THEGREENBOW

Client VPN
Windows Enterprise 6.85

Guide de Déploiement

Dernière mise à jour : 29 mars 2021

Table des matières

1 Introduction

Le Client VPN Windows Enterprise est conçu pour être facilement déployé et administré.

A ce titre, le logiciel intègre de nombreuses fonctions qui permettent à l'administrateur réseau de préconfigurer l'installation avant un déploiement, d'installer ou de mettre à jour le logiciel à distance, ou encore d'administrer le logiciel et les politiques de sécurité VPN de façon centralisée.

Le Client VPN Windows Enterprise est packagé dans un installer Microsoft MSI, permettant le déploiement et la mise à jour du logiciel à l'aide des fonctions de déploiement de Microsoft Windows et les Politiques de Groupe (GPO). En outre, il est possible de mettre en place tous les paramètres d'installation dans un fichier utilisé par le logiciel pour se configurer automatiquement lors du déploiement.

Ce document décrit les options d'administration et de configuration du Client VPN Windows Enterprise.
Il propose aussi un ensemble d'exemples de mise en œuvre de ces options, qui illustrent la façon de gérer le logiciel.

De nombreuses options peuvent être configurées pendant l'installation du logiciel Client VPN Windows Enterprise:
- Options d'activation logiciel : numéro de licence, email d'activation, activation masquée, etc.
- Propriétés graphiques : interface masquée à l'utilisateur, customisation de menus, etc.
- Options d'intégration PKI : caractérisation des certificats ou des supports token oucartes à puce, etc.
- Politique de sécurité VPN à déployer
- Propriété de l'installation : installation masquée, etc.
- Etc.

Des options supplémentaires peuvent être utilisées avec le logiciel lui-même, une fois l'installation effectuée :
- Gestion de la configuration VPN : import, export, signature, etc.
- Gestion du logiciel : start, stop, etc.
- Gestion du tunnel VPN : open, close, status
- Etc.

2 Considérations de sécurité

2.1 Configuration du poste hôte

La machine sur laquelle est installé et exécuté le Client VPN Windows Enteprise doit être saine et correctement administrée. En particulier :
1/ Elle dispose d'un anti-virus dont la base de données est régulièrement mise à jour,
2/ Elle est protégée par un pare-feu qui permet de maîtriser les communications entrantes et sortantes du poste qui ne passent pas par le Client VPN,
3/ Son système d'exploitation est à jour des différents correctifs
4/ Sa configuration permet d'éviter les attaques menées localement (analyse de la mémoire, patch ou corruption de binaire).

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

- Guide d'hygiène informatique
- Guide de configuration
- Mises à jour de sécurité
- Mot de passe

Il est recommandé d'exécuter l'installation du Client VPN Windows Enterprise sur une machine vierge de toute installation précédente. A ce titre, il est recommandé de désinstaller une version précédente du logiciel le cas échéant avant d'installer cette version. De même il est recommandé d'exécuter l'installation depuis un répertoire vierge, en particulier dans le cas d'une installation customisée avec un fichier de configuration joint.

2.2 Droits d'exécution

Le Client VPN Windows Enterprise est conçu pour pouvoir être installé avec les droits « administrateur », et être ensuite complètement utilisable avec des droits « utilisateur » stricts, ceci quelle que soit la plate-forme Windows utilisée.

Dans la mesure où certaines opérations sont interdites en mode « utilisateur » (par exemple la désinstallation du logiciel), il est fortement recommandé de déployer le logiciel en respectant cette utilisation des droits :

- Installation en mode « administrateur »
- Utilisation en mode « utilisateur »

2.3 Configuration pour l'utilisateur final

Le Client VPN Windows Enterprise est conçu pour pouvoir être utilisé, simultanément et de façon cloisonnée, par un administrateur (installation, configuration initiale personnalisation) et par l'utilisateur final.

Toute l'interface du logiciel peut être paramétrée pour ne laisser à l'utilisateur final qu'un nombre restreint d'opérations disponibles (ouvrir ou fermer un tunnel VPN).

De même, le logiciel peut être intégralement configuré, dès son installation ou son déploiement, pour réserver strictement l'accès aux politiques de sécurité VPN à l'administrateur seul.

Les options de configuration du logiciel décrites dans la suite de ce document permettent précisément de mettre en place ce cloisonnement, afin de mettre œuvre le Client VPN dans les meilleures conditions de sécurité et de fiabilité possibles.

2.4 Gestion multi-utilisateurs

Le Client VPN Windows Enterprise présente la même configuration VPN (politique de sécurité) 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).

2.5 Gestion des politiques de sécurité VPN

Le Client VPN Windows Enterprise offre en standard un ensemble d'options de ligne de commande permettant l'importation, l'exportation, le remplacement ou l'application de nouvelles politiques de sécurité VPN.

Ces options sont destinées à être utilisées pour des scripts de déploiement du logiciel, pour des opérations de mises à jour ou de maintenance à distance, pour la réalisation d'automatisations diverses telles que les ouvertures et fermetures automatiques de tunnel VPN.

Ce document décrit la façon d'utiliser ces différentes options de ligne de commande, pour ne pas mettre en péril l'intégrité ou la confidentialité des politiques de sécurité VPN.

2.6 Authentification de l'utilisateur

Comme détaillé dans le « Guide Utilisateur du Client VPN Windows Enterprise » (tgbvpn_ug_fr.pdf), il est recommandé de privilégier l'utilisation de certificat, si possible stocké sur token ou sur carte à puce, pour assurer l'authentification forte de l'utilisateur lors de l'ouverture du tunnel VPN.

Les options de configuration du logiciel concernant la mise en œuvre de cette fonction sont détaillées dans un document dédié : « Gestion des PKI, certificats, tokens et cartes à puce » (tgbvpn_ug_pki_smartcard_fr.pdf)

2.7 Protection des données sensibles

Comme détaillé dans le « Guide Utilisateur du Client VPN Windows Enterprise » (tgbvpn_ug_fr.pdf), il est recommandé de ne mémoriser aucune donnée sensible dans le fichier de configuration VPN : login / mot de passe X-Auth, pre-shared key ou certificat.

