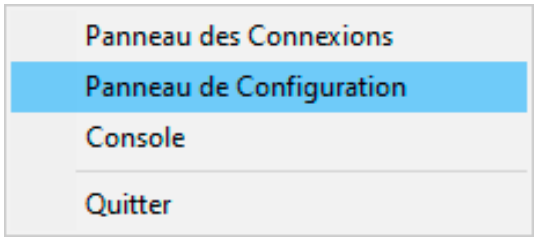
Ensuite, le site web de test TheGreenBow s'affiche automatiquement dans une fenêtre de navigateur :



Vous pouvez également ouvrir le tunnel de test à partir du Panneau de Configuration (cf. chapitre 9 Panneau de Configuration).

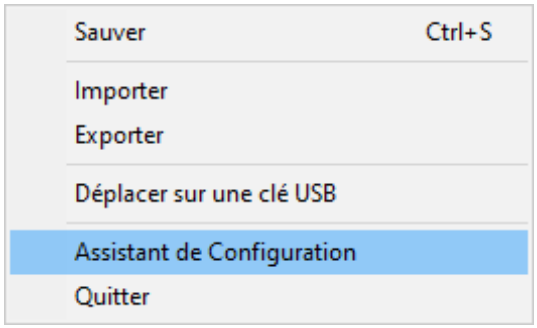
6.4 Configurer un tunnel VPN

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 9 Panneau de Configuration.



Lorsque l'option « Restreindre l'accès du panneau de configuration aux administrateurs » est désactivée (cf. section 24.1 Affichage de l'interface (masquage)), 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 7 Assistant de configuration ci-dessous.

Vous trouverez sur le site web TheGreenBow un grand nombre de guides de configuration pour la plupart des pare-feux / routeurs / passerelles VPN : https://thegreenbow.com/fr/support/guides-dintegration/passerelles-vpn-compatibles/.

6.5 Automatiser l'ouverture du tunnel VPN

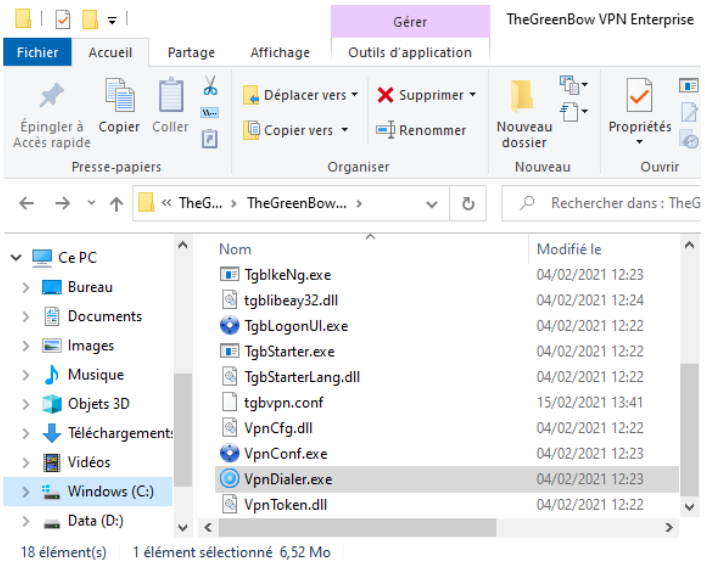
Le Client VPN Windows Enterprise permet d'automatiser l'ouverture d'un tunnel VPN. Il peut s'ouvrir automatiquement des manières suivantes :

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 15 Automatisation) ;
3/ sur insertion d'une clé USB contenant la configuration VPN adéquate (cf. chapitre 22 Mode USB) ;
4/ sur insertion de la carte à puce ou du token contenant le certificat utilisé pour ce tunnel (cf. section 18.8 Utiliser un certificat sur carte à puce ou sur token) ;
5/ 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 21 Gestion du Panneau TrustedConnect).

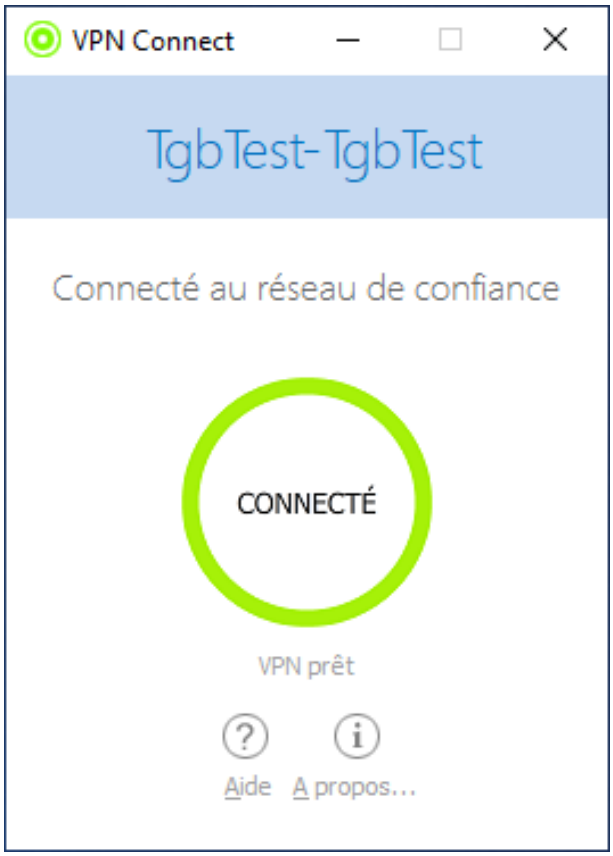
6.6 Ouvrir un tunnel avec le Panneau TrustedConnect

Le Panneau TrustedConnect est décrit au chapitre 10 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.

Lancer le Panneau TrustedConnect à l'aide de l'exécutable `VpnDialer.exe` qui se trouve par défaut dans `C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise`.



Le tunnel « TgbTest-TgbTest », devrait s'ouvrir automatiquement.



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).

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.

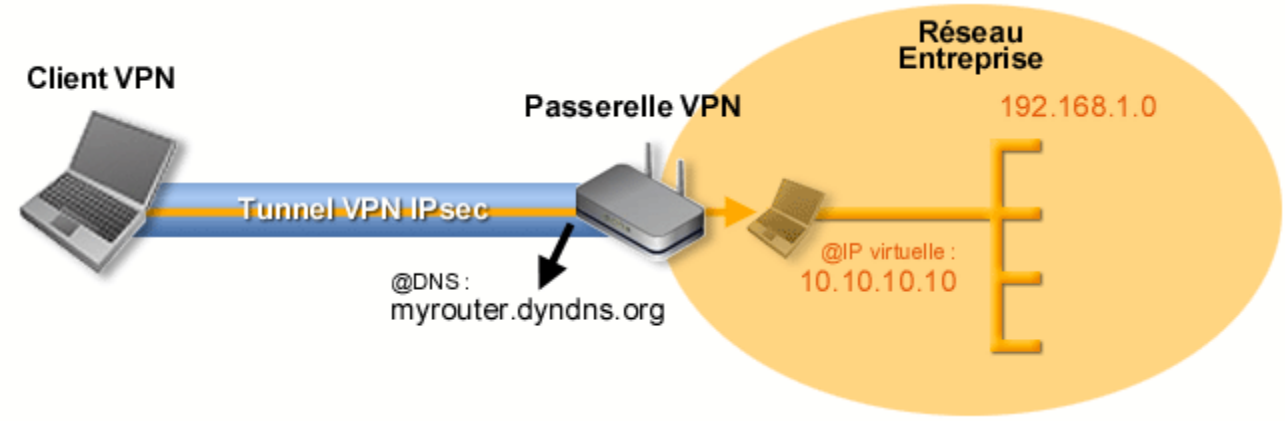
En revanche, lorsque `VpnDialer.exe` (TrustedConnect) est en cours d'exécution, il n'est pas possible de lancer `VpnConf.exe`. Vous devez d'abord quitter `VpnDialer.exe` avant de pouvoir lancer `VpnConf.exe`.

7 Assistant de configuration

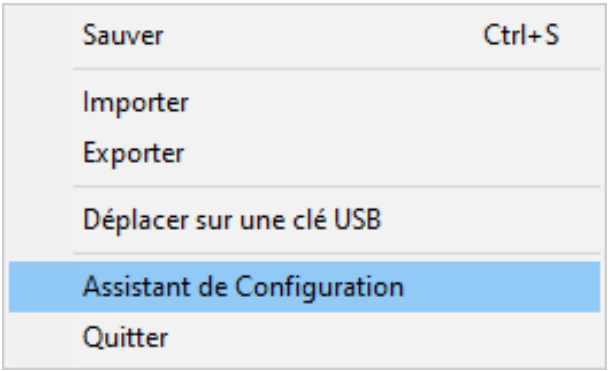
L'assistant de configuration permet de configurer un tunnel VPN en trois étapes simples.

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.



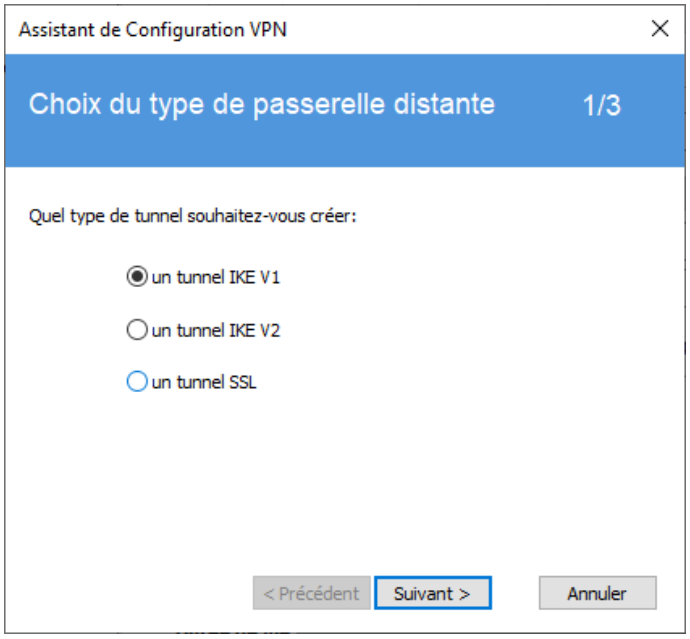
Dans l'interface principale, ouvrez l'assistant de configuration VPN : « Configuration > Assistant de Configuration ».



Recommandation de sécurité : Il est recommandé de configurer des tunnels IKEv2 avec certificat.
Se reporter au chapitre 26 Recommandations de sécurité.

7.1 Étape 1

Choisissez le protocole VPN à utiliser pour le tunnel : IKEv1, IKEv2 ou SSL.

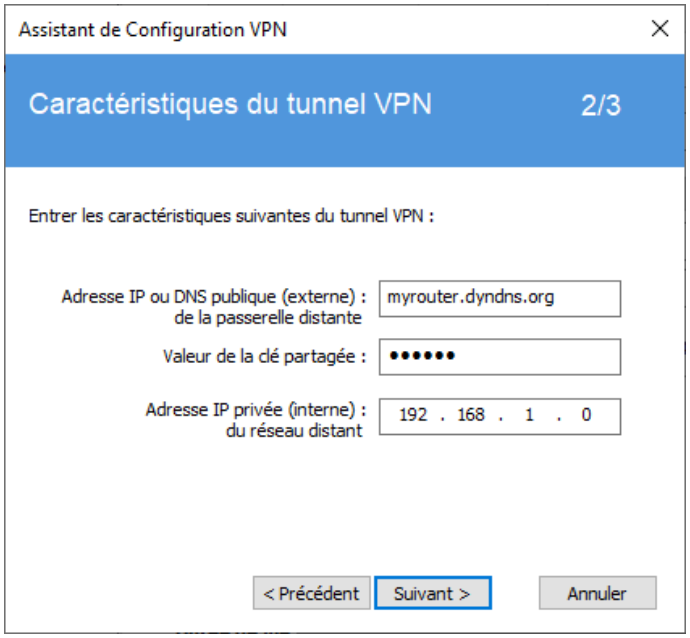


7.2 Étape 2

7.2.1 Pour un tunnel VPN IKEv1

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.
- L'adresse IP du réseau de l'entreprise (exemple : 192.168.1.0). (1)

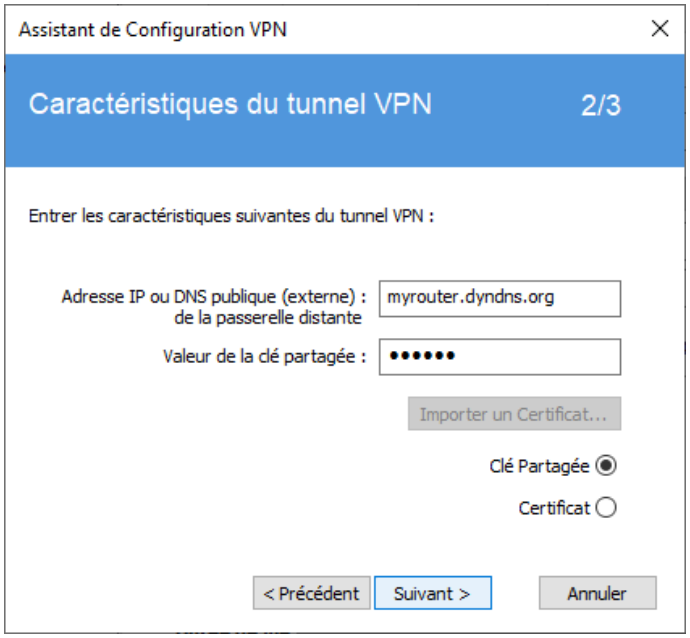


(1) Par défaut, l'adresse du réseau distant est exploitée avec une longueur de préfixe de 24. Cette valeur peut être modifiée ultérieurement.

7.2.2 Pour un tunnel VPN IKEv2

Entrez les valeurs suivantes :

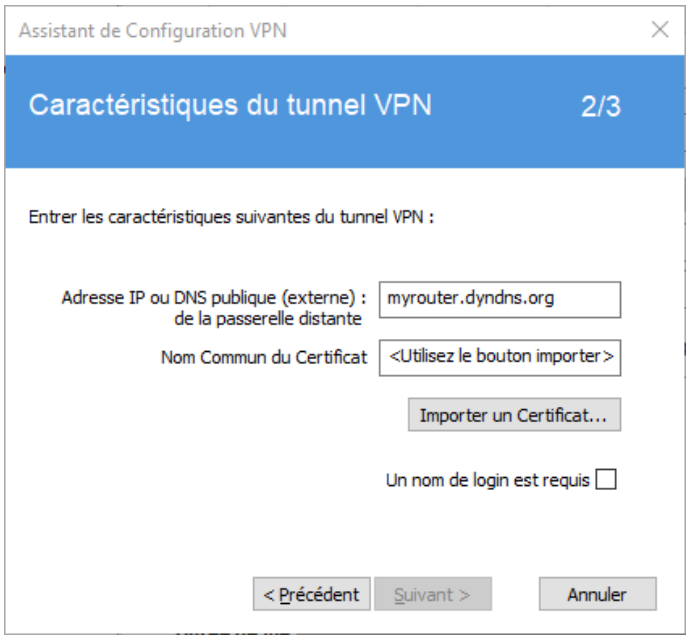
- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (exemple : myrouter.dyndns.org).
- Une clé partagée (« preshared key ») qui doit être configurée de façon identique sur la passerelle.
- OU : Un certificat qui doit être importé grâce au bouton « Importer un Certificat… » (voir section 18.3 Importer un certificat).



7.2.3 Pour un tunnel SSL (OpenVPN)

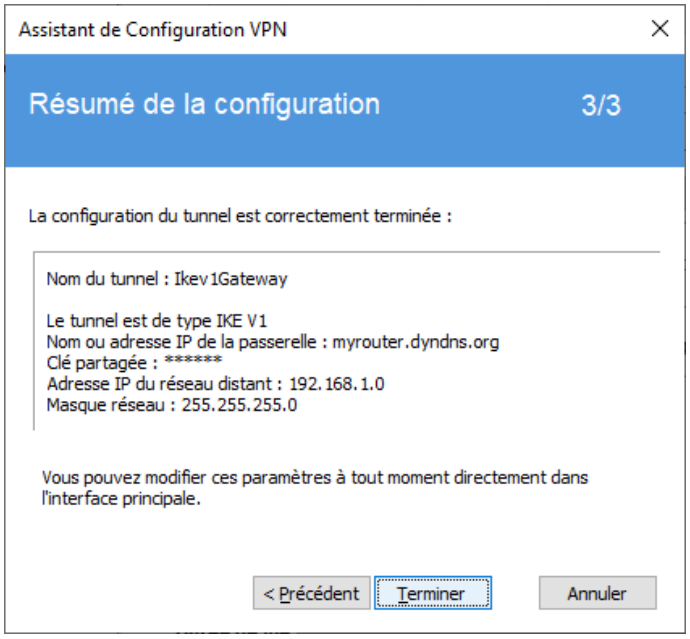
Entrez les valeurs suivantes :

- 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 18.3 Importer un certificat).



7.3 Étape 3

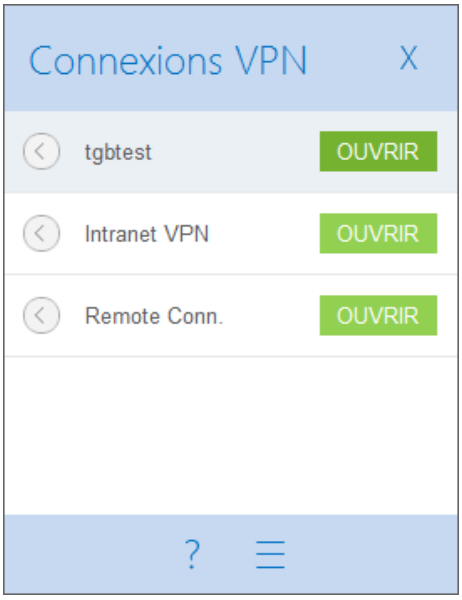
Vérifiez dans la fenêtre de résumé que la configuration est correcte, puis cliquez sur « Terminer ».



Le tunnel qui vient d'être configuré apparaît dans l'arborescence des tunnels de l'interface principale.
Double-cliquez sur le tunnel pour l'ouvrir, ou affiner la configuration via les onglets de l'interface principale.

8 Panneau des Connexions

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



Le Panneau de 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 20 Gestion du Panneau des Connexions.

Pour ouvrir une connexion VPN, cliquez sur le bouton « OUVRIR » associé.
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 24.1 Affichage de l'interface (masquage)).

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 de connexion permettent respectivement de :

Ouvrir la fenêtre « À propos… ».

Ouvrir le Panneau de Configuration.
Attention : l'accès au Panneau de Configuration peut être restreint (cf. section 24.1 Affichage de l'interface (masquage)).

Fermer le Panneau des Connexions

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

- ESC (ou ALT+F4) ferme la fenêtre
- CTRL+ENTER ouvre le Panneau de Configuration (interface principale)
- CTRL+O ouvre la connexion VPN sélectionnée
- CTRL+W ferme la connexion VPN sélectionnée
- Les flèches haut / bas permettent de se déplacer parmi les connexions VPN

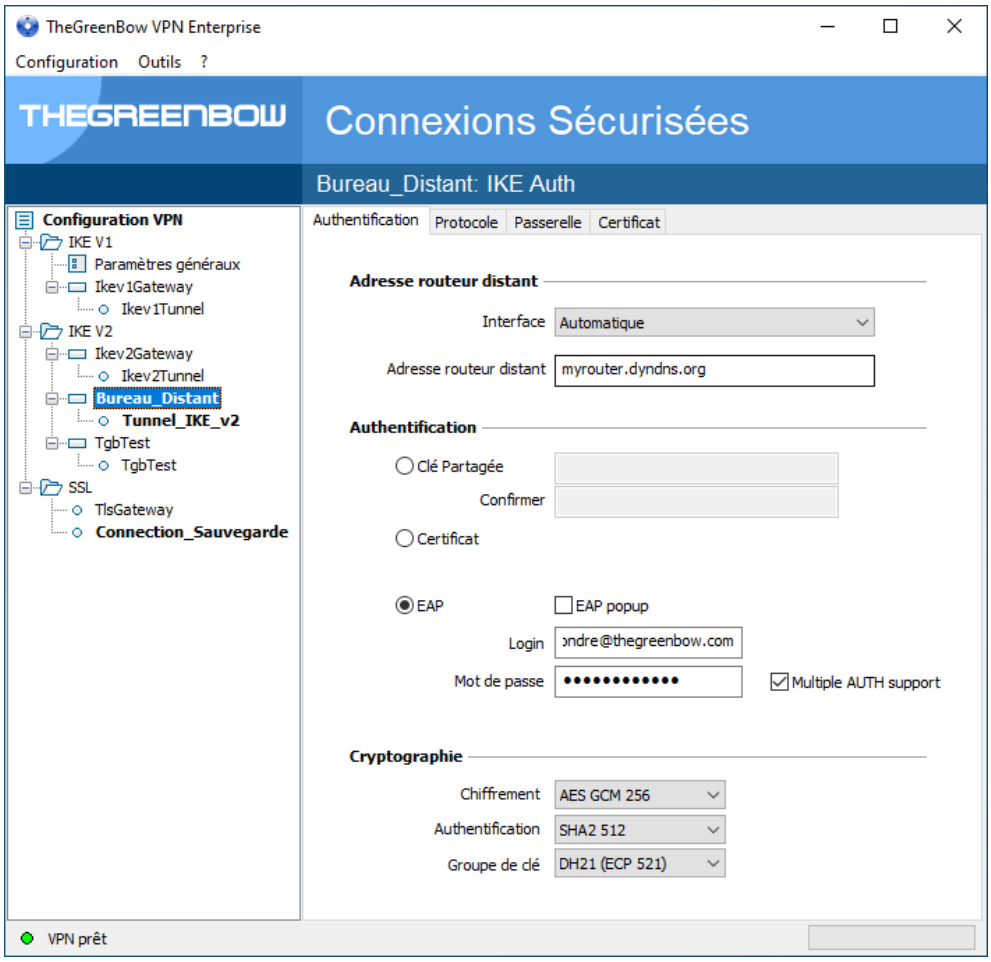
9 Panneau de Configuration

Le Panneau de Configuration est l'interface administrateur du Client VPN Windows Enterprise.

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 6.2 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 des tunnels VPN ;
- des onglets de configuration des tunnels VPN ;
- une barre d'état.



9.1 Menus

Les menus du Panneau de Configuration sont les suivants :

- Configuration
  - Sauver
  - Importer : Importation d'une configuration VPN
  - Exporter : Exportation d'une configuration VPN
  - Déplacer sur une clé USB : Mode USB
  - 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…

9.2 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.

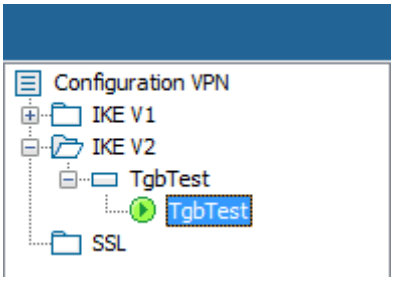
9.3 Raccourcis

CTRL+S	Sauvegarde de la configuration VPN
CTRL+ENTER	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)

9.4 Arborescence des tunnels VPN

9.4.1 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 », 3 niveaux permettent de créer respectivement :

- des tunnels IPsec IKEv1, caractérisés par une Phase 1 et une Phase 2, chaque Phase 1 pouvant contenir plusieurs phases 2 ;
- des tunnels IPsec IKEv2, caractérisés par une IKE Auth et une Child SA, chaque IKE Auth pouvant contenir plusieurs Child SA ;
- des tunnels SSL / TLS.

Un clic sur une Phase 1, Phase 2, 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 VPN IPsec IKEv1
   IKEv1 (Phase 1) : Authentification
   IKEv1 (Phase 2) : IPsec

2. Tunnel VPN IPsec IKEv2
   IKEv2 (IKE Auth) : Authentification
   IKEv2 (Child SA) : IPsec

3. Tunnel VPN SSL
   SSL : TLS

Une icône est associée à chaque tunnel (Phase 2, 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

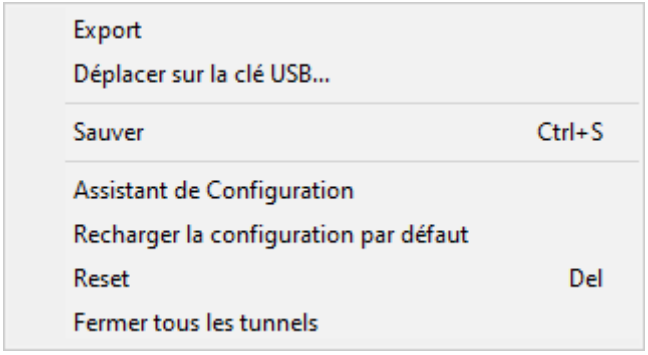
En cliquant successivement deux fois – sans faire de double-clic - sur un élément de l'arborescence, il est possible d'éditer et de modifier le nom de cet élément.
Toute modification non sauvegardée de la configuration VPN est identifiée par le passage en caractères gras de l'élément modifié. L'arborescence repasse en caractères normaux dès qu'elle est sauvegardée.

