Trustway IP Protect

IP PROTECT CLIENT

Guide de déploiement

IP Protect Client

Guide de déploiement

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 déployer le logiciel, avec des licences et des configurations VPN.

Pour la configuration du logiciel, un document complémentaire nommé « Guide Administrateur » est disponible.

Avant de procéder au déploiement de IP Protect Client, veuillez lire attentivement la section « Recommandations de sécurité » du « Guide Administrateur ».

Version du logiciel

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

Chapitre 1. Déploiement du Client VPN

1.1 Introduction

Le déploiement du logiciel s'appuie principalement sur sa capacité à être installé de façon silencieuse, c'est-à-dire, sans sollicitation (question ou alerte) de l'utilisateur.

Ainsi, toutes les options de configuration du logiciel peuvent être transmises à l'installation, via des fichiers d'initialisation, ou via le jeu de paramètres et de propriétés MSI en ligne de commande.

1.2 Personalisation du logiciel

Outre l'utilisation du Panneau de Configuration du logiciel pour générer des configurations VPN à déployer, Trustway IP Protect Client peut être personnalisé au cours de l'installation et lors de sa première utilisation par les trois moyens suivants :

- grâce à un ensemble de paramètres et de propriétés de l'installeur MSI passés en ligne de commande ;
- via un fichier de configuration de l'installation du logiciel (`vpnsetup.ini`) ;
- via un fichier d'initialisation PKCS#11 des tokens ou cartes à puce (`vpnconf.ini`).

Les fichiers de configuration doivent être situés dans les répertoires suivants :

- `vpnsetup.ini` doit être situé dans le répertoire `C:\Windows` ;
- `vpnconf.ini` doit être situé dans le même répertoire que celui dans lequel est installé et s'exécute Trustway IP Protect Client (par défaut : `C:\Program Files\Trustway\Trustway IP Protect Client`).

Ces différents moyens de configuration du logiciel au cours de son installation, permettent par exemple de préparer le déploiement du Client VPN sur des plates-formes hétérogènes, équipées de tokens ou lecteurs de cartes à puce différents, mais dont les certificats à exploiter présentent les mêmes caractéristiques (par exemple, les certificats à utiliser sont de type « authentification »).

Autre exemple : Le Client VPN peut être déployé sur des plates-formes équipées de tokens ou cartes à puce qui lui sont inconnus. Le fichier de configuration permet au Client VPN de les reconnaître.

1.3 Installation silencieuse

Une installation « silencieuse » est une installation qui s'effectue sans sollicitation de l'utilisateur : aucune question ni aucune alerte. L'installation est exécutée intégralement de façon transparente.

Les paramètres de l'installation sont dans ce cas configurés via le jeu de paramètres et de propriétés MSI passés en ligne de commande, ou via le fichier de configuration de l'installation du logiciel `vpnsetup.ini` (voir Chapitre 7 Fichier vpnsetup.ini).

Pour lancer l'installation en mode silencieux, utiliser l'option `/quiet` en ligne de commande.

- Ouvrez la fenêtre de commande Windows en mode administrateur et entrez la ligne de commande suivante :

```
msiexec /i "[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi" /q
```

Exemple

```
msiexec /i "[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi" /q
LICENSE=[numéro_licence]
```

`[répertoire_téléchargement]` est le répertoire où l'installeur a été téléchargé.

Pour plus d'options d'installation en ligne de commande, voir chapitre **Erreur ! Source du renvoi introuvable.**.

1.4 Déploiement d'une mise à jour

Le déploiement d'une mise à jour de Trustway IP Protect Client s'exécute exactement comme le déploiement d'une nouvelle installation.

Dans le cadre d'une mise à jour silencieuse, tout le processus de mise à jour est silencieux (sauvegarde des paramètres, désinstallation de l'ancienne version, installation de la nouvelle version, restauration des paramètres).

1.5 Réparation

La fonction de réparation de l'installateur MSI n'est pas prise en charge pour le moment.

1.6 Désinstallation

La désinstallation du logiciel peut se faire par le panneau de configuration Windows, onglet **Programmes et fonctionnalités**, ou par l'option **Désinstaller** (clic droit sur l'icône Trustway IP Protect Client) du menu Windows.

1.7 Ordre de prise en compte des propriétés et des fichiers

À l'installation, les propriétés passées en ligne de commande sont prioritaires par rapport aux valeurs équivalentes éventuellement présentes dans le fichier `vpnsetup.ini`.

Le fichier `vpnconf.ini` est pris en compte à chaque démarrage de Trustway IP Protect Client.

Chapitre 2. Déploiement de l'activation du logiciel

2.1 Introduction

Les logiciels doivent être activés pour fonctionner au-delà de leur période d'évaluation.

L'activation des logiciels est réalisée en ligne sur un site Internet.

Les paramètres d'activation peuvent être configurés pour être pris en compte automatiquement au cours du processus d'installation et de déploiement du logiciel, soit en ligne de commande, soit dans le fichier de configuration de l'installation vpnsetup.ini. Ces méthodes sont décrites dans les sections ci-dessous

2.2 Activation sur le site Internet

Via l'utilisation des paramètres d'activation, l'activation du logiciel peut être entièrement intégrée dans le processus de déploiement du logiciel, en s'exécutant automatiquement et de façon transparente pour l'utilisateur final.

Pour que l'activation s'exécute automatiquement et de façon transparente pour l'utilisateur, utilisez les options de ligne de commande de l'installeur : `AUTOACTIV` (qui automatise l'activation) et `NOACTIVWIN` (qui masque la fenêtre d'activation), conjointement aux propriétés `LICENSE` et `ACTIVMAIL` comme indiqué à la section 6.5 Activation de la licence.

Ligne de commande pour une activation automatique et silencieuse :

```
msiexec /i "[répertoire_téléchargement]/Trustway_IP_Protect_Client.msi" /q
LICENSE=[numéro_de_licence] ACTIVMAIL=[email_activation] NOACTIVWIN=1 AUTOACTIV=1
```

2.3 Activation dans le tunnel

À partir de la première installation de Trustway IP Protect Client, l'utilisateur dispose de 30 jours (période d'évaluation) pour effectuer l'activation.

L'activation peut s'effectuer manuellement en ouvrant la fenêtre **À propos** de Trustway IP Protect Client (cf. « Guide Administrateur » de Trustway IP Protect Client).

Si la propriété `AUTOACTIV` est à 1, alors Trustway IP Protect Client va tenter de s'activer automatiquement :

1. à chaque démarrage du Client VPN,
2. à chaque ouverture d'un tunnel.

⚠ Si l'activation n'est pas effectuée (manuellement ou automatiquement) dans les 30 jours suivant l'installation du logiciel, il ne sera plus possible d'ouvrir de tunnel et l'activation dans le tunnel ne sera plus possible.

2.4 Identification des activations

Lors d'un déploiement, il est recommandé d'automatiser l'identification des postes sur lesquels l'activation est réalisée. Ceci permettra de gérer facilement les activations/désactivations des licences installées.

Cette identification des postes activés est réalisée en utilisant le champ **E-mail d'activation** pour, par exemple, y renseigner le nom du poste activé, ceci au cours du processus d'installation.

