Trustway IP Protect

# IP PROTECT CLIENT

## Guide Administrateur

# IP Protect Client

## Guide Administrateur

**Mai 2022**

Imprimé en France

Vos suggestions sur la forme, le fond et la présentation de ce manuel sont les bienvenues. Une feuille destinée à recevoir vos remarques se trouve à la fin du présent manuel.

# Table des Matières

# Liste des Figures

Aucune entrée de table d'illustration n'a été trouvée.

# Liste des Tables

Aucune entrée de table d'illustration n'a été trouvée.

# Préface

## Objet du manuel

Ce guide est destiné aux administrateurs IP Protect Client.

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.

## Version du logiciel

La version logicielle minimum correspondant à ce document est **7.0**.

# Chapitre 1. Installation

## 1.1 Introduction

L'installation IP Protect Client s'effectue en exécutant le programme fourni par Trustway.

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 ».

Se reporter à la section 1.2 Procédure d'installation.

### 1.1.1 Conditions d'installation

IP Protect Client fonctionne sur Windows 10 64 bits.

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.

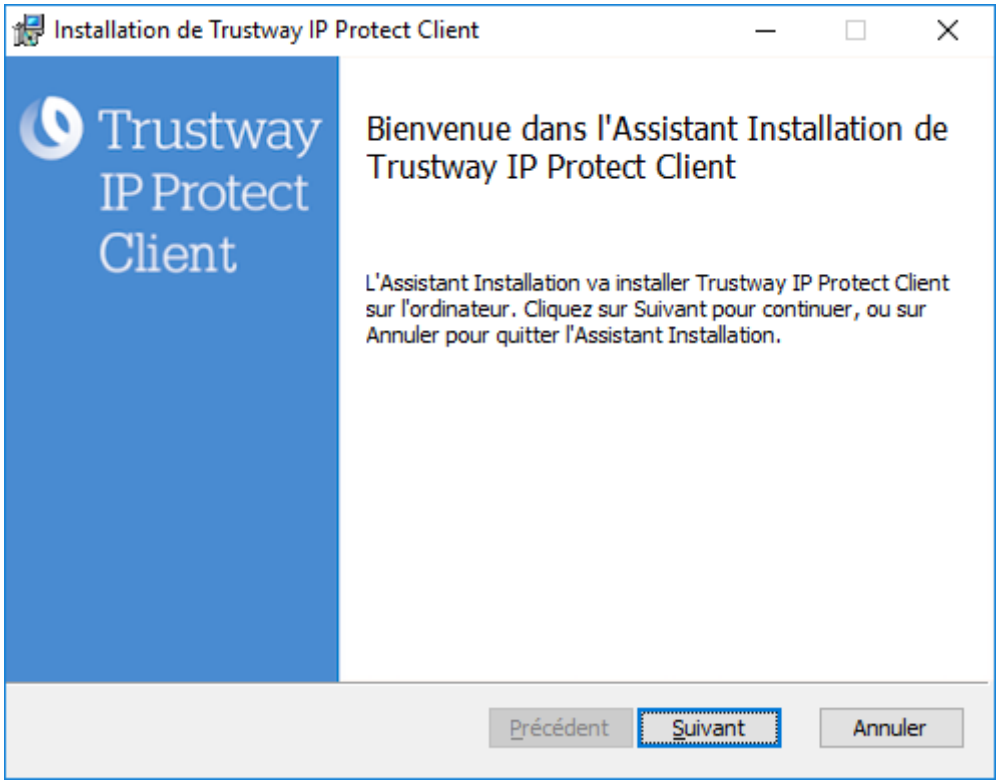
La version IP Protect Client peut être vérifiée par l'utilisateur dans la fenêtre **À propos…** du logiciel.

## 1.2 Procédure d'installation

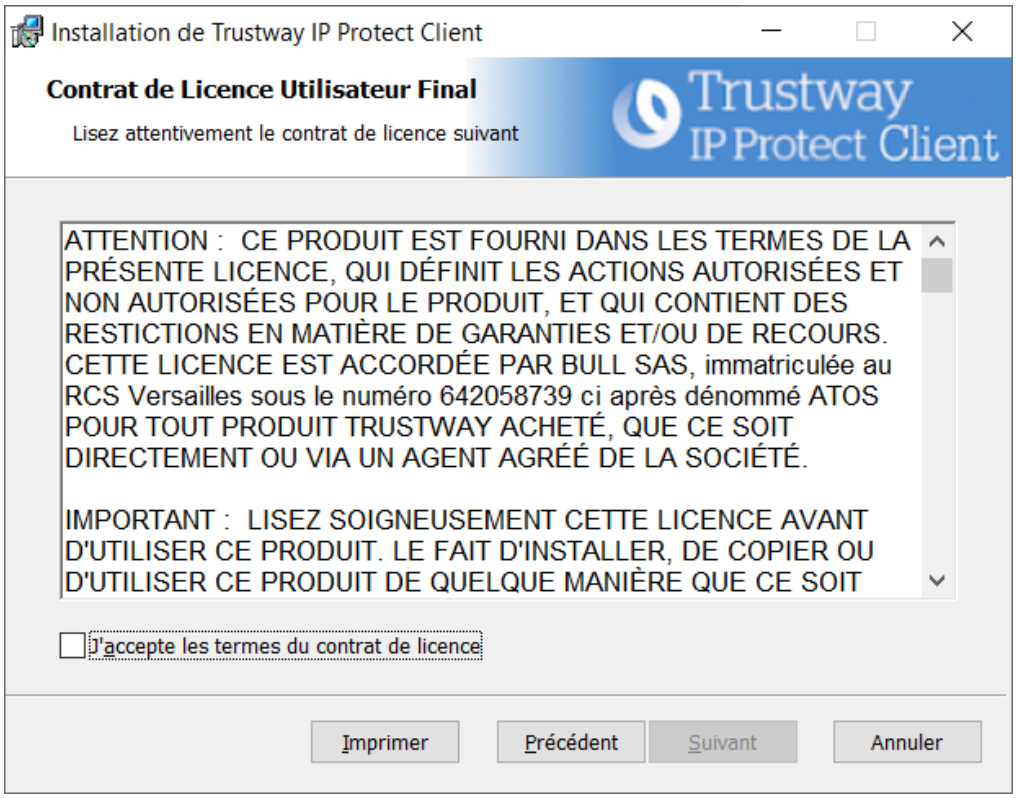
La procédure d'installation est identique qu'il s'agisse d'une première installation ou d'une mise à jour (cf. Chapitre 3 Mise à jour). Lors d'une mise à jour, les paramètres du logiciel, la configuration VPN existante et la licence sont conservés.

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 :

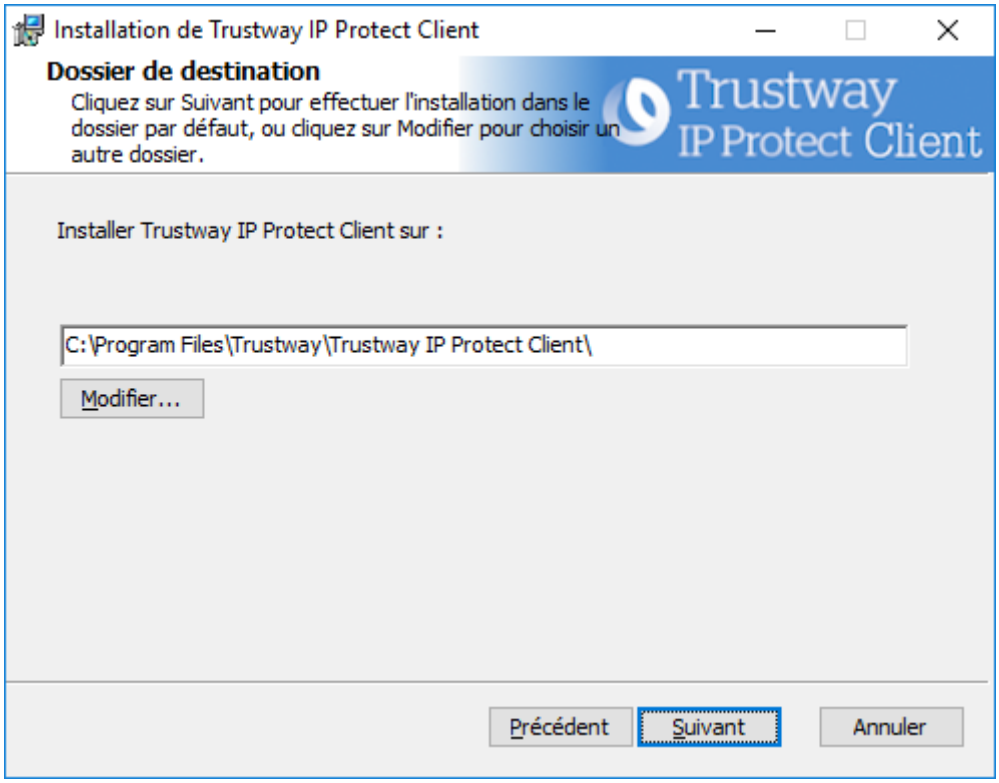



3. Lisez attentivement le Contrat de licence de l'utilisateur final (CLUF). Si vous acceptez tous les termes du contrat, cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**. Dans le cas contraire, vous ne pourrez pas poursuivre l'installation IP Protect Client.

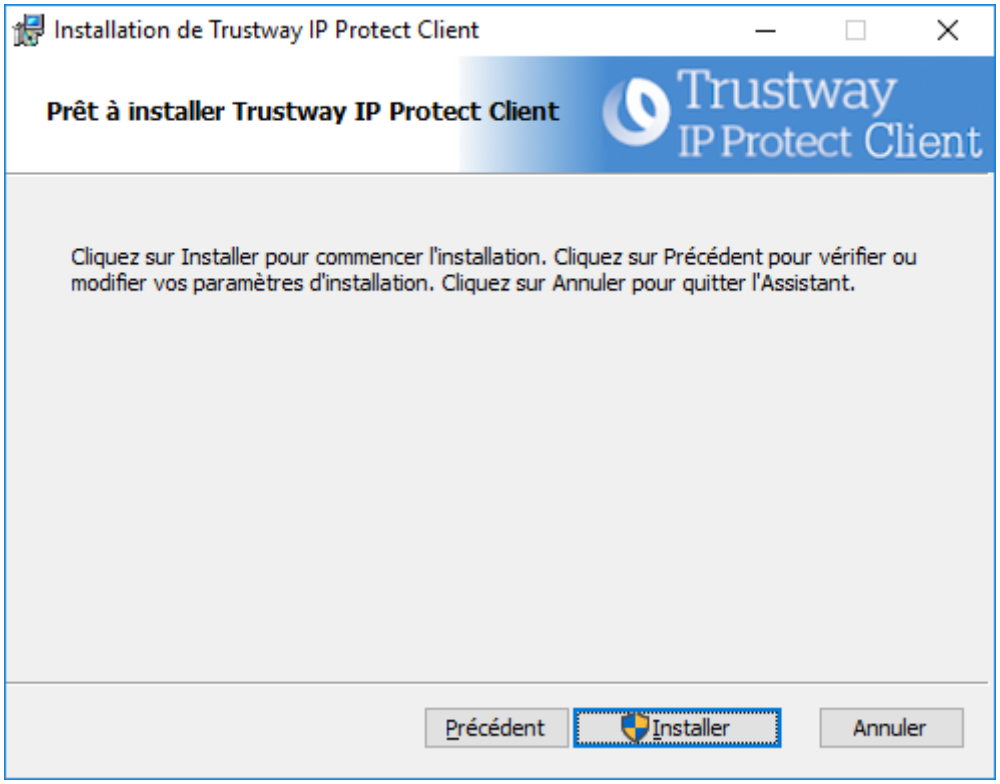
4. Lisez attentivement les informations relatives aux nouveautés et la note de mise à jour concernant la conversion de la configuration VPN existante.

⚠ 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.

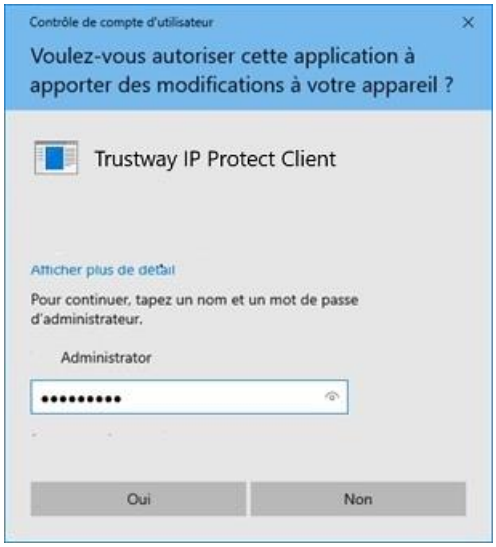
La fenêtre suivante s'affiche :




5. Si vous souhaitez installer IP Protect Client 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 :



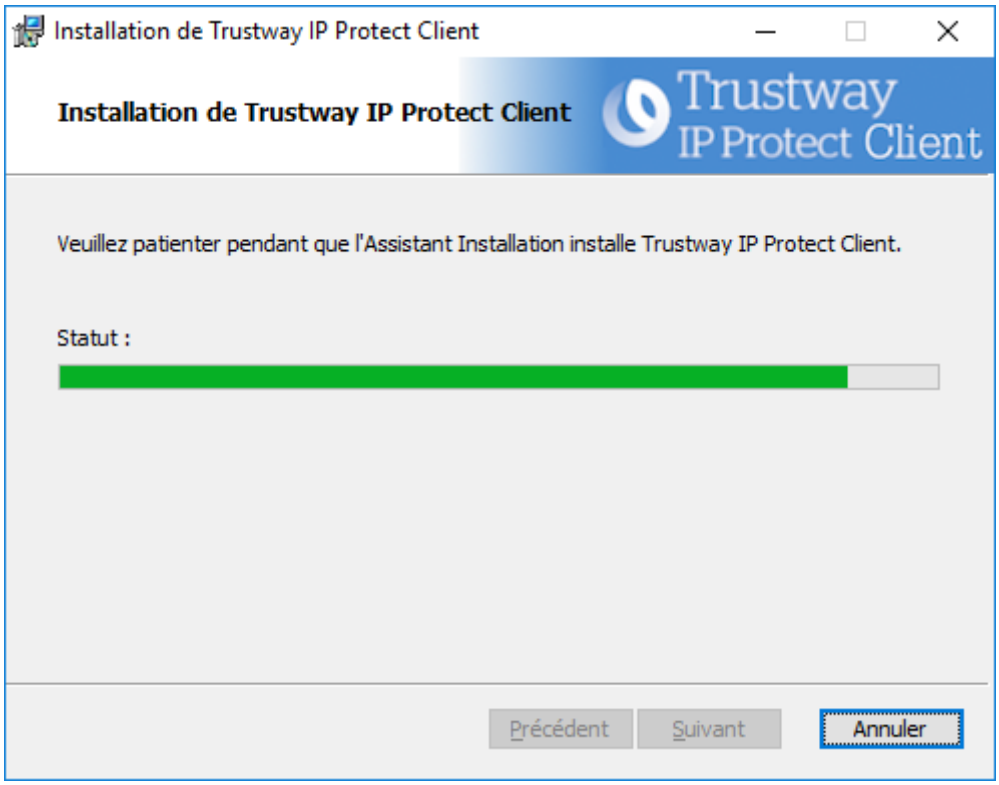

6. Le programme est prêt à installer. Si vous souhaitez revenir en arrière pour vérifier ou modifier vos paramètres d'installation, cliquez sur **Précédent**. Sinon, cliquez sur **Installer**. Si vous effectuez l'installation à partir d'un compte qui ne dispose pas des droits d'administration, la fenêtre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



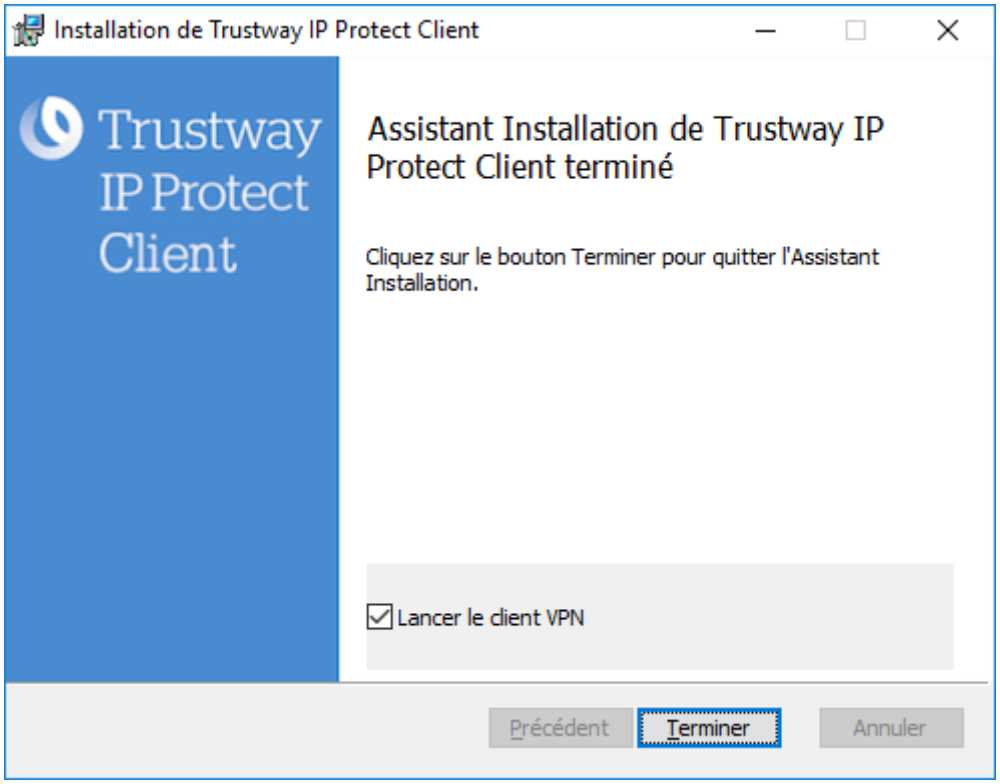

7. Pour poursuivre l'installation, vous devez entrer un nom et mot de passe d'administrateur pour autoriser le programme d'installation d'apporter des modifications à votre ordinateur. Dans le cas contraire, le logiciel ne sera pas installé.

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 :

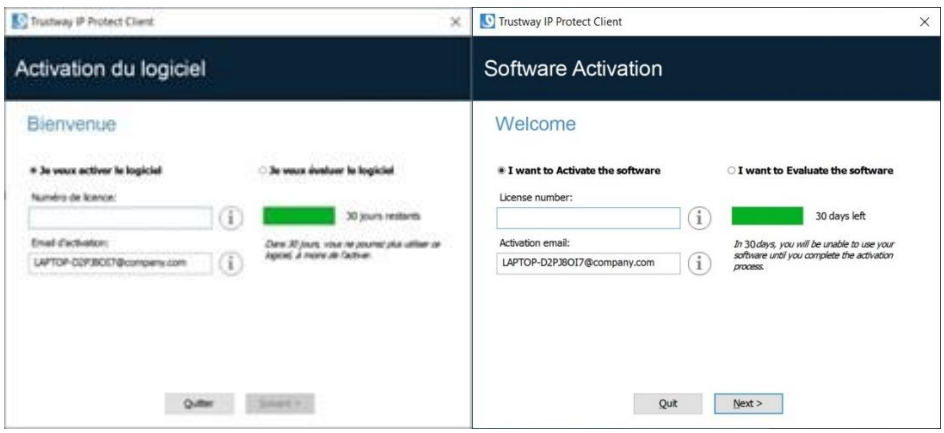



9. Attendez la fin de la l'installation de l'ensemble des composants IP Protect Client. Lorsque l'installation a réussi, la fenêtre suivante s'affiche :




10. Si vous ne souhaitez pas lancer IP Protect Client immédiatement, décochez la case correspondante. Si vous désirez le lancement immédiatement, laisser la case cochée[1]. Pour quitter l'assistant d'installation, cliquez sur **Terminer**.

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




11. IP Protect Client est désormais installé sur votre poste de travail.

[1] Dans le cas d'une mise à jour, si le logiciel a été activé, alors l'écran d'activation n'apparaîtra pas contrairement au cas d'une première installation.

Si vous possédez déjà une licence pour IP Protect Client :

- sélectionnez **Je veux activer le logiciel/I want to Activate the software**,
- entrez le numéro de licence et l'email d'activation,
- puis cliquez sur **Suivant/Next** >.

Pour en savoir davantage sur la procédure d'activation, reportez-vous au Chapitre 2 Activation).

Si vous souhaitez évaluer IP Protect Client :

- sélectionnez **Je veux évaluer le logiciel/I want to Evaluate the software**,
- puis cliquez sur **Suivant/Next >**.

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 1.4 Période d'évaluation.

Si vous n'avez pas de licence et que vous souhaitez en acquérir une, contacter le service commercial Trustway.