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

9.4.2 Menus contextuels

1. Configuration VPN

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



Export	Permet d'exporter la configuration VPN complète.
Déplacer sur la clé USB…	Déplacer la configuration VPN sur une clé USB et initier le Mode USB
Sauver	Permet de sauvegarder la configuration VPN.
Assistant de Configuration	Ouvre l'Assistant de Configuration VPN
Recharger la configuration par défaut	Le Client VPN Windows Enterprise est installé avec une configuration VPN par défaut qui permet de tester l'ouverture d'un tunnel VPN. Ce menu permet de la recharger à tout moment.
Reset	Remise à zéro, moyennant confirmation de l'utilisateur, de la configuration VPN.
Fermer tous les tunnels	Fermeture de tous les tunnels ouverts.

2. IKEv1, IKEv2, SSL

Un clic droit sur les éléments IKEv1, IKEv2 ou SSL affiche le menu contextuel suivant, qui permet d'exporter, de sauvegarder, de créer ou de coller une Phase 1 / IKE Auth / SSL :

Menu IKEv1

Menu IKEv2

Menu SSL

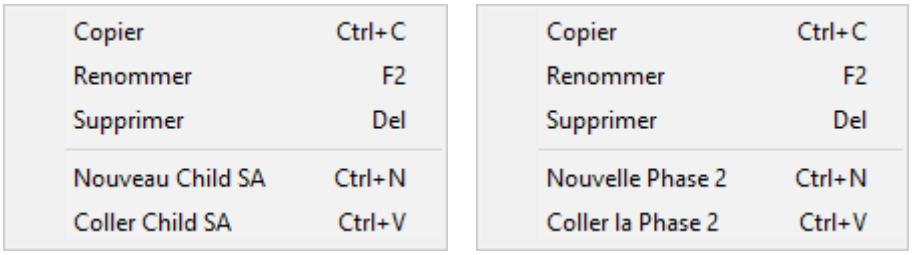
Export	Permet d'exporter tous les tunnels IKEv1 (resp. tous les tunnels IKEv2)
Sauver	Permet de sauvegarder tous les tunnels IKEv1 (resp. tous les tunnels IKEv2)

Nouvelle Phase 1 Nouvelle IKE Auth Nouveau TLS	Permet de créer une nouvelle Phase 1 / IKE Auth / TLS. Les paramètres de cette nouvelle Phase 1/ IKE Auth / TLS sont renseignés avec des valeurs par défaut.
Coller la Phase 1 Coller IKE Auth Coller TLS	Ajoute une Phase 1 / IKE Auth / TLS copiée précédemment dans le presse-papiers.

(1) Ce choix apparaît lorsqu'une Phase 1 / IKE Auth / TLS a été copiée dans le presse-papiers via le menu contextuel associé à cette Phase 1/ IKE Auth / TLS (cf. ci-après).

3. Phase 1 ou IKE Auth

Un clic droit sur une Phase 1 ou IKE Auth affiche le menu contextuel suivant :



Copier	Copie la Phase 1 ou la IKE Auth sélectionnée dans le presse-papier.
Renommer (1)	Permet de renommer la Phase 1 / IKE Auth.
Supprimer (1)	Supprime, moyennant confirmation de l'utilisateur, la Phase 1 ou IKE Auth, incluant toutes les Phases2 (respectivement toutes les Child SA) associées.
Nouvelle Phase 2 Nouvelle Child SA	Ajoute une nouvelle Phase 2 / Child SA à la Phase 1 / IKE Auth sélectionnée.
Coller la Phase 2 (2) Coller Child SA	Ajoute à la Phase 1 / IKE Auth la Phase 2 / Child SA copiée dans le presse-papiers.

(1) Ce menu est désactivé tant qu'un des tunnels de la Phase 1 / IKE Auth concernée est ouvert.
(2) Ce choix apparaît lorsqu'une Phase 2 / Child SA a été copiée dans le presse-papiers via le menu contextuel associé à la Phase 2 / Child SA concernée (cf. ci-après).

4. Phase 2, Child SA ou TLS

Un clic droit sur une Phase 2, une Child SA ou une TLS affiche le menu contextuel suivant :

Menu tunnel fermé

Menu tunnel ouvert

Ouvre Tunnel	Affiché si le tunnel VPN est fermé, permet d'ouvrir le tunnel (Phase 2, Child SA ou TLS) sélectionné
Fermer le tunnel	Affiché si le tunnel VPN est ouvert, permet de fermer le tunnel (Phase 2, Child SA ou TLS) sélectionné
Export (1)	Permet d'exporter la Phase 2 / Child SA / TLS sélectionnée
Copier	Permet de copier la Phase 2 / Child SA / TLS sélectionnée
Renommer (2)	Permet de renommer la Phase 2 / Child SA /TLS sélectionnée
Supprimer (2)	Permet de supprimer, moyennant confirmation de l'utilisateur, la Phase 2 / Child SA / TLS sélectionnée

(1) Cette fonction permet d'exporter le tunnel complet, c'est-à-dire, la Phase 2 et sa Phase 1 associée (ou la Child SA et son IKE Auth associé, ou la TLS), et de créer ainsi une configuration VPN mono-tunnel complètement opérationnelle (qui peut par exemple être importée en étant immédiatement fonctionnelle).
(2) Ce menu est désactivé tant que le tunnel est ouvert

9.4.3 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 une Phase 2 / Child SA / TLS est sélectionnée, ouvre le tunnel VPN correspondant.
CTRL+W	Si une Phase 2 / Child SA / TLS est sélectionnée, 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 une nouvelle Phase 1 / IKE Auth, si la configuration VPN est sélectionnée, ou crée une nouvelle Phase 2 / Child SA / TLS pour la Phase 1 / IKE Auth sélectionnée.
CTRL+S	Sauvegarde la configuration VPN.

10 Panneau TrustedConnect

10.1 Introduction

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

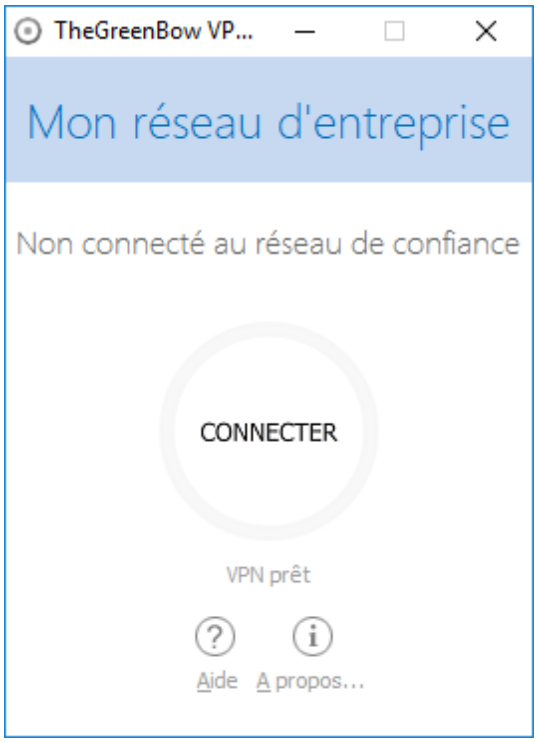
- **TND (Trusted Network Detection)** : permet de déterminer si le poste est à l'intérieur du réseau de confiance en se basant sur des suffixes DNS et l'identification de balises.
- **Always-On** : assure le maintien de la sécurité de la connexion à chaque changement d'interface réseau, par exemple,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

10.2 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.



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.

Le logiciel peut être quitté en cliquant avec le bouton droit sur l'icône TrustedConnect dans la zone de notification et sélectionner « Quitter ».

10.3 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 du Client VPN Windows Enterprise.

Signification des codes couleurs des différentes icônes de 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.

10.4 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 :

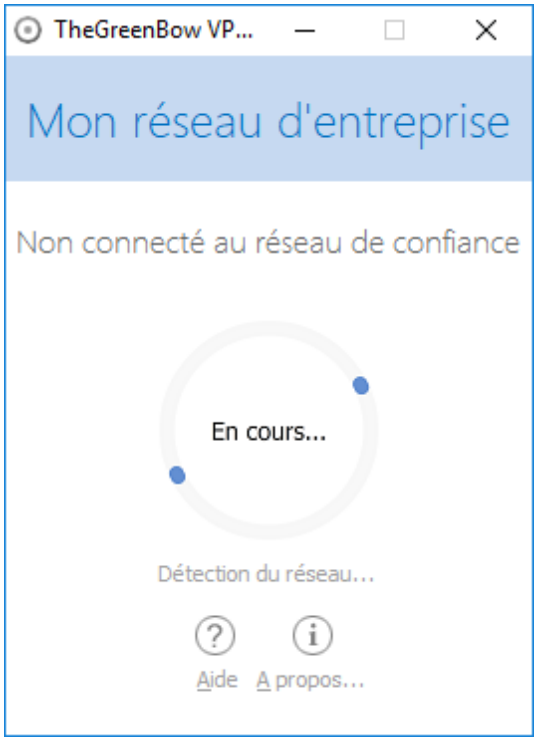
1/ À propos… : ouvre la fenêtre À propos… du logiciel.
1/ Langue : permet de basculer entre le français et l'anglais.
2/ Journaux : permet de démarrer la journalisation. Une fois la journalisation démarrée, deux options supplémentaires s'affichent pour afficher les journaux et arrêter la journalisation.
3/ Redémarrer : permet de redémarrer le tunnel.
4/ Quitter : ferme le tunnel VPN et quitte le logiciel.

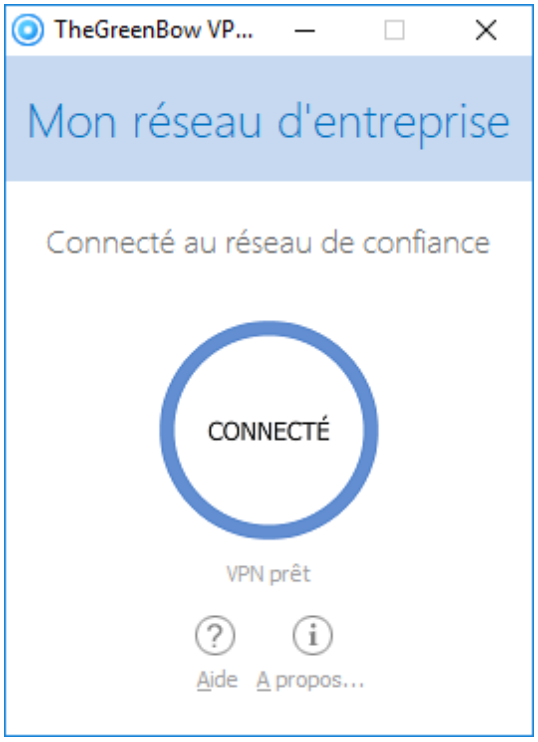
10.5 Utilisation

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

10.5.1 Poste connecté au réseau de l'entreprise

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





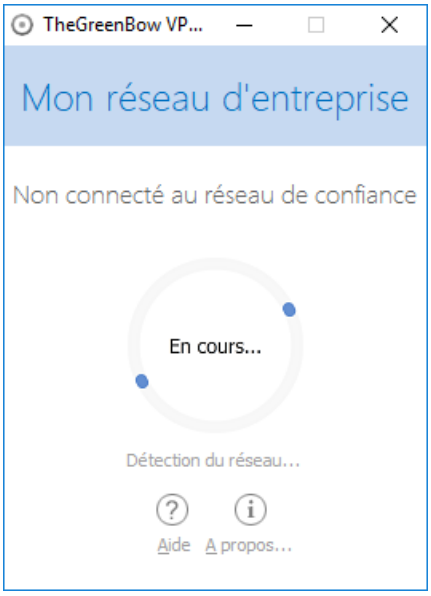
Ensuite, la fenêtre du Panneau TrustedConnect se minimise automatiquement, en barre des tâches ou dans la zone de notification en fonction du comportement configuré par l'administrateur.
☞ Voir le « Guide de déploiement ».

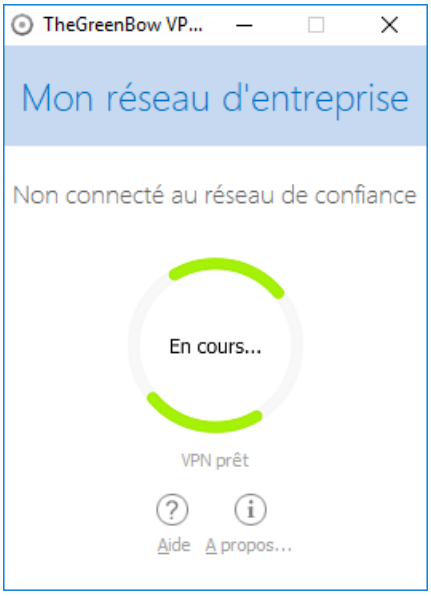
La fenêtre réapparait en sélectionnant l'application depuis la barre des tâches, et dans cet état, il n'y aucune action possible sur l'état de la connexion pour l'utilisateur.

10.5.2 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.



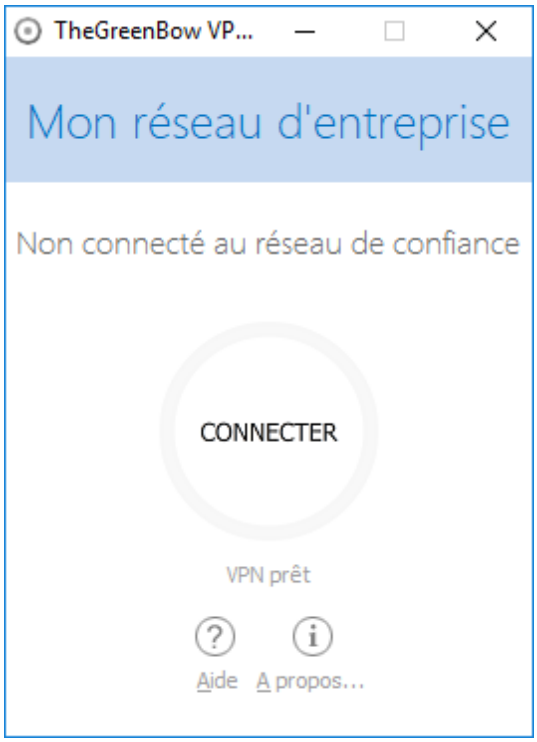


Lorsque la connexion est établie, la fenêtre du Panneau TrustedConnect se minimise automatiquement, en barre des tâches ou dans la zone de notification en fonction du comportement configuré par l'administrateur.

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.

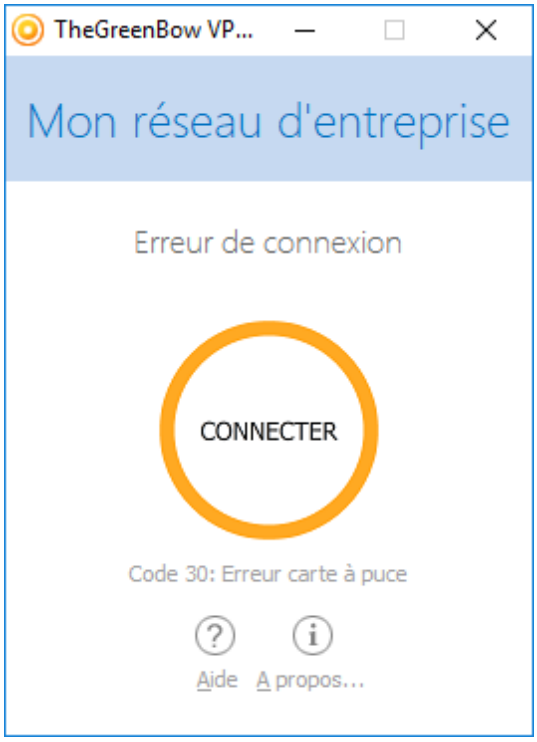
Quand le tunnel est monté et que le poste apparait comme étant sur le réseau de l'entreprise, il est possible de cliquer sur l'anneau indicateur de l'état de connexion pour arrêter le tunnel.

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 :



10.6 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.

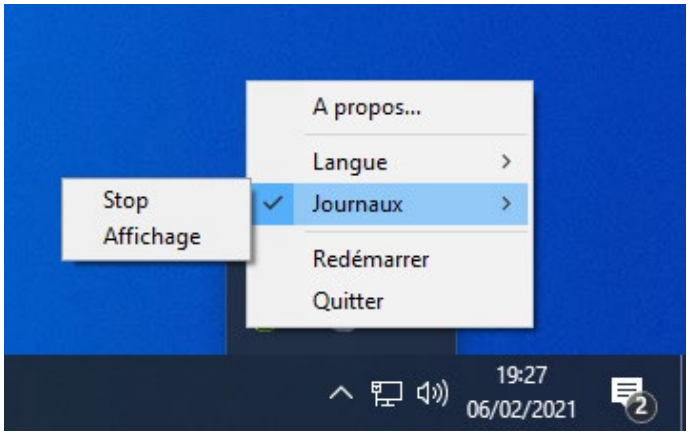


L'administrateur réseau peut être contacté pour résoudre le problème. En fonction du code d'erreur indiqué, il peut fournir des indications ou des explications sur le problème rencontré. Si l'administrateur demande des logs, se reporter à la procédure décrite dans la section suivante.

La liste des codes d'erreurs est fournie en annexe de ce document (cf. section 27.3 Diagnostics du Panneau TrustedConnect).

10.7 Génération de journaux

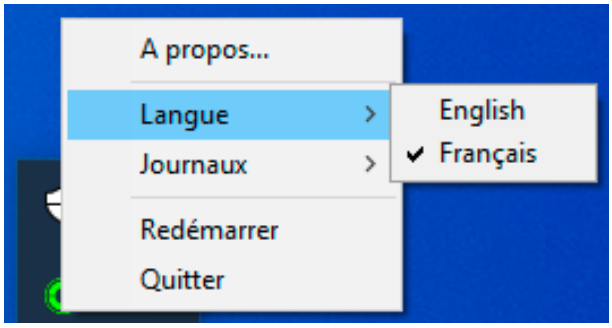
Le Panneau TrustedConnect permet de créer et de consulter des journaux.
Pour initier la création des journaux, depuis l'icône TrustedConnect de la zone de notification, sélectionner l'élément « Journaux », une coche à gauche de cet élément indique ensuite que les journaux sont actifs :



Pour les consulter, aller dans le menu système et sélectionner l'élément « 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.

10.8 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'élément « Langues ». Dans le sous-menu choisir « English » ou « Français » :



10.9 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).

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.

11 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 ;
- lien internet vers le site web TheGreenBow ;
- lorsque le logiciel est activé, le numéro de licence et l'email 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. (1)

(1) 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 le Client VPN Windows Enterprise n'est pas activé, le logiciel tente de se connecter au serveur d'activation pour valider la licence.

12 Importer et exporter la configuration VPN

12.1 Importer une configuration VPN

Le Client VPN Windows Enterprise permet d'importer une configuration VPN de différentes façons :

- par le menu « Configuration > Importer » du Panneau de Configuration (interface principale) ;
- par ligne de commande en utilisant l'option `/import`. (1)

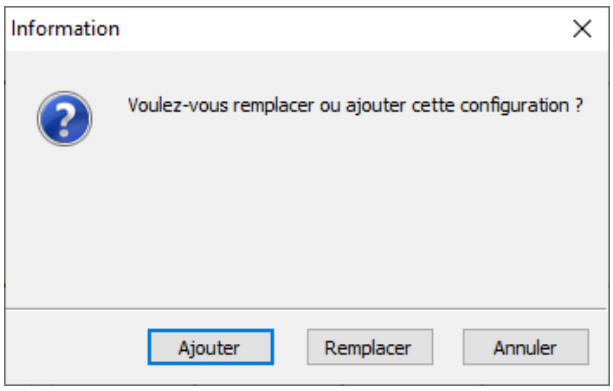
(1) L'utilisation des options de ligne de commande du logiciel est détaillée dans le document « Guide de déploiement ». Y sont en particulier détaillées toutes les options disponibles pour l'importation d'une configuration VPN : `/import`, `/add`, `/replace` ou `/importonce`.

Depuis la version 6.8 du Client VPN Windows Enterprise, le « glisser-déposer » d'un fichier de configuration VPN (fichier `.tgb`) sur le Panneau de Configuration n'est plus pris en charge, car une élévation des privilèges est maintenant nécessaire pour gérer les configurations VPN.

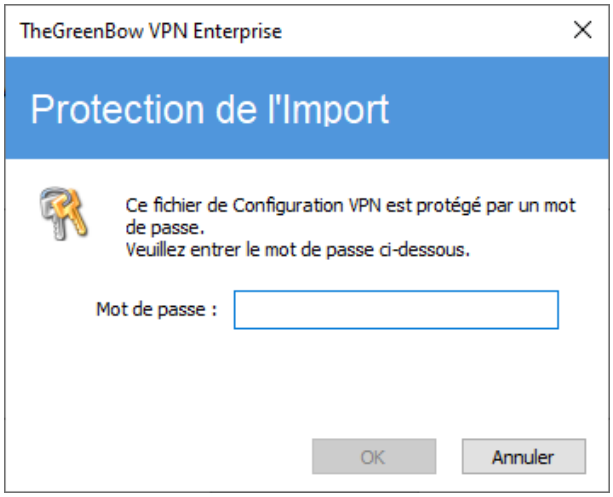
Depuis la version 6.8 du Client VPN Windows Enterprise, la fonction d'import d'une configuration VPN par double-clic sur le fichier de configuration VPN n'est pas disponible.

Le Client VPN Windows Enterprise 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.

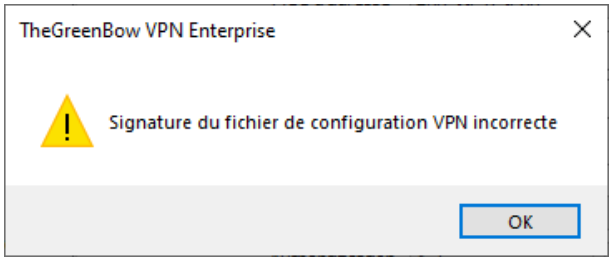
Lors de l'importation d'une configuration VPN, il est demandé à l'utilisateur s'il veut ajouter la nouvelle configuration VPN à la configuration courante, ou s'il veut remplacer (écraser) la configuration courante par la nouvelle configuration VPN :



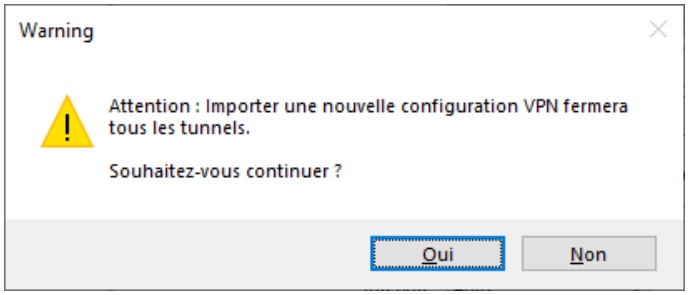
Si la configuration VPN importée a été exportée avec une protection par mot de passe (cf. section 12.2 Exporter une configuration VPN ci-dessous), le mot de passe est demandé à l'utilisateur.



Si la configuration VPN a été exportée avec contrôle d'intégrité (cf. section 12.2 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.

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).

Importation des Paramètres généraux (IKEv1 seul)

Si à l'importation, l'utilisateur choisit « Remplacer », ou si la configuration courante est vide, les paramètres généraux de la configuration VPN importée remplacent les paramètres généraux de la configuration courante.
Si à l'importation, l'utilisateur choisit « Ajouter », les paramètres généraux de la configuration VPN courante sont conservés.

Choix utilisateur à l'importation	Configuration VPN courante vide	Configuration VPN courante non vide
Ajouter	Paramètres généraux remplacés par les nouveaux	Paramètres généraux conservés
Remplacer	Paramètres généraux remplacés par les nouveaux	Paramètres généraux remplacés par les nouveaux

12.2 Exporter une configuration VPN

Le Client VPN Windows Enterprise permet d'exporter une configuration VPN de différentes façons :

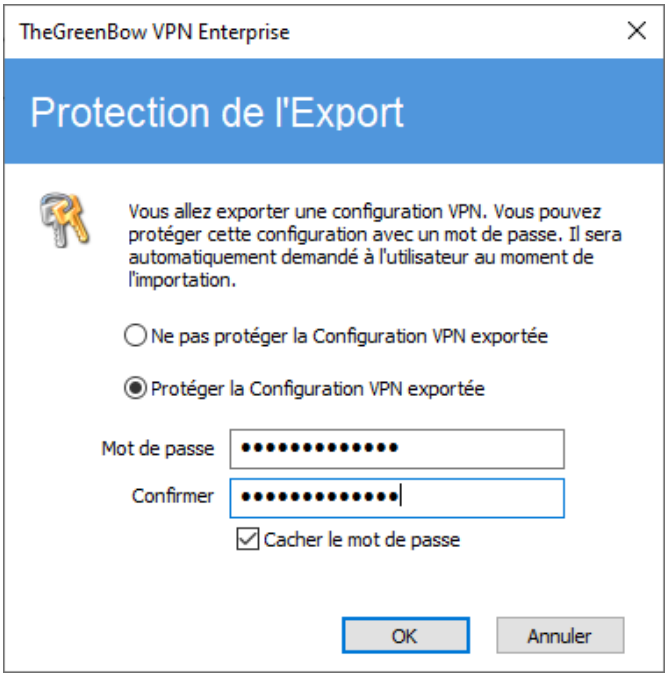
1/ Menu « Configuration > Exporter » : La configuration VPN complète est exportée.
2/ Menu contextuel associé à la racine de l'arborescence VPN > Export : La configuration VPN complète est exportée.
3/ Menu contextuel associé à une Phase 1 (IKEv1) ou à IKE Auth (IKEv2) > Export : Toute la Phase 1 / IKE Auth (incluant les Phases 2 / Child SA qu'elle contient) est exportée.
4/ Menu contextuel associé à une Phase 2 (IKEv1) ou Child SA (IKEv2) > Export : La Phase 2 / Child SA est exportée, avec la Phase 1 / IKE Auth à laquelle elle est associée.
5/ Menu Contextuel associé à une TLS > Export : La TLS est exportée.
6/ Par ligne de commande en utilisant l'option `/export`. (1)

(1) 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`.