2.8 Réinitialisation

L'environnement Windows permet de désinstaller puis de ré-installer le logiciel.
Au cours d'une désinstallation, la politique de sécurité est supprimée. Cette procédure permet de réinitialiser le logiciel dans sa configuration initiale.

2.9 Dépréciation de l'API CSP en IKEv2 et SSL

A partir de la version actuelle, l'API Microsoft CSP (Cryptographic Service Providers) pour l'utilisation des tokens / cartes à puces est dépréciée et n'est plus disponible en IKEv2 ni en SSL. Elle est remplacée par la nouvelle API Microsoft CNG (Cryptography API: Next Generation). Il est toujours possible de forcer l'utilisation de l'API PKCS#11 (cf. chapitre 7.8.2).

Note : lors de l'importation d'un certificat dans le magasin de certificats Windows, une option permet de déterminer l'API qui sera utilisée pour y accéder : CSP ou CNG. Or dans Windows 10, l'API CSP est toujours utilisée par défaut pour

l'importation des certificats RSA. La commande administrateur à utiliser pour forcer un certificat avec l'API CNG est la suivante :

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

Note : l'API CSP est la seule disponible en IKEv1.

3 Déploiement du Client VPN

3.1 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 d'options de ligne de commande.

Il est fortement recommandé de restreindre l'accès aux politiques de sécurité VPN aux seuls administrateurs (comportement par défaut).

3.2 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 d'options de ligne de commande, ou via le fichier d'initialisation « vpnsetup.ini » qui accompagne l'installation (voir chapitre 9).

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

1/ Télécharger le programme d'installation TheGreenBow_VPN_ENTERPRISE.msi depuis http://www.thegreenbow.com
2/ Ouvrir la fenêtre de commande Windows et entrer la ligne de commande :

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet (options supplémentaires, voir chapitre 7)
```

Exemple:

```
[repertoire_telechargement]/TheGreenBow_VPN_ENTERPRISE.msi /quiet LICENSE=[numero_licence]
```

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

3.3 Déploiement d'une mise à jour

Le déploiement d'une mise à jour du Client VPN Windows Enterprise 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).
Lorsque la version installée est antérieure à la version 6.8 et protégée par mot de passe, ce mot de passe doit être renseigné en ligne de commande de la mise à jour.

Exemple : si l'ancienne version installée est protégée par le mot de passe `Tgb@dM1Npwd!`, la ligne de commande de la mise à jour sera la suivante :

```
TheGreenBow_VPN_ENTERPRISE.msi TGBCONF_ADMINPASSWORD=Tgb@dM1Npwd!
```

Note : Les versions 6.8 et suivantes du Client VPN Windows Enterprise ne sont plus protégées par un mot de passe, mais par l'élévation des privilèges (exécution du logiciel en tant qu'administrateur).

Le remplacement de toute ancienne édition Certifiée, Premium ou Enterprise supérieure ou égale à 6.5 est fonctionnelle. Cette mise à jour conserve la configuration VPN.

Note : en revanche, la mise à jour d'une édition Standard, quelle que soit la version, n'est pas possible. Elle requière la désinstallation préalable de cette version. De plus, les configurations VPN ne sont pas compatibles.

3.4 Réparation

La fonction de réparation de l'installateur MSI n'est pas supportée pour le moment.

3.5 Désinstallation

3.5.1 Désinstallation classique

La désinstallation du logiciel peut se faire par le panneau de configuration Windows, onglet « Programmes et fonctionnalités », ou par l'item « Désinstaller » (bouton droit sur l'icône TheGreenBow VPN Enterprise) du menu Windows.

3.5.2 Désinstallation en ligne de commande

La désinstallation du logiciel peut également s'effectuer à l'aide de l'utilitaire Windows msiexec.

Exemple de la ligne de commande:

```
msiexec /x TheGreenBow_VPN_ENTERPRISE.msi
```

Se reporter à la documentation de l'utilitaire msiexec pour plus d'informations.

4 Déploiement de l'activation du logiciel

4.1 Paramètres d'activation

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

Par défaut, l'activation des logiciels est réalisée auprès du serveur d'activation TheGreenBow accessible sur Internet. Lorsque le parc installé du Client n'a pas de connexion à Internet, l'activation des logiciels peut être réalisée auprès d'un serveur d'activation installé chez le Client : le serveur TAS (TheGreenBow Activation Server).

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 vpnsetup.ini. Ces méthodes sont décrites dans les chapitres ci-dessous.

4.2 Déploiement et automatisation de l'activation

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, utiliser les options de ligne de commande de l'installeur : « `AUTOACTIV` » (qui automatise l'activation) et « `NOACTIVWIN` » (qui masque la fenêtre d'activation), conjointement aux paramètres « `LICENSE` » et « `ACTIVMAIL` » comme indiqué au chapitre 7.5.

Ligne de commande pour une activation automatique et silencieuse :

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet LICENSE=[numero_de_licence] ACTIVMAIL=[email_activation]
NOACTIVWIN=1 AUTOACTIV=1
```

Lorsque l'activation du logiciel est effectuée auprès d'un serveur TAS (« TheGreenBow Activation Server », serveur d'activation installé sur l'infrastructure du Client), les paramètres de ce serveur peuvent être spécifiés dans le fichier VpnSetup.ini joint à l'installeur au moment de l'installation (voir chapitre 9 pour le détail des paramètres) ou utiliser les propriétés MSI en ligne de commande « `OSAURL` », « `OSAPORT` » et « `OSACERT` ».