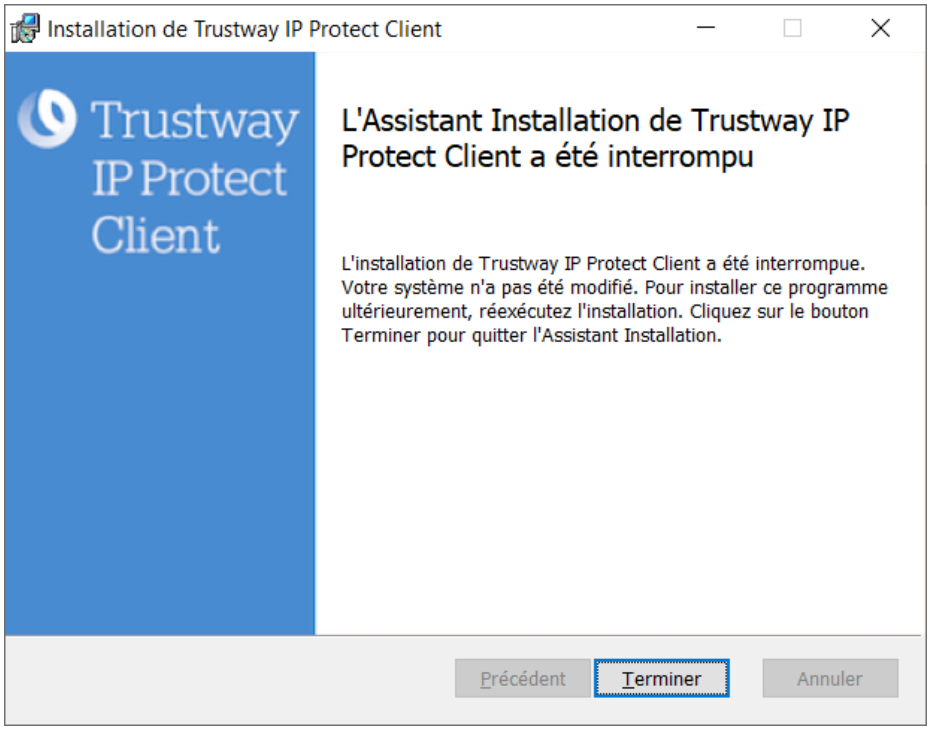
Pour en savoir davantage sur la procédure d'activation, reportez-vous au Chapitre 2 Activation.

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

- Choisir le français comme langue (Cf Chapitre Gestion des langues 23.5).
- Pour commencer à utiliser IP Protect Client immédiatement, reportez-vous au Chapitre 5 Prise en main du logiciel.
- Pour utiliser l'assistant de configuration pour créer une connexion VPN rapidement, reportez-vous au Chapitre 6 Assistant de configuration.
- Pour importer une configuration IP Protect Client compatible avec cette version du logiciel, reportez-vous à la section 11.1 Importer une configuration VPN.
- Pour une présentation détaillée des interfaces disponibles, reportez-vous aux Chapitre 7 Panneau des connexions, Chapitre 8 Panneau de configuration et Chapitre 9 Panneau TrustedConnect.
- Pour une explication complète de l'ensemble des options de configuration d'un tunnel VPN, reportez-vous au Chapitre 12 Configurer un tunnel VPN.
- Pour désinstaller IP Protect Client, reportez-vous au Chapitre 4 Désinstallation.

## 1.3 Interruption de l'installation

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

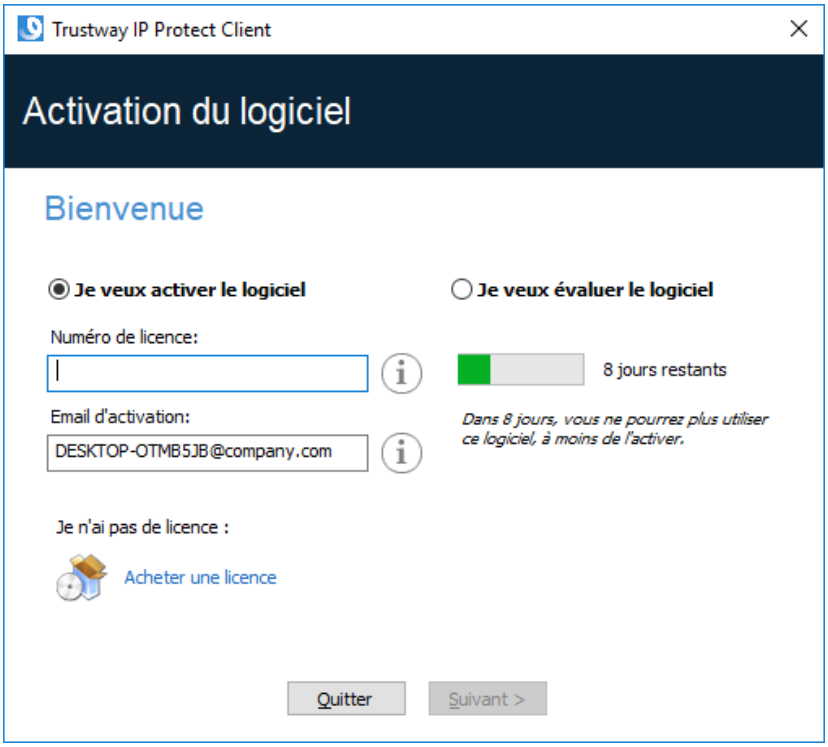



Votre système n'a pas été modifié et vous pouvez reprendre l'installation ultérieurement.

## 1.4 Période d'évaluation

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

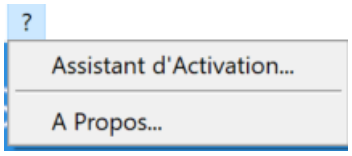
Pendant la période d'évaluation, la fenêtre d'activation est affichée à chaque démarrage du logiciel. Elle indique le nombre de jours d'évaluation restants.




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

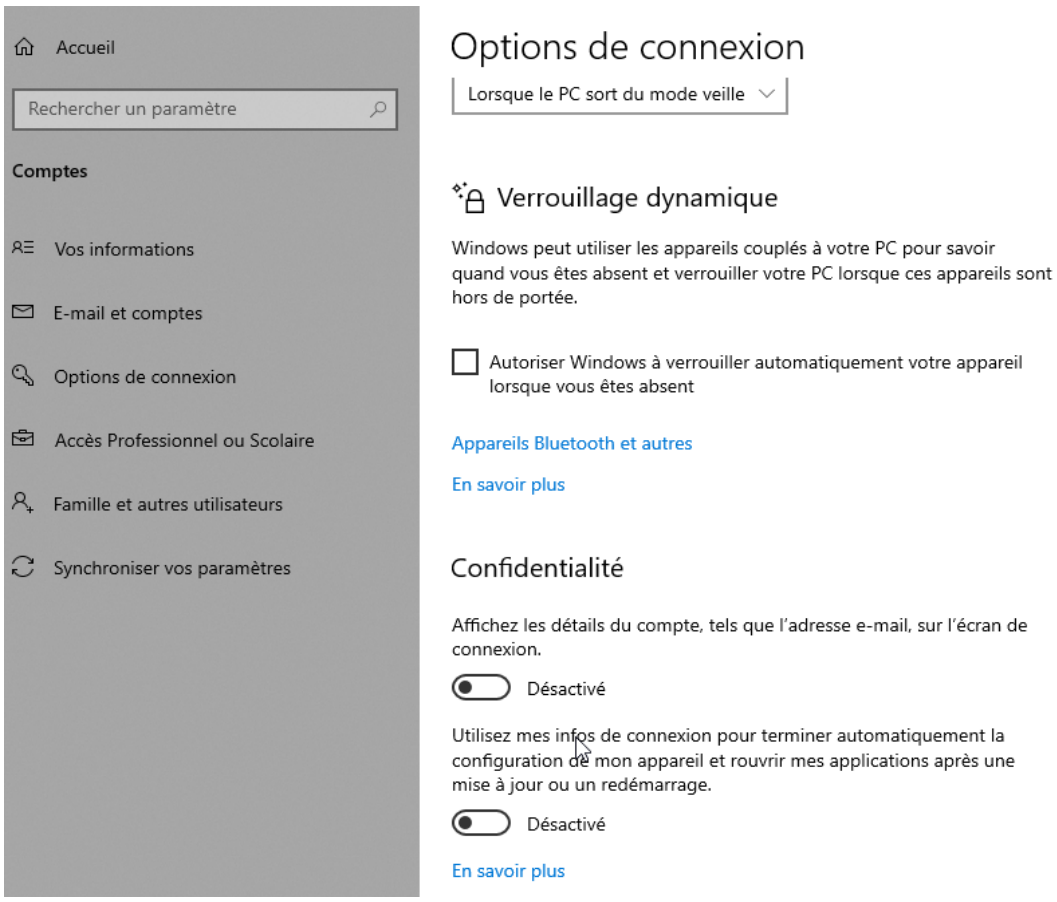
Pendant la période d'évaluation, la fenêtre **À propos…** affiche le nombre de jours d'évaluation restants.


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**).




## 1.5 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 sous les **Options de connexion** dans les **Paramètres** de Windows 10 ci-dessous :



# Chapitre 2. Activation

Si l'activation n'a pas été réalisée lors de l'installation silencieuse – cf. « Guide de Déploiement » – IP Protect Client doit être activé pour fonctionner en dehors de la période d'évaluation.

## 2.1 Étape 1

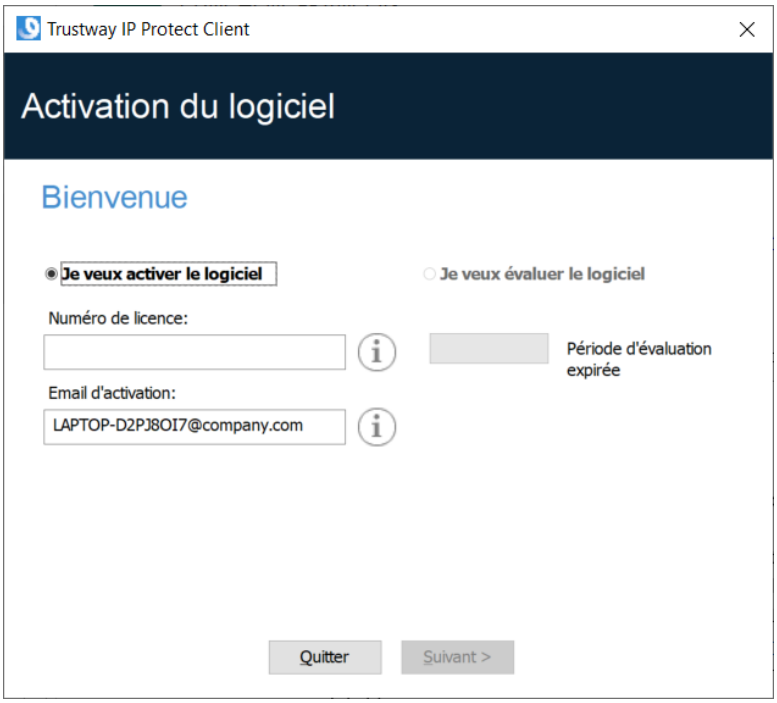
Si vous n'avez pas de licence et que vous souhaitez en acquérir une, contacter le service commercial Trustway.

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.

## 2.2 Étape 2

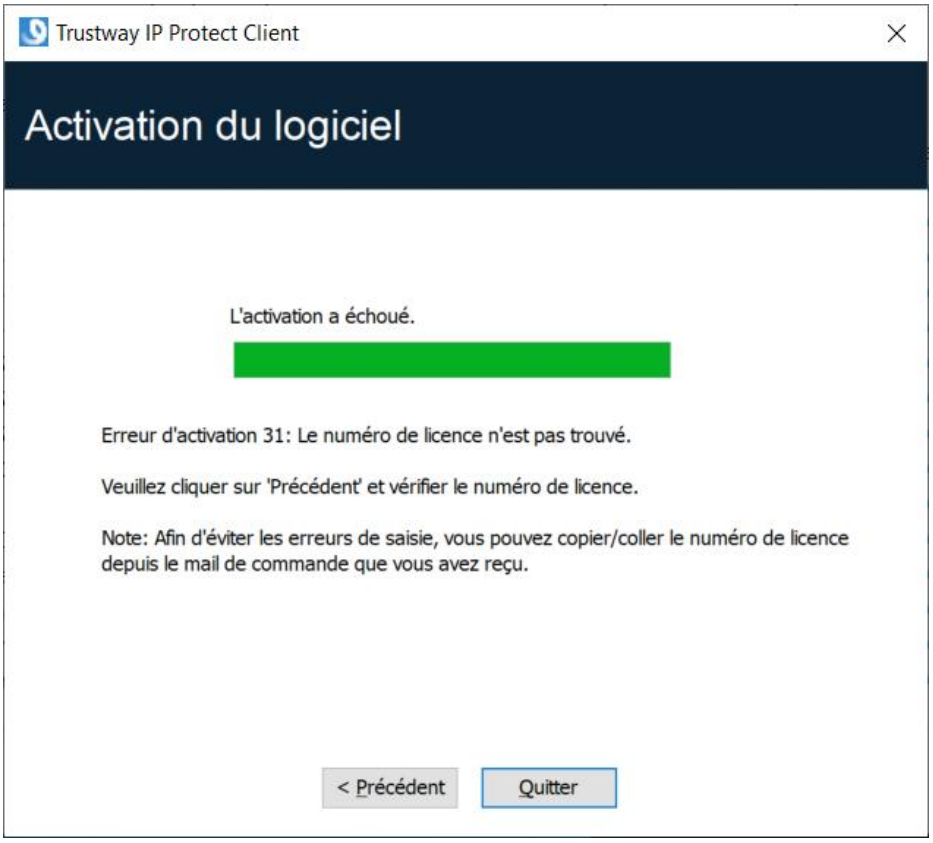
Cliquez sur **Suivant >**, le processus d'activation en ligne s'exécute automatiquement.

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.

## 2.3 Erreurs d'activation

L'activation du logiciel peut ne pas aboutir pour différentes raisons. Chaque erreur est indiquée sur la fenêtre d'activation.

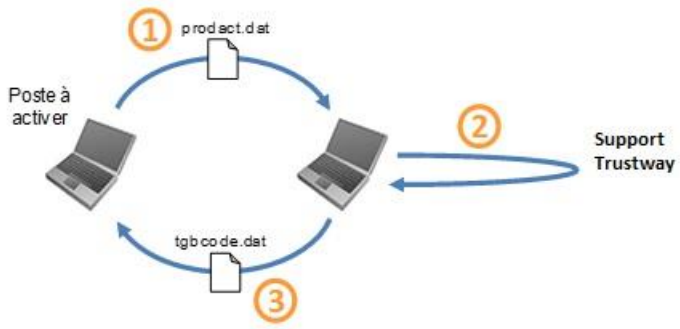



Les erreurs d'activation les plus courantes sont les suivantes :

| 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.<br>Vérifier que la communication n'est pas filtrée par un firewall ou pour un proxy. Le cas échéant, configurer le firewall pour laisser passer la communication, ou le proxy pour la rediriger correctement. |

## 2.4 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. La procédure est la suivante :




| | |
|---|---|
| ① Fichier `prodact.dat` | Sur le poste à activer, récupérer le fichier `prodact.dat` situé dans le répertoire Windows **Documents**.[2] |
| ② ActivationF | Fournir ce fichier au support Trustway qui fournira en retour le fichier `tgbcode`. |
| ③ Fichier `tgbcode` | Copier ce fichier `tgbcode` dans le répertoire Windows **Documents** du poste à activer. Lancer le logiciel: il est activé. |

## 2.5 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.

[2] 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.


Trustway IP Protect Client
Trustway IP Protect Client
Powered by TheGreenBow
Trustway IP Protect Client 7.0
© Atos 2022. All rights reserved
atos.net
Abonnement valide jusqu'au 13/01/2023
C:\Windows\System32\drivers
VpnConf.exe 7.00.116
TgbIkeNG.exe 7.0.0.016
ComLib.dll 7.0.0.016
VpnToken.dll 5.0.0.016
OK

# Chapitre 3. Mise à jour

## 3.1 Procédure de mise à jour

La mise à jour IP Protect Client 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 1.2 Procédure d'installation) à deux exceptions près :

1. Si la licence du produit installé n'est pas compatible avec IP Protect Client, alors la mise à jour n'est pas possible.

   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.

   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 »).

## 3.2 Mise à jour de la configuration VPN

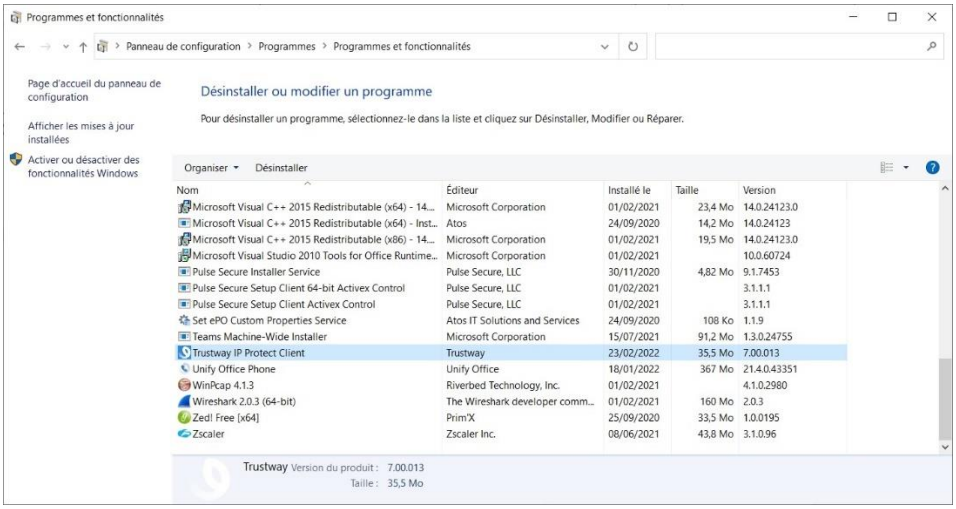
Au cours d'une mise à jour, la configuration VPN est sauvegardée et restaurée.

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.

# Chapitre 4. Désinstallation

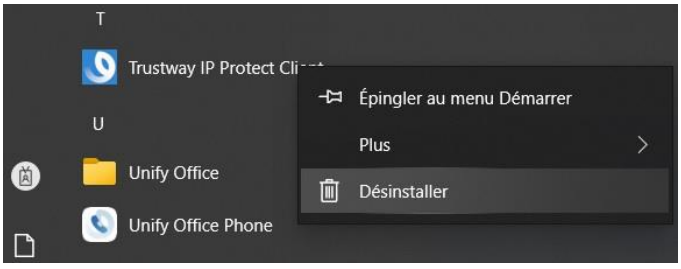
Pour désinstaller IP Protect Client, suivez les étapes ci-dessous :

1. Ouvrez le **Panneau de configuration** Windows.
2. Sélectionnez **Désinstaller un programme**.
3. Sélectionnez Trustway **IP Protect Client** dans la liste de programmes.
4. Cliquez sur **Désinstaller** et suivre les instructions pour désinstaller le programme.




Ou

1. Ouvrez le menu **Démarrer** de Windows.
2. Cliquez avec le bouton droit de la souris sur le programme Trustway **IP Protect Client**, puis sélectionnez **Désinstaller**.




3. Le Panneau de configuration Windows s'affiche. Sélectionnez Trustway **IP Protect Client** 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.

# Chapitre 5. Prise en main du logiciel

## 5.1 Introduction

L'interface graphique IP Protect Client permet :

- de configurer le logiciel lui-même (mode de démarrage, langue, contrôle d'accès, etc.),
- de gérer les configurations des tunnels VPN, les certificats, l'importation, l'exportation, etc.,
- d'utiliser les tunnels VPN (ouverture, fermeture, identification des incidents, etc.),
- 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.

## 5.2 Démarrer le logiciel

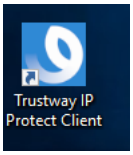
Une fois l'installation ou la mise à jour terminée, si vous avez laissé la case **Lancer le client VPN** cochée et que vous n'avez pas activé le logiciel, la fenêtre d'activation s'affiche (cf. Chapitre 2 Activation). Lorsque le logiciel est activé ou que vous avez choisi de l'évaluer, IP Protect Client se lance minimisé et l'icône IP Protect Client 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 IP Protect Client, 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.

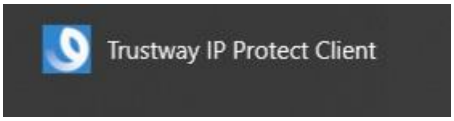
IP Protect Client peut être lancé directement en double-cliquant sur cette icône.




Le Client VPN se lance minimisé et l'icône IP Protect Client 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, IP Protect Client peut être lancé depuis le menu Démarrer de Windows en cliquant sur le programme IP Protect Client.

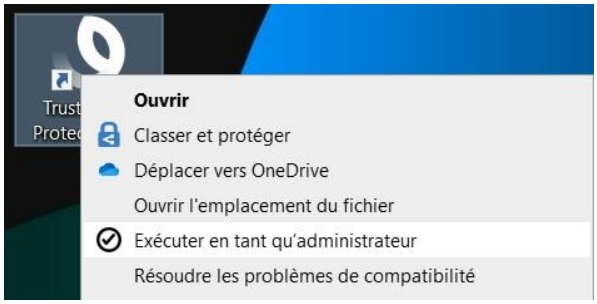



Le Client VPN se lance minimisé et l'icône IP Protect Client apparaît dans la barre des tâches (cf. paragraphe Icône en barre des tâches ci-dessous).