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

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.

Qu'elle soit exportée chiffrée ou « en clair », la configuration VPN exportée peut être protégée en intégrité.
La protection en intégrité de la configuration VPN exportée est une fonction activable 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).

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 12.1 Importer une configuration VPN ci-dessus).

12.3 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 12.1 Importer une configuration VPN ci-dessus).

12.4 Scinder une configuration VPN

En utilisant les différentes options d'exportation (exportation d'une Phase 1 / IKE Auth / TLS avec toutes les Phases 2 / Child SA / TLS associées, ou exportation d'un tunnel simple), il est possible de scinder une configuration VPN en autant de « sous-configurations » que désiré (cf. section 12.2 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.

13 Configurer un tunnel VPN

13.1 VPN SSL, IPsec IKEv1 ou IPsec IKEv2

Le Client VPN Windows Enterprise permet de créer et de configurer plusieurs types de tunnels VPN.
Il permet aussi, le cas échéant, de les ouvrir simultanément.

Le Client VPN Windows Enterprise permet de configurer des tunnels
- IPsec IKEv1
- IPsec IKEv2
- SSL

La méthode pour créer un nouveau tunnel VPN est décrite dans les sections précédentes : 7 Assistant de configuration et 9.4.2 Menus contextuels.

Recommandation de sécurité : Il est recommandé de configurer des tunnels IKEv2 avec certificat.
Se reporter au chapitre 26 Recommandations de sécurité.

13.2 Modification et sauvegarde de la configuration VPN

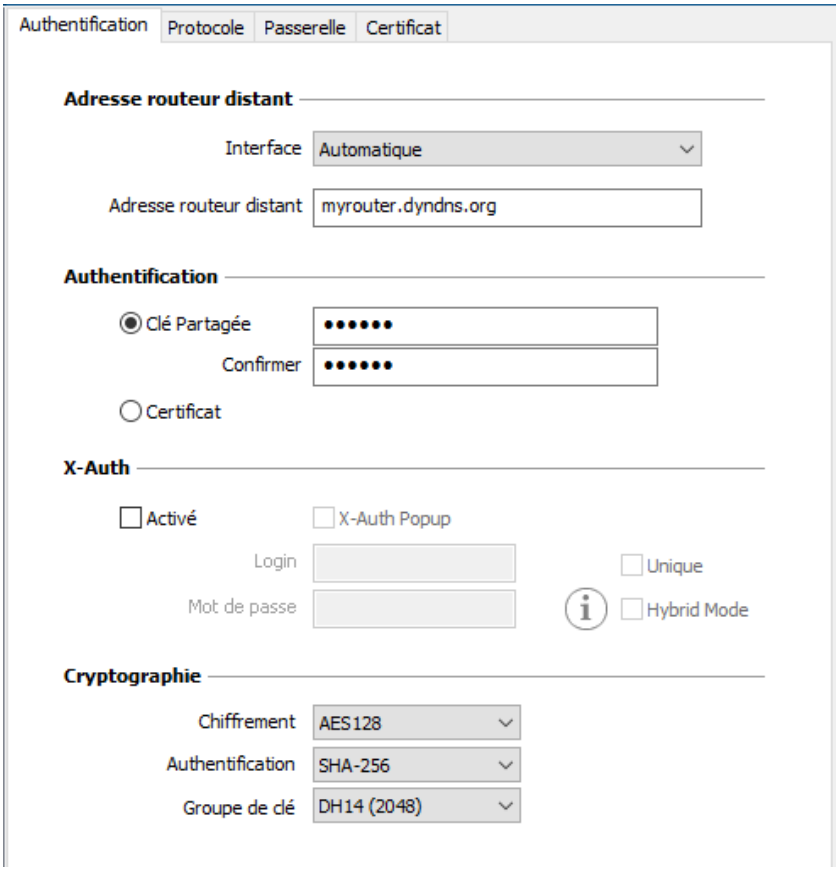
Le Client VPN Windows Enterprise permet d'effectuer des modifications dans les tunnels VPN, et de tester « à la volée » ces modifications, ceci sans avoir besoin de sauvegarder la configuration VPN.
Toute modification dans la configuration VPN est illustrée dans l'arborescence par le passage en caractères gras du nom de l'élément modifié.

À tout moment, la configuration VPN peut être sauvegardée :
- par CTRL+S,
- via le menu « Configuration > Sauver ».

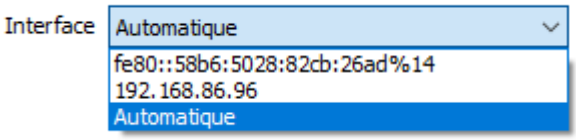
Si une configuration VPN est modifiée et que l'utilisateur quitte l'application sans l'avoir sauvegardée, il est alerté.

13.3 Configurer un tunnel IPsec IKEv1

13.3.1 Phase 1 : Authentification



Adresses

Interface	Adresse IP 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 (IPv4 ou IPv6) 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.

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.

Se reporter au chapitre 26 Recommandations de sécurité.

Certificat	Utilisation de Certificat pour l'authentification de la connexion VPN.

L'utilisation de Certificat apporte une plus grande sécurité dans la gestion des connexions VPN (authentification mutuelle, vérification des durées de vie, révocation, etc.).

Se reporter au chapitre 26 Recommandations de sécurité.

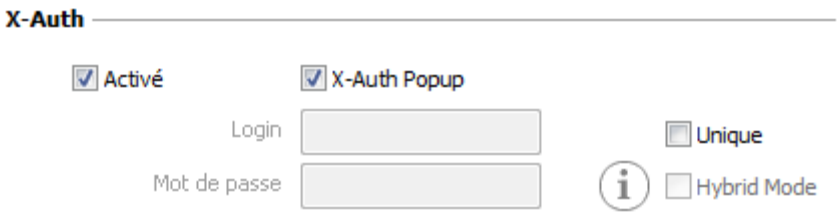
Se reporter au chapitre dédié : 18 Gestion des certificats.

Gestion X-Auth

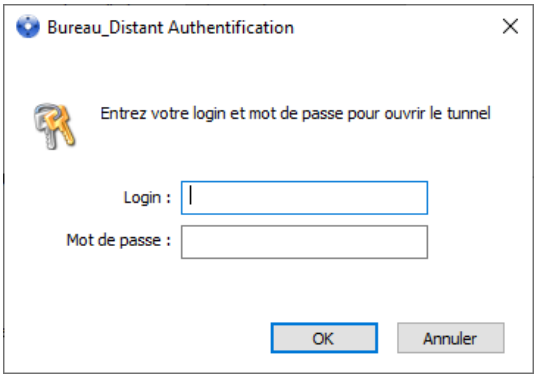
X-Auth est une extension du protocole IKE (Internet Key Exchange).

La fonction X-Auth est utilisée pour conditionner l'ouverture du tunnel VPN à la présentation, par l'utilisateur, d'un login et d'un mot de passe.

Cette fonction nécessite une configuration équivalente sur la passerelle VPN.

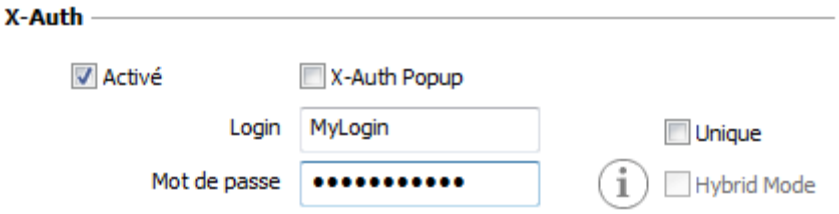


Lorsque la case « X-Auth Popup » est cochée, une fenêtre demande à chaque ouverture de tunnel VPN, le login et le mot de passe d'authentification de l'utilisateur (la fenêtre de demande de login et de mot de passe a pour titre le nom du tunnel, pour éviter les confusions).



Sur expiration du temps d'attente de cette fenêtre (configurable dans les paramètres généraux), un message d'alerte avertit l'utilisateur qu'il doit rouvrir le tunnel.

Le Client VPN permet de mémoriser les login et mot de passe X-Auth dans la configuration VPN. Ces login et mot de passe sont alors automatiquement présentés à la passerelle VPN au cours de l'ouverture du tunnel.



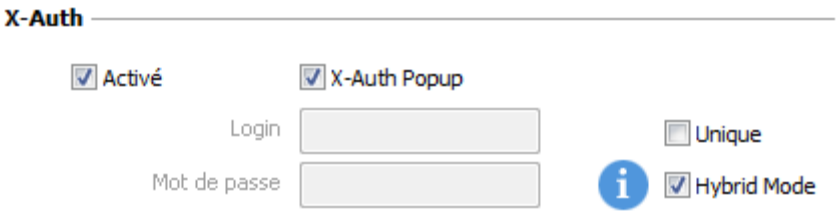
Cette possibilité facilite l'utilisation et le déploiement du logiciel. Elle reste néanmoins moins sécurisée que la présentation dynamique de la fenêtre de saisie du login / mot de passe X-Auth.

Il est recommandé de ne pas mémoriser les login et mot de passe X-Auth dans la configuration VPN. Se reporter au chapitre 26 Recommandations de sécurité.

Cocher l'option « Unique » pour ne pas avoir de nouvelle demande de saisie du mot de passe lors d'une renégociation de Phase 1.

Le Mode Hybride est un mode qui réunit deux types d'authentification : l'authentification de la passerelle VPN classique et l'authentification X-Auth pour le Client VPN.

Pour activer le Mode Hybride, il est nécessaire que le tunnel soit associé à un certificat (cf. chapitre 18 Gestion des certificats), et que la fonction X-Auth soit configurée.



Cryptographie

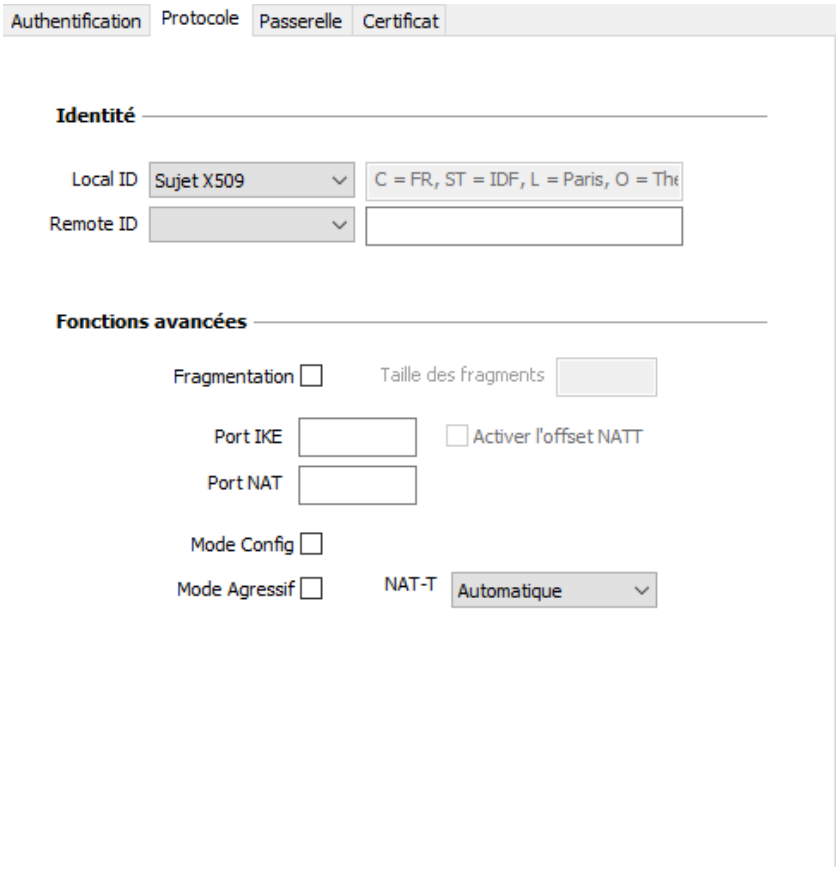
Chiffrement	Algorithme de chiffrement négocié au cours de la phase d'authentification (1) : Auto (2), AES-128, AES-192, AES-256.
Authentification	Algorithme d'authentification négocié au cours de la phase d'authentification (1) : Auto (2), SHA2-256, SHA2-384, SHA2-512.
Groupe de clé	Longueur de la clé Diffie-Hellman (1) : Auto (2), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)

(1) Se reporter au chapitre 26 Recommandations de sécurité pour le choix de l'algorithme.

(2) Auto signifie que le Client VPN s'adapte automatiquement aux paramètres de la passerelle. Quand « Auto » est sélectionné, les algorithmes suivants (et leurs diverses combinaisons) sont pris en charge :
- Chiffrement : AES-128, AES-192
- Authentification : SHA2-256, SHA2-384, SHA2-512
- Groupe de clé : DH14 (2048), DH15 (3072), DH16 (4096)

Si la passerelle est configurée avec un algorithme différent, alors le mode « Auto » ne peut être utilisé. L'algorithme doit être explicitement spécifié dans le Client VPN.

13.3.2 Phase 1 : Protocole



Identité

Local ID	Le « Local ID » est l'identifiant de la phase d'authentification (Phase 1) que le Client VPN envoie à la passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : - Adresse IP : 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 - Email : une adresse email (type = USER FQDN), p.ex. support@thegreenbow.com - DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) - Sujet X509 : ce champ est automatiquement renseigné avec le sujet d'un certificat X.509 lorsque le tunnel est associé à un certificat utilisateur (cf. chapitre 18 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 que le Client VPN s'attend à recevoir de la passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : - Adresse IP : une adresse IP (type = IPV4 ADDR), par exemple : 80.2.3.4 - DNS : un nom de domaine (type = FQDN), par exemple : routeur.mondomaine.com - KEY ID : une chaîne de caractères (type = KEY ID), par exemple : 123456 - Email : une adresse email (type = USER FQDN), par exemple : admin@mondomaine.com - DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) Ce paramètre est obligatoire depuis la version 6.8 pour des raisons de sécurité.

Fonctions avancées

Fragmentation / Taille des fragments	Cette option active la fragmentation IKE qui évite que des paquets soient fragmentés (et potentiellement bloqués) au niveau IP. Il est recommandé d'activer cette option (à la fois sur la passerelle et sur le Client VPN) dans le cas où le fournisseur d'accès à Internet a mis en place le NAT de classe transporteur ou carrier-grade NAT (CGN), ce qui empêche le fonctionnement de la fragmentation au niveau IP. 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 Phase 1 (Authentification) s'effectuent sur le protocole UDP, en utilisant par défaut le port 500. Le paramétrage du port IKE permet de passer les équipements réseau (Firewall, routeurs) qui filtrent ce port 500. La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Phase 1 sur un port différent de 500.

Port NAT	Les échanges IKE Phase 2 (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 (Firewall, routeurs) qui filtrent ce port 4500. La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Phase 2 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.
Mode Config	Le Mode Config, une fois activé, permet au Client VPN de récupérer depuis la passerelle VPN des éléments de configuration nécessaires à l'ouverture du tunnel VPN. Voir le paragraphe ci-dessous : Gestion du Mode Config.
Mode agressif	Le Client VPN utilise le mode agressif pour se connecter à la passerelle VPN.
NAT-T	Mode « NAT-Traversal ». Le Client VPN permet de gérer trois types de modes NAT-T :

Désactivé	Empêche le Client VPN et la passerelle VPN de passer en mode NAT-Traversal
Automatique	Laisse le Client VPN et la passerelle VPN négocier le mode NAT-Traversal
Forcé	Le Client VPN force le mode NAT-T par l'encapsulation systématique des paquets IPsec dans des trames UDP. Ceci permet de résoudre les problèmes de NAT-Traversal au travers de certains routeurs intermédiaires.

Gestion du Mode Config

Le Mode Config, une fois activé, permet au Client VPN de récupérer depuis la passerelle VPN des éléments de configuration nécessaires à l'ouverture du tunnel VPN :

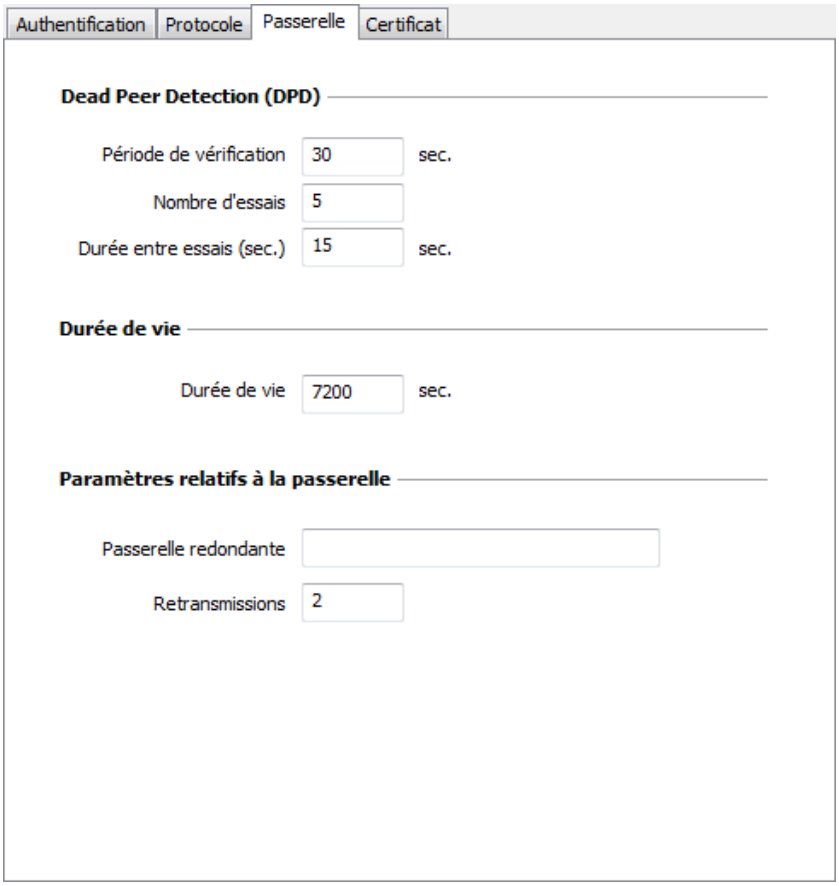
- adresse IP virtuelle du Client VPN,
- adresse d'un serveur DNS (optionnel),
- adresse d'un serveur WINS (optionnel).

Pour que le Mode Config soit opérationnel, il est nécessaire que la passerelle VPN le prenne en charge également.

Lorsque le Mode Config n'est pas activé, les trois informations « Adresse du Client VPN », « Serveur DNS » et « Serveur WINS » sont configurables manuellement dans le Client VPN (cf. sections 13.3.6 Phase 2 : IPsec et 13.3.7 Phase 2 : Avancé).

Réciproquement, lorsque le Mode Config est activé, les champs de Phase 2 : « Adresse du Client VPN », « Serveur DNS » et « Serveur WINS » sont renseignés automatiquement au cours de l'ouverture du tunnel VPN. Ils sont donc interdits à la saisie (grisés).

13.3.3 Phase 1 : Passerelle



Dead Peer Detection (DPD)

Dead Peer Detection	La fonction de DPD (Dead Peer Detection) permet au Client VPN de détecter que la passerelle VPN devient inaccessible ou inactive. (1) - Période de vérification : Période entre deux messages de vérification DPD envoyés, exprimée en secondes. - Nombre d'essais : Nombre d'essais infructueux consécutifs avant de déclarer que la passerelle VPN est inaccessible. - Durée entre essais : Intervalle entre les messages DPD quand aucune réponse n'est reçue de la passerelle VPN, exprimée en secondes.

(1) La fonction de DPD est active une fois le tunnel ouvert (phase 1 montée). 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.

Durée de vie

Durée de vie	Les durées de vie sont échangées lors de la montée du tunnel. (1) À échéance de la durée de vie, la Phase 1 est renégociée. La valeur par défaut de la durée de vie de la Phase 1 est de 2700 s (45 min).

(1) Les durées de vie sont échangées entre le Client VPN et la passerelle VPN. Toutefois, certaines passerelles se limitent à retourner la valeur de la durée de vie proposée par le Client VPN. Quelle que soit la méthode, le Client VPN applique toujours la durée de vie envoyée par la passerelle VPN.

Paramètres relatifs à la passerelle

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. ☞ Voir le chapitre 14 Passerelle redondante.
Retransmissions	Nombre de retransmissions de messages protocolaires IKE sur non-réponse de la passerelle. À l'issue de ces retransmissions, le tunnel est déclaré en échec.

13.3.4 Phase 1 : Certificat

☞ Voir le chapitre 18 Gestion des certificats.

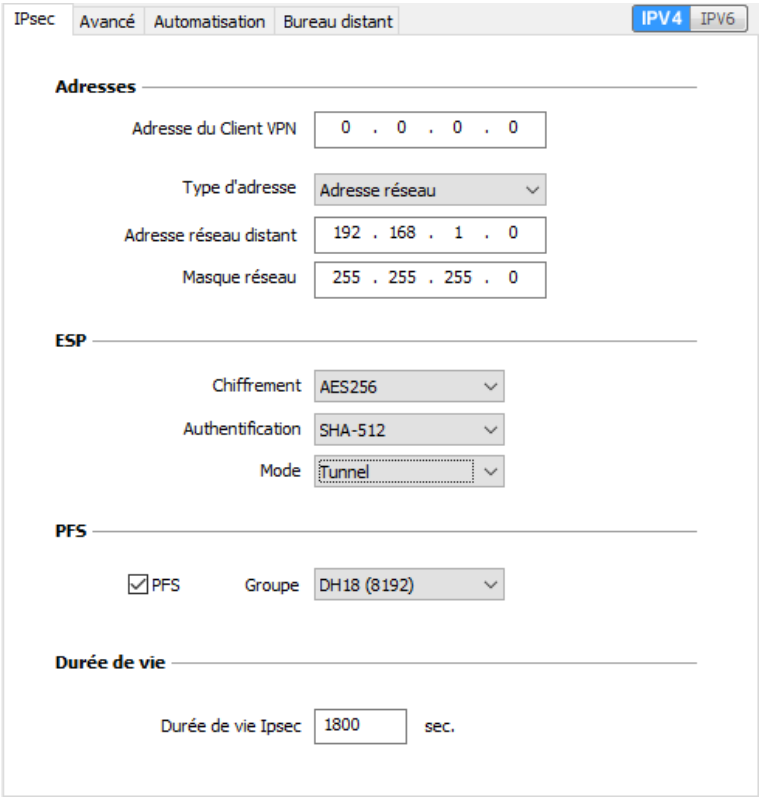
13.3.5 Phase 2

La Phase 2 d'un tunnel VPN est la phase IPsec. Cette Phase sert à la négociation des paramètres de sécurité qui seront appliqués aux données transmises dans le tunnel VPN.

Pour configurer les paramètres de Phase 2, sélectionnez cette Phase 2 dans l'arborescence du Panneau de Configuration. 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 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.

13.3.6 Phase 2 : IPsec



Adresses

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. Quand le champ est à « 0.0.0.0 », le logiciel prend automatiquement l'adresse IP physique du poste comme adresse IP virtuelle fournie à la passerelle.

Si le Mode Config est activé, ce champ est grisé (non disponible à la saisie). Il est en effet automatiquement renseigné au cours de l'ouverture du tunnel, avec la valeur envoyée par la passerelle VPN dans l'échange Mode Config.

Type d'adresse	L'extrémité du tunnel peut être un réseau ou un poste distant. ☞ Voir le paragraphe ci-dessous pour la **configuration du Type d'adresse**.

ESP

Chiffrement	Algorithme de chiffrement négocié au cours de la Phase IPsec (1) : Auto (2), AES-128, AES-192, AES-256.
Authentification	Algorithme d'authentification négocié au cours de la Phase IPsec (1) : Auto (2), SHA2-256, SHA2-384, SHA2-512.
Mode	Mode d'encapsulation IPsec : Tunnel ou Transport (1)

(1) Se reporter au chapitre 26 Recommandations de sécurité pour le choix de l'algorithme.

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

PFS

PFS - Groupe	Activable ou pas. Longueur de la clé Diffie-Hellman : DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)

IKEv1 ne propose pas de mode automatique pour le Groupe DH. Il est requis de le connaître a priori.

Se reporter au chapitre 26 Recommandations de sécurité pour le choix de l'algorithme.

Durée de vie

Durée de vie	Les durées de vie sont échangées lors de la montée du tunnel. (1) À échéance de la durée de vie, la phase 2 est renégociée. La valeur par défaut de la durée de vie de la Phase 2 est de 1800 s (30 min).