Script d'installation pour l'invite de commande Windows avec identifiant du poste activé :

```
msiexec /i "[répertoire_téléchargement]/Trustway_IP_Protect_Client.msi" /q
LICENSE=[numéro_de_licence] ACTIVMAIL=%ComputerName%@company.com
NOACTIVWIN=1 AUTOACTIV=1
```

Script d'installation pour Microsoft PowerShell avec identifiant du poste activé :

```
msiexec /i "[répertoire_téléchargement]/Trustway_IP_Protect_Client.msi" /q
LICENSE=[numéro_de_licence] ACTIVMAIL=$env:computername@company.com
NOACTIVWIN=1 AUTOACTIV=1
```

La variable d'environnement `%ComputerName%` ou `$env:ComputerName` est automatiquement renseignée par le système d'exploitation au moment de l'installation, puis utilisé automatiquement par l'activation.

⚠ La valeur de la propriété `ACTIVMAIL` doit toujours être formatée en respectant la syntaxe d'une adresse mail, c'est-à-dire qu'elle doit toujours comporter les caractères « @ » et « . » (point). Si ce n'est pas le cas, l'activation échoue.

Chapitre 3. Déploiement des configurations VPN

3.1 Intégrité d'une configuration VPN

La protection de l'intégrité d'une configuration VPN lorsqu'elle est exportée, ainsi que la vérification de cette intégrité lorsqu'elle est importée est une fonction activable par la propriété `SIGNFILE`. Cette propriété est desactivée par défaut.

Exemple de ligne de commande pour désactiver la signature et vérification de l'intégrité du fichier de configuration (non recommandé) :

```
msiexec /i "[répertoire_téléchargement]/Trustway_IP_Protect_Client.msi" /q SIGNFILE=0
```

Une configuration VPN préconfigurée peut être embarquée avec l'installation de Trustway IP Protect Client. Cette configuration sera automatiquement importée et appliquée au cours de l'installation du logiciel. Elle sera ainsi immédiatement opérationnelle pour l'utilisateur final, dès le premier lancement du Client VPN.

La procédure pour créer une installation de ce type est la suivante :

3. Depuis le Panneau de Configuration de Trustway IP Protect Client, créez la configuration VPN à destination du poste à équiper.
4. Exportez cette configuration VPN (menu **Configuration** > **Export**, cf. « Guide Administrateur » de Trustway IP Protect Client) en la protégeant éventuellement par mot de passe.
5. Transférez le programme d'installation et la configuration VPN sur le poste à équiper.
6. Exécutez l'installation de Trustway IP Protect Client en indiquant les propriétés `TGBCONF_PATH` et `TGBCONF_PASSWORD` (si la configuration est protégée par mot de passe, cf. section 6.4 Configuration VPN). À la fin de l'installation, le Client VPN est installé avec la configuration VPN importée et appliquée.

Exemple

```
msiexec /i "[répertoire_téléchargement]/Trustway_IP_Protect_Client.msi" /q
TGBCONF_PATH=C:\Users\Admin\conf.tgb TGBCONF_PASSWORD=[mot_de_passe]
```

Du point de vue de la sécurité du déploiement, cette méthode exploite la fonction de contrôle d'intégrité des configurations VPN, si activée. Dans ce cas, cette fonction garantit que la configuration importée au moment de l'installation n'a pas été corrompue.

3.2 Déployer la mise à jour d'une configuration VPN

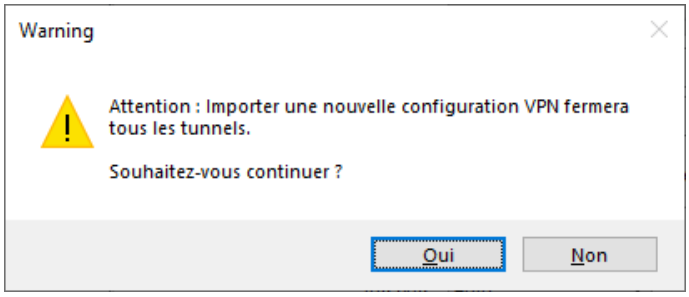
Une fois Trustway IP Protect Client installé, il est possible de mettre à jour sa configuration VPN en utilisant la fonction d'importation d'un fichier de configuration en ligne de commande.

Pour importer une configuration en ligne de commande, procédez comme suit :

7. Créez la configuration VPN à destination du poste à équiper.
8. Exportez cette configuration (menu **Configuration** > **Export**, cf. « Guide Administrateur » de Trustway IP Protect Client). Elle peut être chiffrée par un mot de passe.
9. Transférez cette configuration VPN sur le poste à mettre à jour.
10. Sur le poste cible, utilisez `vpnconf.exe` en ligne de commande, en spécifiant le cas échéant le mot de passe utilisé pour protéger la configuration exportée (cf. options `/add`, `/replace` et `/pwd` détaillées à la section 5.3 Importation).
11. Si un ou plusieurs tunnels sont ouverts, la fenêtre d'avertissement suivante s'affiche :

Si vous souhaitez effectuer une mise à jour silencieuse de la configuration (sans fenêtre d'avertissement), lorsqu'un ou plusieurs tunnels sont ouverts, utilisez les options en ligne de commande (cf. chapitre **Erreur ! Source du renvoi introuvable.**) pour les fermer et éventuellement les rouvrir après.

Lorsque l'accès au **Panneau de Configuration** est restreint aux administrateurs, il est nécessaire de lancer l'interpréteur de lignes de commandes (cmd, PowerShell…) en tant qu'administrateur pour pouvoir utiliser les commandes d'importation ou d'exportation : `/import`, `/importonce`, `/add`, `/replace`, `/export`, `/exportonce`.



Pour plus de détail sur les options de ligne de commande, voir le Chapitre 6 Utilisation en ligne de commande.

Chapitre 4. Déploiement avec tokens ou cartes à puce

4.1 Introduction

Un grand nombre de tokens et de cartes à puce permettant une authentification forte multi-facteurs (MFA) sont prise en charge par Trustway IP Protect Client via l'une des API suivantes : CNG (par défaut) ou PKCS#11.

4.1.1 CNG

CNG signifie « Cryptography API: Next Generation ». C'est une API d'accès aux tokens et aux cartes à puce actuellement fournie par Microsoft. Elle est utilisée par défaut par Trustway IP Protect Client, et ne requiert pas de configuration supplémentaire.

4.1.2 PKCS#11

PKCS#11 est une API d'accès aux tokens ou aux cartes à puce standardisée par RSA Labs. La plupart des tokens ou cartes à puce sont compatibles PKCS#11. L'utilisation de l'API PKCS#11 par Trustway IP Protect Client requiert l'installation préalable sur le poste cible d'un middleware fourni par le fabricant du token ou de la carte à puce.

Pour forcer Trustway IP Protect Client à utiliser l'API PKCS#11 au lieu de l'API CNG, utilisez l'option **Forcer l'utilisation de PKCS#11** (voir la section « Options PKI » dans le « Guide Administrateur » de Trustway IP Protect Client) ou bien la propriété MSI `PKCS11ONLY` à l'installation du logiciel (cf. section 6.7.2 PKCS11ONLY).

