Client VPN
Windows Enterprise 6.87

Guide de déploiement

Dernière mise à jour : 20 juin 2022
Référence de document : 20220620_DG_VPE_6.8_FR_1.9

Table des matières

1 Introduction

Ce guide est destiné aux administrateurs du Client VPN Windows Enterprise.

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 de l'administrateur » est également disponible sur le site TheGreenBow.

Avant de procéder au déploiement du Client VPN Windows Enterprise, veuillez lire attentivement la section « Recommandations de sécurité » du « Guide de l'administrateur ».

2 Déploiement du Client VPN

2.1 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.

2.2 Personnalisation du logiciel

Outre l'utilisation du Panneau de Configuration du logiciel pour générer des configurations VPN à déployer, le Client VPN Windows Enterprise 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 le Client VPN Windows Enterprise (par défaut : `C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise`)

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 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.

2.3 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 8 Fichier vpnsetup.ini).

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

1/ Téléchargez le programme d'installation TheGreenBow_VPN_ENTERPRISE.msi depuis https://thegreenbow.com/.
2/ Ouvrez la fenêtre de commande Windows en mode administrateur et entrez la ligne de commande suivante :

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

Exemple

```
msiexec /i "[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.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 7 Paramètres et propriétés de l'installeur MSI.

2.4 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 :

```
msiexec /i "[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi" /q
TGBCONF_ADMINPASSWORD=Tgb@dM1!
```

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.

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.

2.5 Réparation

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

2.6 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 TheGreenBow VPN Enterprise) du menu Windows.

2.7 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 du client VPN Windows Enterprise.

3 Déploiement de l'activation du logiciel

3.1 Introduction

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

Par défaut, l'activation des logiciels est réalisée sur le site internet TheGreenBow accessible en ligne.

Lorsque votre parc de machines sur lesquelles les clients VPN sont installés ne dispose pas de connexion à internet, vous pouvez réaliser l'activation des logiciels sur un serveur d'activation installé chez vous : 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 de l'installation `vpnsetup.ini`. Ces méthodes sont décrites dans les sections ci-dessous.

3.2 Activation sur le site internet TheGreenBow

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 7.6 Activation de la licence.

Ligne de commande pour une activation automatique et silencieuse :

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

3.3 Activation sur le TAS

Lorsque l'activation du logiciel est effectuée auprès d'un serveur TAS (« TheGreenBow Activation Server », serveur d'activation installé sur votre infrastructure), il est recommandé de spécifier les paramètres de ce serveur en ligne de commande à l'aide des propriétés MSI `OSAURL`, `OSAPORT` et `OSACERT` (voir chapitre 6 Utilisation en ligne de commande).

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

```
msiexec /i "[répertoire_téléchargement]/TheGreenBow_VPN_ENTERPRISE.msi" /q
LICENSE=[numéro_de_licence] ACTIVMAIL=[email_activation] NOACTIVWIN=1 AUTOACTIV=1
OSAURL=192.168.217.102/osace_activation.php OSAPORT=80 OSACERT="MIICGjCCAYOgAwIBAgIBADANBg [........]
muHf58kMO0jvhkyq24GryqptSaSJqVIA="
```

Il est également possible d'utiliser le fichier `vpnsetup.ini` joint à l'installeur au moment de l'installation (voir chapitre 8 Fichier vpnsetup.ini pour le détail des paramètres).

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="
```

3.4 Activation dans le tunnel

L'activation sur le site internet TheGreenBow ou sur le TAS nécessite une connexion à internet ou au réseau sur lequel se trouve le TAS. À partir de la première installation du Client VPN Windows Enterprise, l'utilisateur dispose de 30 jours (période d'évaluation) pour se connecter à internet ou au réseau sur lequel se trouve le TAS, pour effectuer l'activation.

L'activation peut s'effectuer manuellement en ouvrant la fenêtre « À propos » du Client VPN Windows Enterprise (cf. « Guide de l'administrateur » du Client VPN Windows Enterprise).

Si la propriété `AUTOACTIV` est à 1, alors le Client VPN Windows Enterprise 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. Il faudra alors connecter le poste directement dans le réseau où se trouve le TAS.

3.5 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 « email d'activation » pour, par exemple, y renseigner le nom du poste activé, ceci au cours du processus d'installation.