### Démarrer le Client VPN en tant qu'administrateur

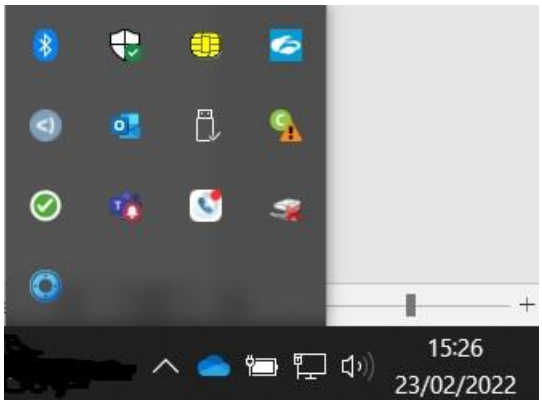
Par défaut, l'accès au **Panneau de Configuration** du Client VPN est réservé aux seuls administrateurs Windows.

Pour lancer le Client VPN en mode administrateur, afin de pouvoir accéder au **Panneau de Configuration**, cliquez sur l'icône **IP Protect Client** 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** IP Protect Client 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

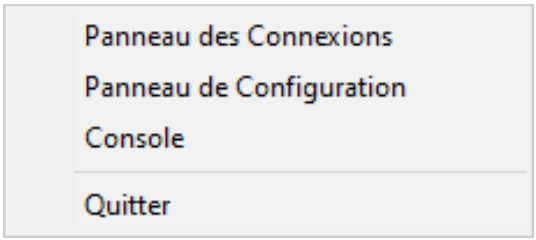
Icône verte : au moins un tunnel VPN est ouvert

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

- **VPN Tunnel ouvert** si un ou plusieurs tunnels sont ouverts.
- **IP Protect Client** 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 IP Protect Client en barre des tâches affiche le menu contextuel associé à l'icône :



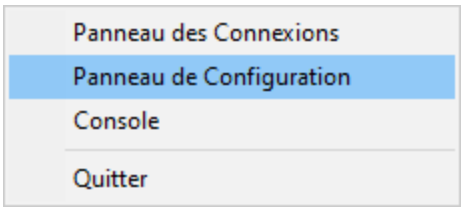

L'administrateur peut limiter les options affichées dans le menu (cf. 23.1 Affichage). Par défaut, les options du menu contextuel sont les suivantes :

- **Panneau des Connexions** : ouvre le Panneau des Connexions.
- **Panneau de Configuration** : ouvre le Panneau de Configuration (si IP Protect Client a été exécuté en tant qu'administrateur).
- **Console** : ouvre la fenêtre des traces VPN.
- **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).

## 5.3 Configurer un tunnel VPN

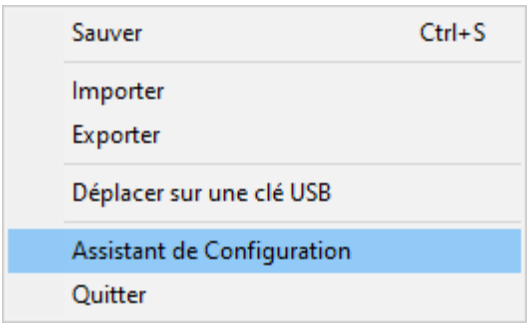
Pour ouvrir le Panneau de Configuration, il faut préalablement avoir lancé IP Protect Client en tant qu'administrateur (cf. paragraphe Démarrer le Client VPN en tant qu'administrateur ci-dessus). Si ce n'est pas le cas, quittez et relancer le Client VPN en tant qu'administrateur. Si c'est le cas, cliquez 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 8 Panneau de configuration.




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

Lorsque l'option **Restreindre l'accès du panneau de configuration aux administrateurs** est désactivée (cf. 23.1 Affichage), 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 6 Assistant de configuration ci-dessous.

## 5.4 Automatiser l'ouverture du tunnel VPN

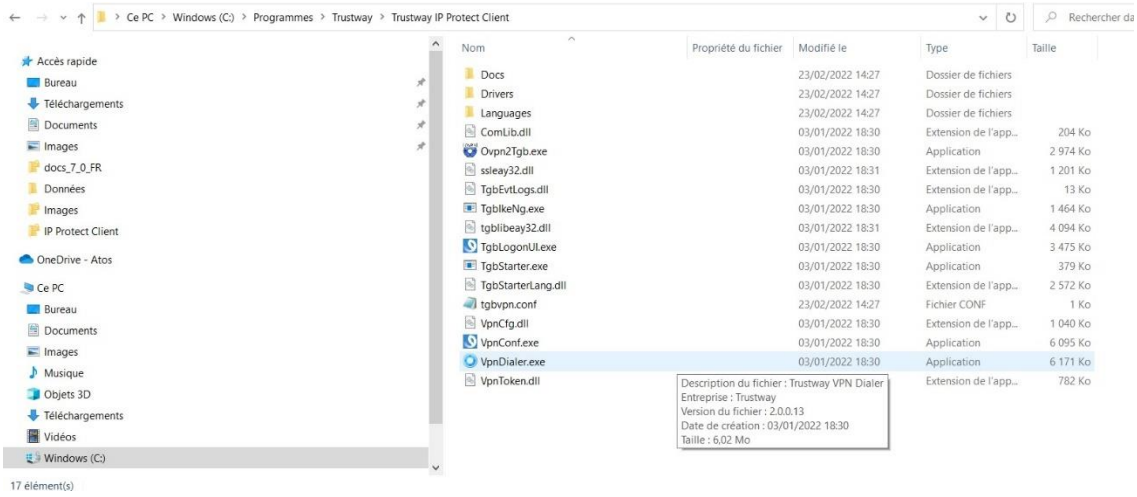
IP Protect Client permet d'automatiser l'ouverture d'un tunnel VPN. Il peut s'ouvrir automatiquement des manières suivantes :

- au démarrage de Windows, avant ou après l'ouverture de la session Windows ;
- sur détection de trafic à destination du réseau distant (cf. Chapitre 14 Automatisation) ;
- sur insertion d'une clé USB contenant la configuration VPN adéquate (cf. Chapitre 21 Mode USB) ;
- sur insertion de la carte à puce (ou du token) contenant le certificat utilisé pour ce tunnel (cf. section 17.5 Utiliser un certificat sur carte à puce ou sur token) ;
- 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 20 Gestion du Panneau TrustedConnect).

## 5.5 Ouvrir un tunnel avec le Panneau TrustedConnect

Le Panneau TrustedConnect est décrit au Chapitre 9 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\Trustway\Trustway IP Protect Client`.




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** de Windows).

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

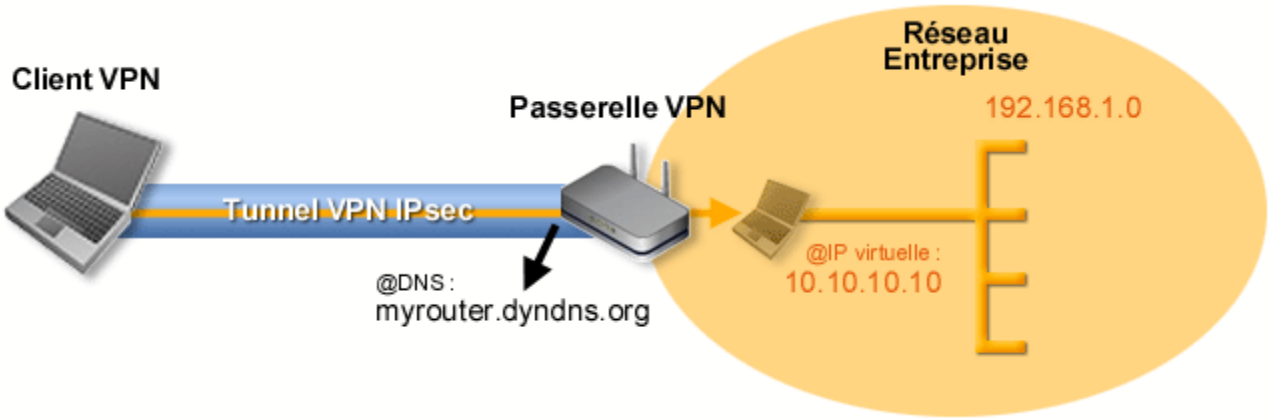
En revanche, lorsque `VpnDialer.exe` (TrustedConnect) est en cours d'exécution, il n'est pas possible de lancer `VpnConf.exe`. Vous devez d'abord quitter `VpnDialer.exe` avant de pouvoir lancer `VpnConf.exe`.

# Chapitre 6. Assistant de configuration

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

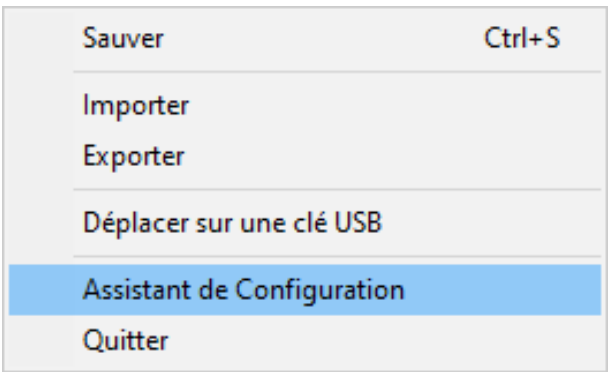
L'utilisation de l'assistant de configuration est illustrée par l'exemple suivant :

- Le tunnel est ouvert entre un poste et un IP Protect 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.



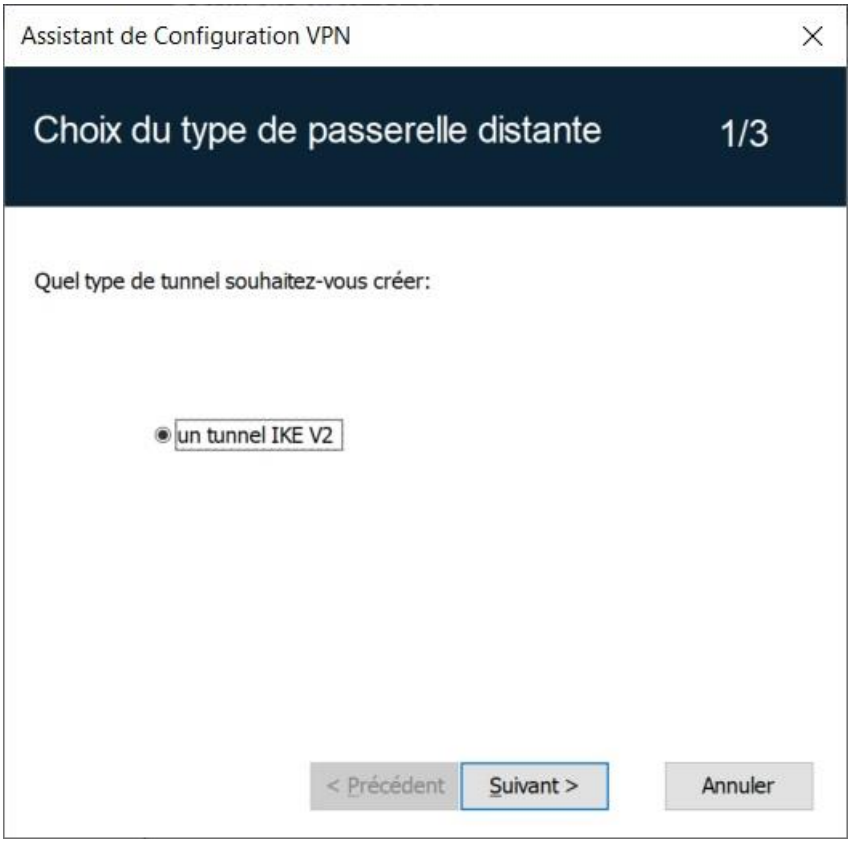

La passerelle VPN est un IP Protect dans la figure ci-dessus.

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




## 6.1 Étape 1

Choisissez IKEv2 comme protocole VPN à utiliser pour le tunnel.




## 6.2 Étape 2

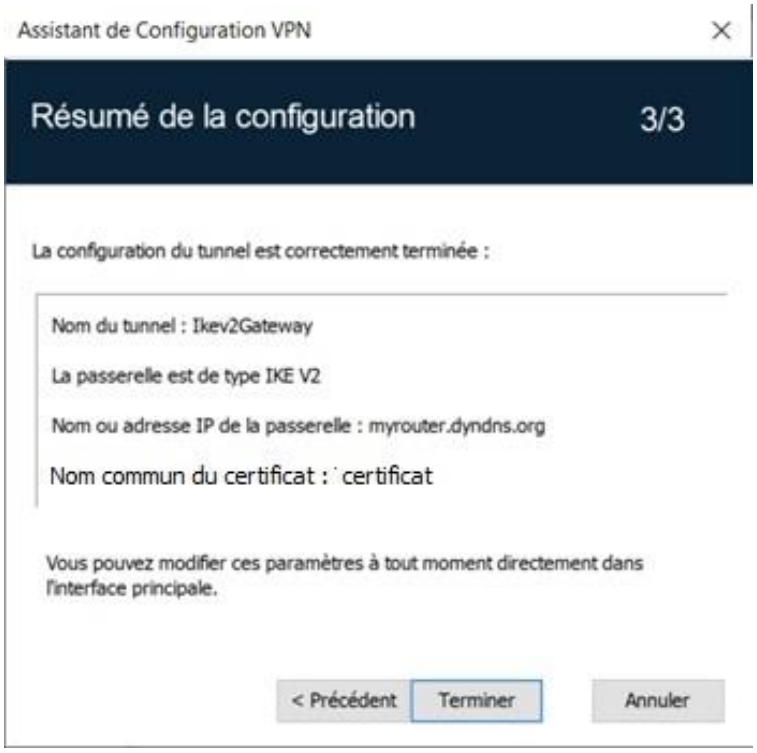
Entrez les valeurs suivantes :

- L'adresse IP ou DNS côté réseau internet de la passerelle VPN (IP Protect) (exemple : myrouter.dyndns.org).
- Un certificat qui doit être importé grâce au bouton **Importer un Certificat…** (voir section 17.4 Importer un certificat).

IP Protect ne permet que l'ouverture de tunnels IKEv2 avec certificat.
Se reporter au Chapitre 25 Recommandations de sécurité.


## 6.3 Étape 3

Vérifiez dans la fenêtre de résumé que la configuration est correcte et cliquer sur **Terminer**.



Le tunnel qui vient d'être configuré apparaît dans l'arborescence des tunnels de l'interface principale.

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

# Chapitre 7. Panneau des connexions

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


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

Voir le Chapitre 19 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 **23**.1 **Affichage** ).

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 **23**.1 Affichage .

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.

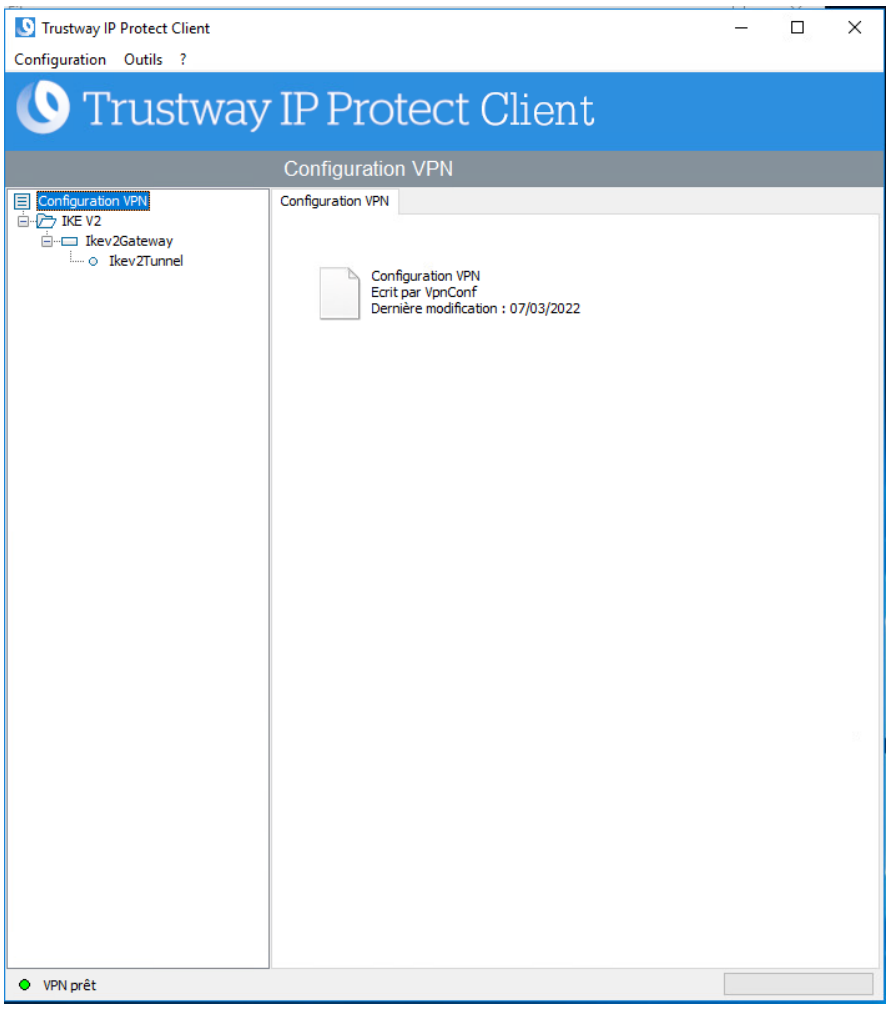
# Chapitre 8. Panneau de configuration

Le Panneau de Configuration est l'interface administrateur IP Protect Client.

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 5.2 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.



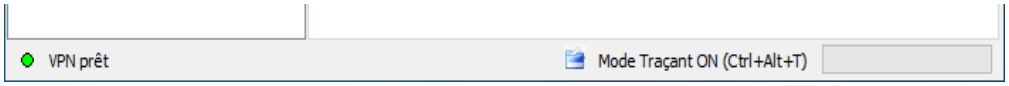
## 8.1 Menus

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 (sans effet)
  - À propos…

## 8.2 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.

## 8.3 Raccourcis

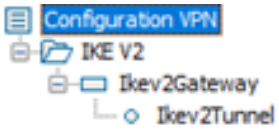
| | |
|---|---|
| CTRL+S | Sauvegarde de la configuration VPN |
| CTRL+ENTER | Permet de basculer sur le **Panneau des Connexions** |
| CTRL+D | Ouvre la fenêtre **Console** de logs VPN |
| CTRL+ALT+R | Redémarrage du service IKE |

| | |
|---|---|
| CTRL+ALT+T | Activation du mode traçant (génération de logs) |

## 8.4 Arborescence des tunnels VPN

### 8.4.1 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 », 2 niveaux permettent de créer des tunnels IPsec IKEv2, caractérisés par une IKE Auth et une Child SA, chaque IKE Auth pouvant contenir plusieurs Child SA ;

Un clic sur IKE Auth ou Child SA ouvre dans la partie droite du Panneau de Configuration les onglets de configuration VPN associés. Voir dans les chapitres suivants :

Tunnel IPsec IKEv2

- IKEv2 (IKE Auth) : Authentification
- IKEv2 (Child SA) : IPsec

Une icône est associée à chaque tunnel (Child SA). 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 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.

## 8.4.2 Menus contextuels

### 8.4.2.1 Configuration VPN

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


| | |
|---|---|
| **Export** | Exporte la configuration VPN complète. |
| **Déplacer sur la clé USB…** | Déplace la configuration VPN sur une clé USB et initie le mode USB |
| **Sauver** | Sauvegarde la configuration VPN. |
| **Assistant de Configuration** | Ouvre l'Assistant de Configuration VPN |
| **Reset** | Remet à zéro la configuration VPN après confirmation par l'utilisateur. |
| **Fermer tous les tunnels** | Ferme tous les tunnels ouverts. |

### 8.4.2.2 IKEv2

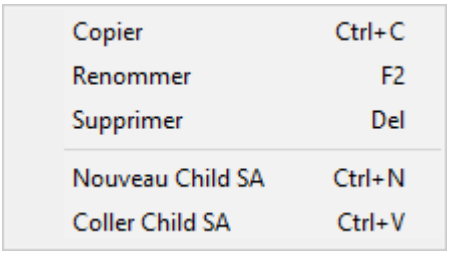
Un clic droit sur les éléments **IKEv2** affiche le menu contextuel suivant, qui permet d'exporter, de sauvegarder, de créer ou de coller un IKE Auth :


Menu IKEv2

| | |
|---|---|
| **Export** | Exporte tous les tunnels IKEv2. |
| **Sauver** | Sauvegarde tous les tunnels IKEv2. |
| **Nouvel IKE Auth** | Crée un nouvel IKE Auth. |
| **Coller IKE Auth** | Ajoute un IKE Auth copié précédemment dans le presse-papiers. |

#### 8.4.2.3 IKE Auth

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




| | |
|---|---|
| **Copier** | Copie l'IKE Auth sélectionné dans le presse-papier. |
| **Renommer**[3] | Renomme l'IKE Auth. |
| **Supprimer**[4] | Supprime l'IKE Auth, y compris toutes les Child SA associées, après confirmation par l'utilisateur. |
| **Nouveau Child SA** | Ajoute une nouvelle Child SA à l'IKE Auth sélectionnée. |
| **Coller Child SA**[5] | Ajoute à l'IKE Auth la Child SA copiée dans le presse-papiers. |

[3] Ce menu est désactivé tant qu'un des tunnels de l'IKE Auth concerné est ouvert.