Trustway IP Protect Client prend en charge les tokens ou cartes à puce compatibles PKCS#11 des principaux fabricants (Gemalto, IN Groupe, Neowave, Feitian, Yubico, etc.) sans configuration supplémentaire.

Pour les tokens ou cartes à puce qui ne sont pas reconnus en standard par Trustway IP Protect Client, le logiciel offre la possibilité de spécifier leurs caractéristiques dans un fichier d'initialisation PKCS#11 appelé `vpnconf.ini`, décrit ci-après.

4.2 Fichier vpnconf.ini

Pour permettre à Trustway IP Protect Client de prendre en charge des tokens ou cartes à puces non reconnus en standard, un fichier `vpnconf.ini` doit être créé dans le répertoire d'installation du Client VPN (par défaut : `C:\Program Files\Trustway\Trustway IP Protect Client`). Il peut être établi avec un éditeur texte classique (p. ex. Bloc-notes).

Les paramètres à indiquer dans le fichier `vpnconf.ini` sont répartis en plusieurs sections :

- une succession de sections (optionnelles) `ATR` qui pemettent de définir les attributs de tokens ou cartes à puce qui ne sont pas reconnus en standard par le logiciel ;
- une section (optionnelle) `ROAMING` qui permet de caractériser le token ou la carte à puce à utiliser lors de l'initialisation du logiciel.

4.2.1 Sections ATR

ATR signifie « Answer To Reset ». C'est un identifiant retourné par le token ou la carte à puce sur commande de réinitialisation. Cet identifiant est lié au fabricant et au modèle de token ou de carte à puce.

Chaque section ATR décrit les caractéristiques nécessaires pour accéder à un token ou une carte à puce, ou à une famille de tokens ou de cartes à puce qui ne sont pas encore connues du logiciel.

Les paramètres à indiquer dans la section ATR sont détaillés dans la table suivante :

Paramètre	Signification
`[ATR#]`	ATR du token ou de la carte à puce à ajouter
`mask`	Masque à utiliser avec cet ATR[1]
`scname`	Nom du token ou de la carte à puce (champ purement descriptif)
`manufacturer`	Nom du constructeur (champ purement descriptif)
`pkcs11dllname`	Nom de la DLL PKCS#11
`dllpath`	Chemin d'accès à la DLL PKCS#11. Le chemin est le chemin complet. Il doit contenir aussi le nom de la DLL[2]
`registry`	Nom de la clef en base de registre indiquant le chemin vers le middleware[3]

[1] Les informations relatives aux ATR et aux masques des ATR sont fournies par les fabricants de tokens ou de cartes à puce. En cas de doute, un masque ne contenant que FF peut être configuré. Les longueurs de l'ATR et du masque doivent être identiques. La ligne `mask` peut ainsi prendre la forme suivante : `mask=FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF`

[2] L'un des deux paramètres `dllpath` ou `registry` doit obligatoirement être défini.

[3] idem

Exemple

```
[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:00:01]
mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"
scname="Nom de la carte"
manufacturer="Nom de la société"
pkcs11dllname="mdlw.dll"
dllpath="C:\chemin\vers\middleware\mdlw.dll"
```

4.2.2 Section ROAMING

La section ROAMING permet de caractériser le token ou la carte à puce à utiliser lorsque l'option **Utiliser le lecteur token/CàP spécifié dans vpnconf.ini** est sélectionnée (voir la section Options PKI dans le « Guide Administrateur » de Trustway IP Protect Client) ou lorsque l'installation du logiciel a été effectuée avec la propriété `SMARTCARDROAMING` égale à 2 ou 3 (voir section 6.7.1 SMARTCARDROAMING).

Les paramètres à indiquer dans la section ROAMING sont détaillés dans la table

Paramètre	Signification
`SmartCardReader`	Nom du lecteur de cartes à puce ou du token à utiliser
`SmartCardMiddleware`	Fichier dll utilisé pour communiquer avec le token ou à la carte à puce
`SmartCardMiddlewareType`	Type de middleware[4]
`SmartCardMiddelwarePath`	Chemin vers le middleware incluant le nom du middleware[5]
`SmartCardMiddlewareRegistry`	Nom de la clef en base de registre indiquant le chemin vers le middleware[6]

suivante :

[4] PKCS#11 est la seule valeur possible pour le paramètre `SmartCardMiddlewareType`.

[5] L'un des deux paramètres `SmartCardMiddlewarePath` ou `SmartCardMiddlewareRegistry` doit obligatoirement être défini.

[6] idem

Les paramètres d'accès à la base de registre doivent respecter la syntaxe suivante :
`CLEF_PRIMAIRE:chemin\\vers\\la\\clef\\spécifique:valeur`

Exemple

```
[ROAMING]
SmartCardReader="Nom de la carte"
SmartCardMiddleware="mdlw.dll"
SmartCardMiddlewareType="PKCS#11"
SmartCardMiddlewareRegistry="HKEY_LOCAL_MACHINE:SOFTWARE\\Fournisseur\\Prod\\CK:PKCS#11DLL"
```

Chapitre 5. Utilisation en ligne de commande

5.1 Introduction

Trustway IP Protect Client offre en standard un jeu d'options de ligne de commande, utilisables dans des scripts ou dans des fichiers batch. Ces options permettent d'effectuer diverses opérations comme : ouvrir ou fermer un tunnel VPN, importer ou exporter une configuration VPN, etc.

La syntaxe des options de ligne de commande est toujours la même :

```
"[répertoire_installation]\vpnconf.exe" [/option[:valeur]]
```

- `[répertoire_installation]` est le répertoire dans lequel se trouve l'exécutable `vpnconf.exe` (soit le répertoire d'installation du logiciel Trustway IP Protect Client).
- Si la valeur contient des espaces (par exemple un répertoire), elle doit être encadrée par des guillemets.
- Toutes les options disponibles sont détaillées ci-dessous.

La ligne de commande `vpnconf.exe` ne peut être lancée lorsque Trustway IP Protect Client est démarré en mode TrustedConnect. Il convient de quitter le Panneau TrustedConnect pour utiliser les options en ligne de commande, avant de le relancer éventuellement.

Dans ce chapitre, le nom du tunnel est composé comme suit :

	Nom Tunnel
IKEv2	IKEAuth-ChildSA

Le nom de tunnel est sensible à la casse. Si le nom comporte des espaces, il convient de le mettre entre guillemets.

5.2 Différence entre import, importonce, add et replace

L'option `/import` permet d'importer une configuration VPN en démarrant en même temps Trustway IP Protect Client, s'il n'est pas déjà démarré.

L'option `/importonce` permet d'importer une configuration VPN sans démarrer Trustway IP Protect Client.

Lorsque Trustway IP Protect Clientest démarré, ces deux options importent simplement la configuration VPN.

Lorsque la configuration VPN courante (avant importation) de Trustway IP Protect Client n'est pas vide, ces deux options affichent une pop-up qui demande à l'utilisateur s'il veut « Ajouter ou remplacer », c'est-à-dire ajouter la nouvelle configuration VPN ou remplacer l'ancienne par la nouvelle.