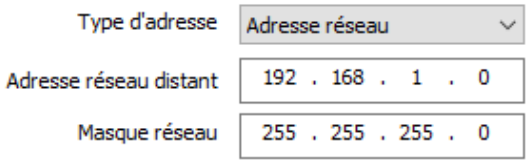
(1) Les durées de vie sont échangées entre le Client VPN et la passerelle VPN. Toutefois, certaines passerelles se limitent à retourner la valeur de la durée de vie proposée par le Client VPN. Quelle que soit la méthode, le Client VPN applique toujours la durée de vie envoyée par la passerelle VPN.

IPv4 / IPv6

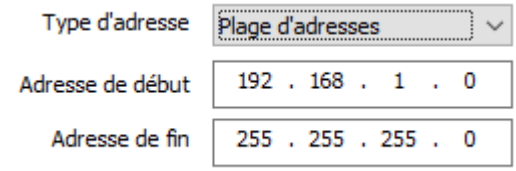
IPv4-IPv6	Voir le chapitre 17 IPv4 et IPv6.

Configuration du Type d'adresse

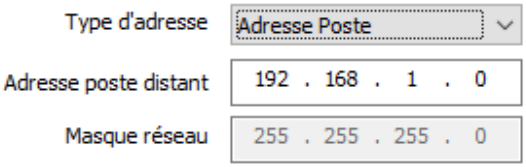
Si l'extrémité du tunnel est un réseau, choisir le type « Adresse réseau » puis définir l'adresse et le masque du réseau distant :



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 :



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).

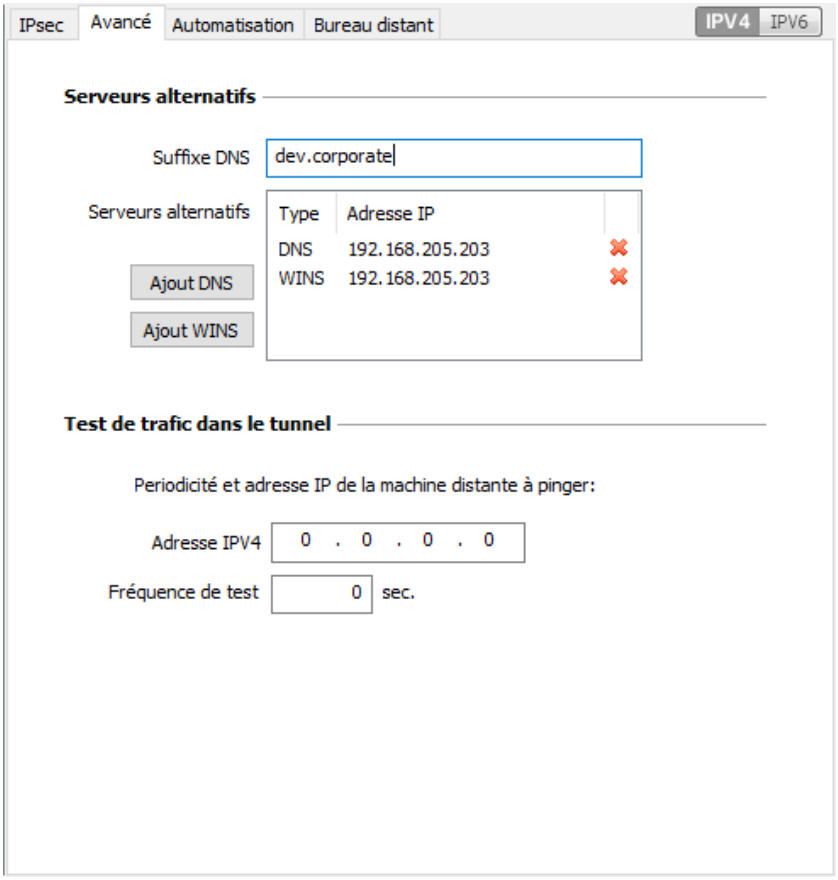
Si l'adresse IP du poste Client VPN fait partie du plan d'adressage du réseau distant (p.ex. @IP poste = 192.168.10.2 et @réseau distant = 192.168.10.x), l'ouverture du tunnel empêche le poste de communiquer avec son réseau local. En effet, toutes les communications sont orientées dans le tunnel VPN.

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 indiquez comme adresse et masque réseau « 0.0.0.0 ».

De nombreux guides de configuration du Client VPN avec différentes passerelles VPN sont disponibles sur le site web TheGreenBow : https://thegreenbow.com/fr/support/guides-dintegration/passerelles-vpn-compatibles/.

13.3.7 Phase 2 : Avancé



Serveurs alternatifs

Suffixe DNS	Suffixe de domaine à ajouter à chaque nom de machine, par exemple : « mozart.dev.corporate ». 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 « IPsec ». Si le Mode Config est activé, 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 Config.

Test de trafic dans le tunnel

Adresse IP	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 puis tente de rouvrir le tunnel automatiquement. 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. 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.

13.3.8 Phase 2 : Automatisation

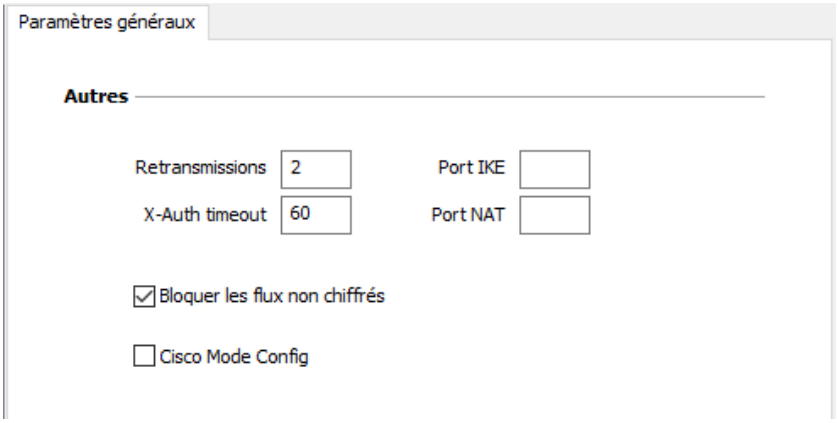
Voir le chapitre 15 Automatisation.

13.3.9 Phase 2 : Bureau distant

Voir le chapitre 19 Partage de bureau distant.

13.3.10 Paramètres généraux

Les paramètres généraux sont les paramètres communs à tous les tunnels IKEv1 (toutes les Phases 1 et toutes les Phases 2).



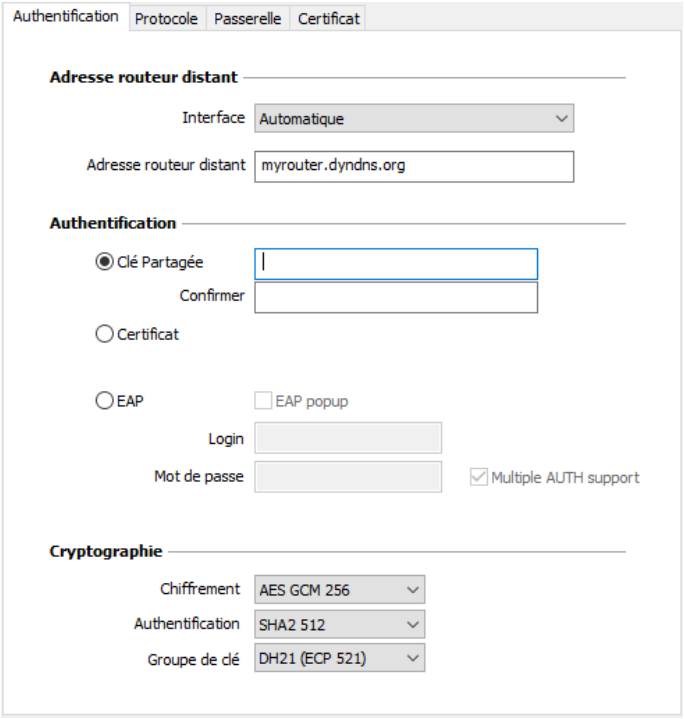
Autres

Retransmissions	Nombre de retransmissions de messages protocolaires IKE avant échec.
X-Auth timeout	Temps pour saisir le login / mot de passe X-Auth
Port IKE	Ce champ permet de configurer le Port IKE pour tous les tunnels IKEv1. Les Port IKE configurables dans chaque tunnel sont prioritaires par rapport à ce paramètre.
Port NAT	Ce champ permet de configurer le Port NAT pour tous les tunnels IKEv1. Les Port NAT configurables dans chaque tunnel sont prioritaires par rapport à ce paramètre.
Bloquer les flux non chiffrés	Lorsque cette option est cochée, seul le trafic passant dans le tunnel est autorisé. Voir la note (1) ci-dessous.
Cisco Mode Config	Cette case doit être cochée pour assurer la compatibilité avec les passerelles de type Cisco ASA

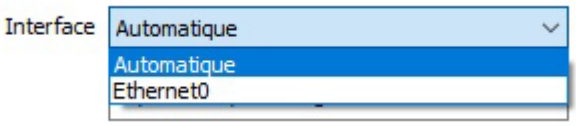
(1) L'option de configuration « Bloquer les flux non chiffrés » accroît « l'étanchéité » du poste, dès lors que le tunnel VPN est ouvert. En particulier, cette fonction permet d'éviter les risques de flux entrants qui pourraient transiter hors du tunnel VPN.
Associée à la configuration « Passer tout le trafic dans le tunnel » (voir la section 13.3.6 Phase 2 : IPsec), cette option permet de garantir une étanchéité totale du poste, dès lors que le tunnel VPN est ouvert

13.4 Configurer un tunnel IPsec IKEv2

13.4.1 IKE Auth : IKE SA



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.
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.

> 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.
>
> Se reporter au chapitre 26 Recommandations de sécurité.

Certificat	Utilisation de Certificat pour l'authentification de la connexion VPN. L'utilisation de Certificat apporte une plus grande sécurité dans la gestion des connexions VPN (authentification mutuelle, vérification des durées de vie, révocation, etc.). Se reporter au chapitre 26 Recommandations de sécurité. ☞ Se reporter au chapitre dédié : 18 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 26 Recommandations de sécurité).
Multiple AUTH Support	Active la combinaison des deux authentifications par certificat puis par EAP. (1)

(1) 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 ».

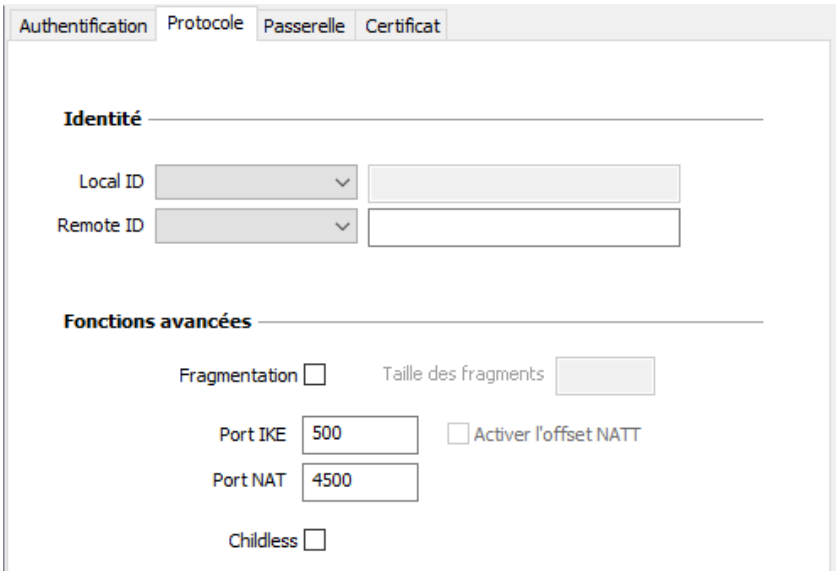
Cryptographie

Chiffrement	Algorithme de chiffrement négocié au cours de la phase d'authentification (1) : Auto (2), AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Authentification	Algorithme d'authentification négocié au cours de la phase d'authentification (1) : Auto (2), SHA2 256, SHA2 384, SHA2 512.
Groupe de clé	Longueur de la clé Diffie-Hellman (1) : Auto (2), DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521).

(1) Se reporter au chapitre 26 Recommandations de sécurité pour le choix de l'algorithme.

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

13.4.2 IKE Auth : Protocole



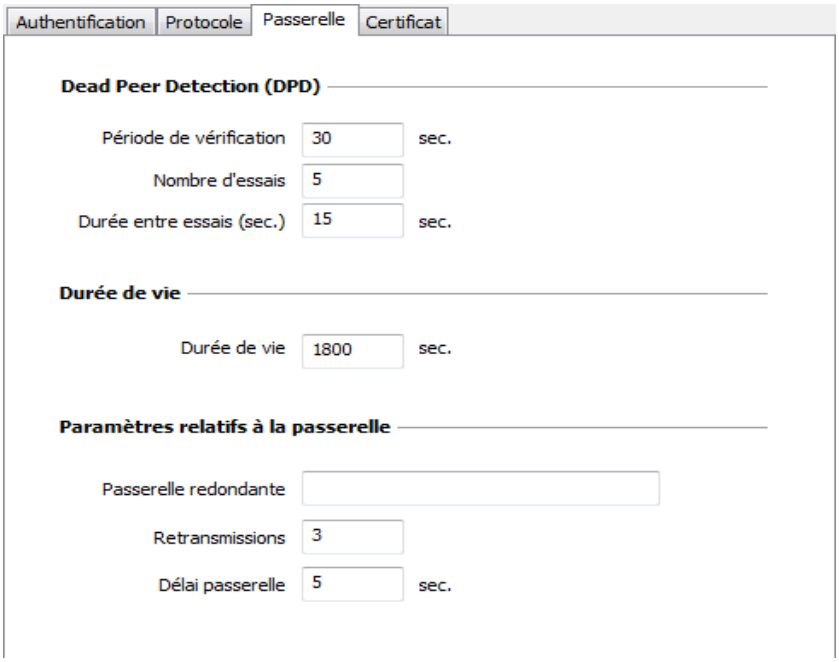
Identité

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 IP : 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 - Email : une adresse email (type = USER FQDN), p.ex. support@thegreenbow.com - DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) - Sujet X509 : ce champ est automatiquement renseigné avec le sujet d'un certificat X.509 lorsque le tunnel est associé à un certificat utilisateur (cf. chapitre 18 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 que le Client VPN s'attend à recevoir de la passerelle VPN distante. Suivant le type sélectionné, cet identifiant peut être : - Adresse IP : une adresse IP (type = IPV4 ADDR), par exemple : 80.2.3.4 - DNS : un nom de domaine (type = FQDN), par exemple : routeur.mondomaine.com - KEY ID : une chaîne de caractères (type = KEY ID), par exemple : 123456 - Email : une adresse email (type = USER FQDN), par exemple : admin@mondomaine.com - DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) Ce paramètre est obligatoire depuis la version 6.8 pour des raisons de sécurité.

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 à la MTU de l'interface physique, par exemple 1300 octets dans le cas d'une MTU classique de 1500.
Port IKE	Les échanges IKE Auth (Authentification) s'effectuent sur le protocole UDP, en utilisant par défaut le port 500. Le paramétrage du port IKE permet de passer les équipements réseau (Firewall, routeurs) qui filtrent ce port 500. 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 Child SA (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 (Firewall, routeurs) qui filtrent ce port 4500. La passerelle VPN distante doit aussi être capable d'effectuer les échanges IKE Child SA sur un port différent de 4500. Pour la connexion à certains pare-feux / passerelles configurés en mode « DR », le NAT-T doit être forcé de bout en bout, et les payloads de détection de NAT ne doivent pas être envoyés par le Client VPN. Pour ce faire, ajouter le paramètre dynamique « NoNATTNegotiation » dans l'onglet « IKE Auth » avec pour valeur « true » (voir le paragraphe Afficher plus de paramètres à la section 24.2 Général).
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.

13.4.3 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. (1) La période de vérification est la période entre deux envois de messages de vérification DPD, exprimée en secondes.
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.

(1) 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.

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 1800 secondes.

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. ☞ Voir le chapitre 14 Passerelle redondante.
Retransmissions	Nombre de retransmissions de messages protocolaires IKE avant échec.

Délai passerelle	Délai entre chaque retransmission

13.4.4 IKE Auth : Certificat

Voir le chapitre : 18 Gestion des certificats.

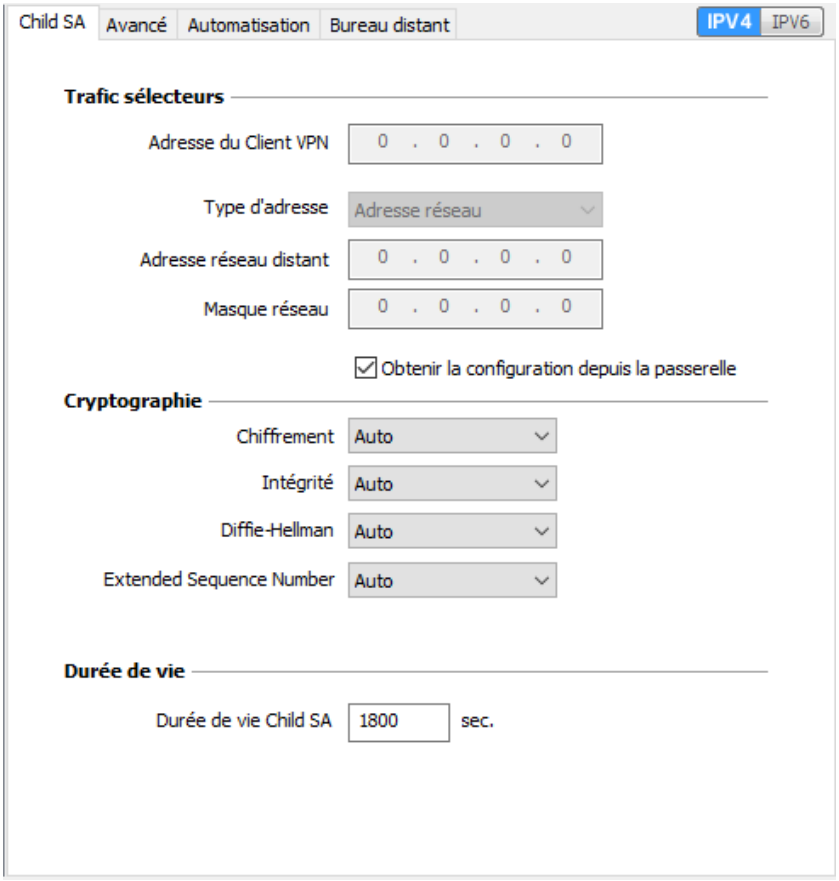
13.4.5 Child SA : Généralités

La « Child SA » d'un tunnel VPN est la phase IPsec. Cette Phase sert à la négociation des paramètres de sécurité qui seront appliqués aux données transmises dans le tunnel VPN.

Pour configurer les paramètres d'une Child SA, sélectionnez cette Child SA dans l'arborescence du Panneau de Configuration. 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 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.

13.4.6 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.

Type d'adresse	L'extrémité du tunnel peut être un réseau ou un poste distant. ☞ Voir le paragraphe ci-dessous pour la **configuration du Type d'adresse**.
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 : Adresses 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.

Cryptographie

Chiffrement	Algorithme de chiffrement négocié au cours de la Phase IPsec (1) : Auto (2), AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Intégrité	Algorithme d'authentification négocié au cours de la Phase IPsec (1) : Auto (2), SHA2 256, SHA2 384, SHA2 512.
Diffie-Hellman	Longueur de la clé Diffie-Hellman (1) : Auto (2), DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521), No Diffie-Hellman.
Extended Sequence Number	Permet l'usage de numéros de séquence étendus de taille 64 bits (cf. RFC 4304) : Auto (2), Non, Oui. Ce mode est recommandé.

(1) Se reporter au chapitre 26 Recommandations de sécurité pour le choix de l'algorithme.

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

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 1800 s (30 min).

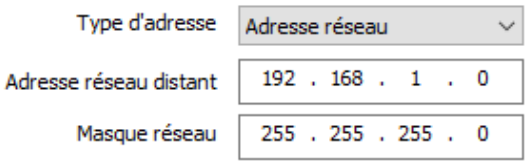
Contrairement à IKEv1, les durées de vie ne sont pas négociées en IKEv2 entre le Client VPN et la passerelle. Ainsi, les durées de vie appliquées au tunnel seront bien celles configurées sur le Client VPN.

IPv4 / IPv6

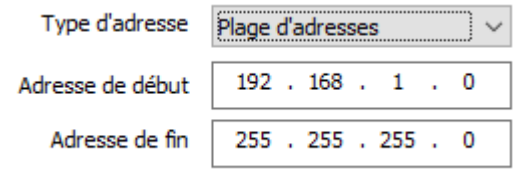
IPv4 / IPv6	☞ Voir le chapitre 17 IPv4 et IPv6.

Configuration du Type d'adresse

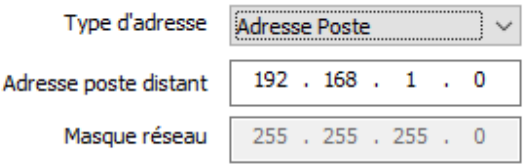
Si l'extrémité du tunnel est un réseau, choisir le type « Adresse réseau » puis définir l'adresse et le masque du réseau distant :



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 :



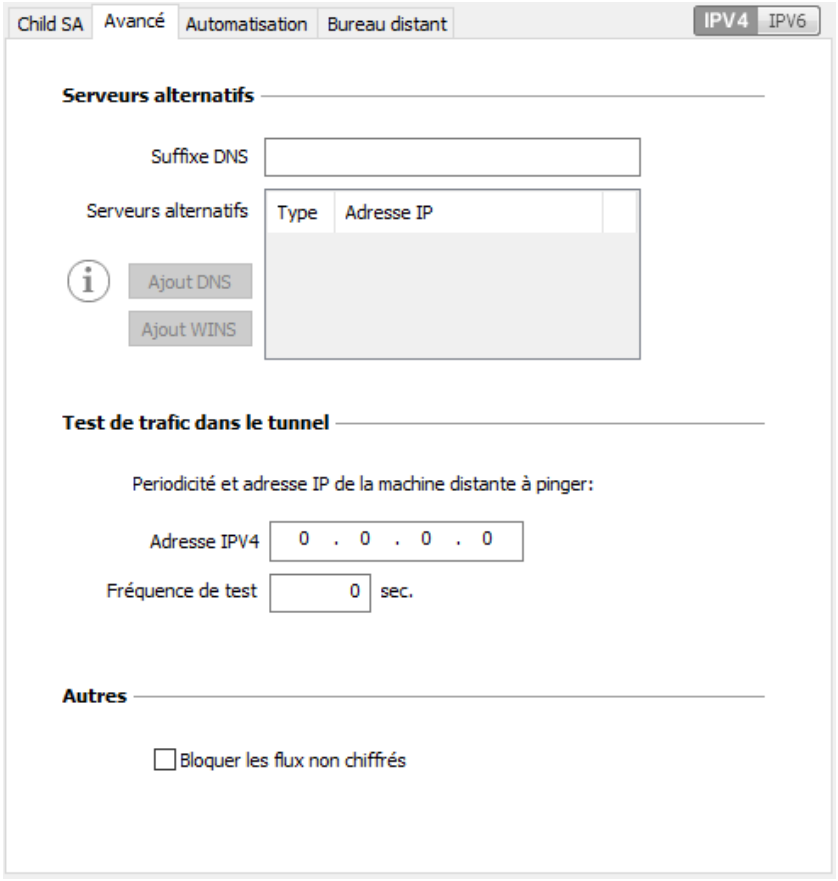
La fonction « Ouverture automatiquement sur détection de trafic » permet d'ouvrir automatiquement un tunnel sur détection de trafic vers l'une des adresses de la plage d'adresses spécifiée (moyennant le fait que cette plage d'adresses soit aussi autorisée dans la configuration de la passerelle VPN).

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.

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 ».

De nombreux guides de configuration du Client VPN avec différentes passerelles VPN sont disponibles sur le site web TheGreenBow : https://thegreenbow.com/fr/support/guides-dintegration/passerelles-vpn-compatibles/.

13.4.7 Child SA : Avancé



Serveurs alternatifs

Suffixe DNS	Suffixe de domaine à ajouter à chaque nom de machine, par exemple : « mozart.dev.thegreenbow ». 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 ». 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. 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. Voir la note (1) ci-dessous.

(1) 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 13.4.6 Child SA : Child SA), cette option permet de garantir une étanchéité totale du poste, dès lors que le tunnel VPN est ouvert.
Ce mode est recommandé.

13.4.8 Child SA : Automatisation

Voir le chapitre 15 Automatisation.