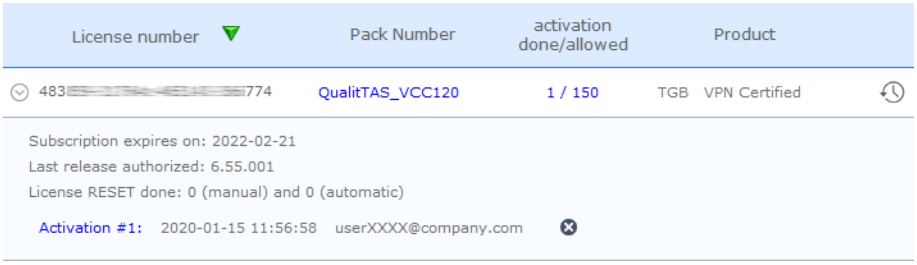
Script d'installation pour l'invite de commande Windows avec identifiant du poste activé :

```
msiexec /i "[répertoire_téléchargement]/TheGreenBow_VPN_ENTERPRISE.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]/TheGreenBow_VPN_ENTERPRISE.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 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 le serveur d'activation sur le site TheGreenBow ou sur votre TAS.



⚠ 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.

4 Déploiement des configurations VPN

4.1 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 désactivée par défaut.

Exemple de ligne de commande pour activer la signature et vérification de l'intégrité du fichier de configuration :

```
msiexec /i "[répertoire_téléchargement]/TheGreenBow_VPN_ENTERPRISE.msi" /q SIGNFILE=1
```

4.2 Déployer une configuration VPN à l'installation

Une configuration VPN préconfigurée peut être embarquée avec l'installation du Client VPN Windows Enterprise. 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 :

1/ Depuis le Panneau de Configuration du Client VPN Windows Enterprise, créez la configuration VPN à destination du poste à équiper.
2/ Exportez cette configuration VPN (menu « Configuration > Export », cf. « Guide de l'administrateur » du Client VPN Windows Enterprise) en la protégeant éventuellement par mot de passe.
3/ Transférez le programme d'installation et la configuration VPN sur le poste à équiper.
4/ Exécutez l'installation du Client VPN Windows Enterprise en indiquant les propriétés `TGBCONF_PATH` et `TGBCONF_PASSWORD` (si la configuration est protégée par mot de passe, cf. section 7.4 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]/TheGreenBow_VPN_ENTERPRISE.msi" /q
TGBCONF_PATH=C:\Users\Admin\conf.tgb TGBCONF_PASSWORD=[mot_de_passe]
```

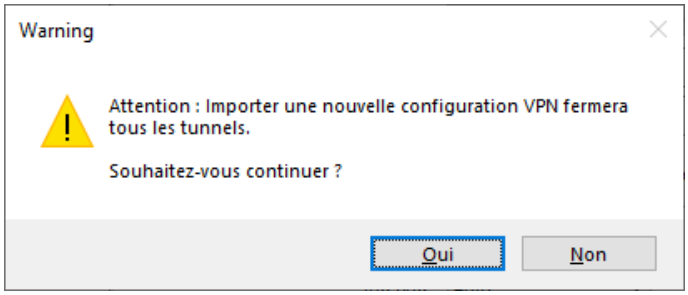
Du point de vue de la sécurité du déploiement, cette méthode exploite la fonction de contrôle d'intégrité des configurations VPN, si activée. Dans ce cas, cette fonction garantit que la configuration importée au moment de l'installation n'a pas été corrompue.

4.3 Déployer la mise à jour d'une configuration VPN

Une fois le Client VPN Windows Enterprise 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 :

1/ Créez la configuration VPN à destination du poste à équiper.
2/ Exportez cette configuration (menu « Configuration > Export », cf. « Guide de l'administrateur » du Client VPN Windows Enterprise). Elle peut être chiffrée par un mot de passe.
3/ Transférez cette configuration VPN sur le poste à mettre à jour.
4/ 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 6.3 Importation).
5/ 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 6 Utilisation en ligne de commande) 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.

5 Déploiement avec tokens ou cartes à puce

5.1 Introduction

Un grand nombre de tokens et de cartes à puce permettant une authentification forte multi-facteurs (MFA) sont prise en charge par le Client VPN Windows Enterprise via l'une des API suivantes : CSP (en IKEv1 uniquement), CNG (par défaut) ou PKCS#11.

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

5.1.1 CSP

CSP signifie « Cryptographic Service Provider ». C'est une API d'accès aux tokens et aux cartes à puce, auparavant fournie par Microsoft, mais qui n'est plus maintenue dans Windows 10 ou 11. Il est fortement recommandé, pour des raisons de sécurité et de performance, d'utiliser des tokens ou cartes à puces compatibles avec les API CNG ou PKCS#11.