Les options `/add` et `/replace` permettent d'éviter cette demande à l'utilisateur : l'option `/add` ajoute systématiquement la configuration VPN, l'option `/replace`

Option	Demande « Ajouter ou remplacer »	Lance le Client VPN s'il n'est pas démarré
`/import`	Oui	Oui
`/importonce`	Oui	Non
`/add`	Non : ajoute la configuration VPN	Non
`/replace`	Non : remplace la configuration VPN	Non

remplace systématiquement l'ancienne configuration par la nouvelle.

Lorsque l'accès au Panneau de Configuration est restreint aux administrateurs, il est nécessaire de lancer l'interpréteur de lignes de commandes (cmd, PowerShell, ...) en tant qu'administrateur pour pouvoir utiliser les commandes d'importation ou d'exportation : `/import`, `/importonce`, `/add`, `/replace`, `/export`, `/exportonce`.

5.3 Importation

5.3.1 /import

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /import:[NomFichierConfig]`

Usage : Cette option est utilisée pour importer une configuration VPN en démarrant Trustway IP Protect Client.

Cette option peut être utilisée pour lancer le logiciel Trustway IP Protect Client avec une configuration VPN donnée.

Si le Client VPN est en cours d'exécution, cette option importe et met à jour la configuration VPN sans arrêter le logiciel. Une fenêtre s'affiche pour demander si la configuration doit être ajoutée ou remplacée. Si un tunnel est ouvert au moment de l'importation, celui-ci est fermé et aucun tunnel n'est ouvert automatiquement.

`[NomFichierConfig]` est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client \vpnconf.exe" /import:"C:\Mes documents\myvpnconf.tgb"`

Si la configuration VPN importée est protégée par un mot de passe, `/import` doit être accompagnée de l'option `/pwd` (voir ci-dessous).

Lorsque la configuration VPN courante n'est pas vide, le logiciel affiche une fenêtre qui demande à l'utilisateur s'il veut ajouter la configuration VPN importée ou remplacer l'ancienne configuration par la nouvelle. Pour éviter l'affichage de cette fenêtre, utiliser les options `/add` ou `/replace` (voir ci-dessous).

5.3.2 /importonce

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /importonce:[NomFichierConfig]`

Usage : Même comportement que l'option `/import`, mais sans démarrer le Client VPN.

`[NomFichierConfig]` est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.

Retour : Voir la note sur les codes retour ci-dessous.

0 : La commande s'est bien déroulée
1 : Le fichier n'a pas été trouvé
2 : La signature du fichier n'est pas correcte
3 : Le mot de passe n'est pas correct (la configuration est protégée)
4 : Le mot de passe est requis et n'a pas été obtenu (fenêtre de demande de mot de passe annulée)

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client" /importonce:"C:\Mes documents\myvpnconf.tgb"`

Lorsque la configuration VPN est vide, les options `/import` et `/importonce` ne demandent rien à l'utilisateur et « ajoutent » la configuration VPN.

Lorsque la configuration VPN courante n'est pas vide, le logiciel affiche une fenêtre qui demande à l'utilisateur s'il veut ajouter la configuration VPN importée ou remplacer l'ancienne par celle importée. Pour éviter l'affichage de cette fenêtre, utiliser les options `/add` ou `/replace` (voir ci-dessous).

La commande `/importonce` est préemptive et bloque la ligne de commande jusqu'à la fin de son exécution.
Elle retourne un code d'erreur dans la variable `ERRORLEVEL` (cf. codes retour ci-dessus).
`/importonce` spécifié sans mot de passe affiche une boîte de dialogue à l'utilisateur si ce mot de passe est requis.

Si l'utilisateur annule la question Ajouter/Remplacer, alors un code retour 1 est mis dans `ERRORLEVEL` (dans un script, l'utilisateur n'est de toute façon pas censé utiliser un `/importonce` s'il souhaite une exécution silencieuse).

5.3.3 /add

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /add:[NomFichierConfig]`

Usage : Permet d'ajouter une configuration VPN.

`[NomFichierConfig]` est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.

Retour : Voir la note sur les codes retour ci-dessous.

0 : La commande s'est bien déroulée
1 : Le fichier n'a pas été trouvé
2 : La signature du fichier n'est pas correcte
3 : Le mot de passe n'est pas correct (la configuration est protégée)
4 : Le mot de passe est requis et n'a pas été obtenu (fenêtre de demande de mot de passe annulée)

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client \vpnconf.exe" /add:"C:\Mes documents\myvpnconf.tgb"`

Si la configuration VPN importée est protégée par un mot de passe `/add` doit être accompagnée de l'option `/pwd` (voir ci-dessous).

La commande `/add` est préemptive et bloque la ligne de commande jusqu'à la fin de son exécution.
Elle retourne un code d'erreur dans la variable `ERRORLEVEL` (cf. codes retour ci-dessus).
`/add` spécifié sans mot de passe affiche une boîte de dialogue à l'utilisateur si ce mot de passe est requis.

5.3.4 /replace

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /replace:[NomFichierConfig]`

Usage : Permet d'ajouter une configuration VPN.

`[NomFichierConfig]` est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.

Retour : Voir la note sur les codes retour ci-dessous.

0 : La commande s'est bien déroulée
1 : Le fichier n'a pas été trouvé
2 : La signature du fichier n'est pas correcte
3 : Le mot de passe n'est pas correct (la configuration est protégée)
4 : Le mot de passe est requis et n'a pas été obtenu (fenêtre de demande de mot de passe annulée)

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client \vpnconf.exe" /replace:"C:\Mes documents\myvpnconf.tgb"`

Si la configuration VPN importée est protégée par un mot de passe `/replace` doit être accompagnée de l'option `/pwd` (voir ci-dessous).

La commande `/replace` est préemptive et bloque la ligne de commande jusqu'à la fin de son exécution.
Elle retourne un code d'erreur dans la variable `ERRORLEVEL` (cf. codes retour ci-dessus).
`/replace` spécifié sans mot de passe affiche une boîte de dialogue à l'utilisateur si ce mot de passe est requis.

5.3.5 /pwd

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /pwd:[Mot_de_passe]`

Usage : Permet de spécifier un mot de passe pour les opérations d'importation et d'exportation des configurations VPN. Cette option est utilisée avec les options : `/import`, `/importonce`, `/add`, `/replace`, `/export`, `/exportonce`.

Dans la ligne de commande, l'option `/pwd` doit être spécifiée après les options d'importation ou d'exportation.

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client \vpnconf.exe" /import:"C:\Mes documents\myvpnconf.tgb" /pwd:monmdp`

D'un point de vue sécurité, il est recommandé de privilégier les options `/importonce`, `/add` et `/replace` pour des opérations de maintenance (versus l'option `/import`), puisque le logiciel est quitté immédiatement après leur exécution.

5.4 Exportation

5.4.1 /export

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /export:[NomFichierConfig]`

Usage : Permet d'exporter une configuration VPN, en démarrant le logiciel IP Protect Client.

Si le logiciel est en cours d'exécution, l'option `/export` exporte la configuration VPN sans l'arrêter.

`[NomFichierConfig]` est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.