13.4.9 Child SA : Bureau distant

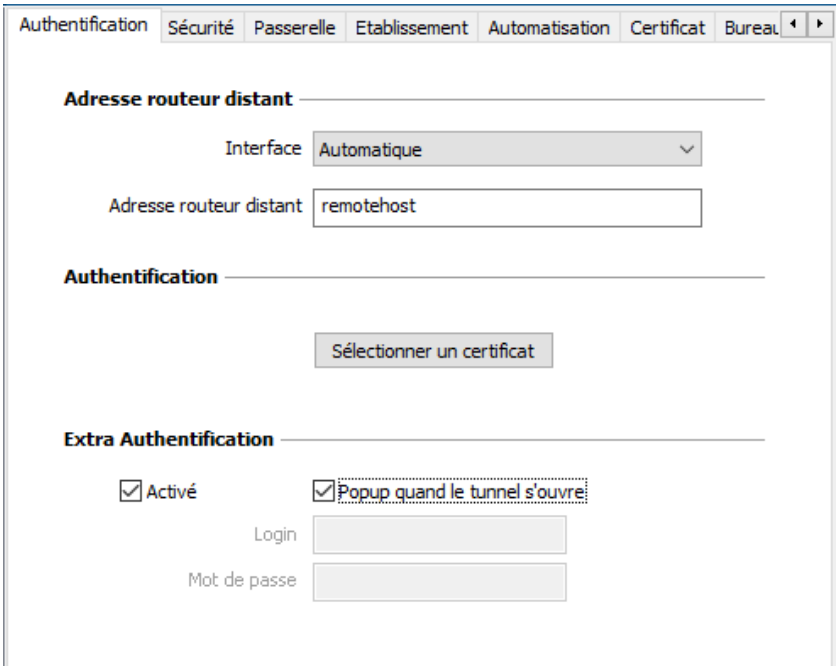
Voir le chapitre 19 Partage de bureau distant.

13.5 Configurer un tunnel VPN SSL

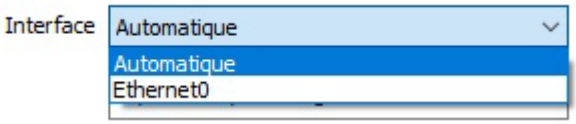
13.5.1 Introduction

Le Client VPN Windows Enterprise permet depuis la version 6 d'ouvrir des tunnels VPN SSL.
Les tunnels VPN SSL du Client VPN Windows Enterprise sont compatibles OpenVPN et permettent d'établir des connexions sécurisées avec toutes les passerelles qui implémentent ce protocole.

13.5.2 Principal



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.

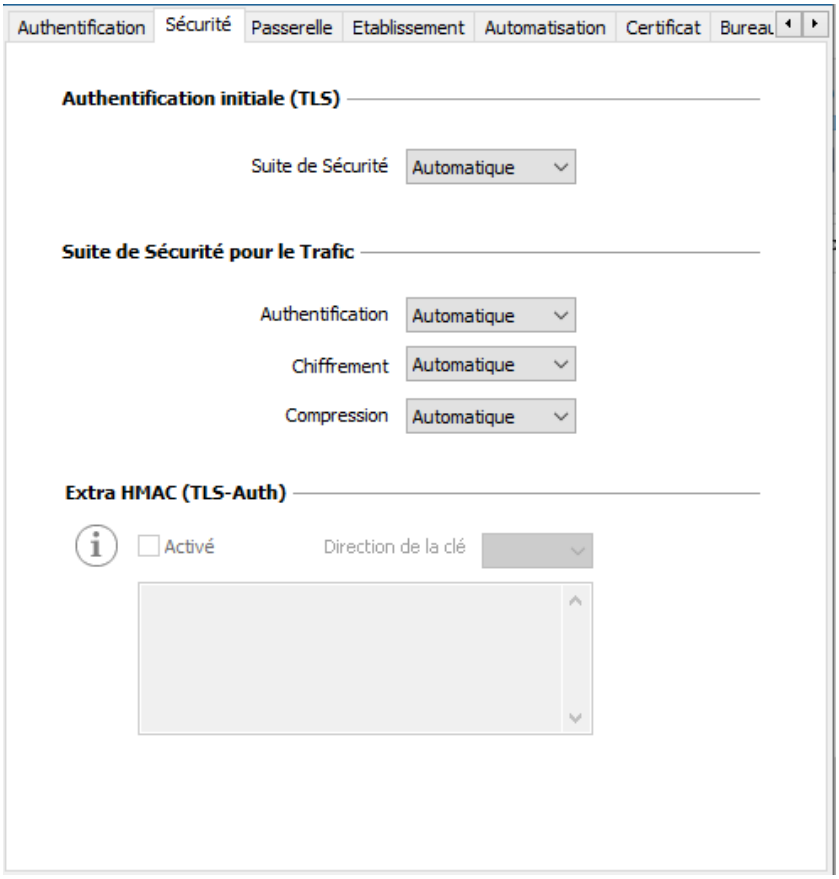
Authentification

Sélectionner un certificat	Sélection du Certificat pour l'authentification de la connexion VPN. ☞ Se reporter au chapitre dédié : 18 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.

13.5.3 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. - Basse : seules les suites cryptographiques faibles sont proposées à la passerelle. Dans la version actuelle, ce sont les suites utilisant des algorithmes de chiffrement de 64 ou 56 bits. - Normale : 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. - Haute : 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. Pour plus d'informations : https://www.openssl.org/docs/man1.1.1/man1/ciphers.html

Suite de Sécurité pour le Trafic

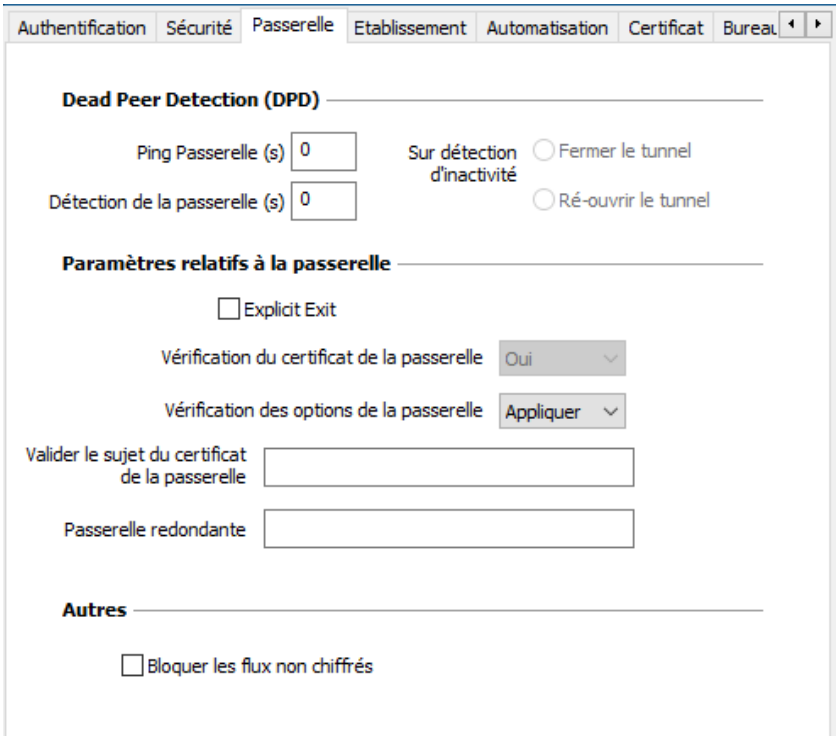
Authentification	Algorithme d'authentification négocié pour le trafic : Automatique (1), MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512. Si l'option « Extra HMAC » est activée (cf. ci-dessous), l'algorithme d'authentification ne peut être « Automatique ». Il doit être configuré explicitement, et doit être identique à celui choisi côté passerelle.
Chiffrement	Algorithme de chiffrement du trafic : Automatique (1), BF-CBC-128, AES-128-CBC, AES-192-CBC, AES-256-CBC.
Compression	Compression du trafic : Auto (1), Lz0, Non, Lz4.

(1) 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 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 »

13.5.4 Passerelle



Dead Peer Detection (DPD)

La fonction DPD (Dead Peer Detection) permet aux deux extrémités du tunnel de vérifier mutuellement leur présence. (1)

Ping passerelle	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	Durée en secondes à l'issue de laquelle, si aucun « ping » n'a été reçu de la passerelle, celle-ci est considérée comme indisponible.
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.

(1) 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.

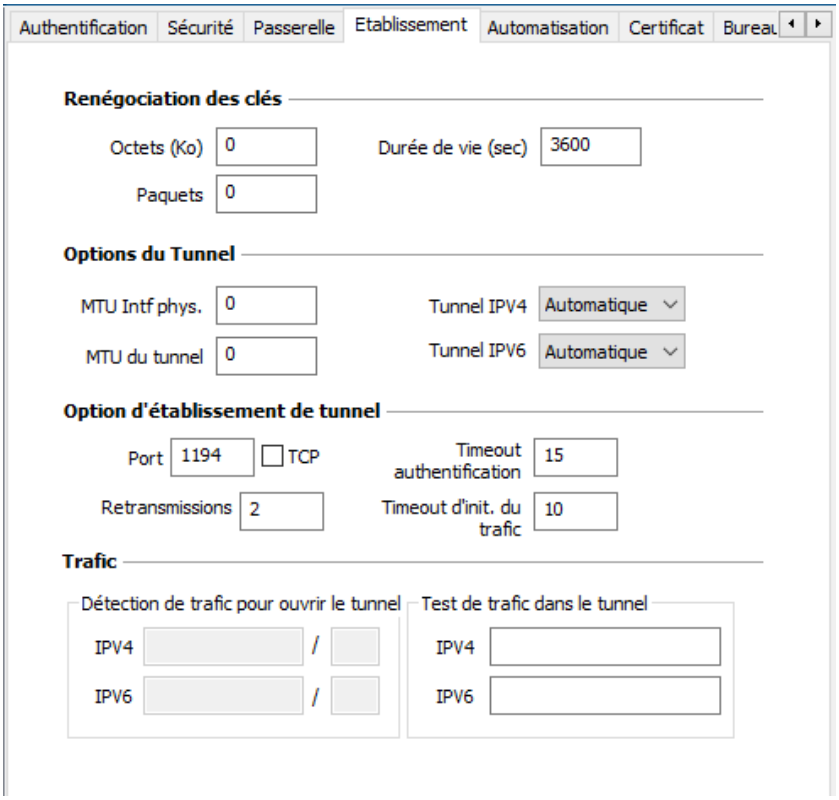
Paramètres relatifs à la passerelle

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 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 24.4 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. ☞ Voir le chapitre 14 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.

13.5.5 Établissement



Renégociation des clés

Octets, Paquets, durée de vie	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 moins un delta fixe.
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 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 Vérifier que les deux choix « Tunnel IPv4 » et « Tunnel IPv6 » ne sont pas tous deux à « Non ».

Option d'établissement du 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 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. Aucune action particulière n'est faite s'il n'y a pas de réponse au « ping ».

13.5.6 Automatisation

Voir le chapitre 15 Automatisation.

13.5.7 Certificat

Voir le chapitre 18 Gestion des certificats.

13.5.8 Bureau distant

Voir le chapitre 19 Partage de bureau distant.

14 Passerelle redondante

Le Client VPN Windows Enterprise 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 des DPD, 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.

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.

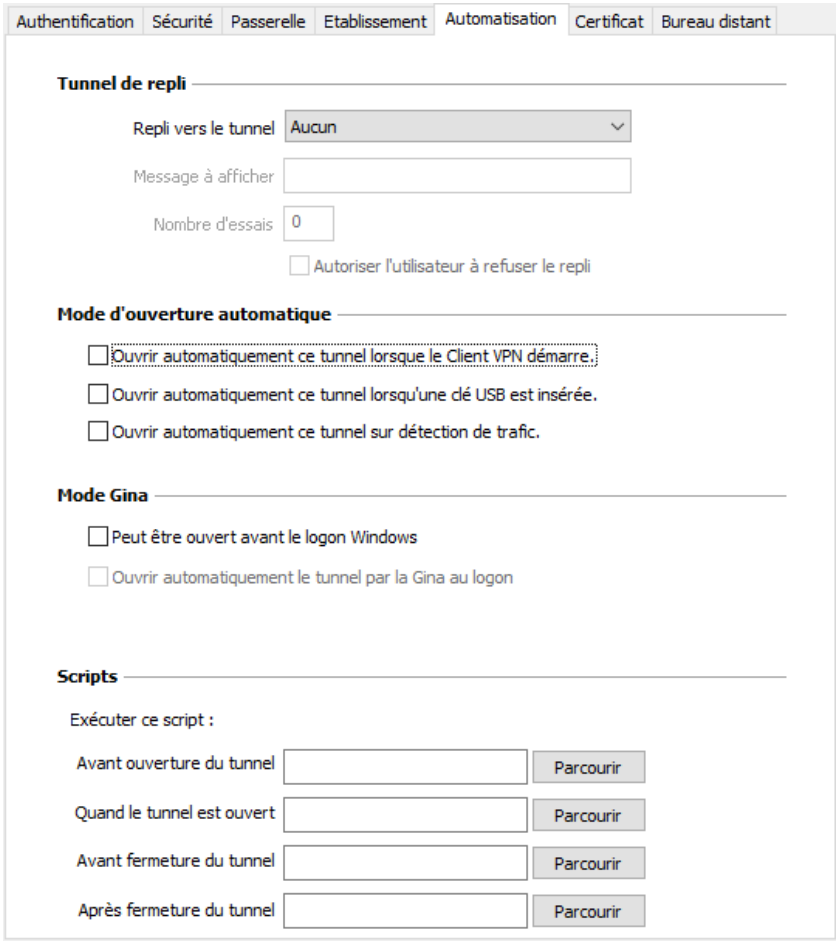
Le Client VPN n'essaye pas de contacter la passerelle redondante si la passerelle initiale est inaccessible à cause d'un problème de résolution DNS.

15 Automatisation

Le Client VPN Windows Enterprise 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 : IKEv1, IKEv2 et SSL.

Pour chaque type de tunnel, le paramétrage des automatisations s'effectue dans l'onglet « Automatisation » du tunnel : Phase 2 (IKEv1), Child SA (IKEv2) ou TLS (SSL).



Tunnel de repli (fallback)

☞ Se reporter au chapitre 16 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 fait partie d'une configuration sur clé USB (voir le chapitre 22 Mode USB, il est ouvert automatiquement sur insertion de cette clé USB. 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 23 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.

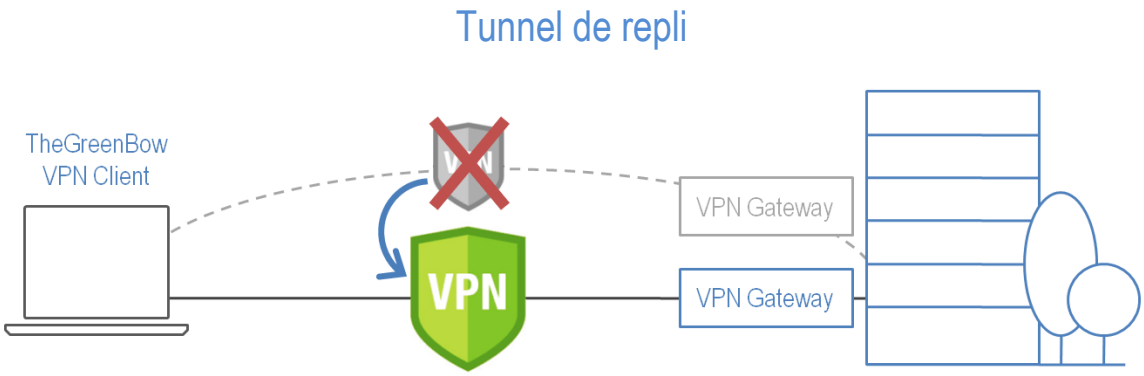
Les applications sont nombreuses :

- 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.

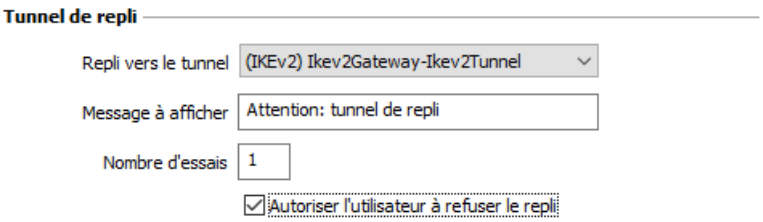
Les scripts ne sont pas configurables pour un tunnel configuré en mode GINA. Les champs de saisie sont désactivés.

16 Tunnel de repli

Le Client VPN Windows Enterprise 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 (IKEv1, IKEv2 ou SSL).



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.

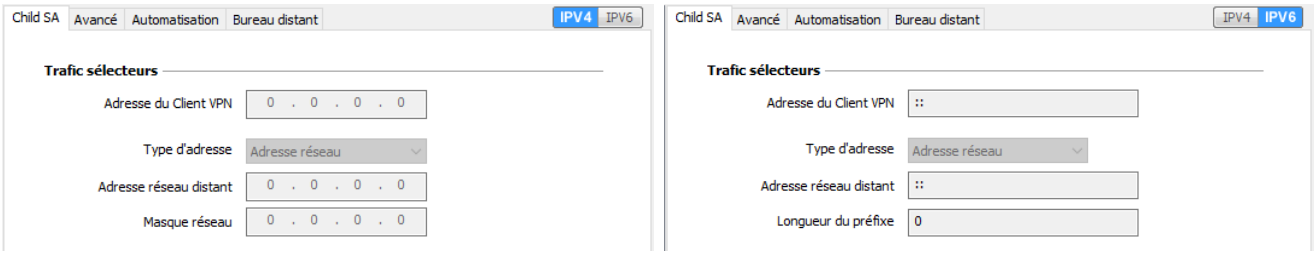
17 IPv4 et IPv6

Le Client VPN Windows Enterprise 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 2. Si les 2 adresses sont fournies, l'adresse IPv4 est privilégiée.

Pour les tunnels VPN IKEv1 et IKEv2, la configuration du protocole IPv4 ou IPv6 est accessible en haut à droite de l'onglet IPsec (pour les Phases 2 d'un tunnel IKEv1) ou Child SA (pour les Child SA d'un tunnel IKEv2).

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



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.

Pour les tunnels SSL, la détection de la configuration protocolaire est automatique. Aucun paramétrage n'est requis. De plus, un tunnel SSL peut supporter du trafic IPv4 et IPv6 simultanément dans un même tunnel : il n'est pas nécessaire de configurer deux tunnels distincts comme pour IKEv1 ou IKEv2.

18 Gestion des certificats

Le Client VPN Windows Enterprise est le logiciel de connexion VPN pour lequel les innovations en matière d'intégration avec les PKI / IGC sont les plus avancées. Le Client VPN Windows Enterprise est ainsi intégrable avec tout type de PKI / IGC, de façon souple, évolutive, automatisable et particulièrement configurable.

Le Client VPN Windows Enterprise offre un ensemble inégalé 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, etc.

Le Client VPN Windows Enterprise implémente en particulier les fonctions et facilités suivantes :

- Exploitation de tout type de support de certificat : carte à puce, token, magasin de certificats, fichier, configuration VPN, clé USB
- Caractérisation du support de certificat à utiliser : sélection automatique parmi plusieurs supports concurrents
- Accès aux cartes à puce et aux tokens en PKCS#11, CSP (IKEv1 uniquement) et CNG
- Prise en compte des formats de certificats X.509 : PKCS#12, PEM, PFX
- Sélection multicritère des certificats à utiliser : sujet, key usage, etc.
- 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 et des CRL
- Gestion des autorités de certification (Certificate Authority : CA)
- Validation des certificats client et passerelle : authentification mutuelle, avec autorité de certification identiques ou différentes (importation de CA spécifiques)
- Possibilité de préconfigurer tous les paramètres PKI / IGC pour une prise en compte automatique lors de l'installation

Le Client VPN Windows Enterprise 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 le Client VPN Windows Enterprise 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 l'onglet « Certificat » du tunnel concerné : Phase 1 (IKEv1) ou IKE Auth (IKEv2) ou TLS (SSL).

18.1 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 :

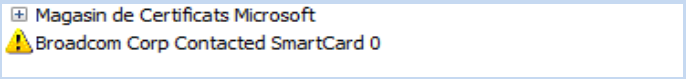
- dans le fichier de configuration VPN (voir ci-dessous « Importer un Certificat ») ;
- dans le magasin de certificats Windows (voir ci-dessous « Magasin de certificats Windows ») ;
- sur une carte à puce ou dans un token (voir ci-dessous « Utiliser un certificat sur carte à puce ou sur token »).

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

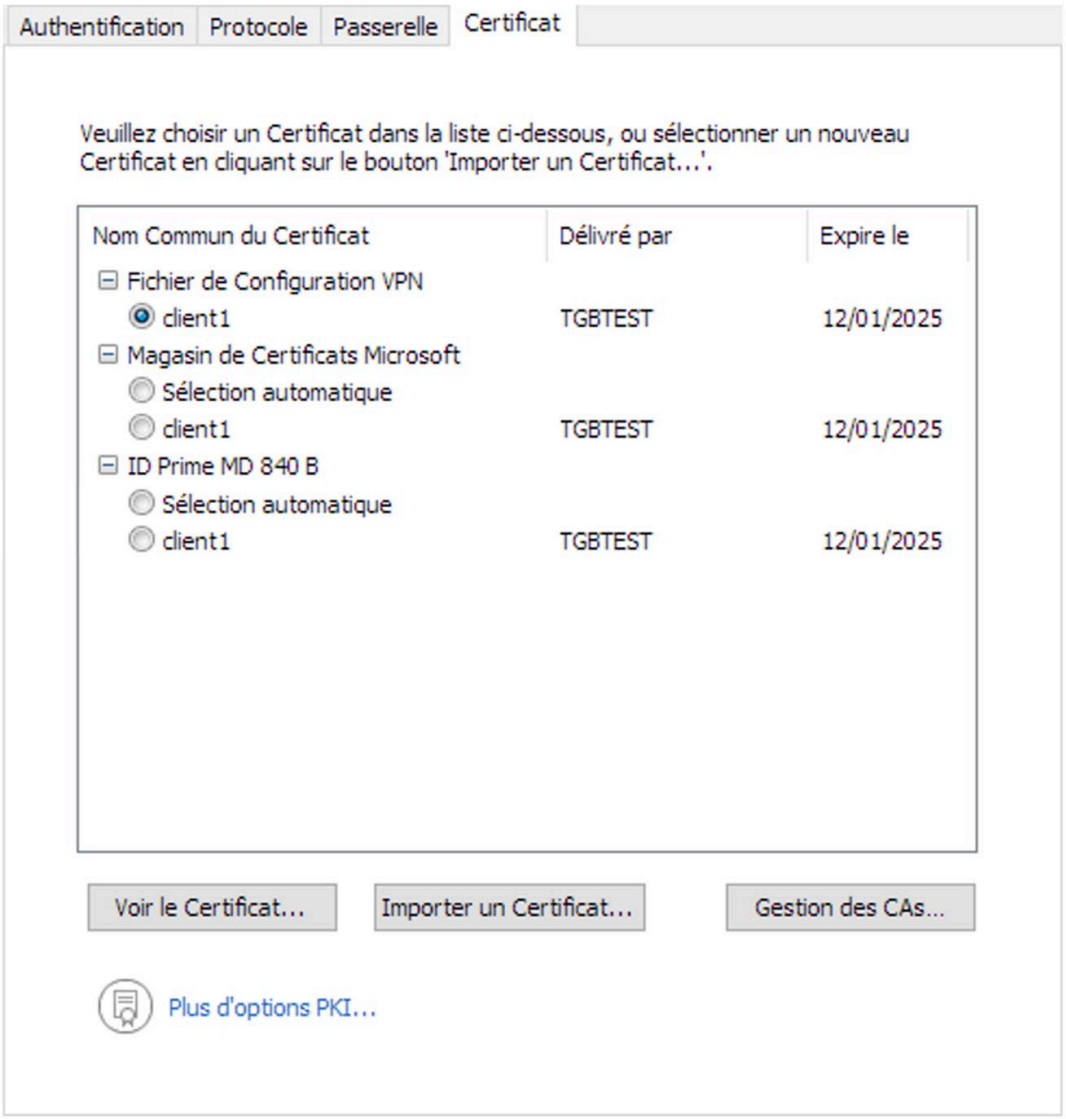
- la carte à puce ou le token est compatible CNG, CSP (IKEv1 uniquement) ou PKCS#11 ;
- le middleware de la carte à puce ou du token est correctement installé sur l'ordinateur ;
- le cas échéant, la carte à puce est correctement insérée dans le lecteur associé.

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

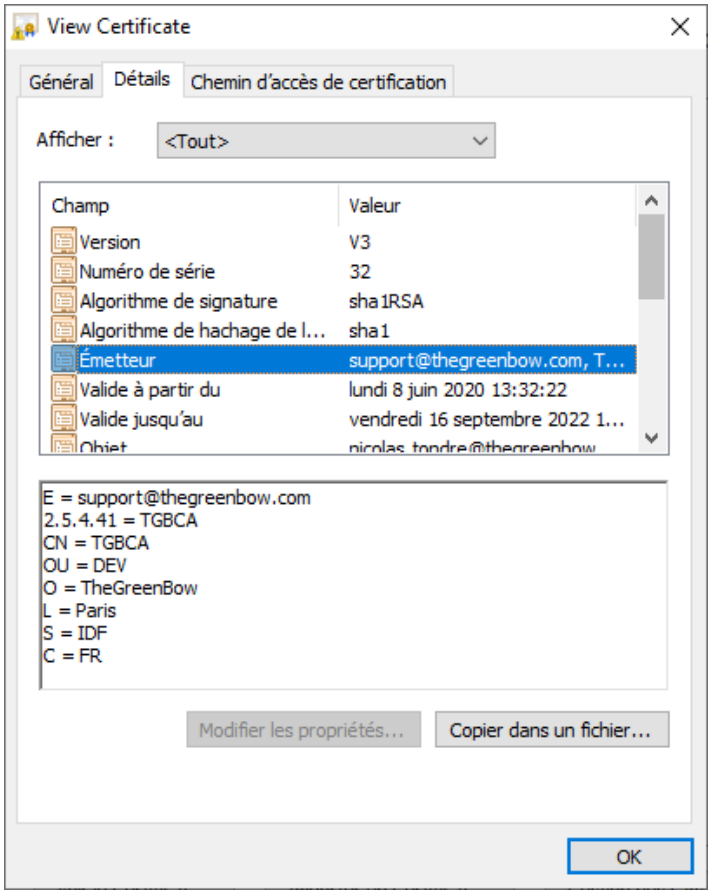
Dans le cas d'un lecteur de cartes à puce, le lecteur s'affiche précédé d'une icône d'alerte si la carte à puce n'est pas insérée.



