THEGREENBOW

TheGreenBow VPN Client

Guide de Déploiement

Table des matières

1 Introduction

1.1 Administration et déploiement du Client VPN TheGreenBow

Le Client VPN TheGreenBow 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.

Ce document décrit les options d'administration et de configuration du Client VPN TheGreenBow.
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 TheGreenBow :
- 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.

1.2 Outils de déploiement

Ce document décrit aussi les différents moyens de déployer le logiciel :
- Depuis un lecteur réseau
- Depuis un CD-ROM / DVD
- Depuis un support amovible type USB, pré-configuré

1.3 VPN Standard, VPN Premium et VPN Certified

Les fonctions de déploiement et d'administration décrites dans ce document sont disponibles dans la version PREMIUM et CERTIFIED du Client VPN. Seule une partie d'entre elles est disponible dans la version standard du Client VPN.
Le cas échéant, la mention "VPN Premium seul" ou "VPN Certified seul" est indiquée.

1.4 Ancienne version

Toutes les options et fonctions décrites dans ce document sont applicables au Client VPN TheGreenBow à partir de la version 4.2 et supérieures. Pour des versions du logiciel antérieures, se reporter aux documents disponibles sur le site web TheGreenBow.

2 Considérations de sécurité

2.1 Configuration du poste hôte

La machine sur laquelle est installé et exécuté le Client VPN TheGreenBow 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

Pour une installation sur poste Windows 7, le guide Microsoft suivant peut aussi être consulté :
Common Criteria Security Target, Windows 7 and Windows Server 2008 R2

Il est recommandé d'exécuter l'installation du Client VPN TheGreenBow 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 TheGreenBow 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 TheGreenBow 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 (masquage des fonctions, mot de passe de contrôle d'accès, etc.)

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 TheGreenBow 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 TheGreenBow 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 TheGreenBow" (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 : le "Guide de Déploiement Options PKI" (tgbvpn_ug_deployment_pki_fr.pdf)

2.7 Protection des données sensibles

Comme détaillé dans le "Guide Utilisateur du Client VPN TheGreenBow" (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.

3 Déploiement du Client VPN

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.

3.1 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.

Note : Suivant la politique de sécurité mise en place sur le poste cible, une notification Windows de lancement du programme peut être affichée. Contacter le support TheGreenBow pour éviter l'affichage de cette fenêtre.

3.2 Créer une installation silencieuse

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

1/ Télécharger le setupTheGreenBow_VPN_Client.exe depuis http://www.thegreenbow.com
2/ Ouvrir la fenêtre de commande windows et entrer la ligne de commande :

```
TheGreenBow_VPN_Client.exe /S (options supplémentaires, voir chap.8.1)
```

Exemple:

```
[setup_dir]/TheGreenBow_VPN_Client.exe /S –license=123456 /D=[install_dir]
```

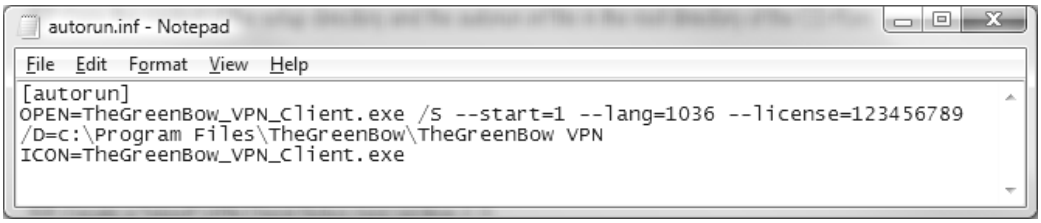
[setup_dir] est le répertoire du setup
[install_dir] est le répertoire où installer le logiciel (par défaut, le répertoire d'installation est : " C:\Program Files\TheGreenBow\TheGreenBow VPN ")
[install_dir] doit être spécifié en entier, l'option /D ne reconnaît pas les répertoire relatifs.
L'option "/D" doit être utilisée en fin de ligne de commande, et sans espace entre l'option, le signe "=" et la valeur.

3.3 Déploiement depuis un CD-ROM

1/ Créer un fichier texte appelé "autorun.inf" dont le contenu est le suivant :

```
[autorun]
OPEN=TheGreenBow_VPN_Client.exe /S /D=c:\Program Files\TheGreenBow\TheGreenBow VPN (+ options
supplémentaires, Cf. chapitre 8)
ICON=TheGreenBow_VPN_Client.exe
```

Exemple:



2/ Copier à la racine du CD-ROM
- Le fichier "autorun.inf"
- Le fichier "TheGreenBow_VPN_Client.exe"

Dès son insertion dans le poste cible, l'installation sera exécutée automatiquement et de façon silencieuse.

Note : Se reporter au chapitre 8 pour les différentes règles de syntaxe des options.

Note : Voir aussi "Enabling and Disabling AutoRun" pour certaines versions de Windows (i.e. http://msdn.microsoft.com/en-us/library/windows/desktop/cc144204%28v=vs.85%29.aspx#floppy).