`/export` peut être utilisé avec `/pwd` pour exporter une configuration VPN en la protégeant par un mot de passe.

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client \vpnconf.exe" /export:"C:\Mes documents\myvpnconf.tgb" /pwd:gq1aRe7`

5.4.2 /exportonce

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /exportonce:[NomFichierConfig]`

Usage : Même comportement que l'option `/export`, mais sans démarrer le logiciel IP Protect Client.

Si le logiciel est en cours d'exécution, l'option `/exportonce` exporte la configuration VPN sans l'arrêter.

`[NomFichierConfig]` est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.

`/exportonce` peut être utilisé avec `/pwd` pour exporter une configuration VPN en la protégeant par un mot de passe.

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client \vpnconf.exe" /exportonce:"C:\Mes documents\myvpnconf.tgb" /pwd:gq1aRe7kP2t`

5.5 Ouverture/fermeture d'un tunnel VPN

Les options `/stop`, `/closeall` et `/status` ne peuvent être exécutées que si Trustway IP Protect Client est déjà lancé et n'est pas démarré en mode TrustedConnect.

Les options `/open` et `/close` peuvent être exécutées sans que Trustway IP Protect Client soit déjà lancé. Dans ce cas, le logiciel est lancé et ne quitte pas, mais il n'y a pas de code de retour pour connaître le résultat de l'exécution.

5.5.1 /stop

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /stop`

Usage : Ferme tous les tunnels VPN ouverts, et arrête le logiciel IP Protect Client.

Exemple :
```
" C:\Program Files\Trustway\Trustway IP Protect Client
\vpnconf.exe" /stop
```

5.5.2 /open

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /open:[NomTunnel]`

Usage : Permet d'ouvrir un tunnel VPN en ligne de commande.

Retour :
0 : Le tunnel est toujours fermé
2 : Le tunnel est maintenant ouvert

Autres : Voir la liste des codes retours ci-dessous.

Exemple :
```
" C:\Program Files\Trustway\Trustway IP Protect Client
\vpnconf.exe" /open:TgbTest-TgbTest

@echo retour = %ERRORLEVEL%

Pause
```

5.5.3 /status

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /status:[NomTunnel]`

Usage : Permet d'obtenir l'état d'un tunnel VPN par ligne de commande.

Retour :
0 : Le tunnel VPN est fermé
1 : Le tunnel VPN est en cours d'ouverture
2 : Le tunnel VPN est ouvert
3 : Le tunnel VPN est en cours de fermeture
4 : Erreur dans l'ouverture du tunnel VPN

Autres : Voir la liste des codes retours ci-dessous.

Exemple :

```
" C:\Program Files\Trustway\Trustway IP Protect Client
\vpnconf.exe" /status:TgbTest-TgbTest

@echo retour = %ERRORLEVEL%

Pause
```

5.5.4 /close

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /close:[NomTunnel]`

Usage : Permet de fermer un tunnel VPN par ligne de commande.

Retour : 0 : Le tunnel VPN est fermé

Autres : Voir la liste des codes retours ci-dessous

Exemple :

```
" C:\Program Files\Trustway\Trustway IP Protect Client
\vpnconf.exe" /close:TgbTest-TgbTest
```

5.5.5 /closeall

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /closeall`

Usage : Permet de fermer tous les tunnels VPN ouverts.

Retour : 0 : Tous les tunnels VPN sont fermés

Autres : Voir la liste des codes retours ci-dessous

Exemple :

```
" C:\Program Files\Trustway\Trustway IP Protect Client
\vpnconf.exe" /closeall
```

5.6 Redémarrage

L'option `/resetike` ne peut être exécutée que si Trustway IP Protect Client est déjà lancé et n'est pas démarré en mode TrustedConnect.

5.6.1 /resetike

Syntaxe : `"[répertoire_installation]\vpnconf.exe" /resetike`

Usage : Permet de redémarrer le service IKE en ligne de commande.

Retour : 0 : Le service IKE est redémarré

Autres : Voir la liste des codes retours ci-dessous

Exemple : `" C:\Program Files\Trustway\Trustway IP Protect Client \vpnconf.exe" /resetike`

5.7 Codes retours

Les options de ligne de commande (`/open`, `/close`, `/status`, `/closeall`, `/resetike`) peuvent retourner les codes suivants :

-1	Impossible d'exécuter la commande : le Client VPN n'est pas encore lancé.
100 à 499	Erreur interne (contacter le support).
500	Le tunnel VPN spécifié n'existe pas (attention à la casse !).
501 à 999	Erreur interne (contacter le support).
1000 à 1999	Autre problème d'accès au tunnel VPN.
1089	Pas de réponse de la passerelle.
1090	La passerelle refuse d'authentifier le client (IKE_AUTH Failed).

Chapitre 6. Paramètres et propriétés de l'installeur MSI

6.1 Introduction

L'installeur de Trustway IP Protect Client est au format Microsoft Installeur (MSI). Il peut être configuré grâce à des paramètres en ligne de commande et des « propriétés ».

Pour installer Trustway IP Protect Client, il est recommandé de lancer la ligne de commande `MSIEXEC` depuis un shell admin avec l'option `/i`, l'option `/q` ou `/quiet` et les propriétés adaptées à votre déploiement.

Exemple

```
msiexec /i [chemin_de_l_installeur] /q
```

Règles de syntaxe : Les options qui requièrent une valeur doivent être spécifiées sans espace entre l'option et sa valeur. Les valeurs qui contiennent des espaces (par exemple des répertoires) doivent être encadrées par des guillements.

Pour plus de détail sur le fonctionnement de `msiexec` et les options d'installation disponibles, consultez la documentation Microsoft : https://docs.microsoft.com/fr-fr/windows-server/administration/windows-commands/msiexec.

6.2 Paramètres MSI en ligne de commande

6.2.1 /i

Syntaxe :	`msiexec /i [chemin_de_l_installeur]`
Usage :	Installe ou met à jour le logiciel Trustway IP Protect Client
Exemple :	`msiexec /i "[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"`

6.2.2 /x

Syntaxe :	`msiexec /x [chemin_de_l_installeur]`
Usage :	Désinstalle le logiciel Trustway IP Protect Client

Exemple : `msiexec /x "[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"`

6.2.3 /q

Syntaxe : `msiexec /q` ou `/quiet`

Usage : Configure l'installation ou la désinstallation en mode silencieux (aucune question ni alerte à l'utilisateur)

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"
/q
```

6.2.4 /L*V!

Syntaxe : `msiexec /L*V! <chemin_fichier_logs>`

Usage : Active la journalisation et comprend une sortie détaillée dans le fichier journal de sortie en spécifiant l'emplacement et le nom du fichier journal de sortie.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"
/L*V! "C:\install.log"
```

6.3 Installation

« `C:\Program Files\Trustway\Trustway IP Protect Client` » est le répertoire d'installation par défaut.

6.3.1 APPLICATIONROOTDIRECTORY

Syntaxe : `APPLICATIONROOTDIRECTORY=[répertoire_installation]`

Usage : `[répertoire_installation]` est le répertoire où le logiciel IP Protet Client doit être installé.