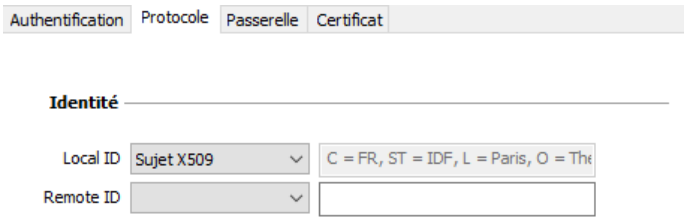
Seuls les certificats présents qui ne sont pas périmés sont affichés.



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



Une fois le certificat sélectionné, le type de Local ID du tunnel passe automatiquement à « Sujet X509 » (alias DER ASN1 DN), et le sujet du certificat est utilisé par défaut comme valeur de ce « Local ID ».



18.2 Sélection automatique du certificat

Dans l'onglet « Certificat » du tunnel concerné, il est possible de choisir le bouton « Sélection automatique » pour les certificats qui se trouvent dans le Magasin de Certificats Windows ou sur un token/carte à puce. Dans ce cas, le Client VPN sélectionnera automatiquement le certificat sur le support concerné en fonction soit :

- de critères globaux définis dans l'onglet « Options PKI » (cf. section 24.4 Options PKI),
- de critères spécifiques à un tunnel, définis à l'aide de paramètres dynamiques (voir ci-après).

Il est possible de combiner la sélection en fonction de l'extension « key usage » et du sujet.

18.2.1 Sélection en fonction de l'extension « key usage »

Le paramètre dynamique « user_cert_keyusage » est utilisé pour caractériser un certificat sur un support donné et pour un tunnel donné en fonction de l'extension key usage.

Pour activer la sélection du certificat en fonction de l'extension key usage, ajouter le paramètre dynamique « user_cert_keyusage » dans l'onglet « IKE Auth » avec l'une des valeurs de la table ci-dessous (voir le paragraphe Afficher plus de paramètres à la section 24.2 Général)).

0 ou non défini	Pas de sélection du certificat en fonction de l'extension « key usage ».
1	Sélection du certificat dont l'extension « key usage » contient la valeur « digitalSignature ».
2	Sélection du certificat dont l'extension « key usage » contient les valeurs « digitalSignature » et « keyEncipherment ».
3	Sélection du certificat dont l'extension « key usage » contient les valeurs « digitalSignature » et « clientAuthentication ».

Ce paramètre dynamique prend la priorité sur le paramétrage global « Utiliser seulement les certificats de type "Authentification" » disponible dans les options PKI (cf. section 24.4 Options PKI) ou défini par la propriété MSI KEYUSAGE (cf. Guide de déploiement).

18.2.2 Sélection en fonction du sujet

Le paramètre dynamique « user_cert_dnpattern » est utilisé pour caractériser un certificat sur un support donné et pour un tunnel donné en fonction du sujet (DN = Distinguished Name) du certificat.

Pour activer la sélection du certificat en fonction du sujet, ajouter le paramètre dynamique « user_cert_dnpattern » dans l'onglet « IKE Auth » avec une chaîne de caractères (voir Afficher plus de paramètres à la section 24.2 Général)).

Lorsque ce paramètre dynamique est renseigné, le Client VPN Windows Enterprise recherche, sur token ou carte à puce et dans le magasin de certificat Windows, le certificat dont le sujet contient la chaîne de de caractères indiquée.

Quand ce paramètre dynamique n'est pas défini, le Client VPN recherche le premier certificat conforme aux autres caractéristiques configurées (extension « key usage »).

Ce paramètre dynamique prend la priorité sur un éventuel paramétrage global par la propriété MSI DNPATTERN (cf. Guide de déploiement).

18.3 Importer un certificat

Le Client VPN Windows Enterprise permet d'importer dans la configuration VPN des certificats au format PEM 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.

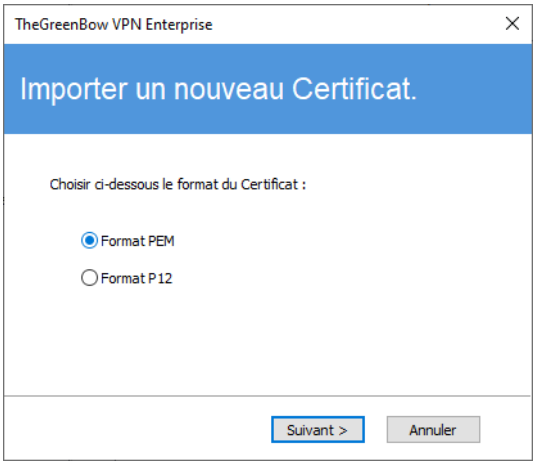
Cette solution présente l'avantage de regrouper le certificat (propre à un utilisateur) et la configuration VPN (a priori générique) dans un fichier unique, facile à transmettre vers le poste utilisateur et à importer dans le Client VPN.

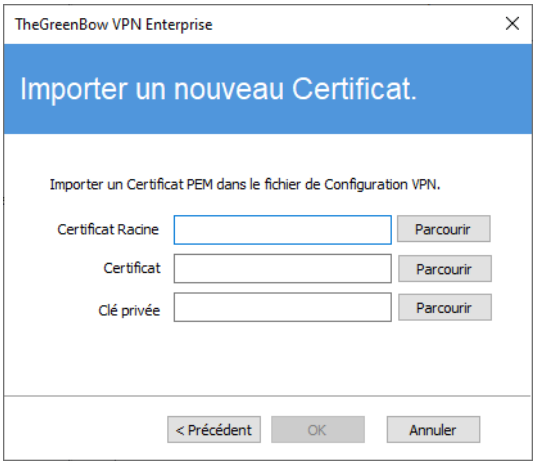
Néanmoins, l'inconvénient de transporter les certificats dans une configuration VPN est que chaque configuration devient alors propre à chaque utilisateur. Cette solution, n'est donc pas préconisée pour un déploiement conséquent.

⚠ 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 12.2 Exporter une configuration VPN), pour éviter que le certificat ne soit visible en clair.

Importer un certificat au format PEM

1/ Dans l'onglet Certificat d'une Phase 2, cliquez sur « Importer un Certificat… ».
2/ Choisissez « Format PEM ».
3/ Sélectionnez (« Parcourir ») le Certificats Racine, Certificat (Utilisateur) et la Clé privée à importer.
4/ Validez.



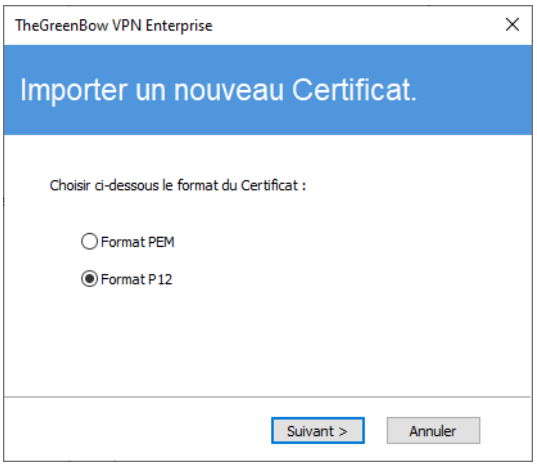


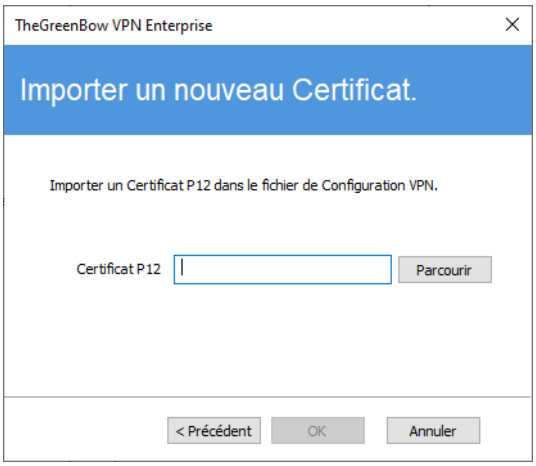
Le certificat apparaît et est sélectionné dans la liste des certificats de l'onglet « Certificat ».
Sauvegarder la configuration VPN : le certificat est sauvegardé dans la configuration VPN.

Importer un certificat au format PKCS#12

1/ Dans l'onglet Certificat d'une Phase 2, cliquez sur « Importer un Certificat… ».
2/ Choisissez « Format P12 ».
3/ Sélectionnez (« Parcourir ») le certificat PKCS#12 à importer.
4/ S'il est protégé par mot de passe, saisissez le mot de passe et validez.

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





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.

18.4 Magasin de certificats Windows

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

- Le certificat doit être certifié par une autorité de certification (ce qui exclut les certificats auto-signés),
- 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 de positionner la propriété `MACHINESTORE` à 1 lors de l'installation du logiciel.

Se reporter au « Guide de Déploiement » pour les instructions correspondantes.

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 Windows « Démarrer », puis dans le champ « Rechercher les programmes et fichiers », entrer « certmgr.msc ».

18.5 Options PKI : caractériser le certificat et son support

Le Client VPN Windows Enterprise 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.

18.6 Certificat de la passerelle VPN

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

Voir paragraphe Vérification des certificats à la section 24.4 Options PKI.

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 CRL (Certificate Revocation List) 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 :

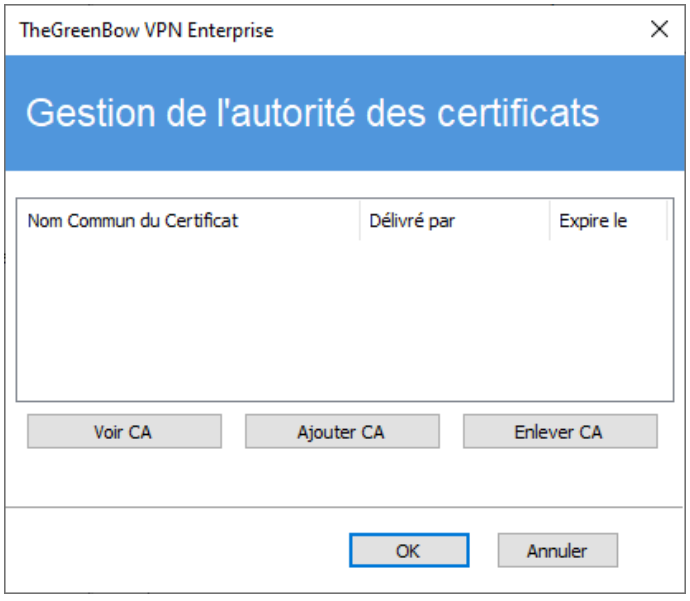
- la vérification de la date d'expiration du certificat,
- la vérification de la date de début de validité du certificat,
- la vérification des signatures de tous les certificats de la chaîne de certificats (y compris le certificat racine, certificats intermédiaires et le certificat du serveur),
- la mise à jour des CRL de tous les émetteurs de certificats de la chaîne de certification,
- la vérification de l'absence de révocation de certificats dans les listes de CRL correspondantes.

18.7 Gestion des CA (Autorités de Certification)

Lorsque le Client VPN Windows Enterprise est configuré pour vérifier les certificats client et passerelle, il est nécessaire d'importer des Autorités de Certification (CA), en complément des certificats exploités.
C'est le cas en particulier à chaque fois que le logiciel ne peut trouver localement le CA du certificat de la passerelle, c'est-à-dire dans les cas suivants :

1/ Le CA du certificat de la passerelle est différent de celui du client, et ce CA passerelle n'est pas présent/accessible sur le poste.
2/ Le CA du certificat de la passerelle est le même que celui du client mais le CA du client est stocké sur une carte à puce ou un token : dans ce cas, il est inaccessible au logiciel.
3/ Le mode EAP est sélectionné (ce mode ne requiert pas certificat client), et le CA du certificat de la passerelle n'est pas présent/accessible sur le poste.

Depuis la version 6.8 du Client VPN Windows Enterprise, pour des raisons de sécurité, il n'est plus possible d'utiliser le magasin de certificats Windows pour accéder aux CA.



1/ Dans la fenêtre « Gestion des CA », cliquer sur « Ajouter CA ».
2/ Choisir le format de CA souhaité (PEM ou DER).
3/ Sélectionner (« Parcourir ») le CA à importer.

Dans la version actuelle du Client VPN Windows Enterprise, il n'est pas possible d'ajouter plus de trois CA dans une configuration.

18.8 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 PIN code d'accès à cette carte à puce ou token est demandé à l'utilisateur à chaque ouverture du tunnel.

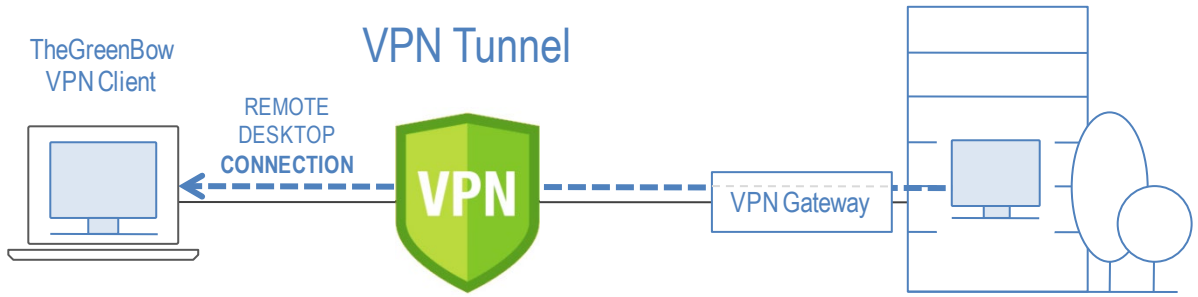
Si la carte à puce n'est pas insérée, ou si le token n'est pas accessible, le tunnel ne s'ouvre pas.
Si le certificat trouvé ne remplit pas les conditions configurées (cf. section 18.5 Options PKI : caractériser le certificat et son support ci-dessus), le tunnel ne s'ouvre pas.
Si le PIN code présenté est erroné, le Client VPN Windows Enterprise avertit l'utilisateur, qui a habituellement trois essais consécutifs avant blocage de la carte à puce ou du token.

Le Client VPN Windows Enterprise 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 15 Automatisation).

19 Partage de bureau distant

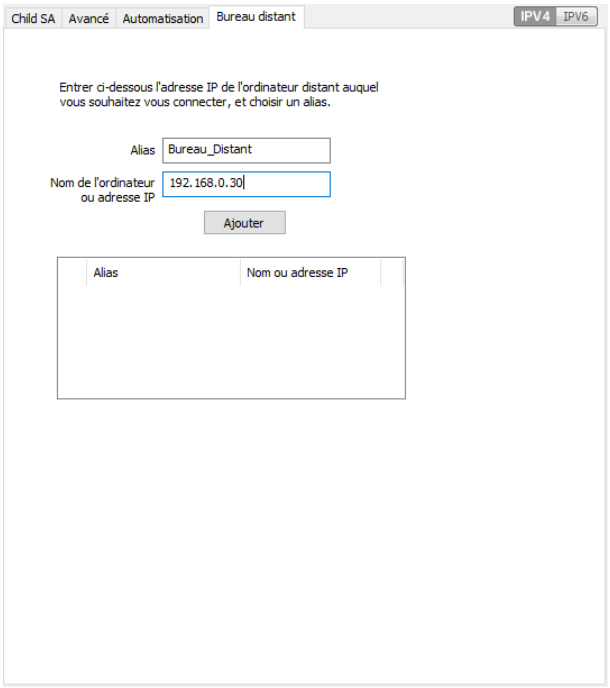
L'ouverture d'une session « Remote Desktop » (partage de bureau distant) au travers d'internet sur un ordinateur Windows distant nécessite habituellement l'établissement d'une connexion sécurisée, ainsi que la saisie des paramètres de connexions (adresse de l'ordinateur distant, etc.).

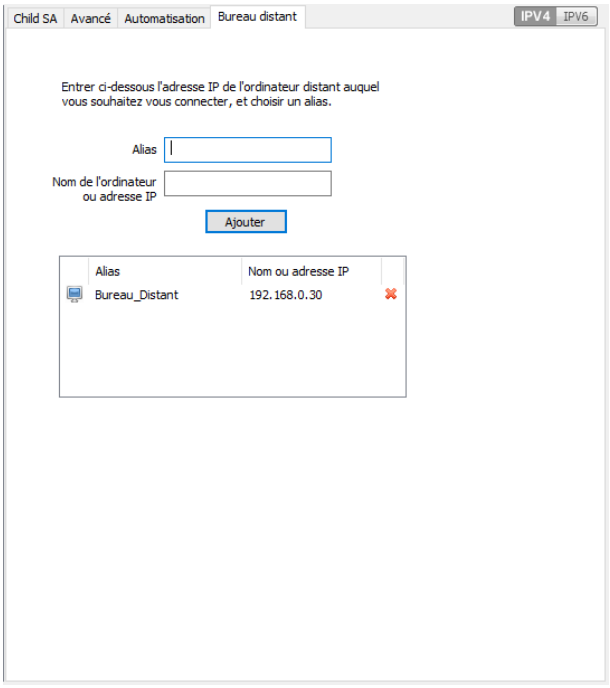
Le Client VPN Windows Enterprise permet de simplifier et de sécuriser automatiquement l'ouverture d'une session « Remote Desktop » : En un seul clic, la connexion VPN s'établit avec le poste distant et la session RDP (Remote Desktop Protocol) est automatiquement ouverte sur ce poste distant.



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

1/ Sélectionnez le tunnel VPN (Phase 2, 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.

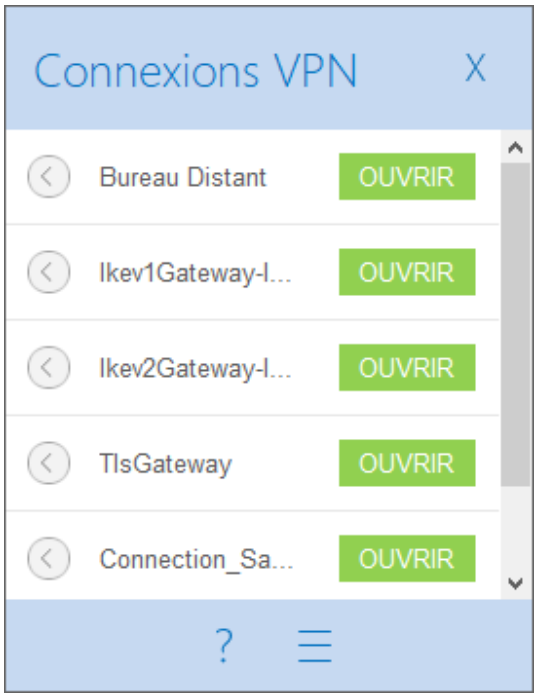




Pour ouvrir cette connexion RDP en un seul clic, il est recommandé de la faire apparaître spécifiquement dans le Panneau des Connexions, en utilisant la fonction de « Gestion du Panneau des Connexions » détaillée ci-après.

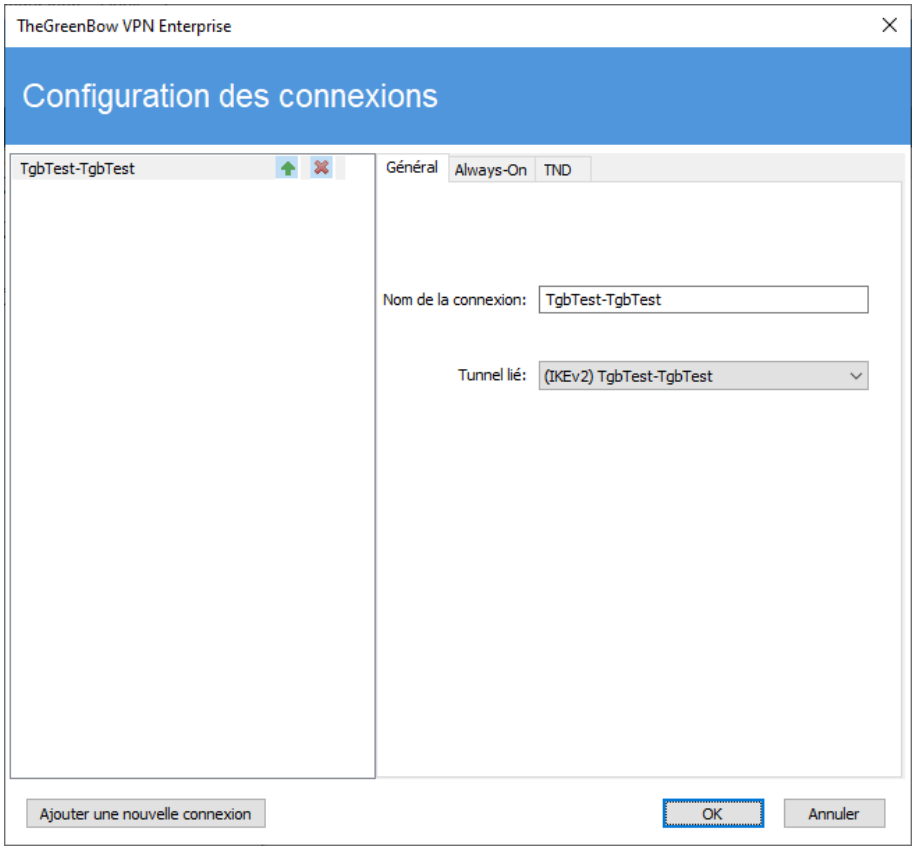
20 Gestion du Panneau des Connexions

Le Panneau des Connexions du Client VPN Windows Enterprise 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.

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.

Les onglets Always-On et TND sont décrits dans le chapitre suivant : Gestion du Panneau TrustedConnect.

21 Gestion du Panneau TrustedConnect

Le Panneau TrustedConnect est décrit dans le chapitre 10 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, se reporter au chapitre 20 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

21.1 Always-On

21.1.1 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)

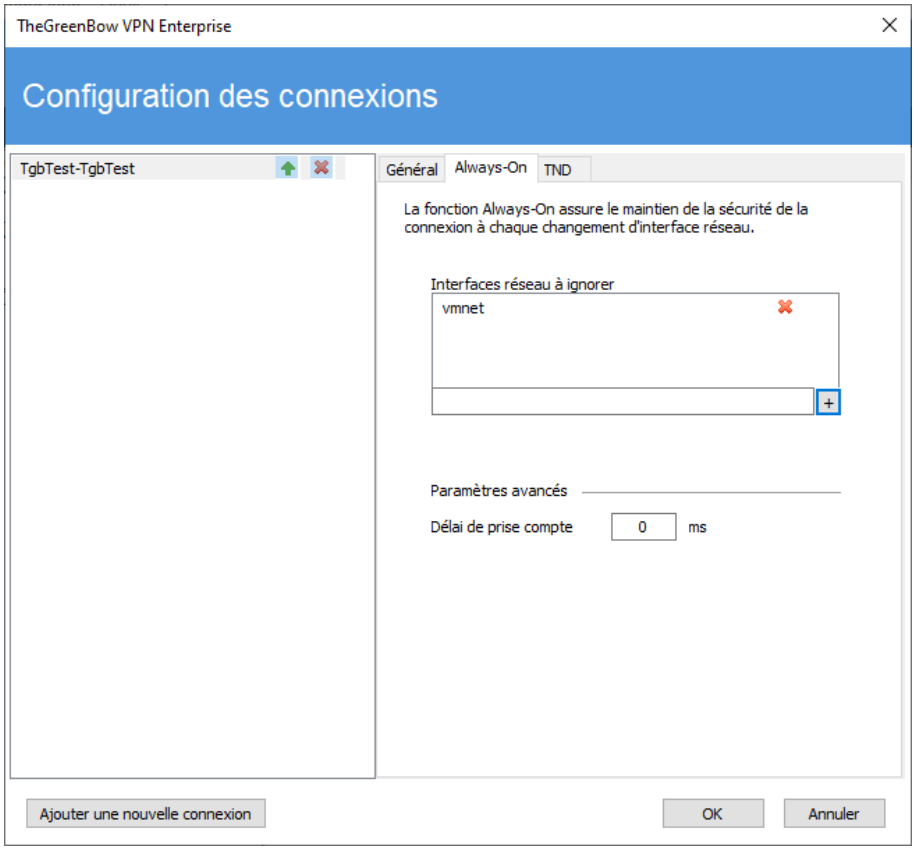
Les évènements réseau déclenchant la reconnexion automatique du tunnel (et la détection du réseau de confiance, le cas échéant), sauf exclusion explicite (voir section 21.1.2 Configuration de Always-On) sont les suivants :

- 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

21.1.2 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). Il est possible de spécifier plusieurs interfaces réseau à exclure en spécifiant les parties de leurs descriptions respectives, séparées par une virgule. Exemple : Pour exclure toutes les interfaces dont le champ description comporte les chaînes de caractères `Hyper-V` et `vmnet`, entrez `Hyper-V,vmnet`.
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.