[4] idem

[5] Ce choix apparaît lorsqu'une Child SA a été copiée dans le presse-papiers via le menu contextuel associé à la Child SA concernée (cf. ci-après).

#### 8.4.2.4 Child SA

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


Menu tunnel fermé


Menu tunnel ouvert

| | |
|---|---|
| **Ouvre Tunnel…** | S'affiche si le tunnel VPN est fermé. Ouvre le tunnel (Child SA) sélectionné. |
| **Fermer le tunnel** | S'affiche si le tunnel VPN est ouvert. Ferme le tunnel (Child SA) sélectionné. |
| **Export**[6] | Exporte la Child SA sélectionnée. |
| **Copier** | Copie la Child SA sélectionnée. |
| **Renommer**[7] | Renomme la Child SA sélectionnée. |
| **Supprimer**[8] | Supprime la Child SA sélectionnée après confirmation par l'utilisateur. |

### 8.4.3 Raccourcis

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

| | |
|---|---|
| F2 | Permet d'éditer le nom de la phase sélectionnée. |

[6] Cette fonction permet d'exporter le tunnel complet, c'est-à-dire, la Child SA et son IKE Auth associé, et de créer ainsi une configuration VPN mono-tunnel complètement opérationnelle (qui peut par exemple être importée en étant immédiatement fonctionnelle).

[7] Ce menu est désactivé tant que le tunnel est ouvert.

[8] idem

| | |
|---|---|
| DEL | Si une phase est sélectionnée, la supprime après confirmation de l'utilisateur.<br><br>Si la configuration VPN est sélectionnée (racine de l'arborescence), propose l'effacement (reset) de la configuration complète. |
| CTRL+O | Si une Child SA est sélectionnée, ouvre le tunnel VPN correspondant. |
| CTRL+W | Si une Child SA est sélectionnée, ferme le tunnel VPN correspondant. |
| CTRL+C | Copie la phase sélectionnée dans le presse-papiers. |
| CTRL+V | Colle (ajoute) la phrase copiée dans le presse-papiers. |
| CTRL+N | Crée un nouvel IKE Auth, si la configuration VPN est sélectionnée, ou crée une nouvelle Child SA pour l'IKE Auth sélectionnée. |
| CTRL+S | Sauvegarde la configuration VPN. |

# Chapitre 9. Panneau TrustedConnect

## 9.1 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.

## 9.2 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**.

## 9.3 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** de IP Protect Client.

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

Cet état signifie que Panneau TrustedConnect ne gère aucune connexion sur le poste de travail. En général, cet état sera rencontré lorsque l'utilisateur demande explicitement la fermeture de sa connexion VPN.

Cet état signifie que le poste de travail est connecté directement au réseau de l'entreprise, considéré comme réseau de confiance.

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

Cet état signifie que la connexion VPN n'a pas pu être établie.

## 9.4 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 :

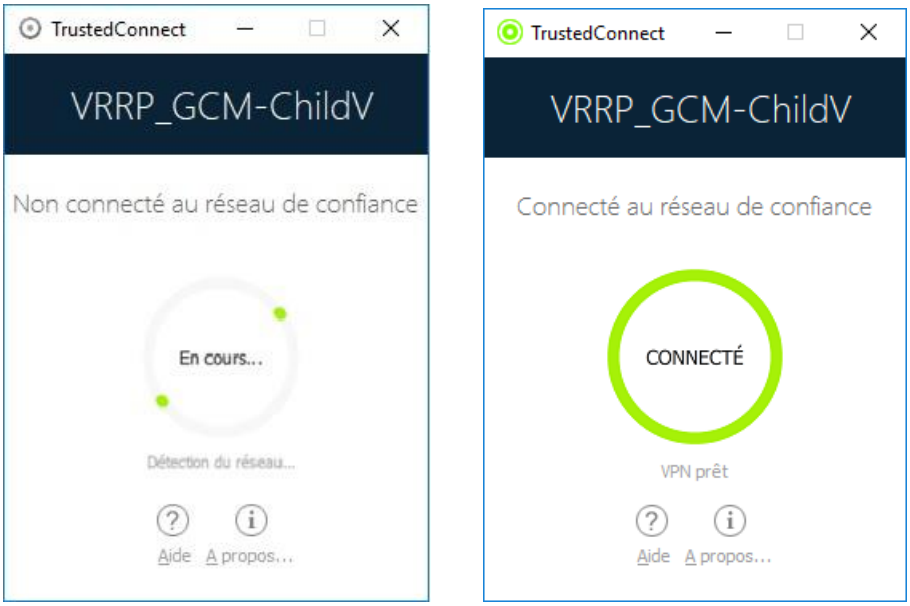
| | |
|---|---|
| **À propos…** | Ouvre la fenêtre À propos… du logiciel. |
| **Langue** | Permet de basculer entre le français et l'anglais. |
| **Journaux** | Démarre la journalisation. Une fois la journalisation démarrée, deux options supplémentaires s'affichent pour afficher les journaux et arrêter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

## 9.5 Utilisation

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

### 9.5.1 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.

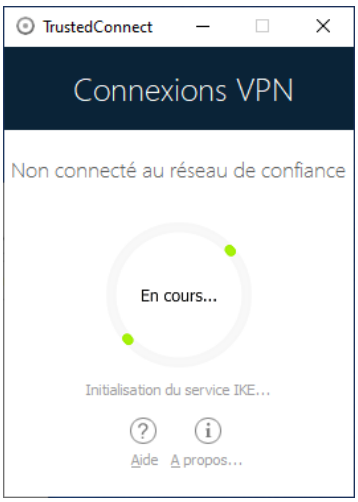
Voir le « Guide de Déploiement ».

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.

### 9.5.2 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. Le chapitre suivant 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 **DÉCONNECTER** 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 :


## 9.6 Cas d'erreurs

Les principaux cas d'erreurs 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.

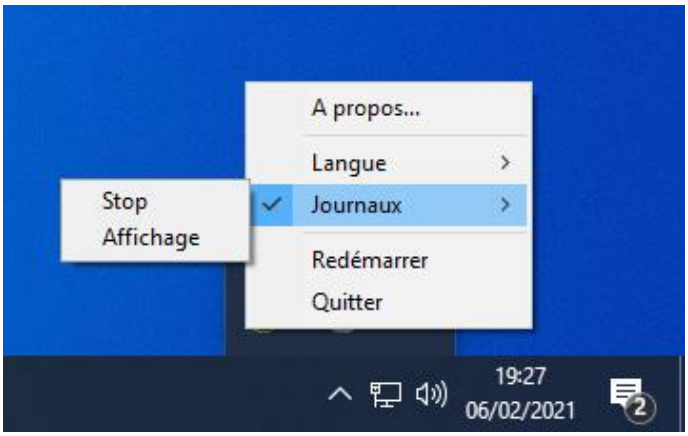

L'administrateur réseau peut être contacté pour résoudre le problème. En fonction du code d'erreur indiqué, il peut fournir des indications ou des explications sur le problème rencontré. Si l'administrateur demande des logs, se reporter à la procédure décrite dans le chapitre suivant.

La liste des codes d'erreurs est fournie en annexe de ce document (cf. section 28.3 Diagnostics du Panneau TrustedConnect).

## 9.7 Génération de journaux

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

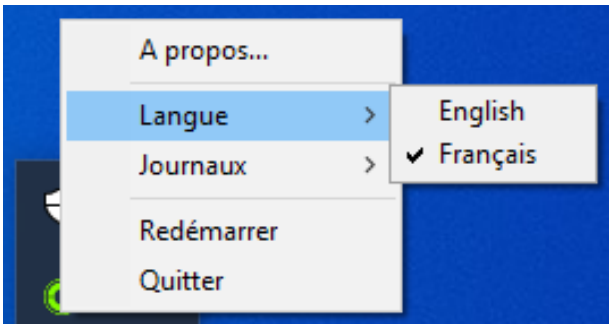
Pour initier la création des journaux, depuis l'icône **TrustedConnect** de la zone de notification, sélectionner l'option **Journaux**, une coche à gauche de cette option indique ensuite que les journaux sont actifs :




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

## 9.8 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'option **Langues**. Dans le sous-menu choisir **English** ou **Français** :




## 9.9 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** de Windows).

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

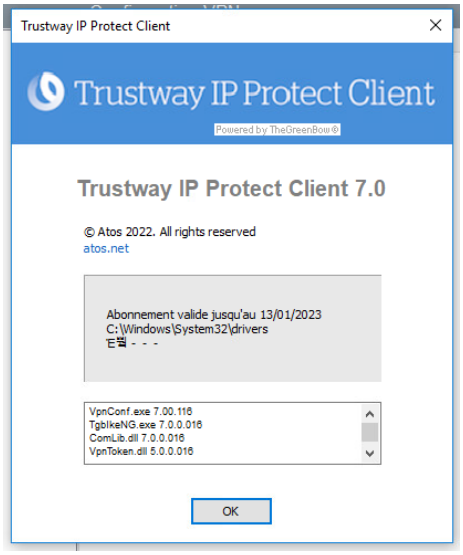
En revanche, lorsque `VpnDialer.exe` (TrustedConnect) est en cours d'exécution, il n'est pas possible de lancer `VpnConf.exe`. Vous devez d'abord quitter `VpnDialer.exe` avant de pouvoir lancer `VpnConf.exe`.

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

# Chapitre 10. Fenêtre « À propos… »

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

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




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

- le nom et la version du logiciel ;
- lorsque le logiciel est activé, le numéro de licence et l'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.[9]

[9] 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 IP Protect Client n'est pas activé, le logiciel tente de se connecter au serveur d'activation pour valider la licence.

# Chapitre 11. Importer et exporter la configuration VPN

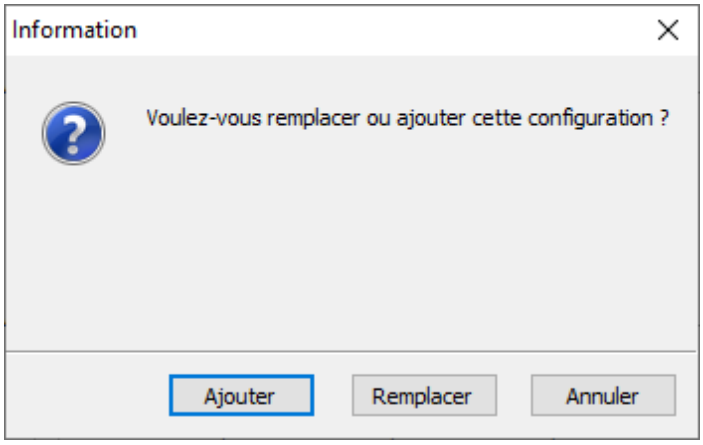
## 11.1 Importer une configuration VPN

IP Protect Client 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`.[10]

IP Protect Client 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 :

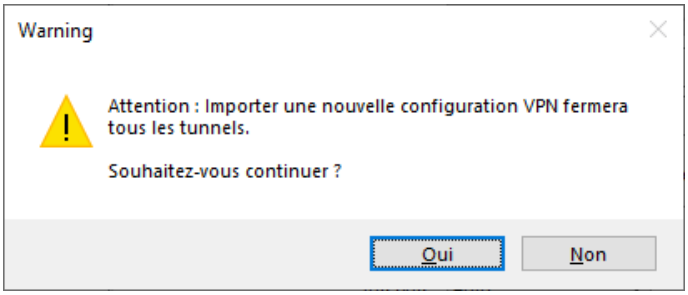



Si la configuration VPN importée a été exportée avec une protection par mot de passe (cf. section 11.2 Exporter une configuration VPN ci-dessous), le mot de passe est demandé à l'utilisateur.

[10] 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`.


Si la configuration VPN a été exportée avec contrôle d'intégrité (cf. section 11.2 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).

## 11.2 Exporter une configuration VPN

IP Protect Client permet d'exporter une configuration VPN de différentes façons :

- Menu **Configuration** > **Exporter** : la configuration VPN complète est exportée.
- Menu contextuel associé à la racine de l'**arborescence VPN** > **Export** : la configuration VPN complète est exportée.
- Menu contextuel associé à **IKE Auth** > **Export** : toute IKE Auth (incluant les Child SA qu'elle contient) est exportée.
- Menu contextuel associé à une **Child SA** > **Export** : la Child SA est exportée, avec l'IKE Auth à laquelle elle est associée.
- Par ligne de commande en utilisant l'option `/export`.[11]

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

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


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

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

Le mot de passe doit contenir au moins 16 caractères.

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 11.1 Importer une configuration VPN ci-dessus).

## 11.3 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 11.1 Importer une configuration VPN ci-dessus).

## 11.4 Scinder une configuration VPN

En utilisant les différentes options d'exportation (exportation d'une IKE Auth avec toutes les Child SA associées, ou exportation d'un tunnel simple), il est possible de scinder une configuration VPN en autant de « sous-configurations » que désiré (cf. section 11.2 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.

# Chapitre 12. Configurer un tunnel VPN

## 12.1 IPsec IKEv2

IP Protect Client permet de créer et de configurer des tunnels VPN IPsec IKEv2.

La méthode pour créer un nouveau tunnel VPN est décrite dans les sections précédentes : Chapitre 6 Assistant de configuration et 8.4 Arborescence des tunnels VPN > 8.4.2 Menus contextuels.

IP Protect ne permet que l'ouverture de tunnels IKEv2 avec certificat conformément au Chapitre 25 Recommandations de sécurité.

## 12.2 Modification et sauvegarde de la configuration VPN

IP Protect Client 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'item modifié.

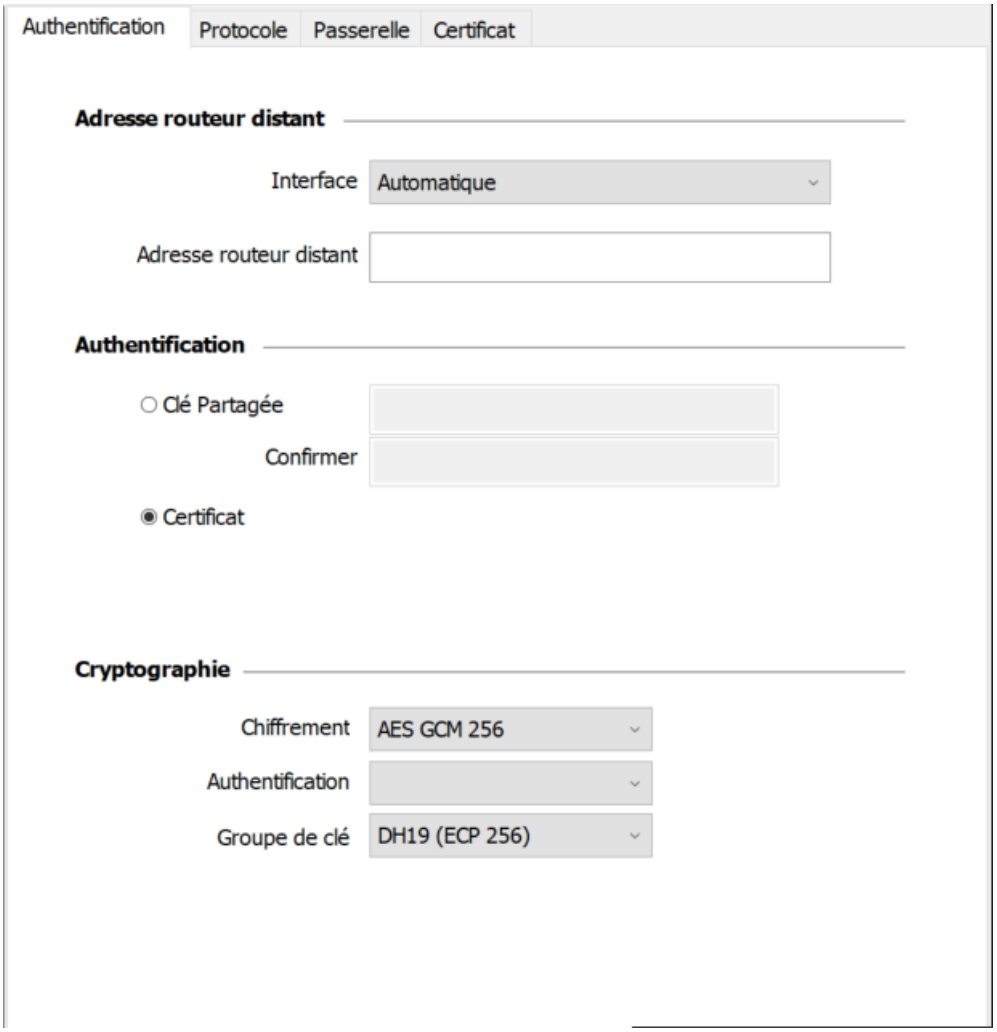
À tout moment, la configuration VPN peut être sauvegardée :

- 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.

## 12.3 Configurer un tunnel IPsec IKEv2

### 12.3.1 IKE Auth : IKE SA




IP Protect n'autorise pas l'authentification par clé partagée ou EAP conformément au Chapitre 25 Recommandations de sécurité.

IP Protect ne supporte que les adresses IPv4.

#### 12.3.1.1 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 (IPv4) ou adresse DNS de la passerelle VPN distante.

Ce champ doit être obligatoirement renseigné.

**Clé partagée** Mot de passe ou clé partagée par la passerelle distante.

IP Protect n'autorise pas l'authentification par clé partagée conformément au Chapitre 25 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 25 Recommandations de sécurité.

Se reporter au chapitre dédié : Chapitre 1 Gestion des certificats

**EAP**

IP Protect n'autorise pas l'authentification par EAP conformément au Chapitre 25 Recommandations de sécurité.

**Multiple AUTH Support**

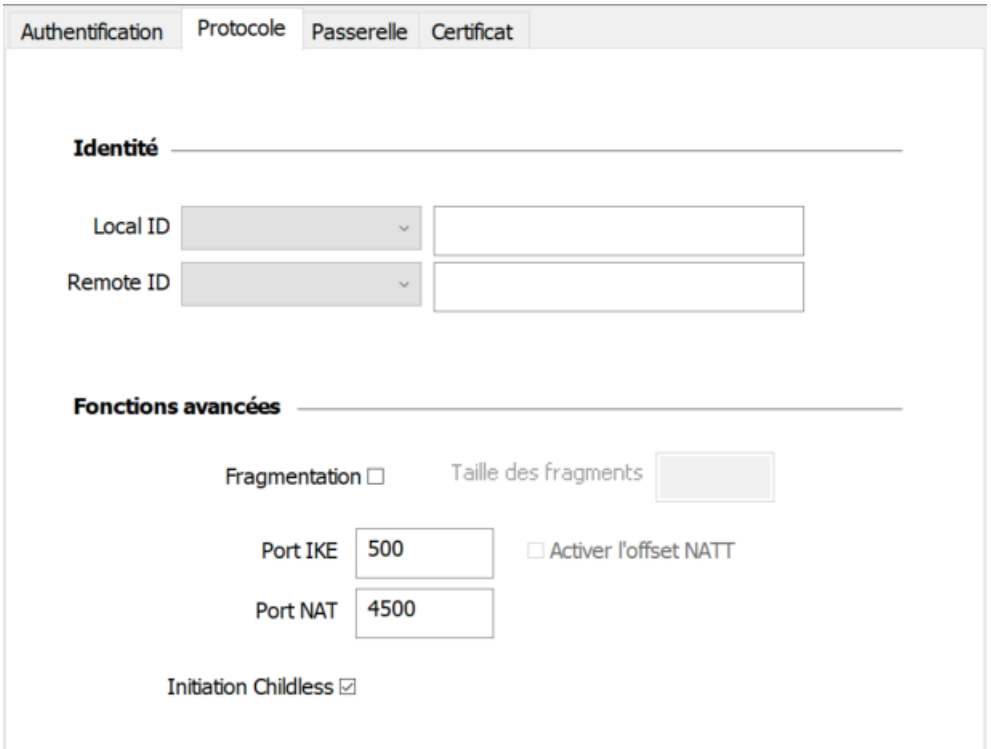
Non supporté par IP Protect conformément au Chapitre 25 Recommandations de sécurité.

#### 12.3.1.2 Authentification

| | |
|---|---|
| **Chiffrement** | Algorithme de chiffrement négocié au cours de la phase d'authentification:<br>AES GCM (256) |
| **Authentification** | Algorithme d'authentification négocié au cours de la phase d'authentification:<br>SHA2 256. |
| **Groupe de clé** | Longueur de la clé Diffie-Hellman:<br>DH19 (ECP 256). |

#### 12.3.1.3 Cryptographie

### 12.3.2 IKE Auth : Protocole



#### 12.3.2.1 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 :

- 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 17 Gestion des certificats)

Ce paramètre est obligatoire.