3.4 Déploiement depuis un lecteur réseau ou un raccourci

1/ Télécharger le Client VPN TheGreenBow
2/ Clic-droit sur l'exécutable "TheGreenBow_VPN_Client.exe"
3/ Sélectionner "Créer un raccourci"
4/ Clic-droit sur le raccourci qui vient d'être créé
5/ Sélectionner "Propriétés"
6/ Dans l'onglet "**Raccourci**", dans le champ "**Cible :**", ajouter les options désirées à la ligne de commandes, en veillant à conserver des espaces entre les différentes options.
7/ Copier le raccourci à l'endroit où l'utilisateur peut l'exécuter (par exemple sur son bureau Windows)

Exemple :

"F:\TheGreenBow_VPN_Client.exe /S --start=1 --lang=1036 /D=C:\Program Files\TheGreenBow\TheGreenBow VPN"

Important : Vérfier la présence d'espace entre chaque argument

3.5 Déploiement grâce à un script

1/ Créer un fichier texte appelé "vpn_setup.bat"
2/ Editer ce fichier (clic droit et sélectionner "Modifier")
3/ Entrer les lignes de commandes à exécuter
4/ Déployer ce fichier batch avec l'exécutable TheGreenBow_VPN_Client.exe

Exemple :

```
cd .\setup
TheGreenBow_VPN_Client.exe /S --lang=1036
cd ..
copy myvpnconfig.tgb C:\Program Files\TheGreenBow\TheGreenBow VPN
cd C:\Program Files\TheGreenBow\TheGreenBow VPN
vpnconf.exe /importonce:myvpnconfig.tgb
```

Dans cet exemple :
- Le répertoire contenant l'installeur du logiciel s'appelle "setup" et est situé dans le répertoire contenant le fichier batch
- Cette installation se termine par l'importation de la politique de sécurité "myvpnconfig.tgb"

Note : Se reporter au chapitre 8 pour les différentes règles de syntaxe des options.

3.6 Déploiement d'une mise à jour

Le déploiement d'une mise à jour du Client VPN TheGreenBow 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 de la politique de sécurité VPN de la précédente version, installation de la nouvelle version, restauration de la politique de sécurité VPN de l'ancienne version.

Note : Si la version du Client VPN installé est inférieure à 4.2, la mise à jour du logiciel nécessite une désinstallation de ce logiciel qui, en standard, n'est pas silencieuse. Pour rendre cette désinstallation silencieuse, contacter le support TheGreenBow.

Note : La mise à jour ou l'installation d'un Client VPN Certifié en remplacement d'un Client VPN "Standard" ou "Premium" nécessite que ces Clients VPN soient désinstallés avant d'effectuer la mise à jour. Si la configuration VPN doit être conservée d'une version à l'autre, contacter le support TheGreenBow.

Note : lorsque qu'un Client VPN Certifié est installé en remplacement d'une version protégée par mot de passe, ce mot de passe est requis pour désinstaller l'ancienne version. La nouvelle est installée avec le mot de passe par défaut "admin".

3.7 Fichier de configuration du setup : vpnsetup.ini

Le fichier vpnsetup.ini permet de configurer l'installation du Client VPN TheGreenBow.
Il permet de définir les paramètres suivants :
- paramètres d'activation du logiciel
- paramètres PKI pour la gestion des tokens, lecteurs de cartes à puce et certificats
- paramètres généraux de fonctionnement

Les commandes et les conditions de mise en œuvre du fichier vpnsetup.ini sont décrites au chapitre 8.2.

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.

Note : Pour toute explication et détail sur les mécanismes d'activation des logiciels et de gestion des licences , se reporter au document tgb_ug_activation_management

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).

En plus des paramètres "numéro de licence" et "email d'activation" requis pour une activation auprès du serveur TheGreenBow, une activation sur serveur TAS requière la définition des paramètres : adresse, port et certificat du serveur d'activation.

Les paramètres "numéro de licence" et "email d'activation" peuvent être spécifiés en ligne de commande de l'installeur du logiciel. Cf. Chap. 8.1 "Options de ligne de commande de l'installeur du Client VPN"
Les paramètres "serveur TAS" doivent être spécifiés dans le fichier VpnSetup.ini associé à l'installeur. Cf. Chap. 8.2 "Fichier de configuration du setup : vpnsetup.ini"

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 paramètres de ligne de commande de l'installeur : "`--autoactiv`" (qui automatise l'activation) et "`--noactiv`" (qui masque la fenêtre d'activation), conjointement aux paramètres "`--license`" et "`--activmail`" comme indiqué au chapitre 8.1 (Options de ligne de commande de l'installeur du Client VPN).

Ligne de commande pour une activation automatique et silencieuse :

```
TheGreenBow_VPN_Client.exe /S --license=[numero_de_licence] --activmail=[email_activation] --
noactiv=1 --autoactiv=1
```

Pour que l'activation soit réalisée auprès d'un serveur TAS, spécifier les paramètres du serveur TAS (URL, Port, Certificat) dans le fichier VpnSetup.ini joint à l'installeur au moment de l'installation (Cf chapitre 8.2 "Fichier de configuration du setup : vpnsetup.ini").