Exemple de ligne de commande pour une activation sur serveur TAS :

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet LICENSE=[numero_de_licence] ACTIVMAIL=[email_activation]
NOACTIVWIN=1 AUTOACTIV=1 OSAURL=192.168.217.102/osace_activation.php OSAPORT=80
OSACERT="MIICGjCCAYOgAwIBAgIBADANBg [........] muHf58kMO0jvhkyq24GryqptSaSJqVIA="
```

Exemple de fichier VpnSetup.ini pour une activation sur serveur TAS :

```
[Activation]
OSAUrl = 192.168.217.102/osace_activation.php
OSAPort = 80
OSACert = "MIICGjCCAYOgAwIBAgIBADANBg [........] muHf58kMO0jvhkyq24GryqptSaSJqVIA="
```

4.3 Activation dans le tunnel

Le logiciel Client VPN Windows Enterprise implémente en standard (toutes versions) la fonction d'activation dans le tunnel :

Dès lors que les propriétés « AUTOACTIV » et « NOACTIVWIN » ont été paramétrées conformément au chapitre précédent, le logiciel vérifie - et le cas échéant met à jour - automatiquement son activation dans le tunnel VPN qui vient de s'ouvrir.

Cet automatisme permet par exemple au logiciel en mode abonnement de vérifier et de mettre à jour automatiquement son activation lors du renouvellement de cet abonnement. Il permet aussi au logiciel de se réactiver automatiquement suite à une mise à jour, de façon transparente pour l'utilisateur.

4.4 Identification des activations

Il est possible, lors d'un déploiement automatisé, d'automatiser aussi l'identification des postes sur lesquels l'activation est réalisée. Ceci permet de gérer facilement les activations/désactivations des licences installées.

Cette identification des postes activés peut être réalisée en utilisant le champ « email d'activation » pour par exemple y renseigner le nom du poste activé, ceci au cours du processus d'installation.

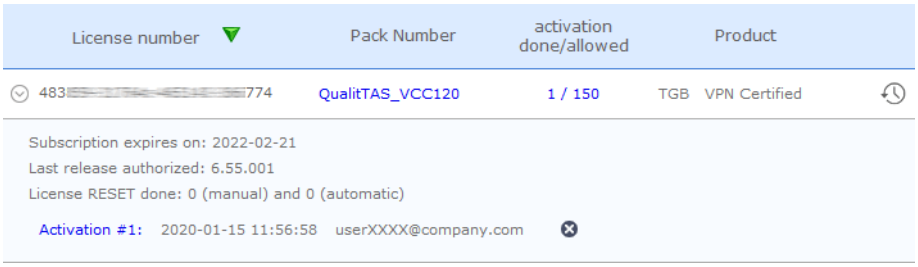
Script d'installation automatisée avec identifiant du poste activé :

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet LICENSE=[numero_de_licence]
ACTIVMAIL=%ComputerName%@company.com
NOACTIVWIN=1 AUTOACTIV=1
```

Batch PowerShell d'installation automatisée avec identifiant du poste activé :

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet LICENSE =[numero_licence]
ACTIVMAIL=$env:computername@company.com
NOACTIVWIN=1 AUTOACTIV=1
```

L'identifiant %ComputerName% est automatiquement renseigné par le système d'exploitation au moment de l'installation, puis utilisé automatiquement par l'activation, pour être finalement affiché dans les pages de visualisation des activations, disponibles sur les serveurs d'activation TheGreenBow ou TAS.



Attention : 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.

5 Déploiement des politiques de sécurité VPN

5.1 Intégrité d'une politique de sécurité VPN exportée

La protection de l'intégrité d'une politique de sécurité VPN lorsqu'elle est exportée est une fonction activable par la propriété « `SIGNFILE` ».

Exemple :

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet SIGNFILE=1
```

5.2 Embarquer une politique de sécurité VPN dans l'installation

Une politique de sécurité VPN (configuration VPN) préconfigurée peut être embarquée avec l'installation du Client VPN Windows Enterprise. Cette politique de sécurité 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 :

1/ Créer la politique de sécurité VPN (Configuration VPN) à destination du poste à équiper
2/ Exporter cette politique de sécurité VPN (menu « Configuration > Export », Cf. Guide Utilisateur du Client VPN Windows Enterprise) en la protégeant éventuellement par mot de passe.
3/ Transférer le setup et la politique de sécurité VPN sur le poste à équiper
4/ Exécuter l'installation du Client VPN en indiquant les propriétés « `TGBCONF_PATH` » et « `TGBCONF_PASSWORD` » (si la politique de sécurité est protégée par mot de passe). A la fin de l'installation, le Client VPN est installé avec la politique de sécurité VPN importée et appliquée.

Exemple :

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet TGBCONF_PATH=C:\Users\Public\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 politiques de sécurité VPN, si activée. Dans ce cas, cette fonction garantit que la politique de sécurité importée au moment de l'installation n'a pas été corrompue.

5.3 Déployer une nouvelle politique de sécurité VPN

5.3.1 Procédure

1/ Créer la politique de sécurité VPN (Configuration VPN) à destination du poste à équiper
2/ Exporter cette politique de sécurité (menu « Configuration > Export », Cf. Guide Utilisateur du Client VPN Windows Enterprise). Elle peut être chiffrée par un mot de passe.
3/ Transférer cette politique de sécurité VPN sur le poste à mettre à jour (mail, partage de fichier, etc.)
4/ Sur le poste cible, utiliser vpnconf.exe en ligne de commande, en spécifiant le cas échéant le mot de passe utilisé pour protéger la configuration exportée (Cf. options /import et /pwd détaillées au chapitre 6.2).

5.3.2 Différence entre *import*, *importonce*, *add*, *replace*

L'option « /import » permet d'importer une politique de sécurité VPN (Configuration VPN) en démarrant en même temps le logiciel Client VPN, s'il n'est pas déjà démarré.

L'option « /importonce » permet d'importer une politique de sécurité VPN (Configuration VPN) sans démarrer le logiciel Client VPN.

Lorsque le logiciel Client VPN est démarré, ces deux options importent simplement la politique de sécurité VPN.

Lorsque la politique de sécurité VPN courante (avant importation) du Client VPN 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 politique de sécurité 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 politique de sécurité VPN, l'option « /replace » remplace systématiquement l'ancienne politique par la nouvelle.

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

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

5.4 Protection de la politique de sécurité VPN

Lorsque l'accès au Panneau de Configuration est restreint aux administrateurs (option d'installation par défaut), 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 ».