**Remote ID**

Le « Remote ID » est l'identifiant de la phase d'authentification que le Client VPN s'attend à recevoir de la passerelle VPN distante.

Suivant le type sélectionné, cet identifiant peut être :

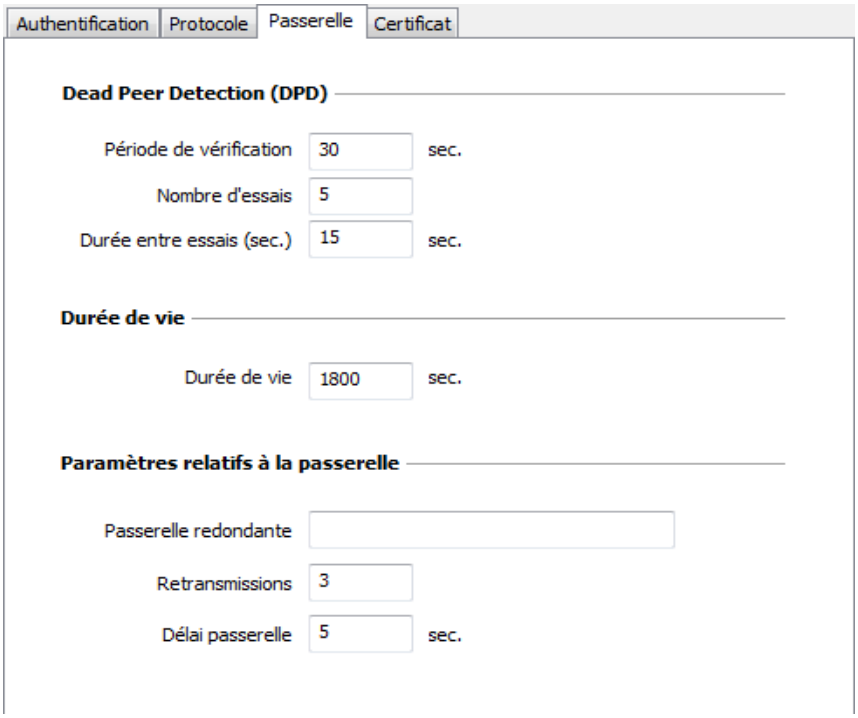
- DER ASN1 DN : le sujet X.509 d'un certificat (type = DER ASN1 DN) en respectant l'ordre du sujet du certificat du chiffreur IP Protect.

Ce paramètre est obligatoire.

### 12.3.2.2 Fonctions avancées

| | |
|---|---|
| **Fragmentation IKEv2** | Active la fragmentation des paquets IKEv2 conformément à la RFC 7383.<br>Cette option ne doit pas être cochée. |
| **Port IKE** | Le port IKE doit être positionné à 4500. |
| **Port NAT** | Le port NAT doit être positionné à 4500. |
| **Activer l'offset NATT** | Cette option doit être cochée. |
| **Childless** | Cette option doit être cochée. |

### 12.3.3 IKE Auth : Passerelle



#### 12.3.3.1 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.[12]<br>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. |

#### 12.3.3.2 Durée de vie

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

#### 12.3.3.3 Paramètres relatifs à la passerelle

[12] 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.

| | |
|---|---|
| **Passerelle redondante** | L'adresse de la passerelle VPN redondante peut être une adresse IP ou DNS.<br><br>⍰⍰ Voir le Chapitre 13 Passerelle redondante. |

| | |
|---|---|
| **Retransmissions** | Nombre de retransmissions de messages protocolaires IKE avant échec. |
| **Délai passerelle** | Délai entre chaque retransmission |

### 12.3.4 IKE Auth : Certificat

⍰⍰ Voir le Chapitre 17 Gestion des certificats.

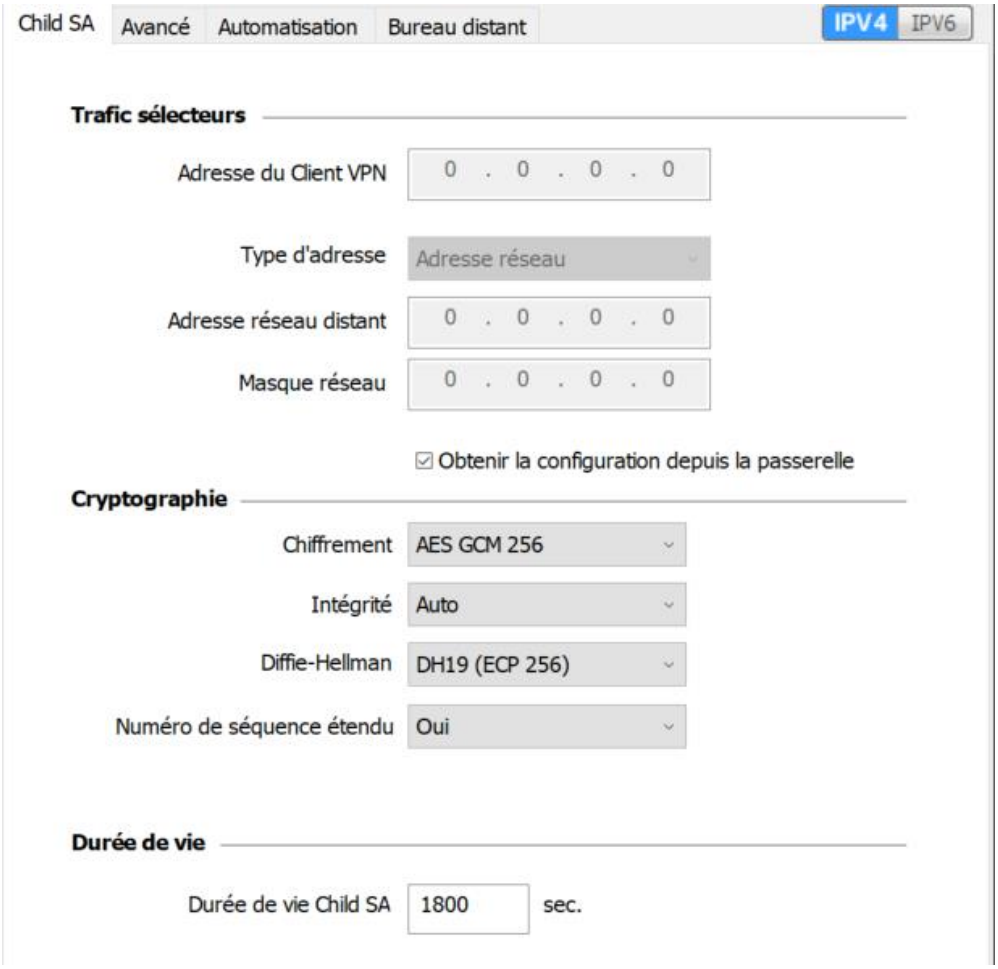
### 12.3.5 Child SA : Généralités

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

Pour configurer les paramètres d'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.

### 12.3.6 Child SA : Child SA



#### 12.3.6.1 Trafic sélecteurs

| | |
|---|---|
| **Adresse du Client VPN** | Grisé car la case « Obtenir la configuration depuis la passerelle » doit être cochée**.** |
| **Type d'adresse** | Grisé car la case « Obtenir la configuration depuis la passerelle » doit être cochée**.** |
| **Obtenir la configuration depuis la passerelle** | Cette case doit être cochée. |

### 12.3.6.2 Cryptographie

**Chiffrement** Algorithme de chiffrement négocié au cours de la phase IPsec:

Seule valeur configurable : AES GCM (256).

**Intégrité** Algorithme d'authentification négocié au cours de la phase IPsec :

Seule valeur configurable : AES GCM (256).

**Diffie-Hellman** Longueur de la clé Diffie-Hellman[13] :

Seule valeur configurable : DH19 (ECP 256).

**Extended Sequence Number** Permet l'usage de numéros de séquence étendus de taille 64 bits (cf. RFC 4304) :

Seule valeur configurable : Oui.

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.

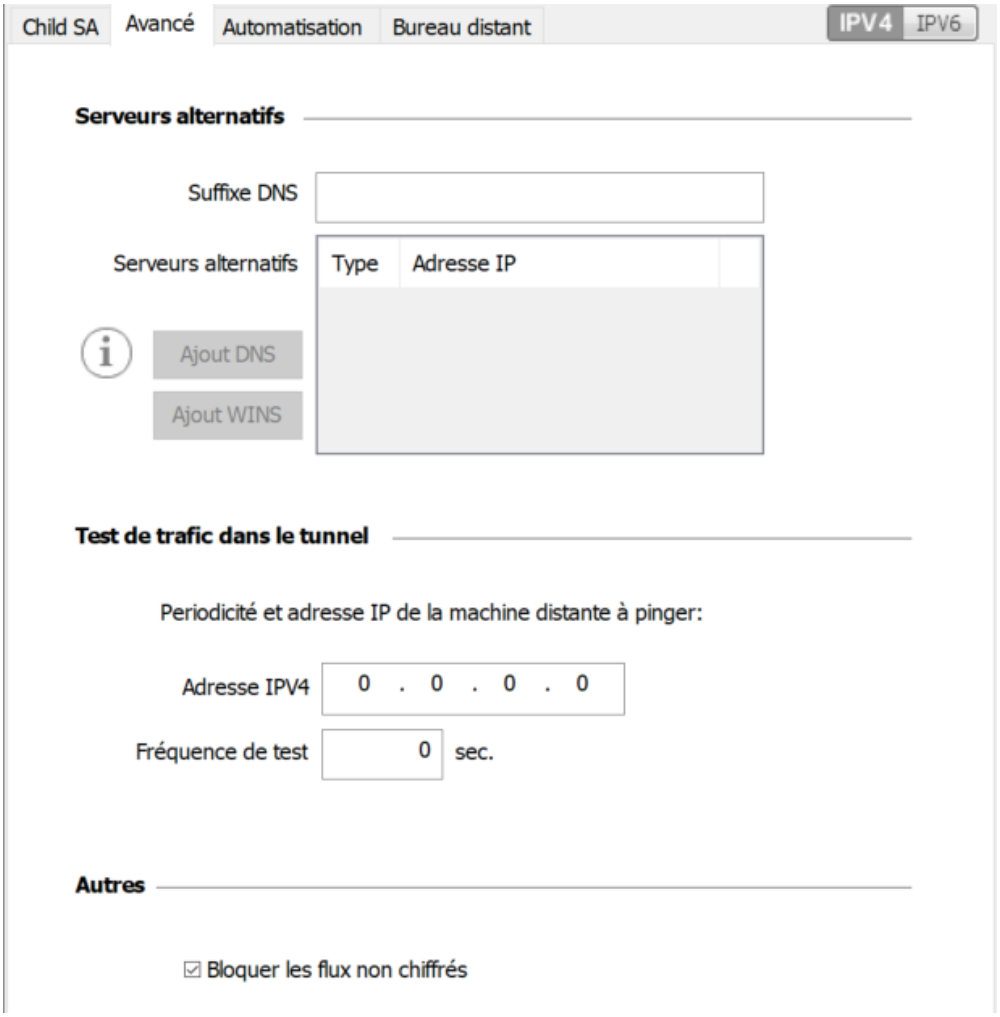
### 12.3.6.3 Durée de vie

**Durée de vie Child SA** Durée en secondes entre deux renégociations.

La valeur par défaut pour la durée de vie Child SA est de 1 800 s (30 min).

[13] Voir note 1.

## 12.3.7 Child SA : Avancé




### 12.3.7.1 Serveurs alternatifs

**Suffixe DNS**

Suffixe de domaine à ajouter à chaque nom de machine, par exemple : `mozart.dev.atos`.

Ce paramètre est optionnel. Lorsqu'il est spécifié, IP Protect Client 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 IPv4 des serveurs DNS (2 maximum) et WINS (2 maximum) accessibles sur le réseau distant.

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.

### 12.3.7.2 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** 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.

Le tunnel doit être configuré en IPv4 (bouton en haut à droite de l'onglet).

**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.

### 12.3.7.3 Autres

| | |
|---|---|
| **Bloquer les flux non chiffrés** | Lorsque cette option est cochée, seul le trafic passant dans le tunnel est autorisé.[14] |

### 12.3.8 Child SA : Automatisation

Voir le Chapitre 14 Automatisation

.

### 12.3.9 Child SA : Bureau distant

Voir le Chapitre 18 Partage de bureau distant.

[14] 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. Ce mode est recommandé.

# Chapitre 13. Passerelle redondante

IP Protect Client permet la gestion d'une passerelle VPN (IP Protect) 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.

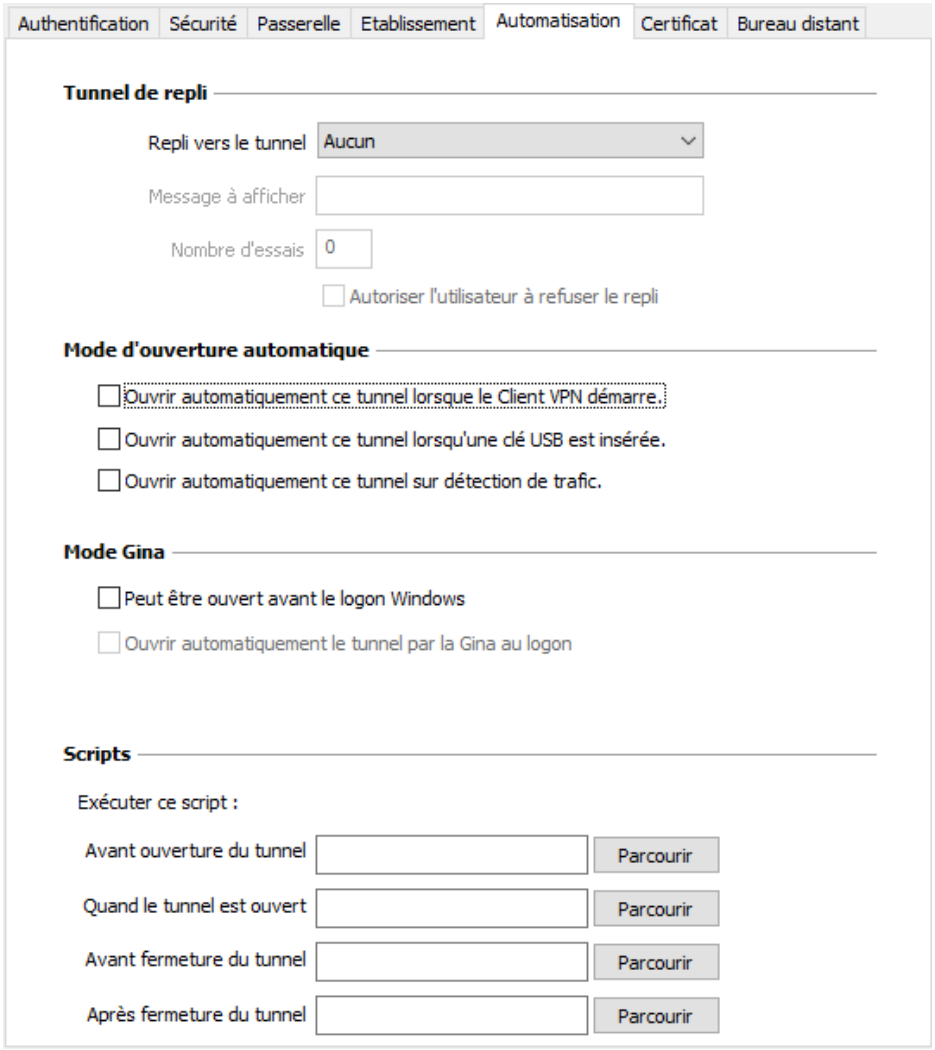
Le Client VPN n'essaye pas de contacter la passerelle redondante si la passerelle initiale est inaccessible à cause d'un problème de résolution DNS.

La passerelle IP Protect propose une solution de redondance basée sur le protocole VRRP pour les communications entre chiffreurs. Les passerelles redondantes dans un groupe VRRP utilisent la même adresse qui est l'adresse IPsec du groupe VRRP. Il faut donc indiquer l'adresse IPsec du groupe VRRP comme adresse de passerelle et cette même adresse IPsec comme adresse de passerelle redondante.
Lorsque c'est DNS qui est utilisé, il faut de même utiliser la même adresse DNS qui représente l'adresse IPsec du groupe VRRP.

# Chapitre 14. Automatisation

IP Protect Client 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.

Le paramétrage des automatisations s'effectue dans l'onglet Automatisation du tunnel : Child SA (IKEv2).




## 14.1 Tunnel de repli (fallback)

☞ Se reporter au chapitre 16 Tunnel de repli.

## 14.2 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 21 Mode USB, il est ouvert automatiquement sur insertion de cette clé USB.<br><br>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. |

## 14.3 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 22 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. |

## 14.4 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 ;

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

- 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 ;

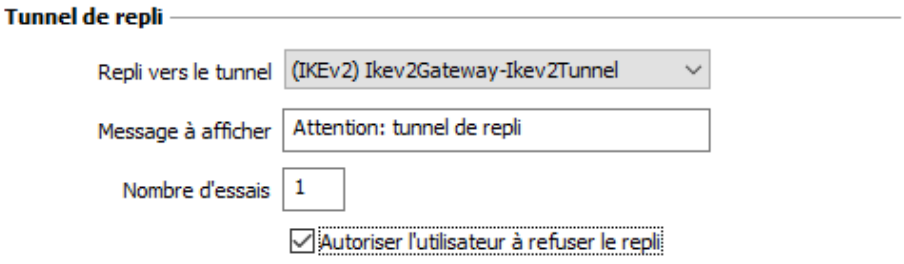
etc.

# Chapitre 15. Tunnel de repli

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

Cette fonction se configure dans l'onglet **Automatisation** de chaque tunnel IKEv2.

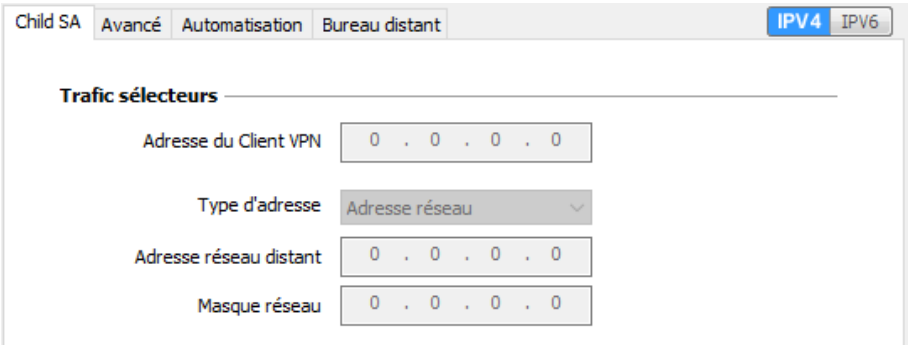
| | |
|---|---|
| **Repli vers le tunnel** | Le champ présente la liste des tunnels vers lequel le logiciel peut basculer automatiquement si le tunnel en cours d'édition est indisponible. |
| **Message à afficher** | Comme cette fonction peut passer automatiquement d'un tunnel à un autre, il est possible 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. |



# Chapitre 16. IPv4 et IPv6

Seul IPv4 est supporté avec la passerelle VPN IP Protect

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



# Chapitre 17. Gestion des certificats

## 17.1 Introduction

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

IP Protect Client implémente en particulier les facilités suivantes :

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

IP Protect Client 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 la carte à puce ou de token, ou encore la possibilité de configurer l'interface PKI / IGC et carte à puce dans l'installeur du logiciel de façon à automatiser le déploiement.

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

1. l'onglet **Certificat** du tunnel concerné : IKE Auth (IKEv2);
2. l'onglet **Options PKI** de la fenêtre **Outils** > **Options** du **Panneau de Configuration** ;

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

3. un fichier de configuration des tokens et cartes à puces : `vpnconf.ini`– voir « Guide de Déploiement ».

## 17.2 Certificat utilisateur

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

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

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

Si ces contraintes ne sont pas respectées, IP Protect Client affichera un avertissement dans la console mais n'empêchera pas la communication avec la passerelle. Celle-ci devrait néanmoins refuser l'authentification de IP Protect Client.

## 17.3 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 Configurer une carte à puce ou un token).

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

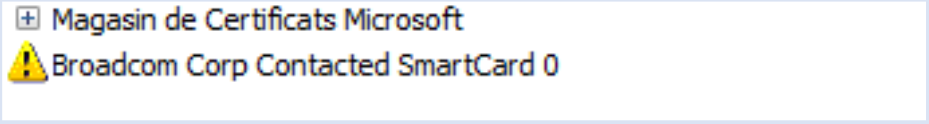
- le token ou la carte à puce est compatible CNG ou PKCS#11 ;
- le middleware du token ou de la carte à puce est correctement installé sur l'ordinateur ;
- le cas échéant, la carte à puce est correctement insérée dans le lecteur associé.

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).