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

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

Activation dans le tunnel

Le logiciel Client VPN TheGreenBow implémente en standard (toutes versions) la fonction d'activation dans le tunnel : Dès lors que les options "`--autoactiv`" et "`--noactiv`" 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.

4.3 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_Client.exe /S --license=[numero_de_licence] --activmail=%ComputerName%@company.com
--noactiv=1 --autoactiv=1
```

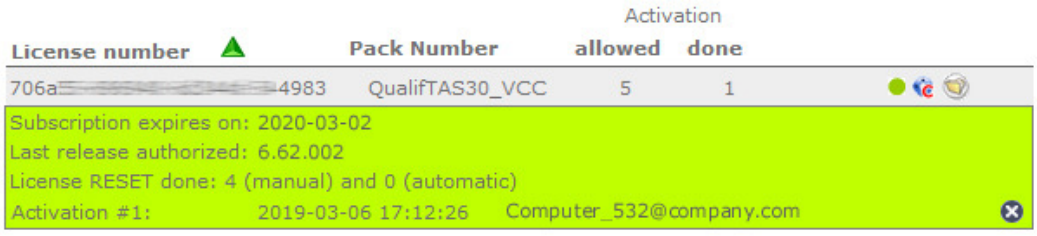
Batch PowerShell d'installation automatisée avec identifiant du poste activé :

```
TheGreenBow_VPN_Client.exe /S --license=[numero_licence]--activmail=$env:computername@company.com
--noactiv=1 --autoactiv=1
```

Autre exemple de script d'installation automatisée avec identifiant du poste activé :

```
set ActivationEmail=%ComputerName%@worldcompany.com
TheGreenBow_VPN_PREMIUM.exe /S --license=xxx --activmail=%ActivationEmail% --noactiv=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 : l'identifiant "`activmail`" doit toujours être formaté en respectant la syntaxe d'une adresse mail, c'est-à-dire qu'il doit toujours comporter les caractères "@" et "." (point). Si ce n'est pas le cas, l'activation échoue.

5 Paramétrage du Client VPN pour l'utilisateur

5.1 Introduction

Le Client VPN TheGreenBow présente à l'utilisateur trois interfaces principales :

1/ Le Panneau de Configuration : Cette interface est utilisée pour configurer la politique de sécurité VPN.
Elle permet toutes les opérations de gestion de la politique de sécurité VPN : création, modification, sauvegarde, exportation, importation.
2/ Le panneau des Connexions : Cette interface permet d'ouvrir et de fermer les tunnels, et d'informer l'utilisateur des éventuels incidents VPN.
3/ Le menu en barre des tâches : Certaines fonctions du logiciel sont accessibles depuis le menu associé à l'icône du logiciel en barre des tâches.

Le Panneau de Configuration donne accès à la politique de sécurité VPN : Il permet de modifier, de sauvegarder, d'importer, d'exporter et d'appliquer toute nouvelle politique de sécurité VPN.
Il est donc fortement recommandé de restreindre son accès, voire son affichage, à l'administrateur seul.

Le Panneau des Connexions ainsi que le menu en barre des tâches peuvent aussi être limités, pour ne présenter à l'utilisateur final qu'un jeu réduit d'opérations autorisées : Il est ainsi possible de configurer l'installation du Client VPN TheGreenBow pour que l'utilisateur final ne puisse qu'ouvrir et fermer un tunnel VPN, aucune autre fonction ne lui étant laissée accessible.

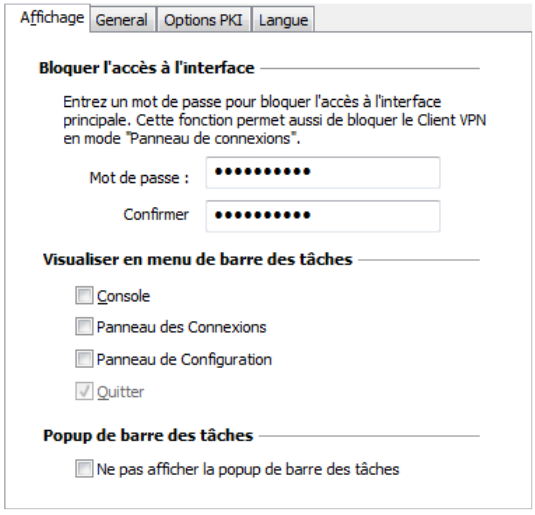
Ces limitations et restrictions d'accès peuvent toutes être configurées au cours de l'installation du logiciel. Les différentes options de configuration font l'objet du chapitre présent.

5.2 Restreindre l'interface par le panneau de configuration

Le Panneau de Configuration peut être masqué ou protégé par mot de passe, les items du menu en barre des tâches peuvent être limités. Ces limitations sont configurables via le Panneau de Configuration du logiciel, comme décrit dans le "Guide Utilisateur du Client VPN TheGreenBow" (référence : tgbvpn_ug_fr).