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.

5.5 Exportation de la politique de sécurité

L'option de ligne de commande « `/export` » permet d'exporter une politique de sécurité VPN (Configuration VPN) en démarrant en même temps le logiciel Client VPN, s'il n'est pas déjà démarré.

L'option « `/exportonce` » permet d'exporter une politique de sécurité VPN (Configuration VPN) sans démarrer le logiciel Client VPN.

Lorsque le logiciel Client VPN est démarré, ces deux options exportent simplement la politique de sécurité VPN.

6 vpnconf en ligne de commande

6.1 Introduction

Le Client VPN Windows Enterprise 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 politique de sécurité VPN, etc.

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

```
[répertoire]\vpnconf.exe [/option[:valeur]]
```

- [répertoire] est le répertoire dans lequel se trouve l'exécutable « vpnconf.exe » (typiquement le répertoire d'installation du logiciel Client VPN)
- 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.

De nombreux exemples de mise en œuvre des options de ligne de commande sont disponible sur le site TheGreenBow à l'url : www.thegreenbow.fr/vpn_tool.html

6.2 Importation

/import

Syntaxe :	/import:[ConfigFileName]
Usage :	Cette option est utilisée pour importer une configuration VPN en démarrant le Client VPN. Cette option peut être utilisée pour lancer le logiciel Client VPN 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. [ConfigFileName] est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces
Exemple :	vpnconf.exe /import:"c:\my documents\myvpnconf.tgb"

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

Note : 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 ». Cf ci-dessous.

/importonce

Syntaxe :	/importonce:[ConfigFileName]
Usage :	Cette option est utilisée pour importer une configuration VPN sans démarrer le Client VPN. Elle peut être utilisée par exemple dans un script d'installation ou de mise à jour.

	Si le Client VPN est en cours d'exécution, cette option importe et met à jour la configuration VPN sans arrêter le logiciel. [ConfigFileName] est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.
Retour :	Cf. Note sur le code 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 :	vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb"

Note : Lorsque la configuration VPN courante n'est pas vide, le logiciel affiche une fenêtre qui demande à l'utilisateur s'il veut ajouter ou remplacer la configuration VPN importée. Pour éviter l'affichage de cette fenêtre, utiliser les options « /add » ou « /replace ». Cf ci-dessous.

Note : 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.

Note : 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).

/add

Syntaxe :	/add:[ConfigFileName]
Usage :	Permet d'ajouter une politique de sécurité VPN. [ConfigFileName] est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.
Retour :	Cf. Note sur le code 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 :	vpnconf.exe /add:"c:\my documents\myvpnconf.tgb"

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

Note : 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.

/replace

Syntaxe :	/replace:[ConfigFileName]
Usage :	Permet d'ajouter une politique de sécurité VPN. [ConfigFileName] est le chemin complet du fichier à importer. Il doit être encadré de guillemets s'il contient des espaces.
Retour :	Cf. Note sur le code 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 : vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb"

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

Note : 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.

/pwd

Syntaxe : /pwd:[Password]

Usage : Permet de spécifier un mot de passe pour les opérations d'importation et d'exportation des politiques de sécurité 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 : vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd=mypwd

6.3 Exportation

/export

Syntaxe : /export:[ConfigFileName]

Usage : Permet d'exporter une politique de sécurité VPN, en démarrant le logiciel Client VPN.
Si le logiciel est en cours d'exécution, l'option /export exporte la configuration VPN sans l'arrêter.
[ConfigFileName] 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 politique de sécurité VPN en la protégeant par un mot de passe.

Exemple : vpnconf.exe /export:"c:\my documents\myvpnconf.tgb"
vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" /pwd:gq1aRe7

/exportonce

Syntaxe : /exportonce:[ConfigFileName]

Usage : Permet d'exporter une politique de sécurité VPN, sans démarrer le logiciel Client VPN.
Si le logiciel est en cours d'exécution, l'option /exportonce exporte la configuration VPN sans l'arrêter.
[ConfigFileName] 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 politique de sécurité VPN en la protégeant par un mot de passe.

Exemple : vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb" /pwd: gq1aRe7

6.4 Ouverture/fermeture d'un tunnel VPN

/stop

Syntaxe : /stop

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

Exemple : vpnconf.exe /stop

/open

Syntaxe : /open:[NomTunnel(1)]

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\TheGreenBow\TheGreenBow VPN\vpnconf" /open:tgbtest-tgbtest
@echo retour = %ERRORLEVEL%
Pause
```

/status

Syntaxe : /status:[NomTunnel(1)]

Usage : Permet d'obtenir le status 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\TheGreenBow\TheGreenBow VPN\vpnconf" /status:tgbtest-
tgbtest
@echo retour = %ERRORLEVEL%
pause
```

/close

Syntaxe : /close:[NomTunnel(1)]

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 : `vpnconf.exe /close:"Home gateway-cnx1"`
(les guillemets sont requis puisque le nom du tunnel contient un espace)

/closeall

Syntaxe :	vpnconf.exe /closeall
Usage :	Permet de fermer tous les tunnels VPN ouverts.
Retour :	0 : Tous les tunnels VPN sont fermé Autres : Voir la liste des codes retours ci-dessous
Exemple :	vpnconf.exe /closeall

6.5 Redémarrage

/resetike

Syntaxe :	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 :	vpnconf.exe /resetike

6.6 Précisions

NomTunnel

(1) Dans ce chapitre le nom du tunnel est composé comme suit :

	Nom Tunnel
IKEv1	Phase1-Phase2
IKEv2	IKEAuth-ChildSA
SSL	TLS

Codes retours des options de ligne de commande

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

-1, -2, -3 : Impossible de trouver l'instance du logiciel Client VPN qui doit exécuter la commande.
100 à 199 : Temps maximum d'exécution de la commande.
200 à 299 : Temps maximum d'exécution de la commande : pas de réponse du logiciel.
300 : Erreur interne
500 : Impossible de trouver le tunnel VPN spécifié
1000 à 1999 : Problème pendant l'ouverture du tunnel VPN
> 10000 : Erreur interne

7 Paramètres de l'installeur MSI

7.1 Introduction

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

Pour installer le Client VPN Windows Enterprise, il est recommandé de lancer la ligne de commande MSIEXEC depuis un shell admin avec l'option /i, l'option /q et les propriétés adaptées à votre déploiement.