Depuis la version 6.85 du Client VPN Windows Enterprise, l'API CSP est uniquement utilisable avec le protocole IKEv1.

5.1.2 CNG

CNG signifie « Cryptography API: Next Generation». C'est une nouvelle API d'accès aux tokens et aux cartes à puce actuellement fournie par Microsoft. Elle est utilisée par défaut par le Client VPN Windows Enterprise avec le protocole IKEv2, et ne requiert pas de configuration supplémentaire.

5.1.3 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 le Client VPN Windows Enterprise 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 le Client VPN Windows Enterprise 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 de l'administrateur » du Client VPN Windows Enterprise) ou bien la propriété MSI `PKCS11ONLY` à l'installation du logiciel (cf. section 7.8.2 PKCS11ONLY).

Le Client VPN Windows Enterprise 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.

Les tokens et cartes à puce pris en charge par le Client VPN Windows Enterprise sont ceux qui sont listés sur le site TheGreenBow à l'adresse https://thegreenbow.com/fr/support/guides-dintegration/tokens-vpn-compatibles/ et pour lesquels la case « PKCS11 » est cochée.
Pour les tokens ou cartes à puce qui ne sont pas reconnus en standard par le Client VPN Windows Enterprise, le logiciel offre la possibilité de spécifier leurs caractéristiques dans un fichier d'initialisation PKCS#11 appelé `vpnconf.ini`, décrit ci-après.

5.2 Fichier vpnconf.ini

Pour permettre au Client VPN Windows Enterprise de prendre en charge des tokens ou cartes à puces non reconnus en standard, un fichier `vpnconf.ini` doit être crée dans le répertoire d'installation du Client VPN (par défaut : `C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise`). 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.

5.2.1 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 (2)

(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:FF:FF`

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

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"
```

5.2.2 Section ROAMING

La section ROAMING permet de caractériser le token ou le lecteur de cartes 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 de l'administrateur » du Client VPN Windows Enterprise) ou lorsque l'installation du logiciel a été effectuée avec la propriété `SMARTCARDROAMING` égale à 2 ou 3 (voir section 7.8.1 SMARTCARDROAMING).

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

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 (1)
`SmartCardMiddelwarePath`	Chemin vers le middleware incluant le nom du middleware (2)
`SmartCardMiddlewareRegistry`	Nom de la clef en base de registre indiquant le chemin vers le middleware (2)

(1) PKCS#11 est la seule valeur possible pour le paramètre `SmartCardMiddlewareType`.
(2) L'un des deux paramètres `SmartCardMiddlewarePath` ou `SmartCardMiddlewareRegistry` doit obligatoirement être défini.

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"
```

6 Utilisation 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 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 Client VPN Windows Enterprise).
- 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 le Client VPN Windows Enterprise 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.

La valeur `NomTunnel` utilisée pour les options `/open`, `/status` et `/close` est composée comme suit (il convient de remplacer le nom de la Phase, IKEAuth, ChildSA ou TLS par le nom choisi dans la configuration) :

	NomTunnel
IKEv1	Phase1-Phase2
IKEv2	IKEAuth-ChildSA
SSL	TLS

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

6.2 Différence entre import, importonce, add, replace

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

L'option `/importonce` permet d'importer une configuration VPN sans démarrer le Client VPN Windows Enterprise.

Lorsque le Client VPN Windows Enterprise est démarré, ces deux options importent simplement la configuration VPN.

Lorsque la configuration VPN courante (avant importation) du Client VPN Windows Enterprise 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` remplace systématiquement l'ancienne configuration par la nouvelle.

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

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`.

6.3 Importation

/import

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

Usage : Cette option est utilisée pour importer une configuration VPN en démarrant le Client VPN Windows Enterprise.
Cette option peut être utilisée pour lancer le logiciel Client VPN Windows Enterprise 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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /import:"C:\Users\Admin\Documents\mavpnconf.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).

/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 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 : `"C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /importonce:"C:\Users\Admin\Documents\mavpnconf.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 d'environnement `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).

/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 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 : `"C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /add:"C:\Users\Admin\Documents\mavpnconf.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.