Exemple

1/ Dans le Panneau de Configuration ouvrir le menu "Outils > Options > Affichage", entrer et confirmer un mot de passe et décocher les items à masquer dans le menu en barre des tâches.
2/ Basculer sur le panneau des connexions (Ctrl + ENTER)
3/ Fermer éventuellement le panneau des connexions



Dans ce mode, le panneau de configuration n'est plus accessible depuis le menu en barre des tâches.
Depuis le panneau des connexions, l'accès au panneau de configuration est protégé par le mot de passe.
Plus aucune opération sur la politique de sécurité VPN n'est possible ni autorisée à l'utilisateur final.

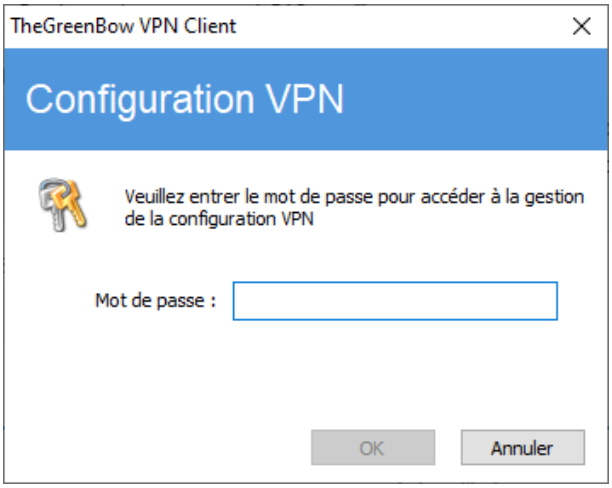
5.3 Restreindre l'interface à l'installation

L'interface utilisateur peut être restreinte grâce aux options d'installation suivantes :

L'option "`--guidefs=user`" ajoutée en ligne de commande du setup configure le logiciel pour ne s'ouvrir que sur le panneau des connexions.

L'option "`--password=[mot_de_passe]`" ajoutée en ligne de commande du setup spécifie à l'installation le mot de passe de protection d'accès au panneau de configuration.

```
TheGreenBow_VPN_Client.exe --guidefs=user --password=Adm1#34Vo
```



Dans cette configuration, l'utilisateur ne peut ouvrir que le Panneau des Connexions, et l'accès au Panneau de Configuration est protégé par mot de passe. Aucune opération sur la politique de sécurité VPN ne lui est autorisée.

Cette configuration est recommandée dans la mesure où elle sécurise complètement l'accès à la politique de sécurité VPN.

L'option "`--guidefs=hidden`" ajoutée en ligne de commande du setup empêche le logiciel d'ouvrir une quelconque interface : panneau des connexions ou panneau de configuration.
Dans cette configuration, l'utilisateur ne voit du logiciel que l'icône en barre des tâches.

Attention : dans les versions précédentes à la version 6.4, le menu accessible sur clic droit sur l'icône en barre des tâches faisait apparaître les connexions VPN. L'utilisateur avait donc la possibilité d'ouvrir/fermer une connexion VPN via ce menu. A partir de la version 6.4, les connexions VPN n'apparaissent plus dans ce menu, l'utilisateur ne peut donc pas ouvrir ou fermer un tunnel. Cette dernière fonction doit être réalisée par un script ou par un automatisme du type "ouvrir le tunnel automatiquement sur détection de trafic". Voir le guide utilisateur du Client VPN.

Mot de passe par défaut :

Dans la version "TheGreenBow VPN Certified", l'accès au panneau de configuration est systématiquement protégé par un mot de passe. Lorsqu'il n'est pas spécifié par l'administrateur (à l'installation ou par configuration), il vaut par défaut "admin". Cf. chapitre 8.1 "Options de ligne de commande de l'installeur du Client VPN"

6 Déploiement des politiques de sécurité VPN

6.1 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 TheGreenBow. 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 TheGreenBow) sans la protéger par mot de passe, et la renommer : "conf.tgb"
3/ Copier la politique de sécurité VPN dans le répertoire dans lequel se trouve le setup du Client VPN (fichier TheGreenBow_VPN_Client.exe)
4/ Transférer ce package (setup + politique de sécurité VPN) sur le poste à équiper
5/ Exécuter l'installation du Client VPN : A la fin de l'installation, le Client VPN est installé avec la politique de sécurité VPN importée et appliquée.

Du point de vue de la sécurité du déploiement, cette méthode exploite la fonction de contrôle d'intégrité des politiques de sécurité VPN (fonction standard du Client VPN). Cette fonction garantit que la politique de sécurité importée au moment de l'installation n'a pas été corrompue.
Pour un déploiement mettant aussi en œuvre la fonction de confidentialité de la politique de sécurité VPN, voir la procédure ci-dessous.

6.2 Déployer une nouvelle politique de sécurité VPN

6.2.1 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 TheGreenBow). 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, ouvrir (double-clic sur le fichier ".tgb") la politique de sécurité VPN : le mot de passe de protection est automatiquement demandé. Une fois le mot de passé correctement renseigné, la politique de sécurité VPN est importée et appliquée.