Exemple

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

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

7.2 Paramètres MSI en ligne de commande

/i

Syntaxe : `msiexec /i [chemin_de_l_installeur]`

Usage : installe le logiciel Client VPN Windows Enterprise

Exemple : `msiexec /i TheGreenBow_VPN_ENTERPRISE.msi`

/x

Syntaxe : `msiexec /x [chemin_de_l_installeur]`

Usage : désinstalle le logiciel Client VPN Windows Enterprise

Exemple : `msiexec /x TheGreenBow_VPN_ENTERPRISE.msi`

/quiet

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

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

Exemple : `msiexec /i TheGreenBow_VPN_ENTERPRISE.msi /quiet`

/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 TheGreenBow_VPN_ENTERPRISE.msi /L*v! "C:\install.log"`

7.3 Installation

7.3.1 APPLICATIONROOTDIRECTORY

Syntaxe : `APPLICATIONROOTDIRECTORY=[rep_install]`

Usage : [rep install] est le répertoire où le logiciel Client VPN doit être installé.
[rep install] nécessite d'être encadré par des guillemets si le répertoire contient des espaces.

Exemple :
```
msiexec /i TheGreenBow_VPN_ENTERPRISE.msi /q
APPLICATIONROOTDIRECTORY="C:\mon repertoire\vpn"
```

Note : « C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise » est le répertoire d'installation par défaut.

7.3.2 TGBCONF_ADMINPASSWORD

Syntaxe : `TGBCONF_ADMINPASSWORD=[mot_de_passe]`

Usage : Mot de passe administrateur utilisé pour protéger l'accès au panneau de configuration dans les versions antérieures à 6.8, le cas échéant. Utilisé pour la mise à jour d'une version antérieure, dont le panneau de configuration était protégé par mot de passe.

7.4 Serveur d'activation TAS

Les paramètres de la section « Activation » définissent les caractéristiques du serveur d'activation TAS (« TheGreenBow Activation Server », serveur d'activation optionnellement installé sur l'infrastructure de l'utilisateur).
Ces paramètres sont : l'adresse du serveur, le port d'accès et le certificat d'authentification de l'activation.

Ces paramètres étant requis pour des configurations spécifiques, ils sont en général fournis par TheGreenBow.

7.4.1 OSACERT

Syntaxe : `OSACERT=[contenu_du_certificat]`

Usage : Certificat utilisé pour s'authentifier au serveur d'activation TAS.

7.4.2 OSAPORT

Syntaxe : `OSAPORT=[port_tas]`

Usage : Port du serveur d'activation TAS.

7.4.3 OSAURL

Syntaxe : `OSAURL=[url_tas]`

Usage : Url du serveur d'activation TAS.

7.5 Activation de la licence

7.5.1 ACTIVMAIL

Syntaxe : `ACTIVMAIL=[activation_email]`

Usage : Permet de configurer l'adresse email utilisée pour l'activation du logiciel. (Cf. « Guide Utilisateur du Client VPN Windows Enterprise » pour les caractéristiques de cette adresse email).

Exemple : `TheGreenBow_VPN_ENTERPRISE.msi ACTIVMAIL=salesgroup@company.com`

7.5.2 AUTOACTIV

Syntaxe : `AUTOACTIV=1`

Usage : Dans le cas d'une mise à jour (i.e. : le numéro de licence et l'adresse email d'activation ont déjà été saisies au cours d'une précédente installation), cette propriété permet de configurer le logiciel pour s'activer automatiquement.

Exemple : `TheGreenBow_VPN_ENTERPRISE.msi AUTOACTIV=1`

7.5.3 LICENSE

Syntaxe : `LICENSE=[numero_licence]`

Usage : Permet de configurer le numéro de licence utilisé pour l'activation du logiciel. (Cf. « Guide Utilisateur du Client VPN Windows Enterprise » pour les caractéristiques de ce numéro de licence).

Exemple : `TheGreenBow_VPN_ENTERPRISE.msi LICENSE=1234567890ABCDEF12345678`

7.5.4 NOACTIVWIN

Syntaxe : `NOACTIVWIN=1`

Usage : Cette option permet d'éviter l'affichage de la fenêtre d'activation.
Associée à l'option « `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.
A 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 réussie à cette échéance.

7.6 Politique de Sécurité VPN

7.6.1 TGBCONF_PATH

Syntaxe : `TGBCONF_PATH=[chemin_fichier_conf]`

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

7.6.2 TGBCONF_PASSWORD

Syntaxe : `TGBCONF_PASSWORD=[mot_de_passe]`

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

7.7 Panneau TrustedConnect

Cette section permet de définir les paramètres du Panneau TrustedConnect (mode utilisateur ou mode GINA).

7.7.1 USEDIALERBYDEFAULT

Syntaxe : `USERDIALERBYDEFAULT=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).

7.7.2 TNDSUFFIXES

Syntaxe : `TNDDNSSUFFIXES=dns.suffix1,dns.suffix2,dns.suffix3`

Usage : Ce paramètre définit la liste des suffixes DNS de confiance.

Cette liste peut être vide ou contenir plusieurs suffixes DNS.
Les suffixes de la liste doivent être séparés par une virgule, sans espace.

7.7.3 TNDHTTPSERVERURL

Syntaxe : `TNDHTTPSERVERURL=www.server1.com,www.server2.com,www.server3.com`

Usage : Ce paramètre définit la liste des URL des serveurs de confiance à utiliser.

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.
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.
Les URL de la liste doivent être séparés par une virgule, sans espace.
Il n'y a pas besoin de faire précéder un URL du préfixe « https:// ».

7.7.4 TNDHTTPSERVERPORT

Syntaxe : `TNDHTTPSERVERPORT=443`

Usage : Ce paramètre définit le port à utiliser pour joindre les serveurs de confiance.