/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 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 :
```
"C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /replace:"C:\Users\Admin\Documents\mavpnconf.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.

/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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /import:"C:\Users\Admin\Documents\mavpnconf.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.

6.4 Exportation

/export

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

Usage : Permet d'exporter une configuration 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.
`[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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /export:"C:\Users\Admin\Documents\mavpnconf.tgb" /pwd:gq1aRe7
```

/exportonce

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

Usage : Même comportement que l'option `/export`, mais sans démarrer le logiciel Client VPN.
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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /exportonce:"C:\Users\Admin\Documents\mavpnconf.tgb" /pwd:gq1aRe7kP2t
```

6.5 Ouverture/fermeture d'un tunnel VPN

Les options `/stop`, `/closeall` et `/status` ne peuvent être exécutées que si le Client VPN Windows Enterprise est déjà lancé et n'est pas démarré en mode TrustedConnect.

Les options `/open` et `/close` peuvent être exécutées sans que le Client VPN Windows Enterprise 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.

/stop

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

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

Exemple :
```
"C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /stop
```

/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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe"
/open:TgbTest-TgbTest
@echo retour = %ERRORLEVEL%
Pause
```

/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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe"
/status:TgbTest-TgbTest
@echo retour = %ERRORLEVEL%
Pause
```

/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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe"
/close:TgbTest-TgbTest
```

/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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe"
/closeall
```

6.6 Redémarrage

L'option `/resetike` ne peut être exécutée que si le Client VPN Windows Enterprise est déjà lancé et n'est pas démarré en mode TrustedConnect.

/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\TheGreenBow\TheGreenBow VPN Enterprise\vpnconf.exe" /resetike`

6.7 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).
1500	:	Le tunnel VPN spécifié n'existe pas (attention à la casse !).

7 Paramètres et propriétés 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` 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.

7.2 Paramètres MSI en ligne de commande

/i

Syntaxe :	`msiexec /i [chemin_de_l_installeur]`
Usage :	Installe ou met à jour le logiciel Client VPN Windows Enterprise
Exemple :	`msiexec /i "[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi"`

/x

Syntaxe :	`msiexec /x [chemin_de_l_installeur]`
Usage :	Désinstalle le logiciel Client VPN Windows Enterprise
Exemple :	`msiexec /x "[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi"`

/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]\TheGreenBow_VPN_ENTERPRISE.msi" /q`

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

7.3 Installation

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

7.3.1 APPLICATIONROOTDIRECTORY

Syntaxe : `APPLICATIONROOTDIRECTORY=[répertoire_installation]`

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

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

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.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi"
TGBCONF_ADMINPASSWORD=Tgb@dM1Npwd!
```

7.3.3 NOAUTORUN

Syntaxe : `NOAUTORUN=1`

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

7.4 Configuration VPN

7.4.1 TGBCONF_PATH

Syntaxe : `TGBCONF_PATH=[chemin_fichier_conf]`

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

7.4.2 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`.

7.5 Serveur d'activation TAS

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

Les valeurs de ces propriétés étant requises pour des configurations spécifiques, elles sont en général fournies par TheGreenBow.

7.5.1 OSAURL

Syntaxe : `OSAURL=[URL_TAS]`

Usage : Cette propriété permet de définir l'URL du serveur d'activation TAS. Elle doit être définie en association avec la propriété `OSAPORT` et, le cas échéant, avec la propriété `OSACERT`.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi"
OSAUrl=192.168.217.102/osace_activation.php
```

7.5.2 OSAPORT

Syntaxe : `OSAPORT=[port_TAS]`

Usage : Cette propriété permet de définir le port du serveur d'activation TAS en association avec la propriété `OSAURL`.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi"
OSAPort=80
```

7.5.3 OSACERT

Syntaxe : `OSACERT=[contenu_du_certificat]`

Usage : Cette propriété permet de définir, le cas échéant, le certificat utilisé pour s'authentifier au serveur d'activation TAS.

Exemple :
```
msiexec /i
"[répertoire_téléchargement]\TheGreenBow_VPN_ENTERPRISE.msi"
OSACert="MIICGjCCAYOgAwIBAgIBADANBg [........]
muHf58kMO0jvhkyq24GryqptSaSJqVIA="
```

7.6 Activation de la licence

7.6.1 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]\TheGreenBow_VPN_ENTERPRISE.msi"
ACTIVMAIL=salesgroup@company.com
```

7.6.2 AUTOACTIV

Syntaxe : `AUTOACTIV=1`

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

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

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

7.6.3 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]\TheGreenBow_VPN_ENTERPRISE.msi"
LICENSE=1234567890ABCDEF12345678
```

7.6.4 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.

7.7 Panneau TrustedConnect

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

7.7.1 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).

7.7.2 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).