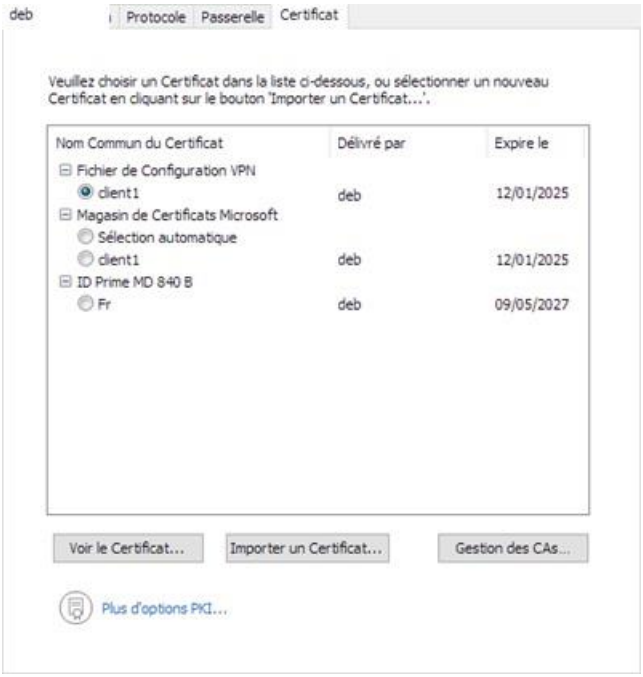
En cliquant sur le support désiré, la liste des certificats qu'il contient est affichée.

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

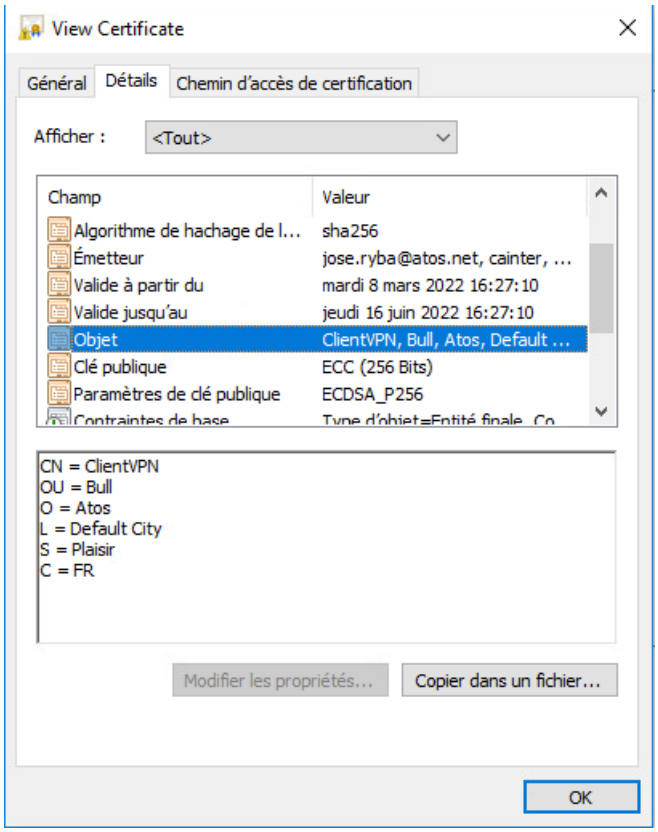
Dans le cas d'un lecteur de carte à puce, le lecteur s'affiche précédé d'une icône d'alerte si la carte à puce n'est pas insérée.



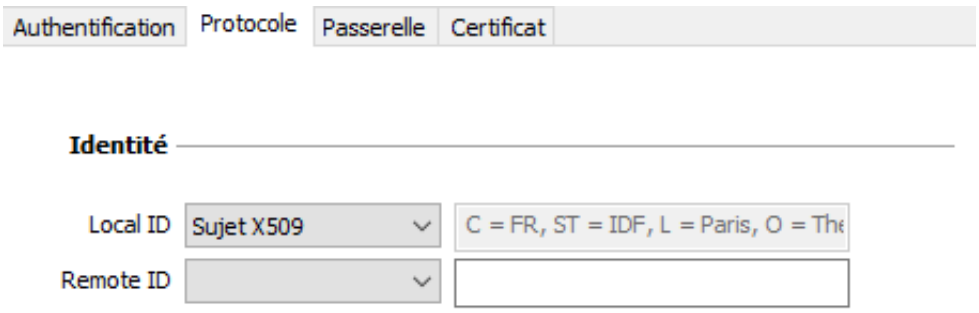

Seuls les certificats présents qui ne sont pas expirés sont affichés.




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**.



## 17.4 Importer un certificat

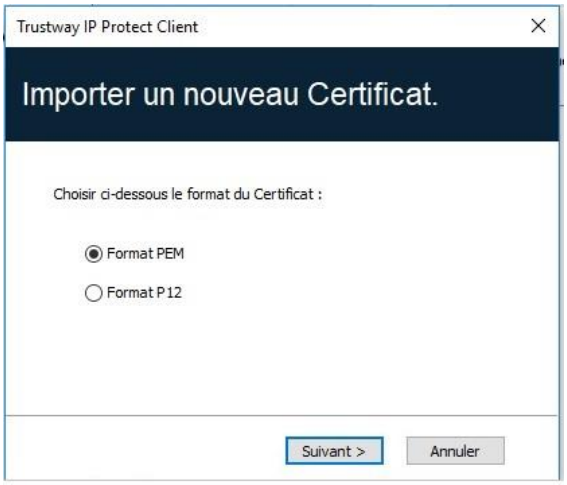
IP Protect Client permet d'importer dans la configuration VPN des certificats au format PEM ou PKCS#12. L'intérêt de cette solution, moins sécurisée que l'utilisation du magasin de certificats Windows, d'un token ou d'une carte à puce, est de faciliter le transport des certificats.

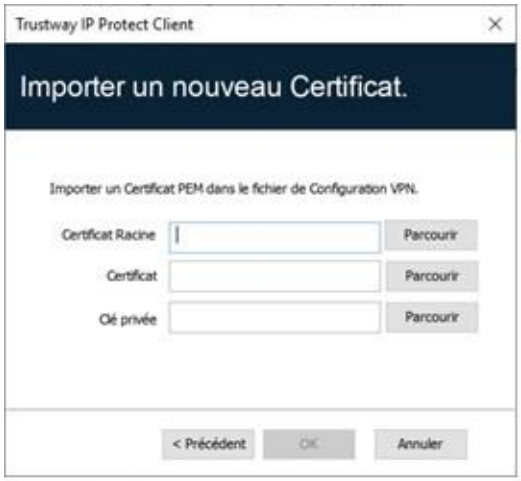
Cette solution présente l'avantage de regrouper le certificat (propre à un utilisateur) et la configuration VPN (a priori générique) dans un fichier unique, facile à transmettre vers le poste utilisateur et à importer dans le Client VPN.

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.

### 17.4.1 Importer un certificat au format PEM

4. Dans l'onglet **Certificat** d'une IKE Auth, cliquez sur **Importer un Certificat…**.
5. Choisissez **Format PEM**.
6. Sélectionnez (**Parcourir**) les **Certificats Racine**, le **Certificat (Utilisateur)** et la **Clé privée** à importer.
7. 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.

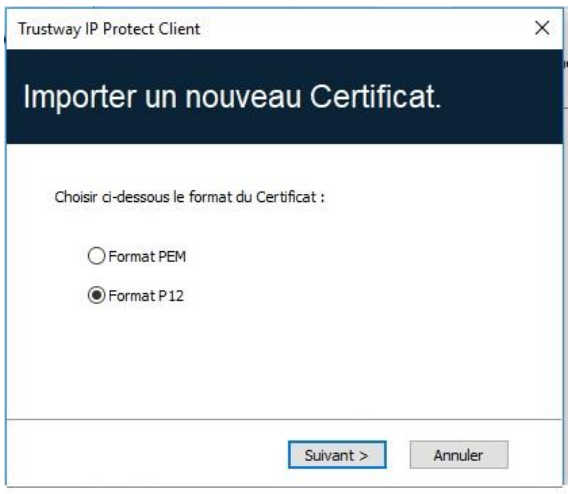
Dès lors qu'un certificat est importé dans une configuration VPN, il est fortement recommandé lors de l'exportation du fichier de configuration, de le protéger par un mot de passe (cf. section 11.2 Exporter une configuration VPN), pour éviter que le certificat ne soit visible en clair

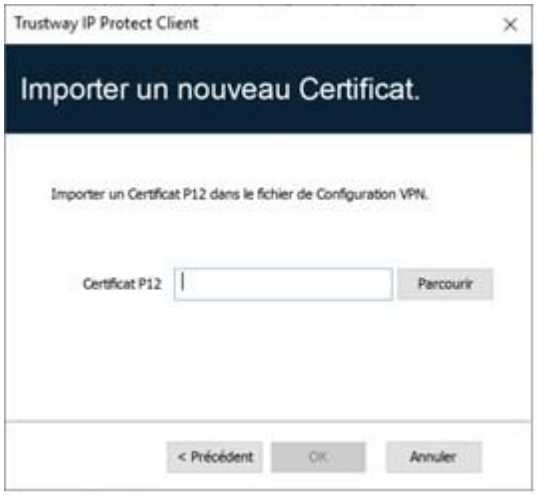
### 17.4.2 Importer un certificat au format PKCS#12

1. Dans l'onglet **Certificat** d'une Child SA, cliquez sur **Importer un Certificat…**.
2. Choisissez **Format P12**.

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

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.




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.

Tous les CA au format PKCS#12 présents dans le fichier seront également importés dans la configuration VPN.

## 17.5 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 17.7 Options PKI : caractériser le certificat et son support ci-dessus), le tunnel ne s'ouvre pas.

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

IP Protect Client 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. 0

La passerelle IP Protect propose une solution de redondance basée sur le protocole VRRP pour les communications entre chiffreurs. Les passerelles redondantes dans un groupe VRRP utilisent la même adresse qui est l'adresse IPsec du groupe VRRP. Il faut donc indiquer l'adresse IPsec du groupe VRRP comme adresse de passerelle et cette même adresse IPsec comme adresse de passerelle redondante.
Lorsque c'est DNS qui est utilisé, il faut de même utiliser la même adresse DNS qui représente l'adresse IPsec du groupe VRRP.

Automatisation).

## 17.6 Magasin de certificats Windows

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

- Le certificat doit être certifié par une autorité de certification (ce qui exclut les certificats auto-signés),

- Par défaut, le certificat doit être situé dans le magasin de certificats « Personnel » (il représente l'identité personnelle de l'utilisateur qui veut ouvrir un tunnel VPN vers son réseau d'entreprise). Pour utiliser le magasin de certificats machine de Windows, il convient 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 **Démarrer** de Windows, puis dans le champ **Rechercher les programmes et fichiers**, entrer `certmgr.msc`.

## 17.7 Options PKI : caractériser le certificat et son support

IP Protect Client 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.

## 17.8 Certificat de la passerelle VPN

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

Voir section 23.4.1 Vérification des certificats.

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

Si l'option est cochée, IP Protect Client 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, IP Protect Client ne sera pas en mesure de valider le certificat de la passerelle.

La vérification de chaque élément de la chaîne implique :

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

- la vérification des CRL de tous les émetteurs de certificats de la chaine de confiance.

### 17.8.1 Contraintes relatives à l'extension Key Usage

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

- être présente,
- être marquée comme critique
- contenir uniquement les valeurs `digitalSignature` et/ou `keyEncipherment`.

Dans le cas où la passerelle VPN ne se conforme pas aux contraintes relatives à l'extension Key Usage mentionnées ci-dessus, il est possible de configurer IP Protect Client pour valider le certificat malgré tout, en ajoutant le paramètre dynamique `allow_server_extra_keyusage` défini à la valeur `true`.

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

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

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

### 17.8.2 Contraintes relatives à l'extension Extended Key Usage

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

- être présente,
- marquée comme non-critique
- uniquement contenir la valeur `id-kp-serverAuth`.

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

Dans cette configuration, le certificat sera également validé si l'extension Extended Key Usage contient la combinaison de valeurs suivante :

- `id-kp-ServerAuth` + `id-kp-ClientAuth`

## 17.9 Gestion des CA (Autorités de Certification)

Lorsque IP Protect Client 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 un token ou une carte à puce : dans ce cas, il est inaccessible au logiciel.

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


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.

## 17.10 Méthodes d'authentification des certificats

IP Protect Client prend en charge la méthode d'authentification des certificats suivante :

- méthode 9 : ECDSA with SHA-256 on the P-256 curve [RFC4754]

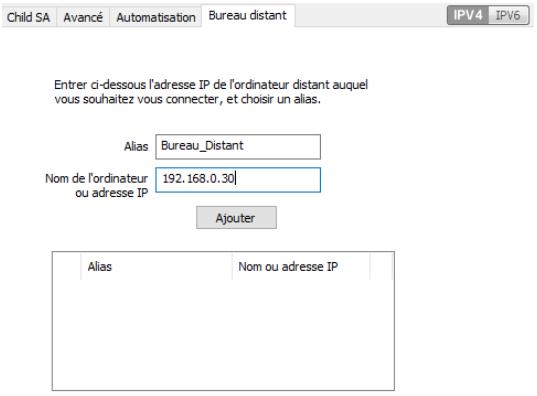
# Chapitre 18. Partage de bureau distant

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.).

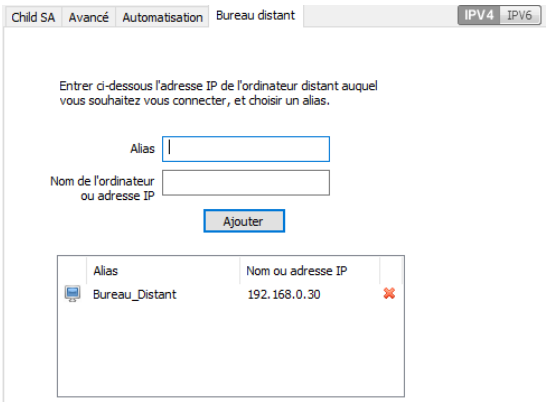
IP Protect Client permet de simplifier et de sécuriser automatiquement l'ouverture d'une session « Remote Desktop » : En un seul clic, la connexion VPN s'établit avec le poste distant et la session RDP (Remote Desktop Protocol) est automatiquement ouverte sur ce poste distant.

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

4. Sélectionnez le tunnel VPN (Child SA) dans lequel sera ouverte la session « Remote Desktop ».
5. Sélectionnez l'onglet **Bureau distant**.
6. 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.




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



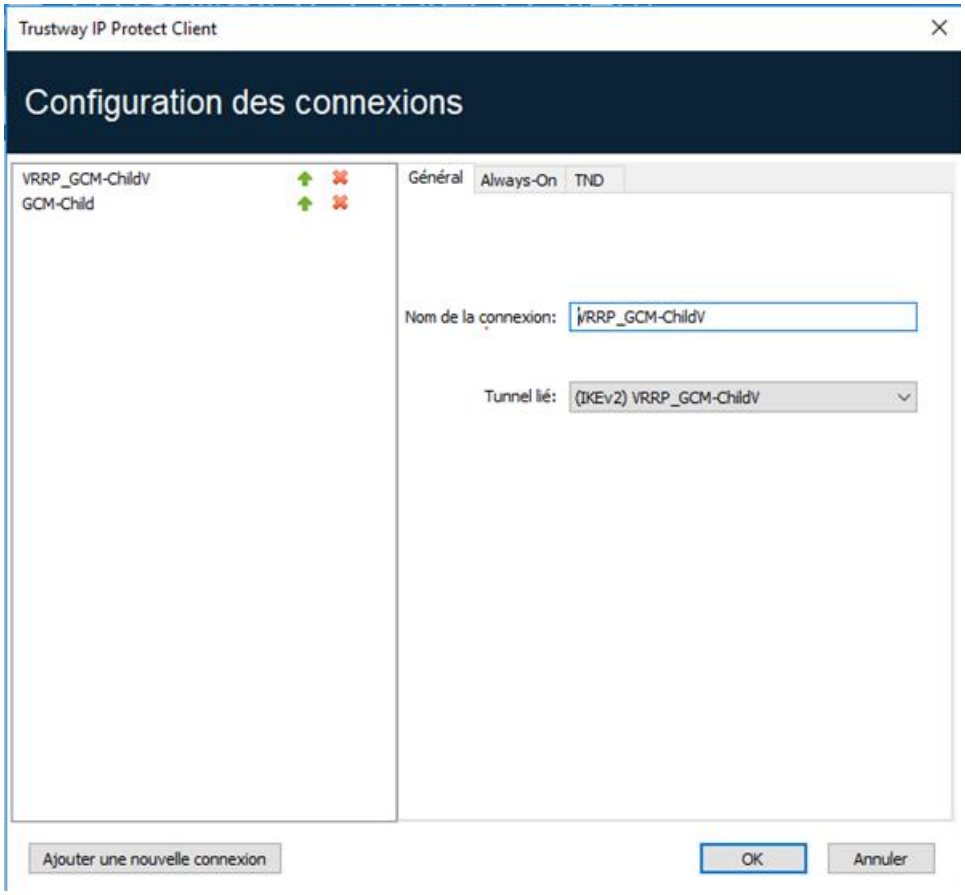

Pour ouvrir cette connexion RDP en un seul clic, il est recommandé de la faire apparaître spécifiquement dans le Panneau des Connexions, en utilisant la fonction de Gestion du Panneau des Connexions détaillée ci-après.

# Chapitre 19. Gestion du Panneau des Connexions

Le **Panneau des Connexions** IP Protect Client est entièrement configurable.


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

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




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

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

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

La partie droite comporte trois onglets :

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

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

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

Les onglets **Always-On** et **TND** sont décrits dans le Chapitre 19 Gestion du Panneau des Connexions ci-dessous.

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.

# Chapitre 20. Gestion du Panneau TrustedConnect

Le **Panneau TrustedConnect** est décrit dans le Chapitre 9 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 :

8. La connexion VPN doit être la première connexion VPN définie dans le **Panneau des Connexions**. Pour configurer cette première connexion, se reporter au Chapitre 19 Gestion du Panneau des Connexions ci-dessus.
9. 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

## 20.1 Always-On

### 20.1.1 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)

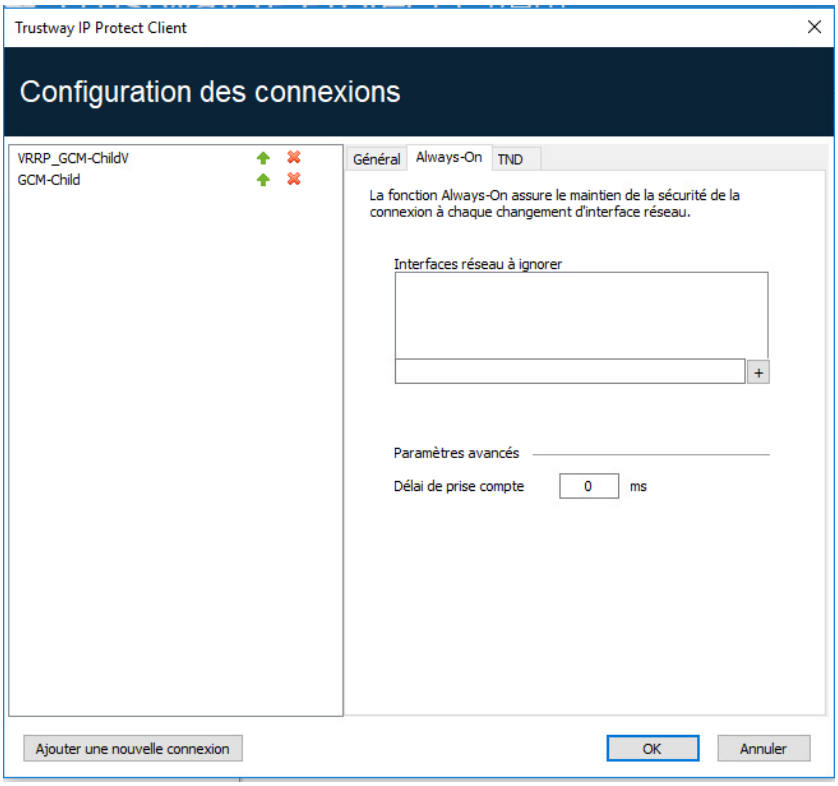
Les évènements réseau déclenchant la reconnexion automatique du tunnel (et la détection du réseau de confiance, le cas échéant), sauf exclusion explicite (voir section 20.1.2 Configuration de Always-On) sont les suivants :

- 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

### 20.1.2 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.

## 20.2 Détection du réseau de confiance (TND)

### 20.2.1 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 :

10. 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).
11. 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.