Il n'est possible de configurer qu'un seul port, qui sera utilisé pour tous les URL.
Si le paramètre 1.1.1 TNDHTTPSERVERPORT n'est pas configuré, le Client VPN utilise par défaut le port 443.

7.7.5 TNDLATENCY

Syntaxe : `TNDLATENCY=3000`

Usage : 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, la propriété TNDLATENCY permet de retarder le déclenchement du mécanisme TND.

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.

7.7.6 AONITFPASSOVER

Syntaxe : `AONITFPASSOVER=HYBER-V`

Usage : Il est possible d'exclure certaines interfaces réseaux de celle qui seront suivies par 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.

Il est aussi possible de spécifier plusieurs interfaces réseau à exclure en spécifiant les parties de leurs descriptions respectives, séparées par une virgule.

Exemple : Pour exclure toute interface dont le champ description comporte la chaîne de caractères 'Hyper-V', utiliser `AONITFPASSOVER=Hyper-V`.

7.7.7 DIALERMINIMIZE

Syntaxe : `DIALERMINIMIZE=5000`

Usage : Il est possible de configurer le délai avant que l'IHM du Client VPN ne soit minimisée, 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 : l'IHM ne se minimise plus automatiquement.
Si ce délai n'est pas configuré, le délai par défaut est de 2000 ms (2 secondes).

7.7.8 DIALERDEFS

Syntaxe : `DIALERDEFS="01 00 00 00"`

Usage : En plus du délai de minimisation, le type de minimisation est configurable : le Panneau TrustedConnect peut être minimisée en barre des tâches ou dans la zone de notification (systray).
Pour que le Panneau TrustedConnect soit minimisé en barre des tâches, entrer 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.

7.7.9 VPNLOGPURGE

Syntaxe : `VPNLOGPURGE=3`

Usage : Cette fonctionnalité 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.

7.7.10 TOKENOUTHANDLE

Syntaxe : `TOKENOUTHANDLE=30`

Usage : Ce paramètre permet de configurer le comportement du Panneau TrustedConnect lorsque le token / carte à puce est extrait du lecteur, alors qu'un tunnel VPN est ouvert.

3 modes sont disponibles sur cet évènement :

- Mode 1 : Le tunnel est fermé immédiatement lors de l'extraction du token / càp. (par défaut)
- Mode 2 : Le tunnel reste ouvert durant un délai configuré
- Mode 3 : Le tunnel reste ouvert indéfiniment
  Remarque : Dans ce mode, si le token / carte à puce est nécessaire pour ouvrir le tunnel VPN, alors la prochaine renégociation échouera.

Par défaut, sans paramétrage le mode 1 est actif.

TokenOutHandle=00 => pas de fermeture de tunnel sur extraction du token / càp (Mode 3)
TokenOutHandle=NN => temps en secondes avant que le tunnel ne soit fermé, sur extraction du token / càp (Mode 2)

7.7.11 GINABEHAVES

Syntaxe : `GINABEHAVES=01`

Usage : Ce paramètre permet de rendre le Panneau TrustedConnect apparent en mode GINA (lock session user).

Note : le champ « Peut être ouvert avant le logon Windows » dans l'onglet « automatisation » du panneau de configuration (cf. Guide Utilisateur) ne s'applique au Panneau TrustedConnect. Il faut donc utiliser ce paramètre pour utiliser le mode GINA avec le Panneau TrustedConnect.

La valeur par défaut est 0 (le Panneau TrustedConnect n'est pas apparent en mode GINA).

7.8 Tokens et cartes à puces

7.8.1 SMARTCARDROAMING

Syntaxe : `SMARTCARDROAMING=01`

Usage : Ce paramètre caractérise le lecteur de carte à puce à utiliser :

Non défini	Lecteur de Carte configuré dans la Configuration VPN Sujet du certificat dans la Configuration VPN
"01"	Lecteur de Carte configuré dans la Configuration VPN Le sujet du certificat dans la Configuration VPN n'est pas pris en compte
"02"	Lecteur de Carte configuré dans le fichier VpnConf.ini Sujet du certificat dans la Configuration VPN.
"03"	Lecteur de Carte configuré dans le fichier VpnConf.ini Le sujet du certificat dans la Configuration VPN n'est pas pris en compte
"04"	1er lecteur de carte branché contenant une carte à puce Sujet du certificat dans la Configuration VPN
"05"	1er lecteur de carte branché contenant une carte à puce Le sujet du certificat dans la Configuration VPN n'est pas pris en compte

7.8.2 PKCS11ONLY

Syntaxe : `PKCS11ONLY=01`

Usage : Ce paramètre caractérise le mode d'accès à la carte à puce / au token :

Non défini	Le mode CNG (Cryptography API: Next Generation) est utilisé (valeur par défaut)
"01"	Force le Client VPN à utiliser le mode PKCS#11

7.8.3 KEYUSAGE

Syntaxe : `KEYUSAGE=01`

Usage : Ce paramètre caractérise le type de certificat utilisé : lorsqu'il est renseigné, le logiciel recherche un certificat de type « Authentification ». Si ce paramètre n'est pas renseigné, le type du certificat n'est pas vérifié.

7.8.4 NOCACERTREQ

Syntaxe : `NOCACERTREQ=01`

Usage : Ce paramètre configure le Client VPN pour gérer des autorités de certification (CA) Client/Passerelle différentes. Il est à renseigner (il peut aussi être configuré par l'interface du logiciel) dès que les certificats Client et Passerelle sont issus de CA différentes.