7.7.3 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 `01000000`.
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.

7.7.4 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.

Cette propriété s'applique non seulement quand le Client VPN est lancé en mode TrustedConnect, mais également quand il est lancé en mode Panneau des Connexions / Panneau de Configuration.

7.7.5 TOKENOUTHANDLE

Syntaxe : `TOKENOUTHANDLE=30`

Usage : Cette propriété permet de configurer le comportement du Client VPN lorsque le token est extrait, ou lorsque la carte à puce est extraite du lecteur, alors qu'un tunnel VPN est ouvert. Cette propriété est également disponible avec le Panneau des Connexions, mais uniquement en modes A et C.

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 ce mode, 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 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).

7.8 Tokens et cartes à puces

7.8.1 SMARTCARDROAMING

Syntaxe : `SMARTCARDROAMING=1`

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

Non défini	Lecteur de cartes à puce ou token configuré dans la configuration VPN Le sujet du certificat est dans la configuration VPN.
1	Lecteur de cartes à puce ou token configuré dans la configuration VPN Le sujet du certificat dans la configuration VPN n'est pas pris en compte.
2	Lecteur de cartes à puce ou token configuré dans le fichier `vpnconf.ini` Le sujet du certificat est dans la configuration VPN.
3	Lecteur de cartes à puce 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 Le sujet du certificat est 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.

7.8.2 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

7.8.3 KEYUSAGE

Syntaxe : `KEYUSAGE=1`

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

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

Lorsque la valeur de la propriété `KEYUSAGE` est définie sur 2, la case à cocher « Utiliser seulement les certificats de type authentification » de l'onglet « Options PKI » est grisée, cf. « Guide de l'administrateur » du Client VPN Windows Enterprise.

7.8.4 NOCACERTREQ

Syntaxe : `NOCACERTREQ=1`

Usage : Cette propriété configure le Client VPN 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.

7.8.5 PKICHECK

Syntaxe : `PKICHECK=1`

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

0 ou non défini	Certificat de la passerelle VPN non vérifié.
1	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.
2	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) – valeur par défaut.
3	Identique à 1.

7.8.6 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`

Depuis la version 6.8 du logiciel, les caractères « 0x » ne doivent plus précéder la valeur de la propriété `X509DirectoryString`.

7.8.7 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.

7.8.8 DNPATTERN

Syntaxe : `DNPATTERN=[texte]`

Usage : Cette propriété permet de caractériser le certificat à utiliser : lorsqu'elle est renseignée, le Client VPN Windows Enterprise recherche, sur token, carte à puce et dans le magasin de certificats Windows le certificat dont le sujet contient `[texte]`.
Quand cette propriété n'est pas définie, le Client VPN recherche le premier certificat conforme aux autres caractéristiques configurées.

7.8.9 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.

7.8.10 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.

7.9 Paramètres généraux

7.9.1 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.

7.9.2 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.

7.9.3 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 ».

En configuration « Tout le trafic dans le tunnel », le Client VPN crée une route par défaut sous Windows pour rediriger tout le trafic vers l'interface virtuelle. Néanmoins, dans certaines conditions, Windows continue d'utiliser la route de l'interface physique. Cette propriété permet de désactiver complètement la route de l'interface physique.

7.9.4 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 ».

Cette propriété peut être utilisée en complément de NOSPLITTUNNELING lorsque Windows continue d'utiliser les DNS de l'interface physique.

7.9.5 NOCFGPKTID

Syntaxe : `NOCFGPKTID=1`

Usage : Cette propriété 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).

7.9.6 PWDUTF8

Syntaxe : `PWDUTF8=1`

Usage : Cette propriété 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).

7.9.7 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.

7.9.8 PKCS1V15SCHEME

Syntaxe : `PKCS1V15SCHEME=2`

Usage : Cette propriété permet de configurer la méthode d'authentification lors de la montée du tunnel.

Non définie	Méthode 14 mise en œuvre
1	HASH_MD5
2	HASH_SHA1 (Method 1)
3	HASH_SHA2_224
4	HASH_SHA2_256
5	HASH_SHA2_384
6	HASH_SHA2_512
7	HASH_MD4
8	HASH_MD5_SHA1

7.9.9 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

7.9.10 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

7.9.11 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 (désactivé).

7.9.12 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.