21.2 Détection du réseau de confiance (TND)

21.2.1 Principe et fonctionnement

Cette fonctionnalité consiste à détecter que 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 les deux méthodes suivantes pour détecter si le poste est sur un réseau de confiance ou non :

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 méthodes sont cumulatives pour détecter que le poste est sur un réseau de confiance : 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 :

- 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,

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.

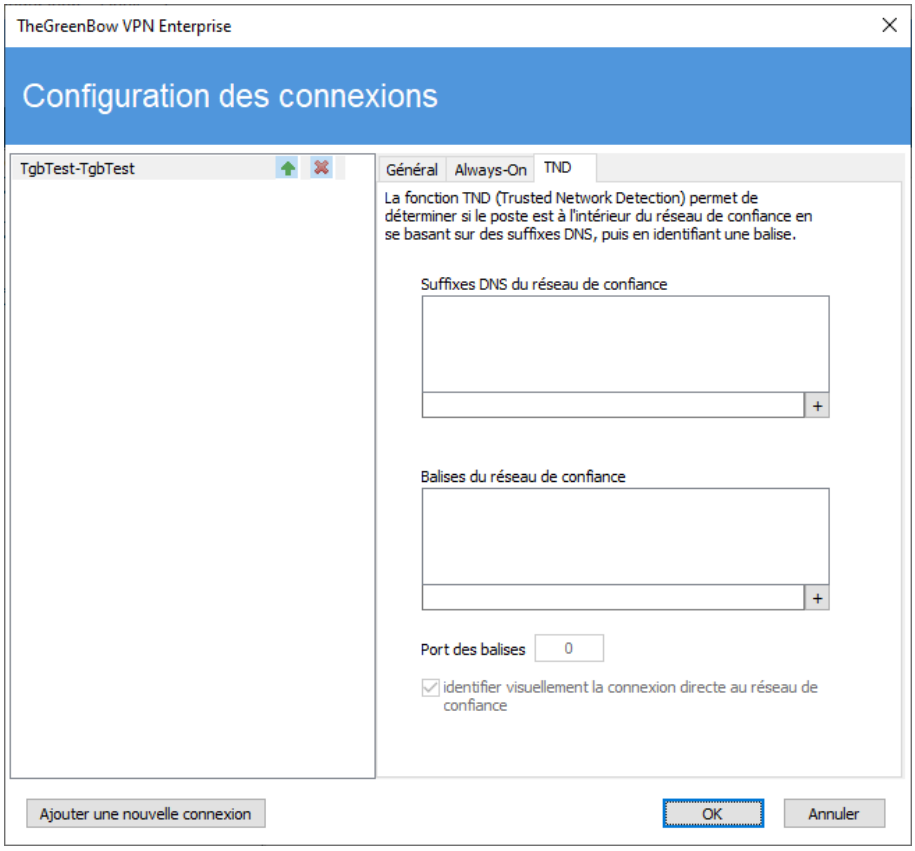
Pour activer la fonctionnalité de détection du réseau de confiance (TND), les paramètres suivants doivent donc être configurés :

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

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).

21.2.2 Configuration de TND

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



Suffixes DNS du réseau de confiance	Ce paramètre définit la liste des suffixes DNS de confiance. Cette liste peut être vide ou contenir plusieurs suffixes DNS. Les suffixes de la liste doivent être séparés par une virgule, sans espace.
Balises du réseau de confiance	Ce paramètre définit la liste des URL des serveurs de confiance à utiliser (par exemple, www.serveur.com). Le Client VPN va chercher à se connecter successivement via https à la page /index.html des serveurs de la liste (par exemple, https://www.serveur.com/index.html), jusqu'à en trouver un accessible et dont le certificat est valide. La liste des serveurs peut être vide : le Client VPN en reste alors à la liste des suffixes DNS pour déterminer si le poste est connecté au réseau de confiance ou pas.
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 tous les serveurs. 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.

21.3 Scripts

Le Panneau TrustedConnect exécute les scripts liés à l'ouverture et à la fermeture d'un tunnel. Pour configurer cette fonctionnalité, se reporter au chapitre 15 Automatisation.

21.4 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).
Ces configurations doivent être effectuées dans les propriétés de l'installeur du Client VPN.
☞ Se reporter au « Guide de déploiement » pour les instructions correspondantes.

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

21.5 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 dans les propriétés de l'installeur du Client VPN.
☞ Se reporter au « Guide de déploiement » pour les instructions correspondantes.

21.6 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.

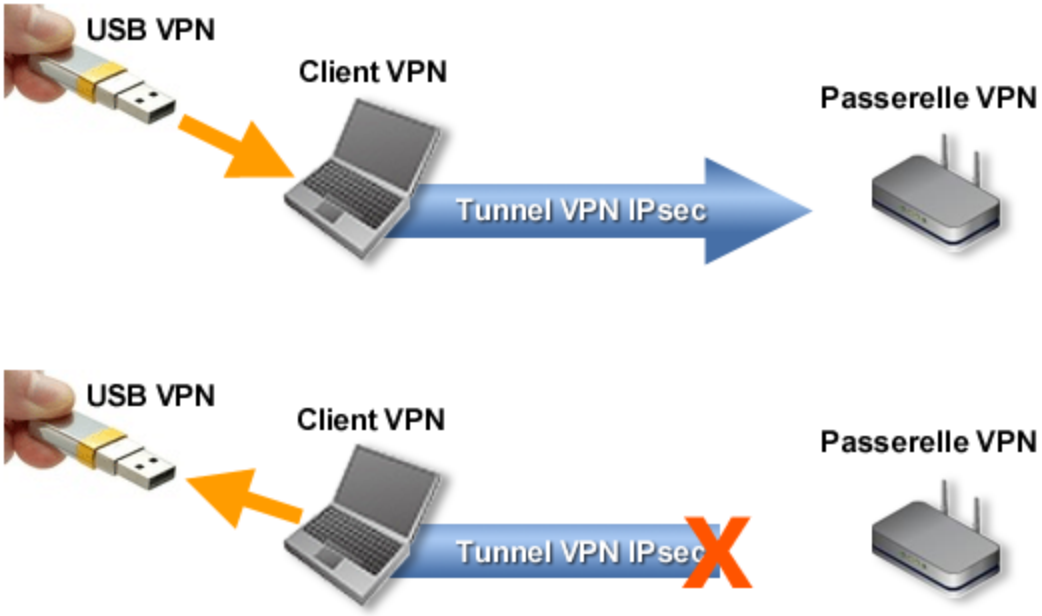
Cette configuration doit être effectuée dans les propriétés de l'installeur du Client VPN.
☞ Se reporter au « Guide de déploiement » pour les instructions correspondantes.

22 Mode USB

22.1 Présentation

Le Client VPN Windows Enterprise offre un mode de gestion d'une connexion VPN inédit : le Mode USB.

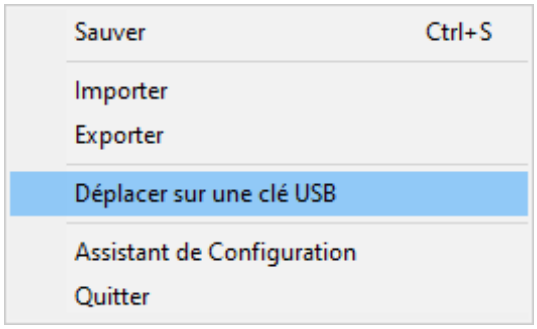
Dans ce mode, la configuration VPN est stockée de façon sécurisée sur support amovible (clé USB), le poste à partir duquel la connexion VPN est ouverte est vierge de tout élément de sécurité VPN, la connexion VPN s'établit automatiquement dès insertion de la clé USB et se ferme dès extraction de la clé USB.



Dans la suite du document, la clé USB contenant la configuration VPN est appelée « clé USB VPN ».

22.2 Configurer le Mode USB

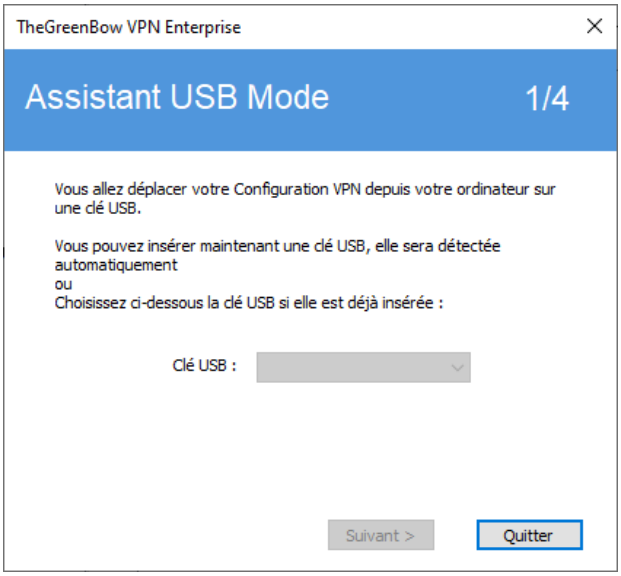
La configuration du Mode USB s'effectue via l'assistant de configuration accessible par le menu « Configuration > Déplacer sur une clé USB » du Panneau de Configuration.



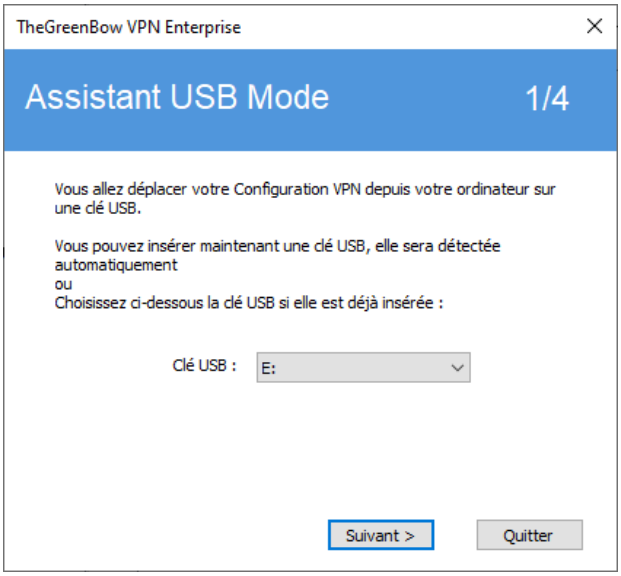
Étape 1 : Choix de la clé USB

L'écran 1 permet de choisir le support amovible (clé USB) sur lequel protéger la configuration VPN.
Si une clé est déjà insérée, elle est automatiquement présentée dans la liste des clés USB disponibles.
Sinon, il suffit d'insérer à cette étape la clé USB choisie, qui sera détectée automatiquement à l'insertion.

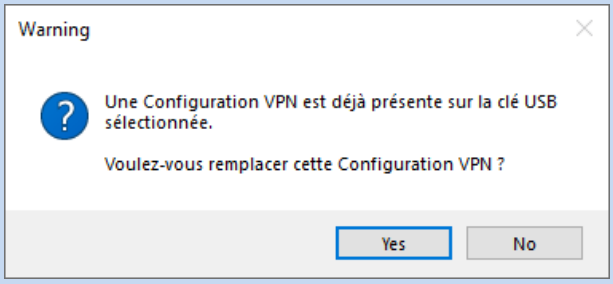
Pas de clé USB insérée



Clé USB déjà insérée



Le mode USB n'autorise la protection que d'une seule configuration VPN sur une clé USB. Si une configuration VPN est déjà présente sur la clé USB insérée, le message d'alerte suivant est affiché :



Lorsqu'une clé USB vierge est insérée et qu'elle est la seule à être insérée sur le poste, l'assistant passe automatiquement à l'étape 2.

Étape 2 : Protection de la configuration VPN en mode USB

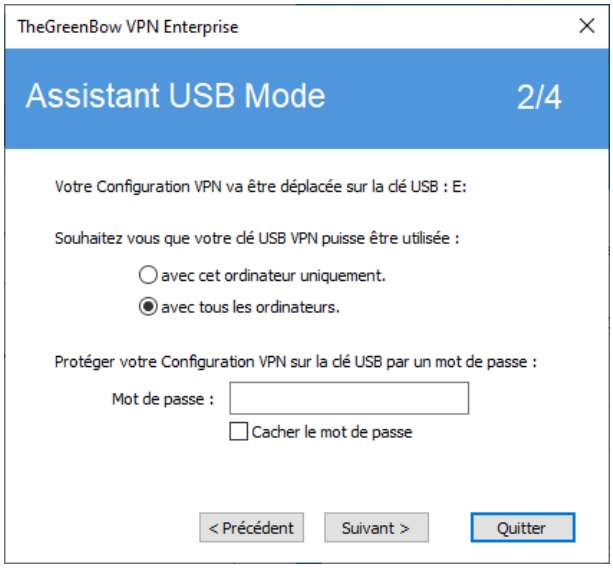
Deux protections sont proposées :

1/ Affiliation au poste de l'utilisateur :

La configuration VPN USB peut être associée de façon unique au poste duquel elle est issue.
Dans ce cas, la clé USB VPN ne pourra être utilisée que sur ce poste.
Dans le cas contraire (la clé USB n'est pas associée à un poste en particulier), la clé USB VPN pourra être utilisée sur n'importe quel poste, équipé du Client VPN.

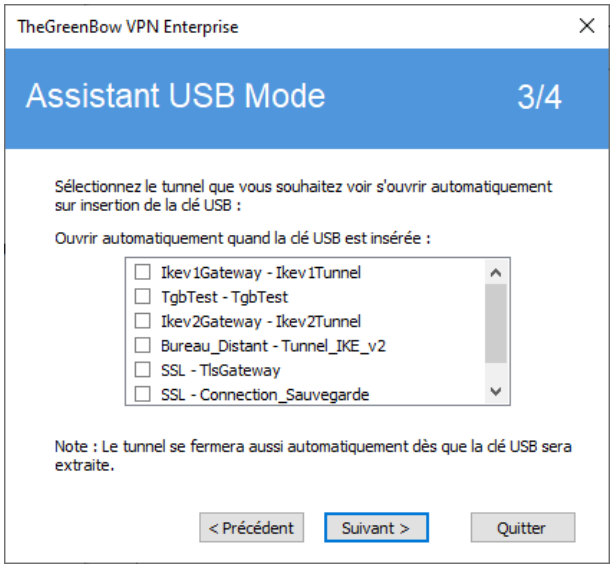
2/ Protection par mot de passe :

La configuration VPN USB peut être protégée par mot de passe.
Dans ce cas, le mot de passe est demandé à chaque insertion de la clé USB VPN.



Étape 3 : Ouverture automatique du tunnel

L'assistant permet de configurer les connexions VPN qui seront automatiquement ouvertes à chaque insertion de la clé USB VPN.



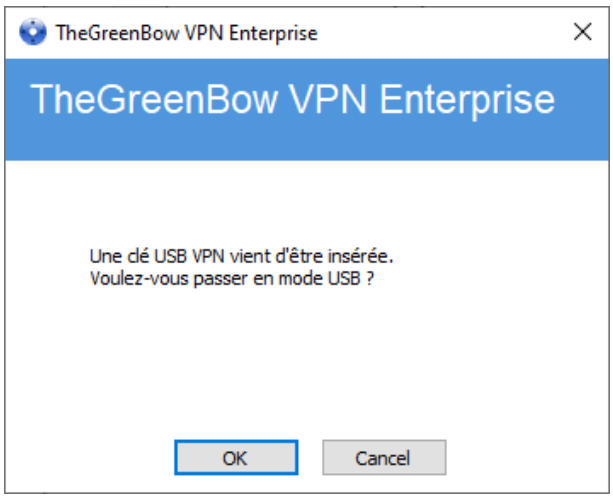
Étape 4 : Résumé

Le résumé permet de valider le bon paramétrage de la clé USB VPN.

Sur validation de cette dernière étape, la configuration VPN du poste est transférée sur la Clé USB.
Elle reste active tant que la Clé USB reste insérée. Sur extraction de la clé USB VPN, le Client VPN revient à une configuration VPN vide.

22.3 Utiliser le Mode USB

Lorsque le Client VPN Windows Enterprise est lancé, avec une configuration VPN chargée ou pas, insérez la clé USB VPN. La fenêtre d'information suivante est automatiquement affichée :



Sur validation, la configuration VPN USB est automatiquement chargée, et, le cas échéant, le(s) tunnel(s) automatiquement ouvert(s). Le mode USB est identifié dans le Panneau de Configuration, par une icône « Mode USB » en haut à droite de l'arborescence :

Sur extraction de la clé USB VPN, les connexions VPN en mode USB sont fermées. La configuration VPN transportée par la clé USB est extraite du poste. (Si une configuration VPN était présente sur le poste avant insertion de la clé USB, elle est restaurée dans le logiciel).

Le Client VPN Windows Enterprise ne prend en compte qu'une seule clé USB VPN à la fois. Tant qu'une clé USB VPN est insérée, l'insertion d'autres clés USB VPN n'est pas prise en compte.

La fonction d'importation est désactivée en Mode USB.

En Mode USB, la configuration VPN peut être modifiée. Les modifications apportées à la configuration VPN sont sauvegardées sur la clé USB VPN.

Le Client VPN ne propose pas d'option directe pour modifier le mot de passe et l'affiliation ou non à un poste.

Pour les modifier, suivez la procédure ci-dessous :

1/ Insérez la clé USB VPN.
2/ Exportez la configuration VPN.
3/ Retirez la clé USB VPN.
4/ Importez la configuration VPN exportée à l'étape 2.
5/ Relancez l'assistant mode USB avec cette configuration et les nouveaux paramètres souhaités.

23 Mode GINA

23.1 Présentation

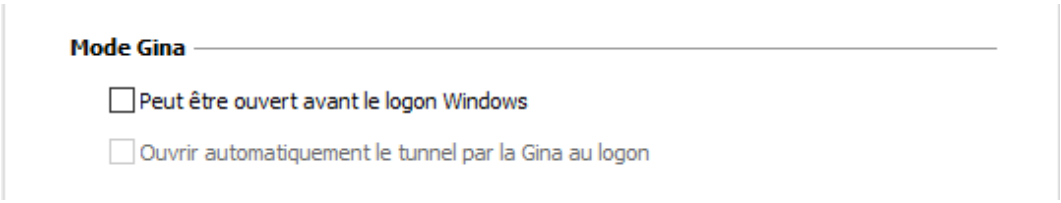
Le mode GINA permet d'ouvrir des connexions VPN avant l'ouverture d'une session Windows.
Cette fonction permet par exemple d'établir une connexion sécurisée vers un serveur de gestion des droits d'accès de façon à obtenir les droits d'accès au poste utilisateur avant l'ouverture de la session utilisateur.

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 24.2 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.
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.

23.2 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 15 Automatisation.



23.3 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 ou au token).

⚠ Si deux tunnels sont configurés en mode GINA, et l'un d'eux en ouverture automatique, il se peut que les deux tunnels s'ouvrent automatiquement.

ℹ 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.

⚠ Limitation : Les scripts et mode USB ne sont pas disponibles pour les tunnels VPN en mode GINA.

⚠ Un tunnel VPN configuré avec un certificat mémorisé dans le magasin de certificats utilisateur 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.

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.

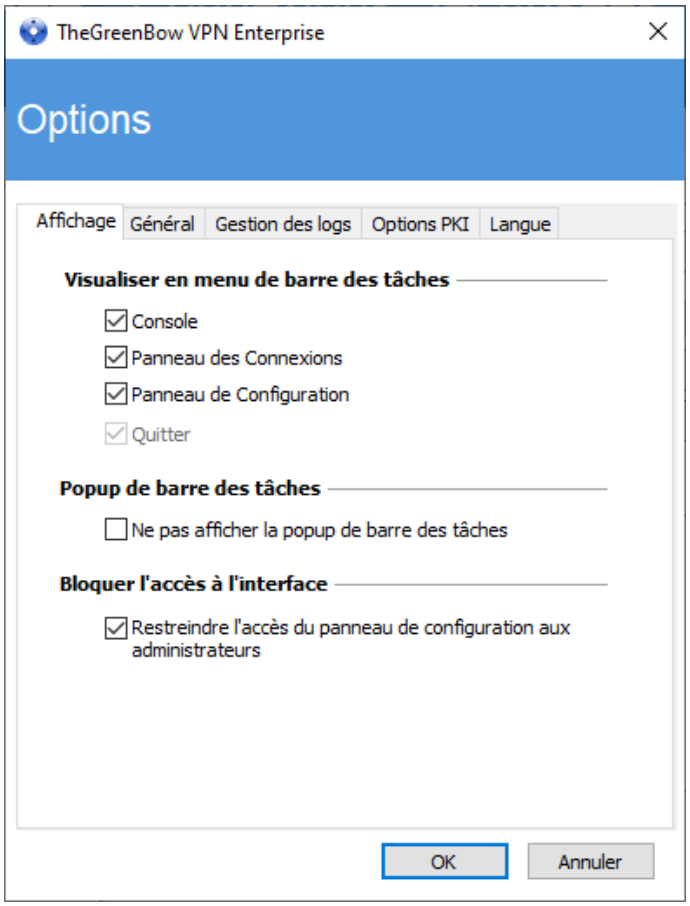
24 Options

24.1 Affichage de l'interface (masquage)

Les options de l'onglet « Affichage » de la fenêtre « Options » permettent de masquer toutes les interfaces du logiciel, en enlevant du menu en barre des tâches les options « Console », « Panneau de Configuration » et « Panneau des Connexions ». Le menu en barre des tâches peut ainsi se réduire à l'option « Quitter ».

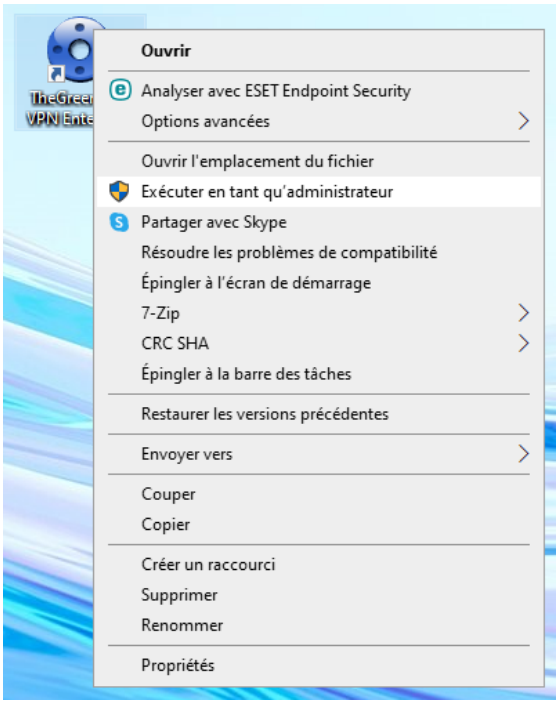
L'option « Quitter » du menu en barre des tâches ne peut être supprimée à partir du logiciel. Elle peut toutefois être supprimée en utilisant les options d'installation (cf. « Guide de déploiement »).

La fenêtre popup d'ouverture et de fermeture du tunnel peut aussi être masquée (option « Ne pas afficher la popup de barre des tâches »).

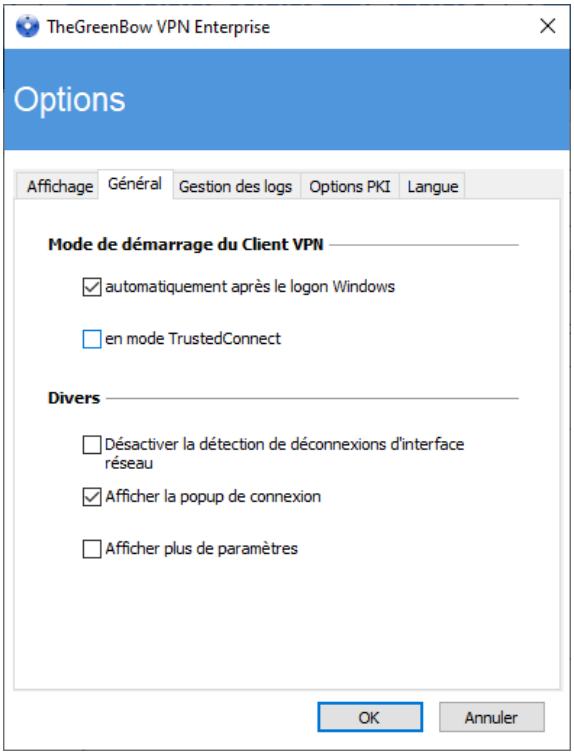


Dans le Client VPN Windows Enterprise, l'interface du Panneau de Configuration est par défaut restreinte aux administrateurs. Pour rendre le panneau de configuration accessible aux utilisateurs, décochez l'option « Restreindre l'accès du panneau de configuration aux administrateurs ».

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



24.2 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 » Windows.
☞ Se reporter à la section 6.2 Démarrer le logiciel.