7.8.5 PKICHECK

Syntaxe : `PKICHECK=01`

Usage : Ce paramètre est utilisé pour caractériser la vérification du certificat de la passerelle VPN :

Non défini	Certificat de la Passerelle VPN non vérifié
"00"	Certificat de la Passerelle VPN non vérifié
"01"	Les caractéristiques suivantes du certificat de la passerelle VPN sont vérifiées : date de validité, chaîne de certification, signature et CRL de chaque certificat de la chaîne de certification.
"02"	Les caractéristiques suivantes du certificat de la passerelle VPN sont vérifiées : date de validité, chaîne de certification, signature de chaque certificat de la chaîne de certification (pas les CRL)
"03"	Identique à « 01 »

7.8.6 X509DIRECTORYSTRING

Syntaxe : `X509DIRECTORYSTRING=14`

Usage : Ce paramètre 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

Note : depuis la version 6.85 du logiciel, les caractères « 0x » ne doivent plus précéder la valeur du paramètre X509DirectoryString.

7.8.7 MACHINESTORE

Syntaxe : `MACHINESTORE=01`

Usage : Ce paramètre permet d'activer l'utilisation du magasin de certificat de la machine et non celui de l'utilisateur. S'il n'est pas défini, c'est le magasin utilisateur qui est utilisé par défaut.

7.8.8 DNPATTERN

Syntaxe : `DNPATTERN=[texte]`

Usage : Ce paramètre permet de caractériser le certificat utilisateur à utiliser : lorsqu'il est renseigné, le Client VPN 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 le pattern « `[texte]` ».
Quand ce paramètre n'est pas défini, le Client VPN recherche le premier certificat conforme aux autres caractéristiques configurées.

7.9 Paramètres généraux

7.9.1 MENUITEM

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

Usage : Permet de définir les items du menu en barre des tâches.
La valeur de menuitem est un champ de bit, chaque bit représente un item du menu en barre des tâches:
1 (1st bit)=Quitter
2 (2nd bit)=Panneau des connexions
4 (3rd bit)=Console
8 (4th bit)=Sauver et Appliquer (obsolète à partir de la version 5)
16 (5th bit)=Panneau de configuration
Par défaut, tous les items sont affichés : valeur = 31 (1F hexa).

Exemple : `MENUITEM=3`
affichera uniquement les items « 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 de 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.

7.9.2 NOAUTORUN

Syntaxe : `NOAUTORUN=1`

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

7.9.3 RESTRICTCONFADMIN

Syntaxe : `RESTRICTCONFADMIN=0`

Usage : Permet de restreindre l'accès au panneau de configuration des connexions aux administrateurs uniquement. Par défaut le panneau de configuration n'est accessible qu'en tant qu'administrateur.

7.9.4 NOSPLITTUNELLING

Syntaxe : `NOSPLITTUNELLING=01`

Usage : Ce paramètre 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 ».

7.9.5 NOSPLITDNS

Syntaxe : `NOSPLITDNS=01`

Usage : Ce paramètre 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 ».

7.9.6 NOPINCODE

Syntaxe : `NOPINCODE=01`

Usage : Ce paramètre permet de ne pas demander de PinCode pour les tokens qui n'en n'ont pas besoin. Par exemple la microSD d'Ercom est dans ce cas.

7.9.7 PINTIMEOUT

Syntaxe : `PINTIMEOUT=120`

Usage : Spécifie une valeur de temporisation en secondes, qui permet de fermer automatiquement la fenêtre de saisie du « Pin Code » quand le timeout échoit.

7.9.8 NOCFGPKTID

Syntaxe : `NOCFGPKTID=01`

Usage : Ce paramètre configure IKEv1 en mode compatible avec les routeurs Cisco ASA pour la fonction Mode Config (IKEv1 accepte l'échange « tronqué » Mode Config des routeurs Cisco ASA).

7.9.9 PWDUTF8

Syntaxe : `PWDUTF8=01`

Usage : Ce paramètre provoque un encodage en UTF8 du mot de passe X-Auth avant de l'envoyer à la passerelle. Ceci permet d'avoir par exemple des accents dans les mots de passe X-Auth (IKEv1 seul).

7.9.10 ROUTINGMODE

Syntaxe : `ROUTINGMODE=01`

Usage : Ce paramètre 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.

7.9.11 PKCS1V15SCHEME

Syntaxe : `PKCS1V15SCHEME=02`

Usage : Ce paramètre permet de configurer la méthode d'authentification lors de la montée du tunnel.

Non définie	Méthode 14 mise en œuvre
"01"	HASH_MD5
"02"	HASH_SHA1 (Method 1)
"03"	HASH_SHA2_224
"04"	HASH_SHA2_256
"05"	HASH_SHA2_384
"06"	HASH_SHA2_512
"07"	HASH_MD4
"08"	HASH_MD5_SHA1

7.9.12 FORCELOCALTRAFFICTOTUNNEL

Syntaxe : `FORCELOCALTRAFFICTOTUNNEL=01`

Usage : En mode « tout dans le tunnel », ce paramètre permet de router le trafic local de l'interface physique dans le tunnel. Si ce paramètre n'est pas présent, par défaut, le mode n'est pas activé.

Non défini	Mode désactivé
"00"	Mode désactivé
"01"	Mode activé

7.9.13 IKESTART

Syntaxe : `IKESTART=1`

Usage : Ce paramètre permet de démarrer le service IKE indépendamment de l'interface du logiciel. Si ce paramètre n'est pas présent, 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

7.9.14 SIGNFILE

Syntaxe : `SIGNFILE=1`

Usage : Permet de forcer la vérification du hash d'intégrité du fichier de configuration VPN.
La valeur par défaut est 0.