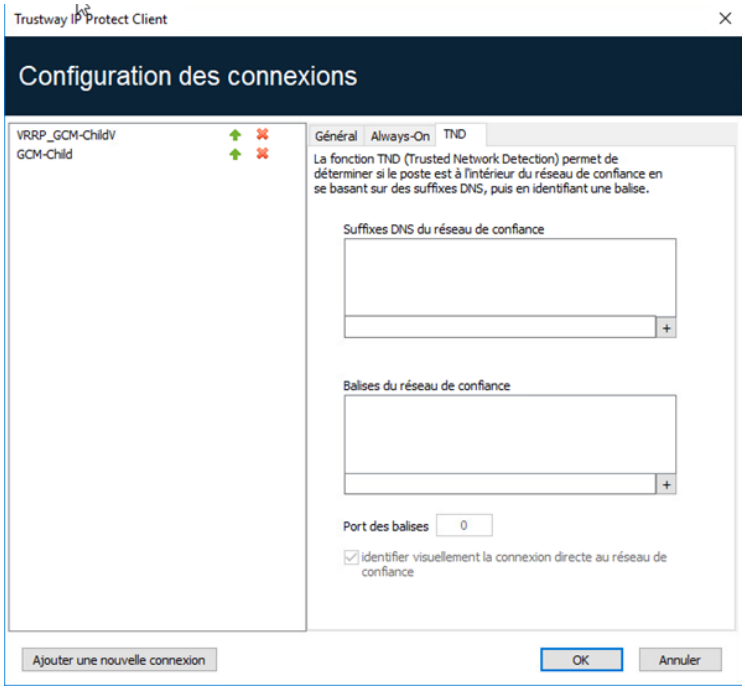
Pour activer la fonctionnalité de détection du réseau de confiance (TND), les paramètres suivants doivent donc être configurés :

- 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).

## 20.2.2 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.<br>Cette liste peut être vide ou contenir plusieurs suffixes DNS.<br>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.<br>La liste des URL 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.<br>Cette liste peut contenir plusieurs URL de serveurs de confiance. Le Client VPN teste alors successivement tous les URL et tous les certificats associés à chaque serveur, jusqu'à en trouver un accessible et valide.<br>Les URL de la liste doivent être séparés par une virgule, sans espace.<br>Il n'y a pas besoin de faire précéder un URL du préfixe `https://`. |
| **Port des balises** | Ce paramètre définit le port à utiliser pour joindre les serveurs de confiance.<br>Il n'est possible de configurer qu'un seul port, qui sera utilisé pour tous les URL.<br>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.<br>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.<br>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. |

## 20.3 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 0

La passerelle IP Protect propose une solution de redondance basée sur le protocole VRRP pour les communications entre chiffreurs. Les passerelles redondantes dans un groupe VRRP utilisent la même adresse qui est l'adresse IPsec du groupe VRRP. Il faut donc indiquer l'adresse IPsec du groupe VRRP comme adresse de passerelle et cette même adresse IPsec comme adresse de passerelle redondante.
Lorsque c'est DNS qui est utilisé, il faut de même utiliser la même adresse DNS qui représente l'adresse IPsec du groupe VRRP.

Automatisation.

## 20.4 Minimisation du Panneau

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

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.

## 20.5 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.

## 20.6 Retrait de token / carte à puce

Il est possible de configurer le comportement du **Panneau TrustedConnect** lorsque le token / carte à puce 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.

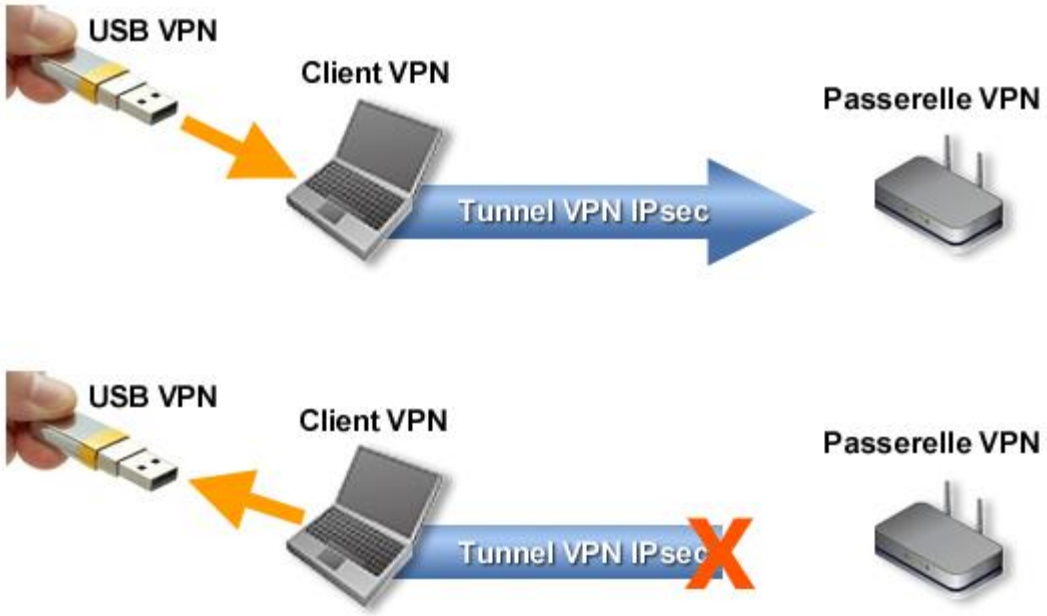
Se reporter au « Guide de Déploiement » pour les instructions correspondantes.

# Chapitre 21. Mode USB

## 21.1 Présentation

IP Protect Client offre le **Mode USB**.

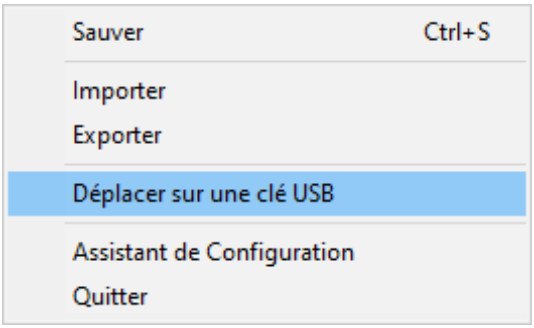
Dans ce mode, la configuration VPN est stockée de façon sécurisée sur support amovible (clé USB), le poste à partir duquel la connexion VPN est ouverte est vierge de tout élément de sécurité VPN, la connexion VPN s'établit automatiquement dès insertion de la clé USB et se ferme dès extraction de la clé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




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

## 21.2 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**.



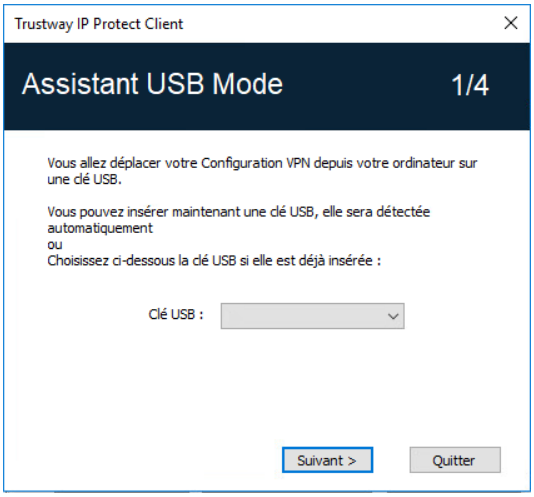

### 21.2.1 Étape 1 : Choix de la clé USB

L'écran 1 permet de choisir le support amovible (clé USB) sur lequel protéger la configuration VPN.

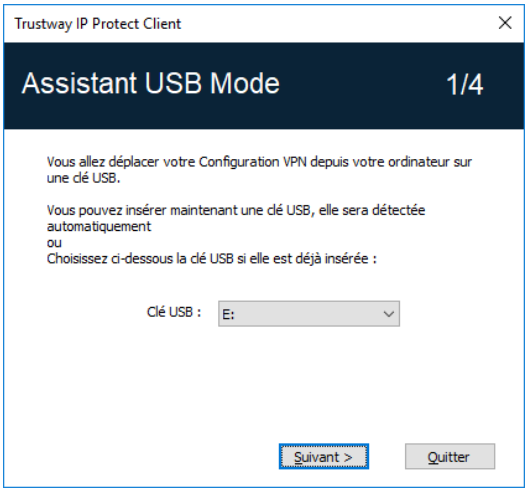
Si une clé est déjà insérée, elle est automatiquement présentée dans la liste des clés USB disponibles.

Sinon, il suffit d'insérer à cette étape la clé USB choisie, qui sera détectée automatiquement à l'insertion.

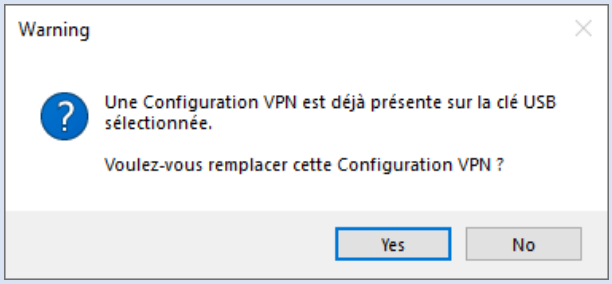
Pas de clé USB insérée




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.

### 21.2.2 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.

   La clé USB VPN ne peut pas être associée à un poste en particulier, mais pourra être utilisée sur n'importe quel poste équipé de IP Protect Client.

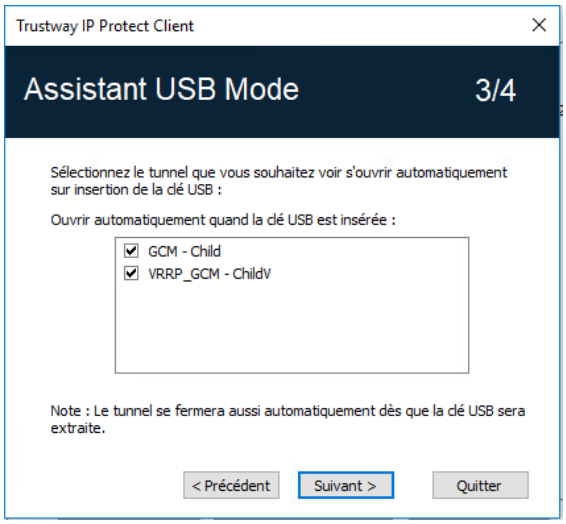
2. Protection par mot de passe :

   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.


### 21.2.3 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.

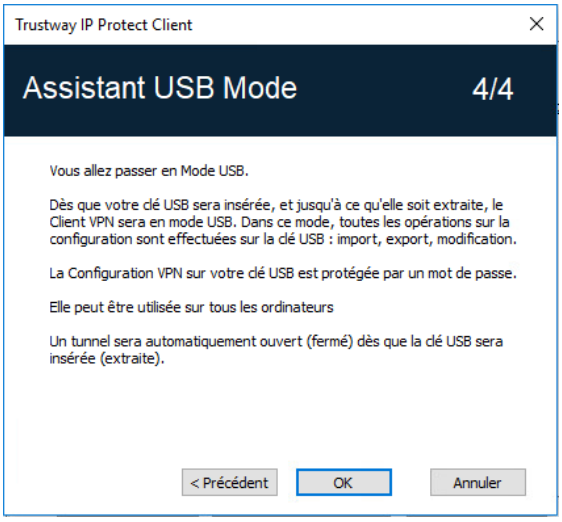



### 21.2.4 Étape 4 : Résumé

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.

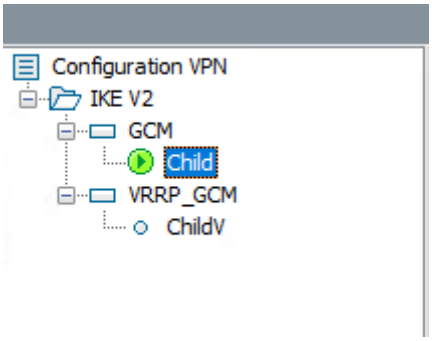
Elle reste active tant que la Clé USB reste insérée. Sur extraction de la clé USB VPN, le Client VPN revient à une configuration VPN vide.




## 21.3 Utiliser le Mode USB

Lorsque IP Protect Client 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).

IP Protect Client 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.

# Chapitre 22. Mode GINA

## 22.1 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.

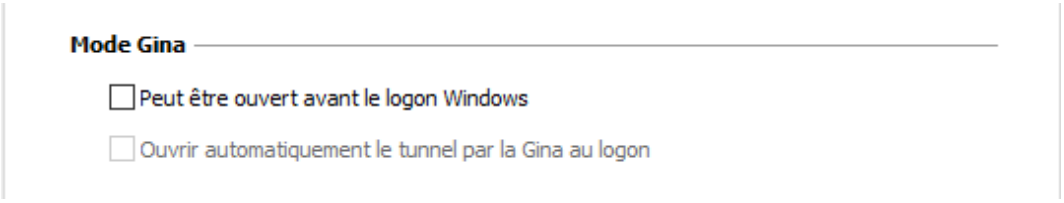
Lorsqu'un tunnel est configuré « en mode GINA », deux cas se présentent :

3. Si le mode de démarrage du Client VPN est configuré en mode **TrustedConnect** (voir Chapitre 23 Options, onglet 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.
4. 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.


## 22.2 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 14 Automatisation.



## 22.3 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 par certificat (l'utilisateur doit alors entrer le code PIN d'accès à la carte à puce).

### Considération de sécurité

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

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 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.

# Chapitre 23. Options

## 23.1 Affichage

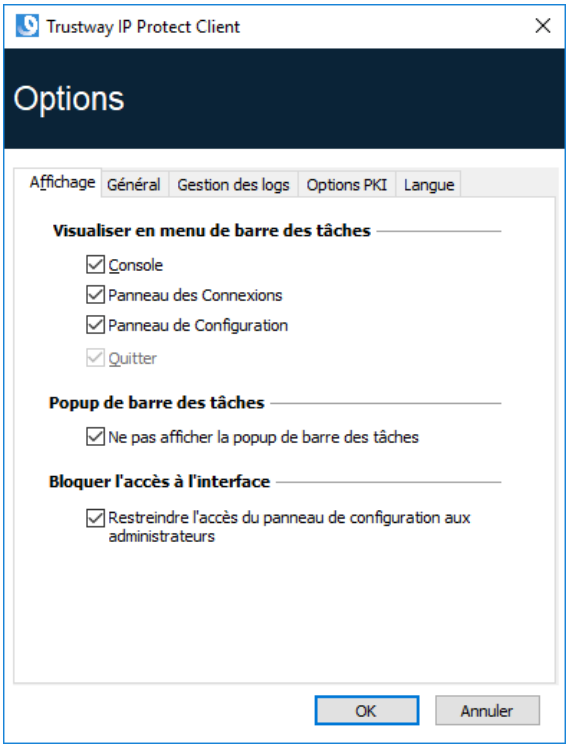
Les options de l'onglet **Affichage** de la fenêtre **Options** permettent de masquer pratiquement toutes les interfaces du logiciel :

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

### 23.1.1 Visualisation des options de menu en barre des tâches

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

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



### 23.1.2 Affichage de la popup glissante en barre des tâches

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

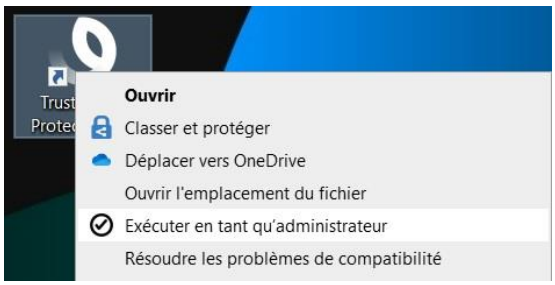
Cette fenêtre identifie l'état du tunnel au cours de son ouverture ou de sa fermeture, et disparaît automatiquement, à moins que la souris ne soit dessus :

| | |
|---|---|
| Tunnel ouvert |  |
| Tunnel fermé |  |
| Incident d'ouverture du tunnel : la fenêtre affiche l'explication succincte de l'incident. |  |

### 23.1.3 Restreindre l'accès au Panneau de Configuration

Dans IP Protect Client, 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 IP Protect Client en mode administrateur, cliquez sur l'icône **IP Protect Client** avec le bouton droit de la souris, puis sélectionnez l'option de menu **Exécuter en tant qu'administrateur**.



## 23.2 Général


### Mode de démarrage de IP Protect Client

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

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

Se reporter à la section 5.2 Démarrer le logiciel.

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

## Désactiver la détection de déconnexion

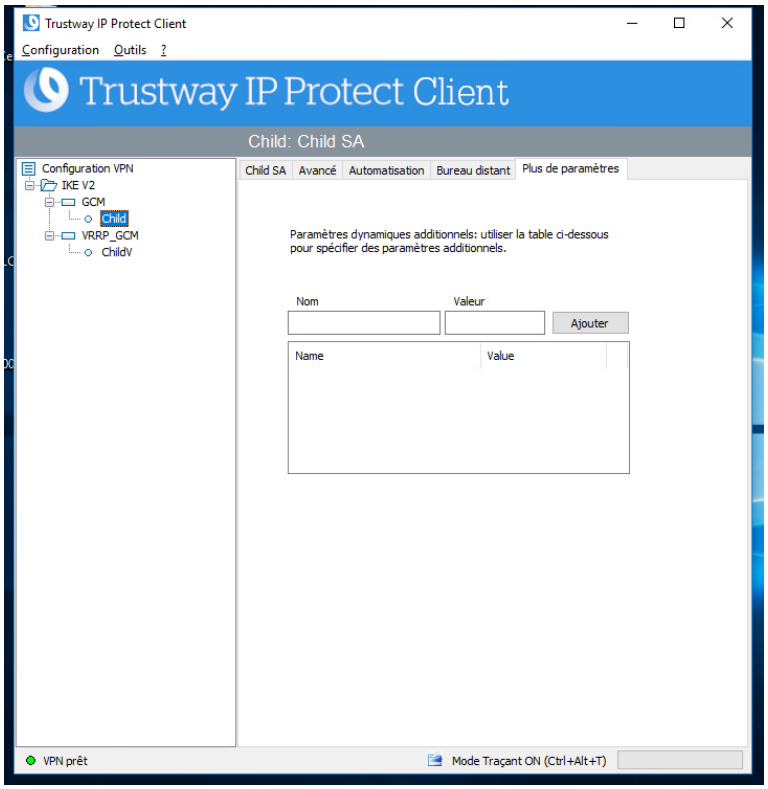
Dans son comportement standard, IP Protect Client ferme le tunnel VPN (de son côté), dès lors qu'il constate un problème de communication avec la passerelle VPN distante.

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

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

## Afficher plus de paramètres

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**.



## 23.3 Gestion des logs

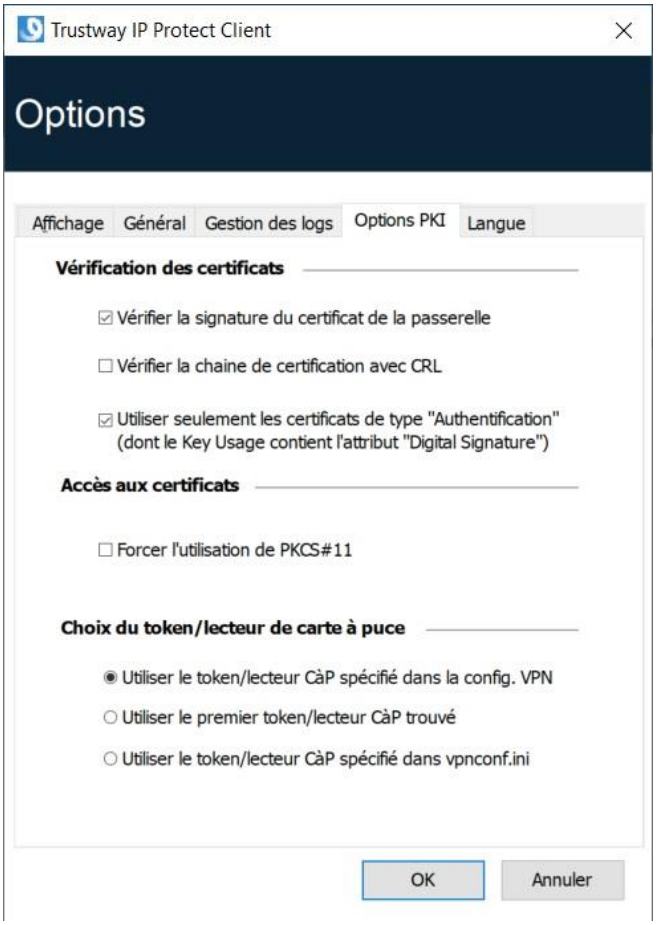
Se reporter à la section 24.1 Logs administrateur.

## 23.4 Options PKI

L'onglet **Options PKI** permet d'affiner la gestion des tokens et des cartes à puce et de caractériser précisément l'accès aux certificatsLes 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 token ou du lecteur de carte à puce 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 IP Protect Client. Ce mécanisme est décrit dans le document « Guide de Déploiement ».



### 23.4.1 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.

**Utiliser seulement les certificats de type Authentification**

Lorsque cette option est cochée, seuls les certificats de type **Authentification** (c'est-à-dire dont l'extension `key usage` contient l'attribut `digitalSignature`) sont pris en compte par le Client VPN.

Cette fonction permet de sélectionner automatiquement un certificat parmi plusieurs stockés sur la même carte à puce ou le même token.

La case à cocher est grisée lorsque la propriété `KEYUSAGE` est définie sur la valeur 2 ou 3 lors de l'installation (cf. « Guide de Déploiement ».