Remarque : Dans la version "TheGreenBow VPN Certified", l'ouverture directe d'un fichier ".tgb" n'est pas autorisée.
L'importation d'une nouvelle politique de sécurité reste néanmoins possible :
1/ via le menu "Configuration > Import" du Panneau de Configuration
2/ ou par 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 8)

6.3 Protéger une politique de sécurité VPN avant déploiement

Comme vu précédemment, le Client VPN vérifie en standard l'intégrité des politiques de sécurité importées et exportées. Il est de plus possible d'assurer leur confidentialité en spécifiant un mot de passe de protection au moment de l'exportation. Ce mot de passe est demandé à leur importation.

6.3.1 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 clé en registry. Cette fonction est activée par défaut dans la version TheGreenBow VPN Certified.

```
HKEY_LOCAL_MACHINE\SOFTWARE\TheGreenBow\TheGreenBow VPN\SignFile=1(binary)
```

6.3.2 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 TheGreenBow) en la protégeant par un mot de passe.
3/ Exécuter l'installation du Client VPN sur le poste cible
4/ Une fois le logiciel installé, transférer la politique de sécurité VPN sur le poste à installer
5/ Importer cette politique de sécurité VPN: soit par ouverture directe du fichier ".tgb", soit par ligne de commande (Cf. options `/import` et `/pwd` détaillées au chapitre 8) soit par le menu "Configuration > Import" du Panneau de Configuration : le mot de passe de protection est demandé.

Remarque : Dans la version "TheGreenBow VPN Certified", l'ouverture directe d'un fichier ".tgb" n'est pas autorisée.
L'importation d'une nouvelle politique de sécurité reste néanmoins possible :
1/ via le menu "Configuration > Import" du Panneau de Configuration
2/ ou par 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 8)

7 Automatisations du logiciel Client VPN

7.1 Batch/script pour ouvrir ou fermer un tunnel

Depuis la version 4.1, le logiciel Client VPN 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

Pour toutes les versions du logiciel Client VPN, 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 (p.ex.: "MonTunnel.tgb")
3/ Créer le script avec la ligne de commande suivante : vpnconf.exe /import:MyTunnel.tgb

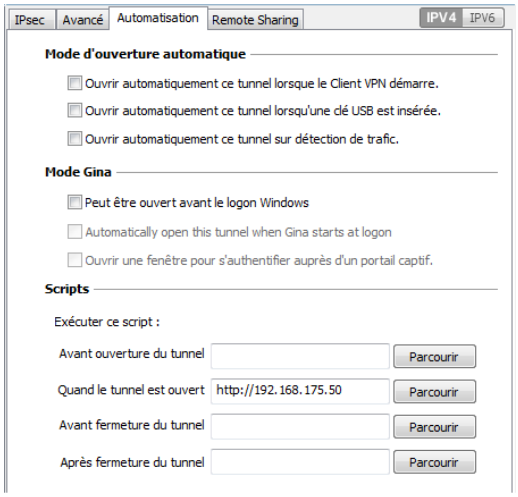
Ce script démarrera le logiciel Client VPN en important la politique de sécurité VPN (Configuration VPN) "MonTunnel.tgb", et ouvrira automatiquement le tunnel VPN.
Pour fermer le tunnel, il est possible d'utiliser la ligne de commande : vpnconf.exe /stop
Qui fermera le tunnel VPN ouvert, avant de quitter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

7.2 Ouvrir une page web à l'ouverture du tunnel

1/ Créer une politique de sécurité VPN (Confirguation 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.



7.3 Ouvrir un tunnel par double-clic sur un icône du bureau

Le Client VPN TheGreenBow permet d'ouvrir un tunnel VPN par double-clic sur un icône du bureau Windows.

7.3.1 Double-clic sur un fichier ".tgb"

1/ Créer une politique de sécurité VPN (Configuration VPN) avec l'option "Ouvrir automatiquement ce tunnel lorsque le Client VPN démarre" sélectionnée.
2/ Exporter cette Configuration VPN dans un fichier (p.ex.: "MonTunnel.tgb")
3/ Déplacer ce fichier, ou faire un raccourci sur ce fichier, sur le bureau Windows

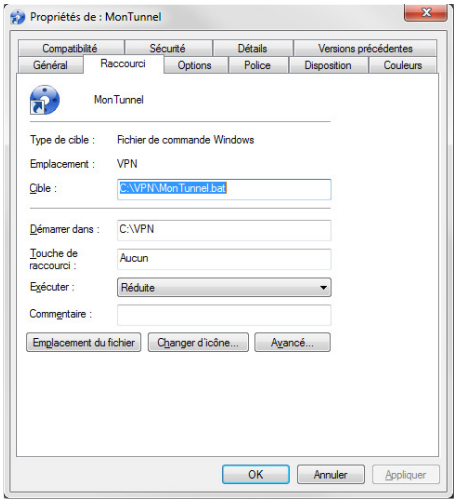
Un double-clic sur l'icône ainsi créé sur le bureau Windows ouvrira le logiciel Client VPN, qui importera automatiquement la Configuration VPN "MonTunnel.tgb" et ouvrira automatiquement le tunnel VPN.