7.9.13 NESTEDTUNNEL

Syntaxe : `NESTEDTUNNEL=1`

Usage : Cette propriété permet d'imbriquer deux tunnels. À utiliser lorsqu'on souhaite qu'un second tunnel se serve de la connexion offerte par un premier tunnel. La passerelle du second tunnel est alors uniquement accessible sur le réseau distant du premier tunnel.
La valeur par défaut est 0 (désactivé).

7.10 Logs

7.10.1 SYSTEMLOGOUTPUT

Syntaxe : `SYSTEMLOGOUTPUT=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

7.10.2 SYSTEMLOGSYSLOGSERVER

Syntaxe : `SYSTEMLOSERVER=syslogserver.company.com`

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

7.10.3 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.

8 Fichier vpnsetup.ini

8.1 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.

⚠ 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, 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 7 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.

ℹ 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`.

8.2 Section [Activation]

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

- `OSAUrl` (cf. section 7.5.1 OSAURL)
- `OSAPort` (cf. section 7.5.2 OSAPORT)
- `OSACert` (cf. section 7.5.3 OSACERT)
- `ActivMail` (cf. section 7.6.1 ACTIVMAIL)
- `AutoActiv` (cf. section 7.6.2 AUTOACTIV)
- `License` (cf. section 7.6.3 LICENSE)
- `NoActivWin` (cf. section 7.6.4 NOACTIVWIN)

8.3 Section [Dialer]

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

- `UseDialerByDefault` (cf. section 7.7.1 USEDIALERBYDEFAULT)
- `DialerMinimize` (cf. section 7.7.2 DIALERMINIMIZE)
- `DialerDefs` (cf. section 7.7.3 DIALERDEFS)
- `VpnLogPurge` (cf. section 7.7.4 VPNLOGPURGE)
- `TokenOutHandle` (cf. section 7.7.5 TOKENOUTHANDLE)
- `GinaBehaves` (cf. section 7.9.12 GINABEHAVES)

8.4 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 7.8.1 SMARTCARDROAMING)
- `PKCS11Only` (cf. section 7.8.2 PKCS11ONLY)
- `KeyUsage` (cf. section 7.8.3 KEYUSAGE)
- `NoCACertReq` (cf. section 7.8.4 NOCACERTREQ)
- `PKICheck` (cf. section 7.8.5 PKICHECK)
- `X509DirectoryString` (cf. section 7.8.6 X509DIRECTORYSTRING)
- `MachineStore` (cf. section 7.8.7 MACHINESTORE)
- `DnPattern` (cf. section 7.8.8 DNPATTERN)

8.5 Section [AddRegKey]

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

- `NoPinCode` (cf. section 7.8.9 NOPINCODE)
- `PinTimeOut` (cf. section 7.8.10 PINTIMEOUT)
- `MenuItem` (cf. section 7.9.1 MENUITEM)
- `RestrictConfAdmin` (cf. section 7.9.2 RESTRICTCONFADMIN)
- `NoSplitTunneling` (cf. section 7.9.3 NOSPLITTUNNELING)
- `NoSplitDNS` (cf. section 7.9.4 NOSPLITDNS)
- `nocfgpktid` (cf. section 7.9.5 NOCFGPKTID)
- `PwdUTF8` (cf. section 7.9.6 PWDUTF8)
- `pkcs1v15scheme` (cf. section 7.9.8 PKCS1V15SCHEME)
- `ForceLocalTraficToTunnel` (cf. section 7.9.9 FORCELOCALTRAFICTOTUNNEL)
- `IkeStart` (cf. section 7.9.10 IKESTART)
- `NestedTunnel` (cf. section 7.9.13 NESTEDTUNNEL)

8.6 Section [Config]

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

- `SignFile` (cf. section 7.9.11 SIGNFILE)

8.7 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 7.10.1 SYSTEMLOGOUTPUT)
- `SystemLogSyslogServer` (cf. section 7.10.2 SYSTEMLOGSYSLOGSERVER)
- `SystemLogSyslogPort` (cf. section 7.10.3 SYSTEMLOGSYSLOGPORT)

8.8 Section [VirtMDriver]

- `RoutingMode` (cf. section 7.9.7 ROUTINGMODE)

8.9 Exemple de fichier vpnsetup.ini

```
[Activation]
OSAUrl=192.168.217.102/osace_activation.php
OSAPort=80
OSACert="ABCDE...."
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=1

[VirtMDriver]
RoutingMode=1

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

9 Contact

9.1 Information

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

9.2 Commercial

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

9.3 Support

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

Aide en ligne

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

FAQ

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

Formulaire de contact

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

THEGREENBOW

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris – France
sales@thegreenbow.com