`[répertoire_installation]` nécessite d'être encadré par des guillemets si le répertoire contient des espaces.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"
APPLICATIONROOTDIRECTORY="C:\mon répertoire\vpn"
```

6.3.2 NOAUTORUN

Syntaxe : `NOAUTORUN=1`

Usage : Cette propriété permet de ne pas lancer Trustway IP Protect Client (quel que soit le mode : Panneau des Connexions, TrustedConnect) au démarrage de Windows. Valeur par défaut 0 (démarrage automatique).

6.4 Configuration VPN

6.4.1 TGBCONF_PATH

Syntaxe : `TGBCONF_PATH=[chemin_fichier_conf]`

Usage : Chemin complet vers le fichier de configuration VPN à utiliser pour cette installation.

6.4.2 TGBCONF_PASSWORD

Syntaxe : `TGBCONF_PASSWORD=[mot_de_passe]`

Usage : Mot de passe utilisé pour protéger la configuration VPN passée en paramètre via la propriété `TGBCONF_PATH`.

6.5 Activation de la licence

6.5.1 ACTIVMAIL

Syntaxe : `ACTIVMAIL=[email_d_activation]`

Usage : Cette propriété permet de configurer l'adresse email utilisée pour l'activation du logiciel.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"
ACTIVMAIL=salesgroup@company.com
```

6.5.2 AUTOACTIV

Syntaxe : `AUTOACTIV=1`

Usage : Cette propriété permet de configurer le logiciel pour qu'il s'active automatiquement. Lorsque la valeur est à 1, Trustway IP Protect Client va tenter de s'activer automatiquement :

12. à chaque démarrage du Client VPN,
13. à chaque ouverture d'un tunnel.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"
AUTOACTIV=1
```

6.5.3 LICENSE

Syntaxe : `LICENSE=[numéro_licence]`

Usage : Cette propriété permet de configurer le numéro de licence utilisé pour l'activation du logiciel.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\Trustway_IP_Protect_Client.msi"
LICENSE=1234567890ABCDEF12345678
```

6.5.4 NOACTIVWIN

Syntaxe : `NOACTIVWIN=1`

Usage : Cette propriété permet d'empêcher l'affichage de la fenêtre d'activation.

Associée à la propriété `AUTOACTIV=1`, elle permet de déployer le logiciel non activé sur les postes utilisateurs, et d'automatiser l'activation depuis ces postes, de façon totalement invisible pour les utilisateurs.

À noter toutefois que la fenêtre d'activation finira par être affichée à l'utilisateur à l'expiration de la période d'évaluation si aucune activation n'a été réalisée avant cette échéance.

6.6 Panneau TrustedConnect

Les propriétés liées au Panneau TrustedConnect sont décrites ci-après.

6.6.1 USEDIALERBYDEFAULT

Syntaxe : `USEDIALERBYDEFAULT=1`

Usage : Le Panneau TrustedConnect est utilisé comme interface utilisateur lorsque cette propriété a pour valeur 1. Le Panneau TrustedConnect se lancera automatiquement au démarrage de la session utilisateur Windows, sauf si la propriété `NOAUTORUN` est mise à la valeur 1 (voir ci-dessous).

6.6.2 DIALERMINIMIZE

Syntaxe : `DIALERMINIMIZE=5000`

Usage : Cette propriété permet de configurer le délai avant que le Panneau TrustedConnect ne soit minimisé, lorsque le poste a été détecté comme étant connecté au réseau de confiance (soit physiquement, soit au travers du tunnel VPN).

Ce délai est configurable en millisecondes.

Si la valeur est 0, la fonctionnalité est désactivée : le Panneau TrustedConnect ne se minimise plus automatiquement.

Si ce délai n'est pas configuré, le délai par défaut est de 2000 ms (2 secondes).

6.6.3 DIALERDEFS

Syntaxe : `DIALERDEFS=01000000`

Usage : Cette propriété permet de configurer le type de minimisation lorsque le délai de minimisation est configuré : le Panneau TrustedConnect peut être minimisé en barre des tâches ou dans la zone de notification (systray).

Pour que le Panneau TrustedConnect soit minimisé en barre des tâches, entrez la valeur `01 00 00 00`.

Si la propriété n'est pas précisée, le Panneau TrustedConnect est minimisé par défaut dans la zone de notification (systray).

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

6.6.4 VPNLOGPURGE

Syntaxe : `VPNLOGPURGE=3`

Usage : Cette propriété permet de configurer le nombre de jours pendant lequel conserver les fichiers de logs.

La valeur s'exprime en nombre de jours.

La valeur par défaut est de 10 jours.

Si la valeur indiquée est à 0, la purge des fichiers de logs est désactivée.

6.6.5 TOKENOUTHANDLE

Syntaxe : `TOKENOUTHANDLE=30`

Usage : Cette propriété permet de configurer le comportement de IP Protect Client lorsque le token est extrait ou lorsque la carte à puce est extraite du lecteur, alors qu'un tunnel VPN est ouvert.

Trois modes sont disponibles sur cet évènement :

Mode A : Le tunnel est fermé immédiatement lors de l'extraction du token / càp. (par défaut).
Mode B : Le tunnel reste ouvert durant un délai configuré (uniquement disponible avec le **Panneau TrustedConnect**).
Mode C : Le tunnel reste ouvert indéfiniment

Remarque : Dans le mode C, si le token ou la carte à puce est nécessaire pour ouvrir le tunnel VPN, alors la prochaine renégociation échouera.

Par défaut, sans paramétrage, le mode A est actif.

`TOKENOUTHANDLE=0` => pas de fermeture de tunnel sur extraction du token / càp (Mode C)

`TOKENOUTHANDLE=N` => Avec le **Panneau TrustedConnect**, temps en secondes avant que le tunnel ne soit fermé, sur extraction du token / càp (mode B).
Avec le **Panneau des Connexions**, le tunnel reste ouvert indéfiniment (mode C).

6.7 Tokens et cartes à puces

6.7.1 SMARTCARDROAMING

Syntaxe : `SMARTCARDROAMING=1`

Usage : Cette propriété caractérise le lecteur de carte à puce ou le token à utiliser :

Non défini Lecteur de carte ou token configuré dans la configuration VPN
Sujet du certificat dans la configuration VPN

1 Lecteur de carte ou token configuré dans la configuration VPN
Le sujet du certificat dans la configuration VPN n'est pas pris en compte

2 Lecteur de carte ou token configuré dans le fichier `vpnconf.ini`
Sujet du certificat dans la configuration VPN.

3 Lecteur de carte ou token configuré dans le fichier `vpnconf.ini`
Le sujet du certificat dans la configuration VPN n'est pas pris en compte

4 1er token ou carte à puce inséré
Sujet du certificat dans la configuration VPN

5 1er token ou carte à puce inséré
Le sujet du certificat dans la configuration VPN n'est pas pris en compte

6.7.2 PKCS11ONLY

Syntaxe : `PKCS11ONLY=1`

Usage : Cette propriété caractérise le mode d'accès à la carte à puce ou au token :

Non défini Le mode CNG (Cryptography API: Next Generation) est utilisé (valeur par défaut)

1 Force l'utilisation du mode PKCS#11

6.7.3 KEYUSAGE

Syntaxe : `KEYUSAGE=1`

Usage : Cette propriété permet de sélectionner un certificat en fonction de son champ « key usage » :

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

  Attention : quand cette valeur est utilisée, seul le certificat qui a la date de validité la plus lointaine est affiché et utilisé (que la propriété `SMARTCARDROAMING` soit activée ou non).