7.9.15 SYSTEMLOGOUTPUT

Syntaxe : `SYSTEMLOGOUTOUT=7`

Usage : Ce paramètre 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

7.9.16 SYSTEMLOGSYSLOGSERVER

Syntaxe : `SYSTEMLOSERVER=syslogserver.company.com`

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

7.9.17 SYSTEMLOGSYSLOGPORT

Syntaxe : `SYSTEMLOGSYSLOGPORT=5514`

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

8 Automatisations du logiciel Client VPN

8.1 Batch/script pour ouvrir ou fermer un tunnel

Le Client VPN Windows Enterprise permet d'ouvrir et de fermer un tunnel par les lignes de commande suivantes, utilisables dans un script :

```
vpnconf.exe /open:NomTunnel
vpnconf.exe /close:NomTunnel
```

Le Nom du Tunnel est composé comme suit :

	Nom du Tunnel
IKEv1	Phase1-Phase2
IKEv2	IKEAuth-ChildSA
SSL	TLS

Il est aussi possible d'ouvrir et de fermer un tunnel par script, via la procédure suivante :
1/ Créer une politique de sécurité VPN (Configuration VPN) avec l'option « Ouvrir automatiquement ce tunnel lorsque le Client VPN démarre » sélectionnée.
2/ Exporter la politique de sécurité VPN (Configuration VPN) dans un fichier (par exemple: « MonTunnel.tgb »)
3/ Créer le script avec la ligne de commande suivante : vpnconf.exe /import:MonTunnel.tgb

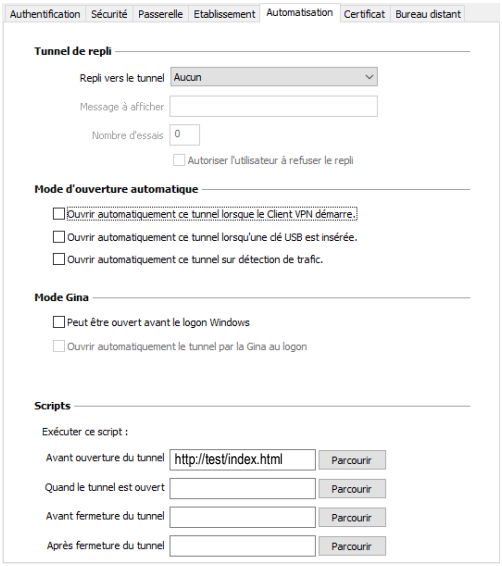
Ce script démarrera le Client VPN Windows Enterprise en important la politique de sécurité VPN (Configuration VPN) « MonTunnel.tgb », et ouvrira automatiquement le tunnel VPN.
Pour fermer le tunnel, il est possible d'utiliser la ligne de commande : vpnconf.exe /stop qui fermera le tunnel VPN ouvert, avant de quitter le logiciel.

8.2 Ouvrir automatiquement une page web à l'ouverture du tunnel

1/ Créer une politique de sécurité VPN (Configuration VPN)

2/ Ouvrir l'onglet « Automatisation » et entrer l'url de la page web à ouvrir (sur le réseau d'entreprise par exemple) dans le champ « Scripts / Quand le tunnel est ouvert »

3/ Ouvrir le tunnel : La page web spécifiée est automatiquement ouverte dès que le tunnel est établi.



9 Fichier VpnSetup.ini

9.1 Introduction

Le fichier VpnSetup.ini permet de configurer l'installation du Client VPN Windows Enterprise à partir d'un fichier, plutôt que par les propriétés en ligne de commande MSI.

Attention : par contrainte de l'installeur Microsoft MSI, contrairement aux versions précédentes du logiciel, le fichier VpnSetup.ini ne doit plus se trouver dans le même répertoire que l'installeur, mais 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 msiexec (voir chapitre Paramètres 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.

Note : les paramètres d'installation et de Politique de sécurité VPN de l'installeur MSI n'ont pas d'équivalent dans le fichier VpnSetup.ini.

9.2 Section [Activation]

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

- OSACert
- OSAPort
- OSAUrl
- ActivMail
- AutoActiv
- License
- NoActivWin

9.3 Section [Dialer]

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

- UseDialerByDefault
- TndSuffixes
- TndHttpServerURL
- TndHttpServerPort
- TndLatency
- AonItfPassover

- DialerMinimize
- DialerDefs
- VpnLogPurge
- TokenOutHandle
- GinaBehaves

9.4 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
- PKCS11Only
- KeyUsage
- NoCACertReq
- PKICheck
- X509DirectoryString
- MachineStore
- DnPattern

9.5 Section [AddRegKey]

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

- MenuItem
- RestricConfAdmin
- NoSplitTunneling
- NoSplitDNS
- NoPinCode
- PinTimeOut
- nocfgpktid
- PwdUTF8
- RoutingMode
- pkcs1v15scheme
- ForceLocalTraficToTunnel
- IkeStart

9.6 Section [Config]

Le paramètre de la section [Config] est les suivant :

- SignFile

9.7 Section [Logs]

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

- SystemLogOutput
- SystemLogSyslogServer
- SystemLogSyslogPort

9.8 Exemple de fichier vpnsetup.ini

```
[Activation]
OSAUrl=192.168.217.102/osace_activation.php
OSAPort=80
OSACert="MIICGjCCAYOgAwIBAgIBADANBg [........] muHf58kMO0jvhkyq24GryqptSaSJqVIA="

[Dialer]
TNDDnsSuffixes=trusted.thegreenbow
TNDHttpsServerUrl=beacon.thegreenbow.com
TNDHttpsServerPort=443


[PKIOptions]
PKICheck=01
Smartcardroaming=01
NoCACertReq=01
KeyUsage=01
PKCS11Only=01
X509DirectoryString=1E
MachineStore=01
DnPattern=thecompany

[AddRegKey]
PinTimeOut=120
PwdUTF8=01
RoutingMode=01
pkcs1v15scheme=02
ForceLocalTraficToTunnel=01
IkeStart=1

[Config]
SignFile=1

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

10 Contact

10.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur les sites :
Anglais : www.thegreenbow.com
Français : www.thegreenbow.fr

10.2 Commercial

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

10.3 Support

Les sites TheGreenBow proposent plusieurs pages concernant le support technique des logiciels :

Support

Anglais : http://www.thegreenbow.com/support.html
Français : http://www.thegreenbow.fr/support.html

Aide en ligne

Anglais : http://www.thegreenbow.com/support_flow.html?product=vpn&lang=en
Français : http://www.thegreenbow.com/support_flow.html?product=vpn&lang=fr

FAQ

Anglais : http://www.thegreenbow.com/vpn_faq.html
Français : http://www.thegreenbow.fr/vpn_faq.html

Contact

Le support technique est accessible via les formulaires disponibles sur le site TheGreenBow ou directement par email à l'adresse : support@thegreenbow.com

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software