Note : Pour des raisons de sécurité, cette fonction n'est pas proposée dans la version "TheGreenBow VPN Certified".

7.3.2 Script avec commande /open

1/ Dans la configuration VPN, créer le tunnel souhaité.
2/ Créer un fichier batch ("MonTunnel.bat" par exemple)qui contient la commande d'ouverture de ce tunnel :
"C:\Program Files (x86)\TheGreenBow\TheGreenBow VPN\vpnconf.exe" /open:nom_du_tunnel
3/ Créer un raccourci sur ce fichier batch sur le bureau
4/ Modifier ce raccourci en lui spécifiant la propriété Exécuter : "Réduite"
5/ Modifier éventuellement son icône et son nom.

Un double-clic sur l'icône ainsi créé sur le bureau Windows ouvre automatiquement le tunnel sélectionné.



7.4 Difference 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 demandent à l'utilisateur s'il veut "Ajouter ou remplacer" la nouvelle politique de sécurité VPN.
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" la remplace systématiquement.

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.

7.4.1 Protection de la politique de sécurité VPN

Lorsque l'accès au Panneau de Configuration (interface principale du logiciel) est protégé par mot de passe (appelé "mot de passe administrateur"), il est obligatoire d'ajouter ce mot de passe, en ligne de commande via l'option "/pwd", à toutes les commandes d'importation ou d'exportation : "/import", "/importonce", "/add", "/replace", "/export", "/exportonce".

Si le mot de passe administrateur n'est pas spécifié dans la ligne de commande, l'opération d'importation ou d'exportation est refusée.

L'option /pwd est aussi utilisée pour importer ou exporter une configuration protégée par mot de passe.
Cette fonction de sécurité implique donc que, lorsque l'accès au Panneau de Configuration est protégé par mot de passe, l'importation ou l'exportation d'une politique de sécurité chiffrée par mot de passe différent n'est pas possible en ligne de commande. Elle reste possible en utilisant les menus du Panneau de Configuration.

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.

7.5 Options d'exportation "/export", "/exportonce"

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.

7.5.1 Protection de la politique de sécurité VPN

Il est possible et recommandé de conditionner l'utilisation de cette option de ligne de commande à l'utilisation du mot de passe administrateur :

Lorsque l'accès au Panneau de Configuration (interface principale du logiciel) est protégé par mot de passe (appelé "mot de passe administrateur"), il est obligatoire d'ajouter ce mot de passe, en ligne de commande via l'option "/pwd", à toutes les commandes d'exportation : "/export", "/exportonce".

D'un point de vue sécurité, il est recommandé de privilégier l'option "/exportonce" à l'option "/export pour des opérations de maintenance, puisque le logiciel est quitté immédiatement après son exécution.

8 Manuel de référence

8.1 Options de ligne de commande de l'installeur du Client VPN

L'installeur (setup) du Client VPN TheGreenBow peut être configuré grâce à un jeu d'options de ligne de commande.

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 guillemets.

/S

Syntaxe :	/S ("S" en majuscule)
Usage :	Configure l'installation en mode silencieux (aucun question ni alerte à l'utilisateur)
Exemple :	TheGreenBow_VPN_Client.exe /S

/D

Syntaxe :	/D=[rep_install] ("D" en majuscule)
Usage :	[rep install] est le répertoire où le logiciel Client VPN doit être installé. [rep install] ne nécessite pas d'être encadré par des guillemets, même si le répertoire contient des espaces. Le répertoire doit être indiqué en entier. Cette option ne prend pas en compte les répertoires relatifs (du type "../../myrep"). Attention : Il est obligatoire que cette option soit la dernière de la ligne de commande.
Exemple :	TheGreenBow_VPN_Client.exe /S /D=C:\mon repertoire\vpn
Note :	Le répertoire d'installation par défaut du Client VPN est C:\Program Files\TheGreenBow\TheGreenBow VPN.

--license

Syntaxe :	--license=[numero_licence] ("license" est précédé de 2 tirets)
Usage :	Permet de configurer le numéro de licence utilisé pour l'activation du logiciel. (Cf. "Guide Utilisateur du Client VPN TheGreenBow" pour les caractéristiques de ce numéro de licence).
Exemple :	TheGreenBow_VPN_Client.exe --license=1234567890ABCDEF12345678

--activmail

Syntaxe :	--activmail=[activation_email] ("activmail" est précédé de 2 tirets)
Usage :	Permet de configurer l'adresse email utilisée pour l'activation du logiciel.
Exemple :	TheGreenBow_VPN_Client.exe --activmail=salesgroup@company.com
Note :	Ce champ peut être utilisé pour référencer une autre information qu'une adresse email (par exemple un identifiant du poste sur lequel le logiciel est activé, Cf. chapitre 4). Sa syntaxe doit néanmoins être toujours celle d'une adresse mail, c'est-à-dire toujours comporter les caractères "@" et "." (point). En version VPN PREMIUM, le champ "email d'activation" est rempli par défaut avec le "username" et le " hostname " du poste sur lequel le logiciel est installé (sous la forme "%*username*%%*hostname*%@company.com"). Ce mécanisme donne un moyen à l'administrateur qui gère

	une licence logicielle "master" d'identifier unitairement chaque poste activé. Cela lui permet de gérer les activations et désactivations logicielles de façon déterministe (Cf. chapitre 4).