Lorsque la valeur de la propriété `KEYUSAGE` est définie sur 2 ou 3, la case à cocher « Utiliser seulement les certificats de type authentification » de l'onglet « Options PKI » est grisée, cf. « Guide Administrateur » Trustway IP Protect Client.

6.7.4 NOCACERTREQ

Syntaxe : `NOCACERTREQ=1`

Usage : Cette propriété configure IP Protect Client pour gérer des autorités de certification (CA) client/passerelle différentes. Elle est à renseigner (elle peut aussi être configurée par l'interface du logiciel) dès que les certificats client et passerelle sont issus de CA différentes.

6.7.5 PKICHECK

Syntaxe : `PKICHECK=1`

Usage : Cette propriété est utilisée pour caractériser la vérification du certificat de la passerelle VPN IP Protect:

0 ou non défini	Certificat de la passerelle VPN IP Protect non vérifié.
1	Les caractéristiques suivantes du certificat de la passerelle VPN IP Protect sont vérifiées : date de validité, chaîne de certification, signature et CRL de chaque certificat de la chaîne de certification.
2	Les caractéristiques suivantes du certificat de la passerelle VPN IP Protect sont vérifiées : date de validité, chaîne de certification, signature de chaque certificat de la chaîne de certification (pas les CRL) – valeur par défaut.
3	Identique à 1.

6.7.6 X509DIRECTORYSTRING

Syntaxe : `X509DIRECTORYSTRING=14`

Usage : Cette propriété caractérise l'identifiant attendu pour le Remote ID :

Non défini	Type attendu pour l'identifiant : `teletexString`
14	Type attendu pour l'identifiant : `teletexString`
13	Type attendu pour l'identifiant : `printableString`
1C	Type attendu pour l'identifiant : `universalString`
0C	Type attendu pour l'identifiant : `utf8String`
1E	Type attendu pour l'identifiant : `bmpString`

Les caractères « 0x » ne doivent plus précéder la valeur de la propriété `X509DirectoryString`.

6.7.7 MACHINESTORE

Syntaxe : `MACHINESTORE=1`

Usage : Cette propriété permet d'activer l'utilisation du magasin de certificat de la machine et non celui de l'utilisateur. Si elle n'est pas définie, c'est le magasin utilisateur qui est utilisé par défaut.

6.7.8 DNPATTERN

Syntaxe : `DNPATTERN=[texte]`

Usage : Cette propriété permet de caractériser le certificat utilisateur à utiliser : lorsqu'elle est renseignée, Trustway IP Protect Client recherche, sur token ou carte à puce et dans le magasin de certificat Windows depuis la version 6.5x, le certificat dont le sujet contient `[texte]`.

Quand cette propriété n'est pas définie, le IP Protect Client recherche le premier certificat conforme aux autres caractéristiques configurées.

6.7.9 NOPINCODE

Syntaxe : `NOPINCODE=1`

Usage : Cette propriété permet de ne pas demander de code PIN pour les tokens qui n'en n'ont pas besoin. Par exemple, c'est le cas de la microSD d'Ercom.

6.7.10 PINTIMEOUT

Syntaxe : `PINTIMEOUT=120`

Usage : Cette propriété spécifie une valeur de temporisation en secondes, qui permet de fermer automatiquement la fenêtre de saisie du code PIN quand le délai de temporisation arrive à échéance.

6.8 Paramètres généraux

6.8.1 MENUITEM

Syntaxe : `MENUITEM=[0..31]`

Usage : Cette propriété permet de définir les options du menu en barre des tâches.

La valeur de la propriété `MENUITEM` est un champ de bits, chaque bit représente une option du menu en barre des tâches :

1 (1er bit) ⇨ **Quitter**

2 (2e bit) ⇨ **Panneau des Connexions**

4 (3e bit) ⇨ **Console**

8 (4e bit) ⇨ **Sauver** et **Appliquer** (obsolète à partir de la version 5)

16 (5e bit) ⇨ **Panneau de Configuration**

Par défaut, toutes les options de menu sont affichées : valeur = 31 (1F hexa).

Exemple : `MENUITEM=3`

Affichera uniquement les options **Panneau des Connexions** et **Quitter**.

0 N'affiche pas le menu en barre des tâches

1 Affiche **Quitter**

2 Affiche **Panneau des Connexions**

3 Affiche **Panneau des Connexions** et **Quitter**

4 Affiche **Console**

5 Affiche **Console** et **Quitter**

6 Affiche **Panneau des Connexions** et **Console**

7 Affiche **Panneau des Connexions**, **Console** et **Quitter**

Etc.

6.8.2 RESTRICTCONFADMIN

Syntaxe : `RESTRICTCONFADMIN=0`

Usage : Cette propriété permet de restreindre l'accès au Panneau de Configuration aux administrateurs uniquement. Par défaut, le Panneau de Configuration n'est accessible qu'en tant qu'administrateur.

6.8.3 NOSPLITTUNNELING

Syntaxe : `NOSPLITTUNNELING=1`

Usage : Cette propriété provoque la désactivation de la route par défaut de l'interface physique quand le tunnel est monté. N'agit que sur les tunnels dont la configuration est « Tout le trafic dans le tunnel ».

6.8.4 NOSPLITDNS

Syntaxe : `NOSPLITDNS=1`

Usage : Cette propriété fait en sorte que les DNS de l'interface virtuelle soient aussi appliqués à l'interface physique, quand le tunnel est monté. N'agit que sur les tunnels dont la configuration est « Tout le trafic dans le tunnel ».

6.8.5 ROUTINGMODE

Syntaxe : `ROUTINGMODE=1`

Usage : Cette propriété permet de ne pas faire passer le trafic local de l'interface physique dans le tunnel. Seuls les flux qui viennent de l'interface virtuelle sont pris en compte.

6.8.6 FORCELOCALTRAFICTOTUNNEL

Syntaxe : `FORCELOCALTRAFICTOTUNNEL=1`

Usage : En mode « tout dans le tunnel », cette propriété permet de router le trafic local de l'interface physique dans le tunnel. Si cette propriété n'est pas présente (par défaut), le mode n'est pas activé.

0 ou non défini	Mode désactivé
1	Mode activé

6.8.7 IKESTART

Syntaxe : `IKESTART=1`

Usage : Cette propriété permet de démarrer le service IKE indépendamment de l'interface du logiciel. Si cette propriété n'est pas présente (par défaut), ce mode n'est pas activé.

Non défini	Le mode n'est pas activé
1	Le mode est activé
Autre valeur	Le mode n'est pas activé

6.8.8 SIGNFILE

Syntaxe : `SIGNFILE=1`

Usage : Cette propriété permet de forcer la vérification du hash d'intégrité du fichier de configuration VPN.