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 assure une meilleure stabilité du tunnel VPN sur des réseaux physiques peu fiables, typiquement les réseaux satellite.

En mode TrustedConnect, il n'est pas recommandé de cocher cette option.

Afficher la popup de connexion

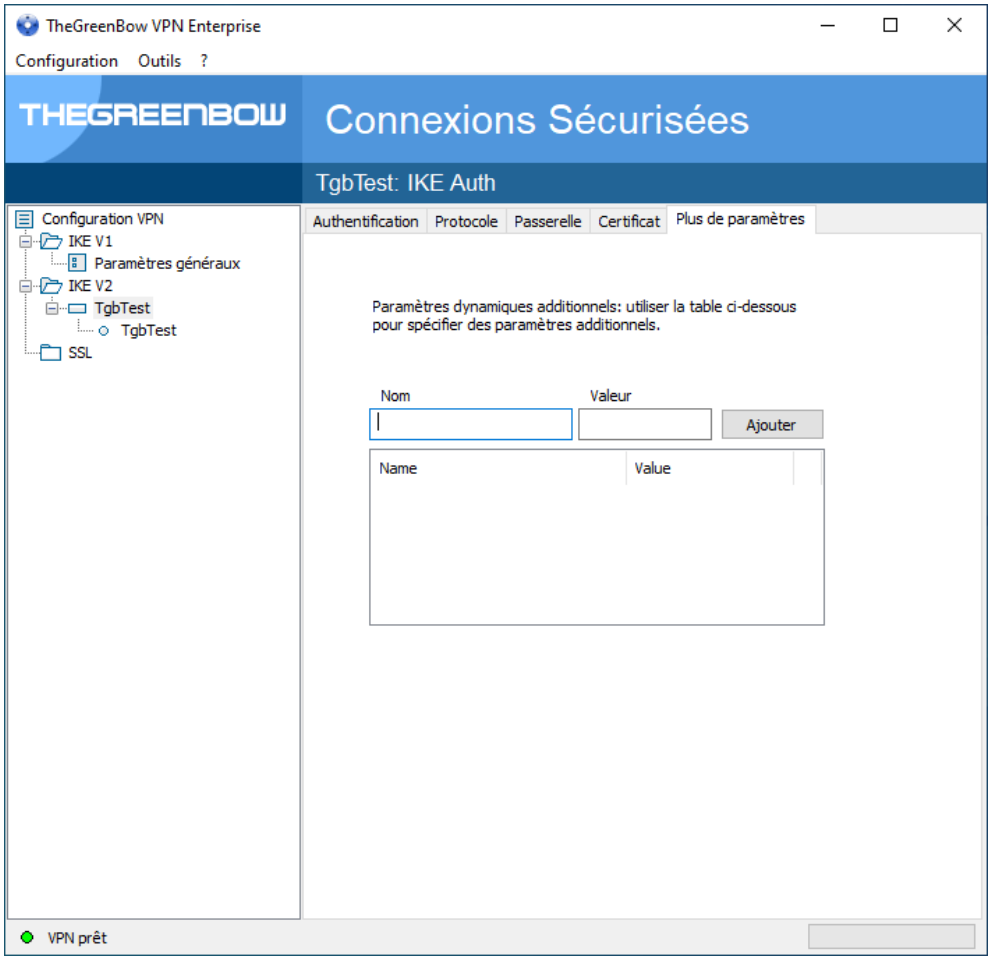
Une fenêtre de connexion est automatiquement affichée à chaque connexion VPN établie.
Il est possible ici de désactiver l'affichage de cette fenêtre en décochant la case « Afficher la popup de connexion ».

Afficher plus de paramètres

Le Client VPN Windows Enterprise permet si besoin de configurer des paramètres additionnels, qui ne sont pas documentés dans le présent document.

Dans certaines circonstances, le support TheGreenBow peut vous proposer d'ajouter des paramètres (Nom, Valeur) 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, cocher l'option « Afficher plus de paramètres ».



24.3 Gestion des logs

Se reporter à la section 25.1 Logs administrateur.

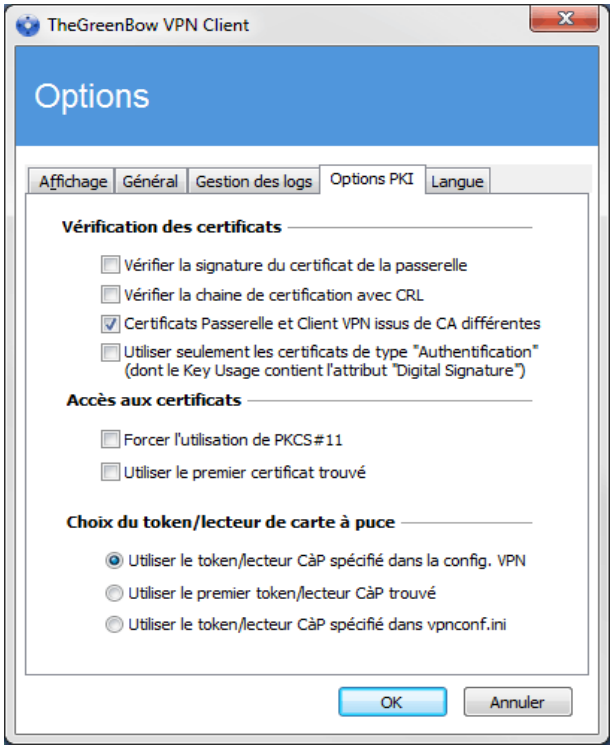
24.4 Options PKI

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.

Dans le cadre du déploiement du logiciel, toutes ces options peuvent être préconfigurées au cours de l'installation du logiciel Client VPN Windows Enterprise. 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. Point de sécurité : 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, la CRL (Certificate Revocation List) du certificat de la passerelle VPN est vérifiée, 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.
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 la valeur « 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 `KEYUSAGE` est définie sur la valeur 2 ou 3 lors de l'installation (cf. « Guide de déploiement »).

Cette option permet de configurer globalement la caractérisation des certificats pour l'ensemble des tunnels du Client VPN. Pour caractériser de façon distincte les certificats de chaque tunnel, il convient d'utiliser les paramètres dynamiques décrits dans la section 18.1 Sélectionner un certificat (onglet « Certificat »).

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.

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.

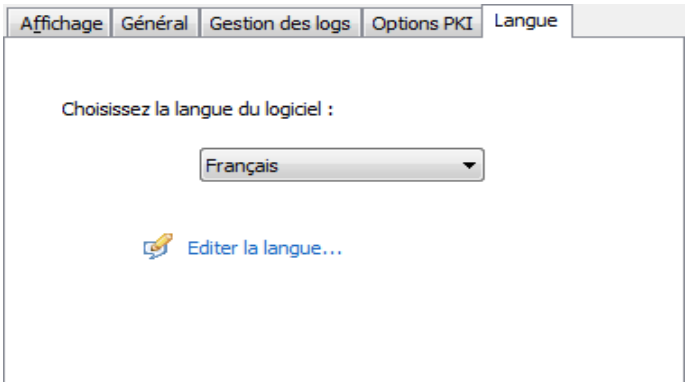
Voir le « Guide de déploiement ».

24.5 Gestion des langues

24.5.1 Choix d'une langue

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

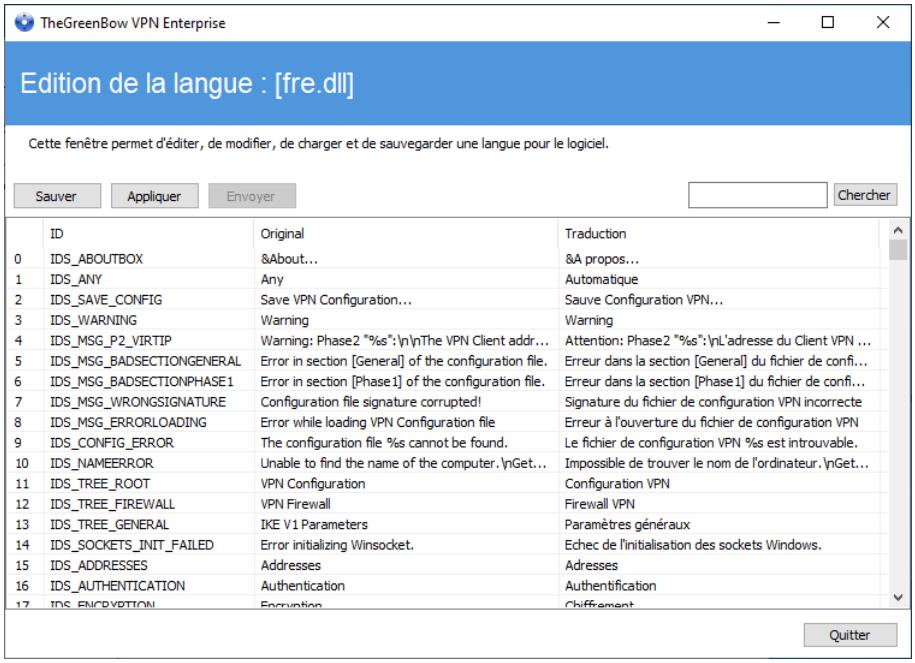
Pour choisir une autre langue, ouvrez le menu « Outils > Options », puis sélectionnez l'onglet « Langue ».
Choisissez la langue souhaitée dans la liste déroulante proposée :



La liste des langues disponibles en standard dans le logiciel est donnée en annexe à la section 27.4 Caractéristiques techniques du Client VPN Windows Enterprise.

24.5.2 Modification ou création d'une langue

Le Client VPN Windows Enterprise 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 est affichée :



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 :

1/ De traduire chaque chaîne de caractère en cliquant sur la ligne correspondante
2/ 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)
3/ De sauvegarder les modifications (bouton « Sauver »).

Toute langue modifiée ou créée est sauvegardée dans un fichier « .lng ».

4/ D'appliquer immédiatement une modification au logiciel : cette fonction permet de valider en temps réel la pertinence d'une chaîne de caractère ainsi que son bon affichage (bouton « Appliquer »).
5/ D'envoyer à TheGreenBow une nouvelle traduction (bouton « Envoyer »).

Le nom du fichier de langue en cours d'édition est rappelé dans l'entête de la fenêtre de traduction.

Toute traduction envoyée à TheGreenBow est publiée, après vérification, sur le site TheGreenBow, puis intégrée dans le logiciel, en général dans la version officielle publiée, suivant la réception de la traduction.

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.

25 Logs administrateur, console et traces

Le Client VPN Windows Enterprise 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 TheGreenBow pour le diagnostic d'incident logiciels.

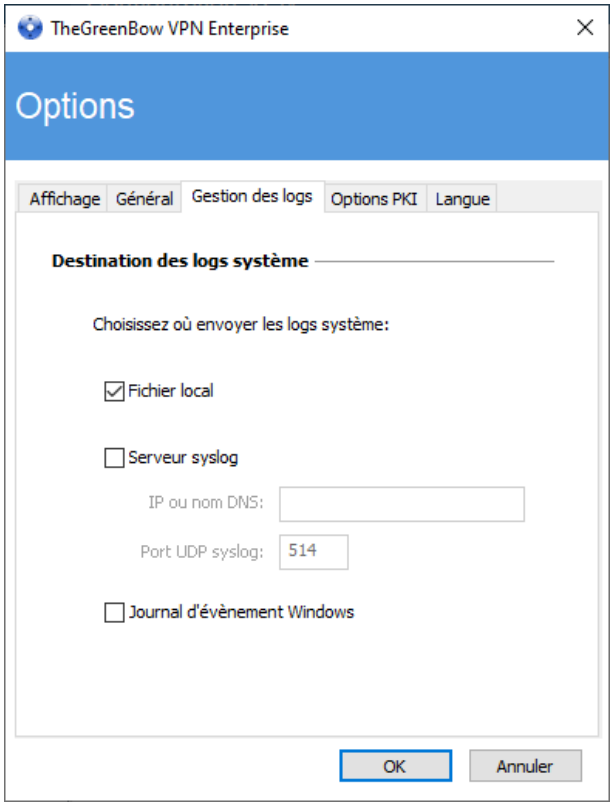
25.1 Logs administrateur

Le Client VPN Windows Enterprise 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.

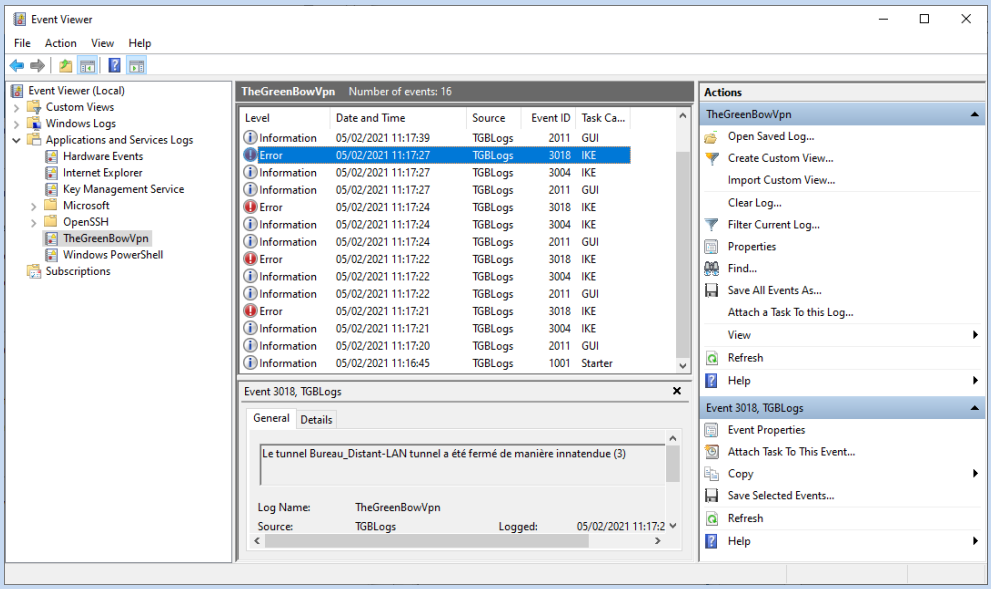
Les logs collectés peuvent être au choix et/ou simultanément :

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

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



Le chemin d'accès aux logs du Client VPN Windows Enterprise dans le gestionnaire d'évènements Windows (Event Viewer) est le suivant :



Les logs administrateur sont listés à la section 27.2 Logs administrateur dans les annexes.

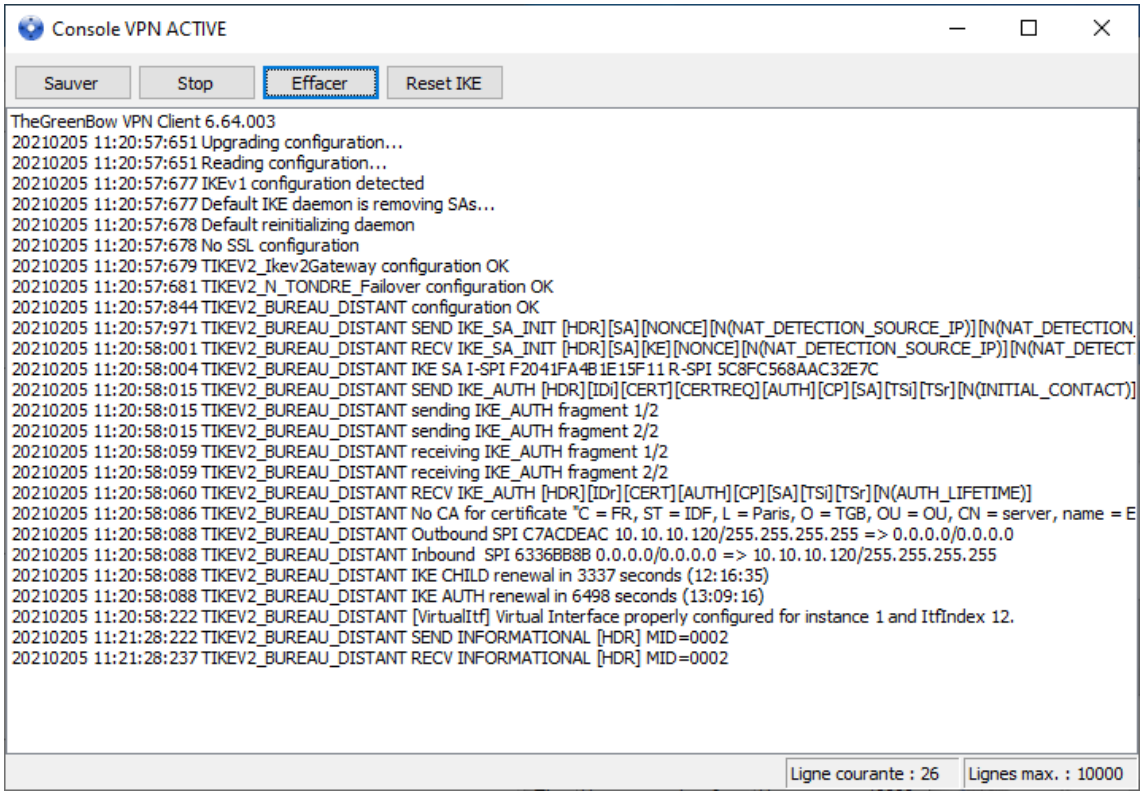
Lorsque les logs administrateur sont stockés dans un fichier local, le chemin de ces logs est le sous-répertoire « System » du répertoire des logs : « C:\ProgramData\TheGreenBow\TheGreenBow VPN\LogFiles\System ».

Ce répertoire peut être lu dans tous les modes, mais n'est accessible en écriture qu'en mode Administrateur.

25.2 Console

La Console peut être affichée par les moyens suivants :

- menu « Outils > Console » du Panneau de Configuration (interface principale) ;
- 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.

25.3 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 du Client VPN Windows Enterprise génère les logs de son activité. Les logs générés sont mémorisés dans un dossier accessible en cliquant sur l'icône « Dossier » bleu dans la barre d'état du Panneau de Configuration (interface principale).

L'activation des logs 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 logs traçants sont conservés 10 jours. Au-delà de cette période, le logiciel purge automatiquement les fichiers.

Lorsqu'ils sont mémorisés dans un fichier local, les logs « administrateur » ne sont pas purgés.

26 Recommandations de sécurité

26.1 Hypothèses

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

1/ 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.
2/ 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.
3/ 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.
4/ Le poste de l'utilisateur est sain et correctement administré. Il dispose d'un anti-virus à jour et est protégé par un pare-feu.
5/ 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].
6/ La fonction de journalisation du produit est activée et correctement configurée. Les administrateurs sont responsables de la consultation régulière des journaux.

26.2 Poste de l'utilisateur

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

1/ elle dispose d'un anti-virus dont la base de données est régulièrement mise à jour ;
2/ 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 ;
3/ son système d'exploitation est à jour des différents correctifs ;
4/ 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

26.3 Administration du Client VPN

Le Client VPN Windows Enterprise 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 du Client VPN Windows Enterprise), comme détaillé à la section 24.1 Affichage de l'interface (masquage).

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 le Client VPN Windows Enterprise 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).

26.4 Configuration VPN

26.4.1 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 :

1/ Ne pas utiliser le mode EAP (mot de passe / login) seul, mais uniquement en combinaison avec un certificat.
2/ 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 13.4.1 IKE Auth : IKE SA, paragraphe Authentification).
3/ Ne pas importer de certificat dans la configuration VPN (fonction décrite à la section 18.3 Importer un certificat), et privilégier l'utilisation de certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows.
4/ Ne pas utiliser le mode « Clé partagée » (fonction décrite à la section 13.4.1 IKE Auth : IKE SA) et privilégier le mode « Certificat » avec des certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows.
5/ Ne pas exporter la configuration VPN en clair, c'est-à-dire non protégée par un mot de passe (fonction décrite à la section 12.2 Exporter une configuration VPN).

26.4.2 Authentification de l'utilisateur

Les fonctions d'authentification de l'utilisateur proposées par le Client VPN Windows Enterprise 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

26.4.3 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 24.4 Options PKI.

26.4.4 Protocole

Il est recommandé de ne configurer que des tunnels IKEv2.

26.4.5 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.

☞ Se reporter au paragraphe Configuration du Type d'adresse de la section 13.4.6 Child SA : Child SA et au paragraphe Autres de la section 13.4.7 Child SA : Avancé.

26.4.6 Mode GINA

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

26.4.7 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.

27 Annexes

27.1 Raccourcis

Panneau des Connexions

- ESC Ferme la fenêtre.
- CTRL+ENTER 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 du Panneau de Configuration

- 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 une phase 2 est sélectionnée, ouvre le tunnel VPN correspondant.
- CTRL+W Si une phase 2 est sélectionnée, 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 une nouvelle phase 1, si la configuration VPN est sélectionnée, ou crée une nouvelle phase 2 pour la phase 1 sélectionnée.
- CTRL+S Sauvegarde la configuration VPN.

Panneau de Configuration

- CTRL+ENTER 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.

27.2 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_PWDSET	2004	Info	Admin password has been changed.
LOGID_PWDCHECK	2005	Error/Info	Admin password has been verified (status %d).
LOGID_PWDRESET	2006	Warning	Admin password has been reset.
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.
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.
LOGID_TUNNELDATA_UL	3020	Info	%d bytes sent inside the tunnel.
LOGID_TUNNELDATA_DL	3021	Info	%d bytes received inside the tunnel.

27.3 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.
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 à support@thegreenbow.com 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 (se reporter 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 (se reporter 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 poste) distant(e). **Attention** : le Remote ID sur le routeur est le Local ID sur le Client VPN et inversement !

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 à support@thegreenbow.com en joignant l'ensemble des fichiers de log.
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 à support@thegreenbow.com 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 à support@thegreenbow.com 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 à support@thegreenbow.com 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.
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 à support@thegreenbow.com 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.

27.4 Caractéristiques techniques du Client VPN Windows Enterprise

Général

Version Windows	Windows 10 & 11, 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
Mode USB	Plus aucune configuration VPN sur le poste Ouverture du tunnel sur insertion d'une clé USB configurée VPN Fermeture automatique du tunnel sur extraction de la clé USB configurée VPN
Gina	Ouverture d'un tunnel avant le logon Windows par : GINA / Credential providers sur Windows 10 & 11
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
Media	Ethernet, DSL, câble, Wi-Fi, 4G, 5G, satellite

Protocoles	IPsec IKEv1 ou IKEv2 (IKE basé sur OpenBSD 3.1 (ISAKMPD)) SSL Diffie-Hellmann DH groupe 14 à 21
Modes	Main mode (mode principal) et Aggressive mode (mode agressif)
Mode Config / Mode CP	Récupération automatique des paramètres réseaux depuis la passerelle VPN

Cryptographie

Chiffrement	Symétrique : AES CBC/CTR/GCM 128/192/256bits Asymétrique : RSA Diffie-Hellman : DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521) Hash: SHA2-256, SHA2-384, SHA2-512
Authentification	Administrateur : Protection de l'accès aux configurations VPN Utilisateur : - X-Auth statique ou dynamique (demande à chaque ouverture du tunnel) - Hybrid Authentication - Pre-shared key - EAP (MSCHAP-V2) - Multiple Auth
IGC / PKI	- Prise en charge des certificats au format X.509: PKCS#12, PEM - Multi-support : magasin de certificats Windows, carte à puce, token, fichier de configuration - Prise en charge de la CRL (Certificate Revocation List) - 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, CSP (IKEv1 uniquement) et CNG - Vérification des certificats « Client » 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	RFC3706. 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

27.5 Licences tierces

27.5.1 OpenSSL

OpenSSL est distribué sous la licence Apache 2.0 reproduite ci-dessous.

```
                                 Apache License
                           Version 2.0, January 2004
                        https://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.

      "Work" shall mean the work of authorship, whether in Source or
      Object form, made available under the License, as indicated by a
      copyright notice that is included in or attached to the work
      (an example is provided in the Appendix below).

      "Derivative Works" shall mean any work, whether in Source or Object
      form, that is based on (or derived from) the Work and for which the
      editorial revisions, annotations, elaborations, or other modifications
```

represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this

```
      License. However, in accepting such obligations, You may act only
      on Your own behalf and on Your sole responsibility, not on behalf
      of any other Contributor, and only if You agree to indemnify,
      defend, and hold each Contributor harmless for any liability
      incurred by, or claims asserted against, such Contributor by reason
      of your accepting any such warranty or additional liability.

   END OF TERMS AND CONDITIONS
```

27.5.2 LZ4

Lz4 est distribué sous la licence BSD simplifiée reproduite ci-dessous.

```
LZ4 Library
Copyright (c) 2011-2020, Yann Collet
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this
  list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this
  list of conditions and the following disclaimer in the documentation and/or
  other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

28 Contact

28.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur le site :
https://thegreenbow.com/

28.2 Commercial

Contact téléphonique : +33.1.43.12.39.30
Contact mail : sales@thegreenbow.com

28.3 Support

Le site TheGreenBow propose plusieurs pages concernant le support technique des logiciels :

Aide en ligne

https://thegreenbow.com/fr/support/assistance/

FAQ

https://thegreenbow.com/fr/faq/

Formulaire de contact

Le support technique est accessible via un formulaire disponible sur le site TheGreenBow à l'adresse :
https://thegreenbow.com/fr/support/assistance/support-technique/

THEGREENBOW

Vos connexions protégées
en toutes circonstances

14, rue Auber
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com