--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), le paramètre "--autoactiv=1" permet de configurer le logiciel pour s'activer automatiquement.
Exemple :	TheGreenBow_VPN_Client.exe --autoactiv=1
Note:	L'option "--autoactiv" doit être la dernière de la ligne de commande.

--noactiv

Syntaxe :	--noactiv=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.
Exemple :	TheGreenBow_VPN_Client.exe --noactiv=1

--start

Syntaxe :	--start=[1|2] ("start" est précédé de 2 tirets)
Usage :	Permet de configurer le mode de démarrage du logiciel Client VPN : 1 : automatique après le logon Windows (en même temps que l'ouverture de la session Windows) 2 : manuellement (p.ex. par double-clic sur l'icône de l'application) Par défaut, le logiciel Client VPN démarre automatiquement à l'ouverture de la session Windows (mode 1)
Exemple :	TheGreenBow_VPN_Client.exe --start=2

--password

Syntaxe :	--password=[mot_de_passe] ("password" est précédé de 2 tirets)
Usage :	Permet de protéger par un mot de passe l'accès au Panneau de Configuration, et donc à la politique de sécurité VPN. Le mot de passe est demandé à l'ouverture du Panneau de configuration, depuis le menu en barre des tâches, ou depuis le Panneau des Connexions. Le mot de passe ne doit pas contenir d'espace. La longueur maximale du mot de passe est de 15 caractères. Note : Dans la version "TheGreenBow VPN Certified", l'accès au panneau de configuration est systématiquement protégé par un mot de passe. Lorsqu'il n'est pas spécifié à l'installation grâce à "--password", il vaut par défaut "admin".
Exemple :	TheGreenBow_VPN_Client.exe --password=adm253q

--guidefs

Syntaxe :	--guidefs=[user|hidden] ("guidefs" est précédé de 2 tirets)
Usage :	Permet de définir l'apparence du logiciel Client VPN lorsqu'il démarre. "user" : Restreint l'interface au panneau des connexions seul. "hidden" : Aucun panneau (ni connexion ni configuration) n'est accessible. Seul l'icône en barre des tâches est visible. L'utilisateur ne peut ouvrir ou fermer manuellement un tunnel (cette fonction doit être automatisée via un script ou via l'un des automatismes proposés par le Client VPN).
Exemple :	TheGreenBow_VPN_Client.exe --guidefs=hidden
Note :	Attention, l'option "--guidefs=user" doit obligatoirement être accompagnée de l'option "--password" qui permet de définir un mot de passe de protection de l'accès au Panneau de Configuration.

--menuitem

Syntaxe :	--menuitem=[0..31] ("menuitem" est précédé de 2 tirets)
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 :	TheGreenBow_VPN_Client.exe --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.
Note :	L'option `"--menuitem"` est prioritaire sur l'option `"--guidefs=hidden"`. L'option `"--guidefs=hidden "` réduit les items du menu en barre des tâches à "Quitter" et "Console". Mais du fait de cette priorité, les deux options `"--guidefs=hidden --menuitem=1"` auront pour effet de réduire le menu en barre des tâches à l'item "Quitter" uniquement.

--pkicheck

Syntaxe :	--pkicheck=1
Usage :	VPN Premium seul Cette option vaut 1 ou n'est pas configurée. Elle force le Client VPN à vérifier l'autorité de certification racine du certificat reçu de la gateway. La mise en œuvre de cette option est détaillée dans le document "Gestion des PKI, certificats, tokens et cartes à puce" disponible sur le site TheGreenBow.
Exemple :	TheGreenBow_VPN_Client.exe --pkicheck=1

--smartcardroaming

Syntaxe :	--smartcardroaming=1
Usage :	VPN Premium seul Cette option vaut 1, 2, 3, 4 ou 5. Elle permet de caractériser les tokens, lecteurs de cartes à puce et les certificats à utiliser pour ouvrir un tunnel VPN. Elle permet en particulier de déployer le Client VPN sur un parc de postes équipés de tokens ou de lecteurs de cartes à puce hétérogènes. La mise en œuvre de cette option est détaillée dans le document "Gestion des PKI, certificats, tokens et cartes à puce" disponible sur le site TheGreenBow

--lang

Syntaxe :	--lang=[language code]
Usage :	Cette option spécifie la langue d'installation et d'utilisation du logiciel Client VPN. Les langues disponibles sont indiquées ci-dessous.
Exemple :	TheGreenBow_VPN_Client.exe --lang=1040 installe le Client VPN en italien.