La valeur par défaut est 0.

6.8.9 GINABEHAVES

Syntaxe : `GINABEHAVES=1`

Usage : Dans son comportement par défaut, le mode GINA affiche un panneau sur l'écran d'ouverture de session Windows permettant d'ouvrir un ou plusieurs tunnels avant d'ouvrir une session Windows. En revanche, ce panneau ne s'affiche pas sur l'écran de verrouillage lorsque l'utilisateur a verrouillé la session.

Cette propriété permet de rendre visible le panneau du mode GINA sur l'écran de verrouillage.

La valeur par défaut est 0.

6.9 Logs

6.9.1 SYSTEMLOGOUTPUT

Syntaxe : `SYSTEMLOGOUTOUT=7`

Usage : Cette propriété permet de sélectionner la sortie des logs administrateur. Les sorties peuvent être combinées, par exemple pour combiner les 3 sorties, utiliser la valeur 7.

- 0 Pas de logs système
- 1 Fichiers de logs
- 2 Serveur syslog
- 4 Observateur d'évènements Windows

6.9.2 SYSTEMLOGSYSLOGSERVER

Syntaxe : `SYSTEMLOSERVER=syslogserver.company.com`

Usage : Cette propriété permet de préciser l'adresse IP ou nom de la machine à destination des syslog.

6.9.3 SYSTEMLOGSYSLOGPORT

Syntaxe : `SYSTEMLOGSYSLOGPORT=5514`

Usage : Cette propriété permet de préciser le port de la machine à destination des syslog. Le port par défaut est 514.

Chapitre 7. Fichier vpnsetup.ini

7.1 Introduction

Le fichier `vpnsetup.ini` permet de configurer l'installation de Trustway IP Protect Client à partir d'un fichier, plutôt que par les propriétés en ligne de commande MSI.

Par contrainte de l'installeur Microsoft MSI, le fichier `vpnsetup.ini` doit se trouver dans le dossier `C:\Windows`.

Le fichier `vpnsetup.ini` permet de définir les paramètres suivants :

- paramètres d'activation du logiciel
- paramètres du Panneau TrustedConnect
- paramètres PKI pour la gestion des tokens, lecteurs de cartes à puce et certificats
- paramètres généraux de fonctionnement
- paramètres des logs système
- autres paramètres

Le nom des paramètres du fichier `vpnsetup.ini` est identique à celui des propriétés de l'installeur MSI (voir Chapitre 6 Paramètres et propriétés de l'installeur MSI, à la différence près que la casse n'est pas prise en compte (il est donc possible de mélanger des majuscules et des minuscules).

Il peut être édité avec un éditeur de texte classique (par exemple : Bloc-notes). Comme tous les fichiers de type `ini`, il est structuré en sections. Les paramètres doivent se trouver dans la section appropriée, telle que précisé ci-après.

Les propriétés d'installation et de configuration VPN de l'installeur MSI, à savoir `APPLICATIONROOTDIRECTORY`, `TGBCONF_ADMINPASSWORD`, `NOAUTORUN`, `TGBCONF_PATH` et `TGBCONF_PASSWORD` n'ont pas d'équivalent dans le fichier `vpnsetup.ini`.

7.2 Section [Activation]

Les paramètres de la section `[Activation]` sont les suivants :

- `ActivMail` (cf. section 6.5.1)
- `AutoActiv` (cf. section 6.5.2)
- `License` (cf. section 6.5.3)
- `NoActivWin` (cf. section 6.5.4)

7.3 Section [Dialer]

Les paramètres de la section `[Dialer]` sont les suivants :

- `UseDialerByDefault` (cf. section 6.6.1)
- `DialerMinimize` (cf. section 6.6.2)
- `DialerDefs` (cf. section 6.6.3)
- `VpnLogPurge` (cf. section 6.6.4)
- `TokenOutHandle` (cf. section 6.6.5)
- `GinaBehaves` (cf. section 6.8.9)

7.4 Section [PKIOptions]

Les paramètres définis dans la section `[PKIOptions]` permettent de caractériser l'usage par le logiciel des cartes à puce, des tokens, et des certificats :

- `SmartcardRoaming` (cf. section 6.7.1)
- `PKCS11Only` (cf. section 6.7.2)
- `KeyUsage` (cf. section 6.7.3)
- `NoCACertReq` (cf. section 6.7.4)
- `PKICheck` (cf. section 6.7.5)
- `X509DirectoryString` (cf. section 6.7.6)
- `MachineStore` (cf. section 6.7.7)
- `DnPattern` (cf. section 6.7.8)

7.5 Section [AddRegKey]

La section `[AddRegKey]` est utilisée pour définir les paramètres généraux de fonctionnement :

- `NoPinCode` (cf. section 6.7.9)
- `PinTimeOut` (cf. section 6.7.10)
- `MenuItem` (cf. section 6.8.1)
- `RestrictConfAdmin` (cf. section 6.8.2)
- `NoSplitTunneling` (cf. section 6.8.3)
- `NoSplitDNS` (cf. section 6.8.4)
- `ForceLocalTraficToTunnel` (cf. section 6.8.6)
- `IkeStart` (cf. section 6.8.7)

7.6 Section [Config]

Le paramètre de la section `[Config]` est le suivant :

- `SignFile` (cf. section 6.8.8)

7.7 Section [Logs]

La section `[Logs]` est utilisée pour définir les options des logs système. Les paramètres de cette section sont les suivants :

- `SystemLogOutput` (cf. section 6.9.1)
- `SystemLogSyslogServer` (cf. section 6.9.2)
- `SystemLogSyslogPort` (cf. section 6.9.3)

7.8 Section [VirtMDriver]

Le paramètre de la section `[VirtMDriver]` est le suivant :

- `RoutingMode` (cf. section 6.8.5)

7.9 Exemple de fichier vpnsetup.ini

```
[Activation]
activmail=john.doe@company.com
AutoActiv=1
License=123456-123456-123456
NoActivWin=1

[Dialer]
UseDialerByDefault=1
DialerMinimize=5000
DialerDefs=01000000
VPNLogPurge=3
TokenOutHandle=30
GINABEHAVES=1

[PKIOptions]
PKICheck=1
SmartcardRoaming=1
NoCACertReq=0
KeyUsage=1
PKCS11Only=1
X509DirectoryString=14
DnPattern=company
MachineStore=1

[AddRegKey]
ForceLocalTraficToTunnel=1
IkeStart=1
pintimeout=120
NoPinCode=1
MenuItem=4
RestrictConfAdmin=1
NoSplitTunneling=1
NoSplitDNS=1

[Config]
SignFile=0

[VirtMDriver]
RoutingMode=1

[Logs]
SystemLogOutput=7
SystemLogSyslogServer=syslogserver.company.com
SystemLogSyslogPort=5514
```

Chapitre 8. 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

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 un ensemble de clients VPN compatibles avec les spécifications ANSSI IPSec DR. Il s'agit d'un produit différent du Groupe de TVPN-clients ci-dessus.

Un GVPNC ne peut être placé que dans un domaine de type « System » dont la politique de sécurité est Tunnel AES en mode « SAs générées par IKE ».

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).