### 23.4.2 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 puces ou tokens.

Lorsque cette option est cochée, le Client VPN ne prend en compte que l'API PKCS#11 pour accéder au certificat des lecteurs de cartes à puce et tokens.

### 23.4.3 Choix du token/lecteur de carte à puce

**Utiliser le token/lecteur CàP spécifié dans la config. VPN**

Le Client VPN utilise les lecteurs ou tokens spécifiés dans le fichier de configuration VPN pour y chercher un certificat.

**Utiliser le premier token/lecteur CàP trouvé**

Le Client VPN utilise le premier lecteur de 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 carte à puce ou les tokens à utiliser pour y chercher un certificat.

Voir le « Guide de Déploiement ».

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.

## 23.5 Gestion des langues

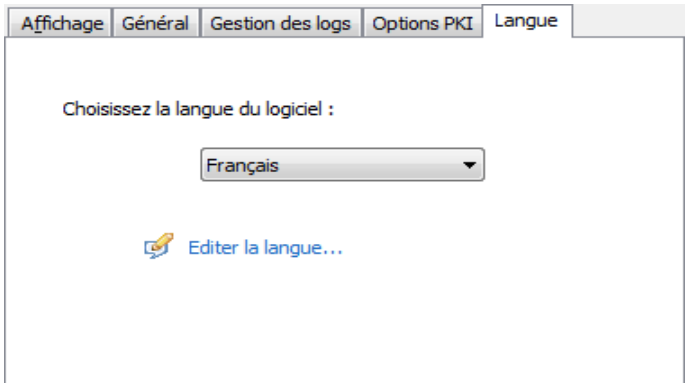
### 23.5.1 Choix d'une langue

IP Protect Client 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 28.4

Caractéristiques techniques IP Protect Client.

# Chapitre 24. Logs administrateur, console et traces

IP Protect Client propose trois types de logs :

5. Les **logs administrateur** sont spécifiquement dédiés au rapport d'activité et d'utilisation du logiciel.
6. 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.
7. Le **mode traçant** fait produire par chaque composant du logiciel le log de son fonctionnement interne. Ce mode est destiné au support pour le diagnostic d'incident logiciels.

## 24.1 Logs administrateur

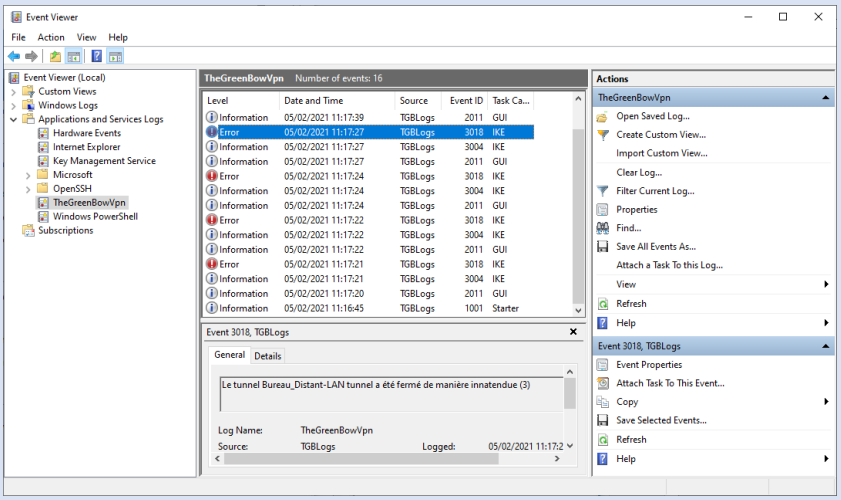
IP Protect Client permet de collecter des logs de type **administrateur** : ouverture de tunnel, certificat expiré, durée de connexion, login/mot de passe erroné, modification de la configuration VPN, import ou export de cette configuration, etc. Les **logs administrateur** offrent en particulier un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

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

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

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


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



Les logs administrateur sont listés à la section 28.2 Logs administrateur dans les annexes.

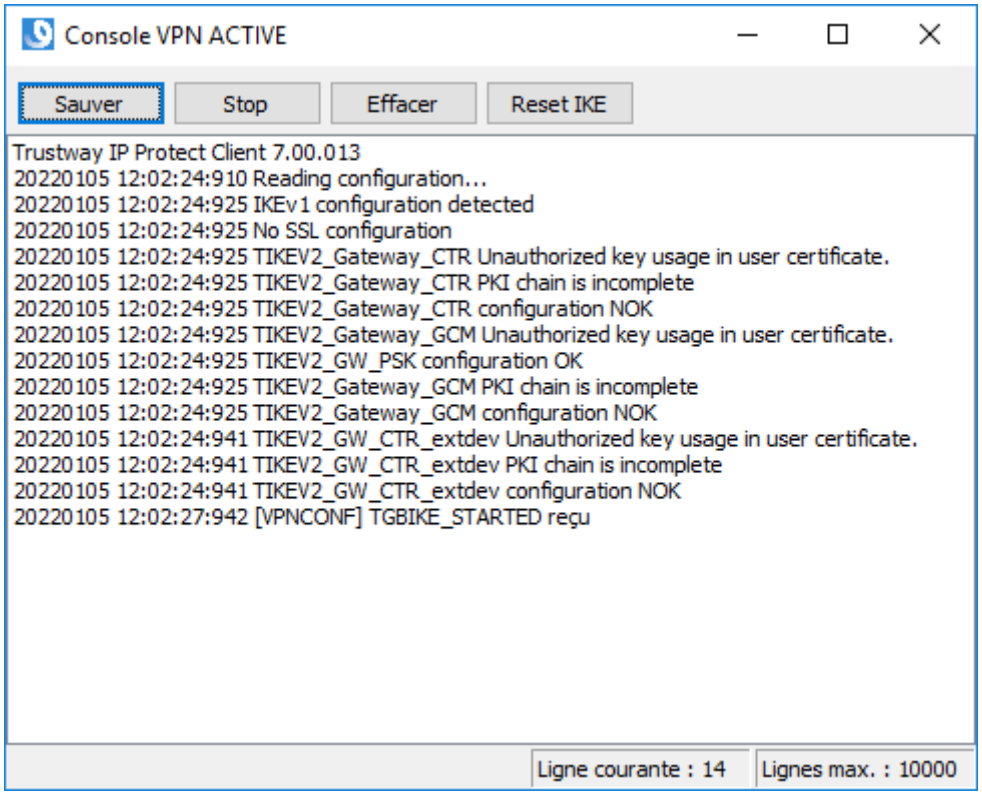
Lorsque les logs administrateur sont stockés dans un fichier local, le chemin de ces logs est le sous-répertoire **System** du répertoire des logs : `C:\ProgramData\Trustway\Trustway IP Protect Client\LogFiles\System`.

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

## 24.2 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.

## 24.3 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 de IP Protect Client génère les logs de son activité. Les logs générés sont mémorisés dans un dossier accessible en cliquant sur l'icône **Dossier** bleue dans la barre d'état du **Panneau de Configuration** (interface principale).


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.

Les **logs administrateur** lorsqu'ils sont mémorisés dans un fichier local ne sont pas purgés.

# Chapitre 25. Recommandations de sécurité

## 25.1 Hypothèses

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

### 25.1.1 Profil et responsabilités des administrateurs

- L'administrateur système et réseau et l'administrateur sécurité chargés respectivement de l'installation du logiciel et de la définition des politiques de sécurité VPN sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et les procédures d'administration.
- L'administrateur sécurité s'assure régulièrement que la configuration du produit est conforme à celle qu'il a mise en place et effectue les mises à jour requises le cas échéant.
- La fonction de journalisation du produit est activée et correctement configurée. Les administrateurs sont responsables de la consultation régulière des journaux.

### 25.1.2 Profil et responsabilités de l'utilisateur

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

### 25.1.3 Respect des règles de gestion des éléments cryptographiques

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

## 25.2 Poste de l'utilisateur

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

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

- Sa configuration permet d'éviter les attaques menées localement (analyse de la mémoire, patch ou corruption de binaire).

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

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

## 25.3 Administration du Client VPN

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

Il est recommandé de protéger l'accès à la configuration VPN par un mot de passe et de limiter la visibilité du logiciel à l'utilisateur final (comportement par défaut de IP Protect Client), comme détaillé à la section 23.1 Affichage.

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

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

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

Enfin, il est à noter que IP Protect Client 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).

## 25.4 Configuration VPN

### 25.4.1 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 ou imposé dans certains cas de ne pas utiliser les facilités suivantes offertes par le logiciel :

- Ne pas utiliser le mode EAP,

- Ne pas importer de certificat dans la configuration VPN (fonction décrite à la section 17.4 Importer un certificat), et privilégier l'utilisation de certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows,
- Ne pas utiliser le mode « Clé partagée » (fonction décrite à la section 12.3.1 IKE Auth : IKE SA) et privilégier le mode « Certificat » avec des certificats stockés sur support amovible (token) ou dans le magasin de certificats Windows,
- Ne pas exporter la configuration VPN en clair, c'est-à-dire non protégée par un mot de passe (fonction décrite à la section 11.2 Exporter une configuration VPN).

### 25.4.2 Authentification de l'utilisateur

Les fonctions d'authentification de l'utilisateur proposées par IP Protect Client 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 |
|---|---|
| Certificat mémorisé dans la configuration VPN | |
| Certificat dans le magasin de certificats Windows | |
| Certificat sur carte à puce ou sur token | forte |

### 25.4.3 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 23.4 Options PKI.

Il est recommandé de ne pas configurer IP Protect Client pour valider les certificats non conformes aux contraintes relatives aux extensions Extended Key Usage et Key Usage (ne pas utiliser le paramètre dynamique `allow_server_and_client_auth`).

### 25.4.4 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 aux sections 12.3.6 Child SA : Child SA et 12.3.7 Child SA : Avancé.

### 25.4.5 Mode GINA

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

### 25.4.6 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.

# Chapitre 26. Environnement de la certification

Dans le cadre de la certification de IP Protect Client, les recommandations de sécurité spécifiées au Chapitre 25 Recommandations de sécurité s'appliquent. De plus les exigences suivantes doivent être respectées :

1. Les administrateurs s'assurent que les fonctions hors du cadre de l'évaluation sont bien désactivées dans la configuration et que cette dernière est non accessible à l'utilisateur.
2. Le poste de l'utilisateur est dédié à un seul utilisateur, pas de comptes utilisateurs multiples.
3. La fonction de journalisation du produit est activée et configurée pour envoyer les journaux dans des fichiers locaux ou sur un serveur syslog. Les administrateurs sont responsables de la configuration et de la sécurité de ce dernier. Dans le cas des journaux locaux, la protection en modification est assurée par Windows (droit administrateur pour l'écriture).

# Chapitre 27. Support

En cas de problème avec l'un de nos produits, ou pour toute question relative à ceux-ci, les moyens d'accès au support Trustway sont précisés ci-dessous.
Il y a désormais deux outils distincts :

**1. « SOL » (Support On Line), pour les outils autres que l'ouverture de tickets :**

- Téléchargement des versions
- Accès aux informations techniques (BLL et manuels)
- Accès via : http://support.bull.com/ols
- Login & Password obtenus lors de la première connexion par fourniture d'un n° de série (et zip code) d'un matériel Trustway sous contrat de support
- Si le matériel n'est plus sous contrat, le login est supprimé. Il faut alors recommencer la procédure d'inscription une fois le contrat renouvelé
- Suivre le lien http://support.bull.com/ols/online/calls/new-subscription pour l'aide à la première connexion.

**2. « A-Smile » (Anciennement « Bull Tickets ») pour signaler et suivre les questions et problèmes :**

- Accès via " https://tickets.bull.com/otrs/customer.pl
- Login : votre adresse mail en minuscules
- Password : obtenu lors de la première connexion via le formulaire de contact ou en passant par vos interlocuteurs du support (srv.support-trustway@atos.net). Le Password peut être récupéré à postériori en cliquant sur « mot de passe oublié »
- Pour plus de détail sur l'utilisation de « A-Smile », se reporter à la notice d'utilisation

*mode-operat-client-fr-V5.4.4.pdf*

- Précisez à l'ouverture du ticket qu'il s'agit de produits Trustway.

Vous pouvez également ouvrir un ticket via le CAU (Centre d'Appel Unique) en téléphonant au numéro suivant : **08 20 08 20 00.**

N'hésitez pas à nous joindre en utilisant l'adresse email du support srv.support-trustway@atos.net.
Pour ouvrir un ticket, nous vous recommandons d'utiliser l'application A-Smile.
Trustway Products Support Team

BULL S.A.S., An Atos Compagny
Rue Jean Jaurès - BP 68
78340 Les Clayes Sous-Bois - FRANCE

# Chapitre 28. Annexes

## 28.1 Raccourcis

### 28.1.1 Panneau des Connexions

| | |
|---|---|
| ESC | Ferme la fenêtre. |
| CTRL+ENTRÉE | Ouvre le Panneau de Configuration (interface principale). |
| Flèches | Les flèches haut et bas permettent de sélectionner une connexion VPN. |
| CTRL+O | Ouvre la connexion VPN sélectionnée. |
| CTRL+W | Ferme la connexion VPN sélectionnée. |

### 28.1.2 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.<br>Si la configuration est sélectionnée (racine de l'arborescence), propose l'effacement (reset) de la configuration complète. |
| CTRL+O | Si une Child SA est sélectionnée, ouvre le tunnel VPN correspondant. |
| CTRL+W | Si une Child SA 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 un nouvel IKE Auth, si la configuration VPN est sélectionnée, ou crée une nouvelle Child SA pour l'IKE Auth sélectionné. |
| CTRL+S | Sauvegarde la configuration VPN. |

### 28.1.3 Panneau de Configuration

| | |
|---|---|
| CTRL+ENTRÉE | Permet de basculer au Panneau des Connexions. |
| CTRL+D | Ouvre la fenêtre « Console » de traces VPN. |
| CTRL+ALT+R | Redémarrage du service IKE. |
| CTRL+ALT+T | Activation du mode traçant (génération de logs). |
| CTRL+S | Sauvegarde la configuration VPN. |

## 28.2 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_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 |

| ID Log define | ID Log value | Severity | Log string |
|---|---|---|---|
| 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. |

## 28.3 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**<br>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**<br>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)<br>• Réimporter la configuration VPN puis réimporter le certificat concerné.<br>• Créer un ticket au support en joignant l'ensemble des fichiers de log. |
| 3 | **Problème de configuration**<br>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**<br>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**<br>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. |

| Code | Diagnostic | Solution |
|---|---|---|
| 6 | **Problème de configuration**<br><br>Le message **Remote ID other than expected** a été reçu. Cela signifie que la valeur du **Remote ID** ne correspond pas à la valeur attendue par la passerelle VPN distante. | • Vérifier que le paramètre **Local ID** de l'onglet **Protocole** du client VPN correspond au Remote ID de la passerelle (ou du poste) distant(e). **Attention** : le Remote ID sur le routeur est le Local ID sur le Client VPN et inversement ! |
| 7 | **Certificat passerelle**<br><br>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.<br>• Vérifier la date de début de validité du certificat de la passerelle.<br>• 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).<br>• Vérifier la mise à jour des CRL de tous les émetteurs de certificats de la chaîne de certification.<br>• Vérifier l'absence de révocation de certificats concernés dans les listes de CRL correspondante.<br>• 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.<br>• 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**<br><br>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**<br><br>La passerelle a refusé les éléments d'authentification de l'utilisateur. | • Vérifier le certificat utilisateur.<br>• 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 ! |

| Code | Diagnostic | Solution |
|---|---|---|
| | | • Vérifier les logs de la passerelle distante pour obtenir plus d'informations sur ce problème. |
| **13** | **Problème de configuration**<br>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.<br>• Créer un ticket au support en joignant l'ensemble des fichiers de log. |
| **14** | **Configuration réseau**<br>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.<br>• Créer un ticket ausupport en joignant l'ensemble des fichiers de log. |
| **15** | **Configuration réseau**<br>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.<br>• Changer l'adresse IP fournie par la passerelle au client VPN. |
| **16** | **Configuration réseau**<br>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.<br>• Créer un ticket au support en joignant l'ensemble des fichiers de log. |
| **24** | **Problème de configuration**<br>La suite d'algorithmes cryptographiques 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.<br>• 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**<br>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.<br>• Vérifier que le réseau distant (paramètre **Adresse réseau distant**) indiqué dans la configuration du client VPN est acceptable côté passerelle. |
| **26** | **Problème de configuration**<br>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**. |

| Code | Diagnostic | Solution |
|---|---|---|
| **27** | **Erreur passerelle**<br>La passerelle a reporté une erreur non prise en charge par le client VPN. | • Analyser les logs côté passerelle.<br>• Récupérer les fichiers de logs de l'utilisateur, leur analyse est nécessaire.<br>• Créer un ticket au support en joignant l'ensemble des fichiers de log. |
| **28** | **Erreur login/mot de passe**<br>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.<br>• Vérifier que l'utilisateur connaît ses identifiants s'il en a besoin lors de l'établissement de la connexion. |
| **30** | **Erreur carte à puce**<br>Impossible d'accéder au certificat stocké sur carte à puce ou token. | • Vérifier que le matériel de carte à puce ou de token est correctement configuré sur le poste de travail, et accessible depuis le client VPN. |
| **31** | **Délai d'authentification portail captif expiré**<br>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**<br>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**<br>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**<br>Une erreur s'est produite pendant l'initialisation du daemon IKE. | • Récupérer les fichiers de logs de l'utilisateur.<br>• Créer un ticket au support en joignant l'ensemble des fichiers de log. |
| **103** | **Erreur DNS**<br>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.<br>• Vérifier que le mode filtrant ne bloque pas lui-même l'accès aux requêtes DNS.<br>• Remplacer des noms DNS par des adresses IP. |
| **200** | **Activation du logiciel**<br>Le logiciel n'est pas activé et la période d'essai terminée. | • Récupérer les fichiers de logs de l'utilisateur.<br>• Vérifier l'activation du logiciel. |

## 28.4 Caractéristiques techniques IP Protect Client

### 28.4.1 Général

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

### 28.4.2 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 |
| **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) |

### 28.4.3 Connexion / Tunnel

| | |
|---|---|
| **Mode de connexion** | Peer-to-gateway |
| **Réseaux** | IPv4 |
| **Protocoles** | IPsec / IKEv2 |
| **Modes** | Main mode (mode principal) et Aggressive mode (mode agressif) |
| **Mode Config / Mode CP** | Récupération automatique des paramètres réseaux depuis la passerelle VPN |

### 28.4.4 Cryptographie

**Chiffrement, Groupes de clé, Hash (IKEv2)**

Symétrique : AES GCM 256bits

Diffie-Hellman : DH19 (ECP 256)

Hash: SHA-256

**Authentification de l'utilisateur**

Administrateur : Protection de l'accès aux configurations VPN

Utilisateur :

- Certificats X.509
- Méthode 9 : ECDSA "secp256r1" with SHA-256 on the P-256 curve [RFC4754]

**Authentification des certificats**

**IGC / PKI**

- Prise en charge des certificats X.509
- Import de fichierscertificats au format PKCS#12, PEM/PFX
- Multi-support : magasin de certificats Windows, carte à puce, token, fichier de configuration
- Prise en charge de la CRL (Certificate Revocation List)
- SélectionDétection automatique du lecteur de cartes à puce ou du token / carte à puce en fonction de critères
- Accès aux tokens / cartes à puce et aux tokens en PKCS#11 et CNG
- Vérification des certificats « Client » et « Passerelle »
- Validation compètecomplète de la chaîne des certificats « utilisateur » et « passerelle »

### 28.4.5 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) |

### 28.4.6 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 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 |

## 28.5 Licences tierces

### 28.5.1 OpenSSL

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

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

### 28.5.2 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.
```

# Glossaire

## C

**CA**

Certificate Authority. Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fournis

**Certificat**

En tant que composants du protocole X.509, les certificats sont attribués par une autorité de certification ; ils fournissent le moyen de vérifier l'identité d'une entité client ou serveur, et servent à véhiculer leur clé publique.

**Certificat root**

Certificat auto-signé.

**Chaîne complète de certificats**

Chaîne de certificats dont le dernier élément est un certificat root.

**Chaîne de certificats**

Ensemble ordonné de 'n' certificats concaténés, le certificat de rang 'i + 1' étant le signataire du certificat de rang 'i'.

**CRL**

Certificate Revocation List. Liste des identifiants des certificats qui ont été révoqués ou invalidés et qui ne sont donc plus dignes de confiance.

## G

**GVPNC**

L'objet GVPNC représente dans la configuration de la passerelle IP Protect sur le TDM un ensemble de IP Protect Clients.

## I

**IKE (Internet Key Exchange)**

Protocole d'établissement de VPN (SAs).

**IP (Internet Protocol)**

Protocole utilisé pour envoyer des datagrammes sur l'Internet.

**IPSEC (IP SECurity)**

Protocole sécurisé sur réseaux IP.

## O

**OCSP**

Protocole de vérification en ligne de la non révocation d'un certificat auprès d'un répondeur OCSP.

## U

**UDP (User Datagram Protocol)**

Protocole de transport non fiable sur IP.

## V

**VPN (Virtual Private Network)**

Réseau sécurisé sur un réseau public (non sécurisé).