	ISO 639-2 code	Code	Langue	Nom français
1	EN	1033 (default)	English	Anglais
2	FR	1036	Français	Français
3	ES	1034	Español	Espagnol
4	PT	2070	Português	Portugais
5	DE	1031	Deutsch	Allemand
6	NL	1043	Nederlands	Hollandais
7	IT	1040	Italiano	Italien
8	ZH	2052	简化字	Chinois simplifié
9	SL	1060	Slovenscina	Slovène
10	TR	1055	Türkçe	Turc
11	PL	1045	Polski	Polonais
12	EL	1032	ελληνικά	Grec
13	RU	1049	Русский	Russe
14	JA	1041	日本語	Japonais
15	FI	1035	Suomi	Finois
16	SR	2074	српски језик	Serbe
17	TH	1054	ภาษาไทย	Thai
18	AR	1025	عـربي	Arabe
19	HI	1081	हिन्दी	Hindi
20	DK	1030	Danske	Danois
21	CZ	1029	Český	Tchèque
22	HU	1038	Magyar nyelv	Hongrois
23	NO	1044	Bokmål	Norvégien
24	FA	1065	ی‌فـارس	Persan
25	KO	1042	한국어	Coréen

8.2 Fichier de configuration du setup : vpnsetup.ini

Le fichier vpnsetup.ini permet de configurer l'installation du Client VPN TheGreenBow.

Il doit être situé dans le même répertoire que l'exécutable d'installation : TheGreenBow_VPN_Client.exe.
Le fichier vpnsetup.ini peut être édité avec un éditeur de texte classique (p.ex. notepad)

Fichier de type "ini", il est structuré en sections, et permet de définir les paramètres détaillés ci-dessous.

8.2.1 Section Activation

Dans cette section sont définis les paramètres qui permettent au logiciel de s'activer auprès d'un serveur d'activation TAS (TheGreenBow Activation Server).

OSAUrl

Syntaxe :	OSAUrl = *[url du serveur d'activation]*
Usage :	OSAUrl est l'adresse réseau du serveur d'activation utilisé pour activer les licences logicielles. L'url peut comporter une adresse IP ou un nom DNS. Le protocole ou le préfixe http:// n'a pas besoin d'être ajouté.

OSAPort

Syntaxe :	OSAPort = 80
Usage :	OSAPort est le port TCP utilisé pour l'échange d'activation entre le Client VPN et le serveur d'activation.

Cert

Syntaxe :	Cert = "*[certificat]*"
Usage :	Cert est le certificat utilisé pour l'activation. Il est fourni par TheGreenBow et ne doit pas être modifié.

8.2.2 Section PKIOptions

Dans cette section sont définis les paramètres PKI pour la gestion des tokens, lecteurs de cartes à puce et certificats.
Ces paramètres sont détaillés dans le document " tgbvpn_ug_pki_smartcard" : "Gestion des PKI, certificats, tokens et cartes à puce", chapitre 5.2.

8.2.3 Section AddRegKey

Dans cette section sont définis les paramètres généraux de fonctionnement.

NoSplitTunneling

Syntaxe :	NoSplitTunneling=01
Usage :	Ce paramètre provoque la désactivation de la route par défaut de l'interface physique (via le paramètre IgnoreDefaultRoute) quand le tunnel est monté. N'agit que sur les tunnels dont la configuration est "Tout le trafic dans le tunnel"

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".

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.

PinTimeOut

Syntaxe :	NoTimeOut=120
Usage :	Spécifie une valeur de timeout en secondes, qui permet de fermer automatiquement la boite de dialogue du PinCode quand le timeout échoit.

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).

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.

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.

8.2.4 Exemple de fichier vpnsetup.ini

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

[PKIOptions]
PkiCheck=01
SmartCardRoaming=01
NoCACertReq=01

[AddRegKey]
PinTimeOut=120
PwdUTF8=01
RoutingMode=01
```

8.3 Options de ligne de commande du logiciel Client VPN

Le Client VPN TheGreenBow 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

/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 ou si l'accès à l'interface de configuration (Panneau de Configuration) est protégée par un mot de passe, /import doit être accompagnée de l'option /pwd. Cf chapitre 7.4.1 et option "/pwd" 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 ou remplacer la configuration VPN importée. 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 : Si la configuration VPN importée est protégée par un mot de passe ou si l'accès à l'interface de configuration (Panneau de Configuration) est protégé par un mot de passe, /importonce doit être accompagnée de l'option /pwd. Cf chapitre 7.4.1 et option "/pwd" 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 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)

/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. Cf chapitre 7.4.1 et option "/pwd" ci-dessous.
Exemple :	vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" /pwd:gq1aRe7

Note : Si l'accès à l'interface de configuration (Panneau de Configuration) est protégé par un mot de passe, ce mot de passe doit obligatoirement être spécifié dans la ligne de commande via l'option /pwd. Cf chapitre 7.4.1 et option "/pwd" ci-dessous.

/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. Cf chapitre 7.4.1 et option "/pwd" ci-dessous.
Exemple :	vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb" /pwd:gg1

Note : Si l'accès à l'interface de configuration (Panneau de Configuration) est protégé par un mot de passe, ce mot de passe doit obligatoirement être spécifié dans la ligne de commande via l'option /pwd. Cf chapitre 7.4.1 et option "/pwd" ci-dessous.

/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 ou si l'accès à l'interface de configuration (Panneau de Configuration) est protégé par un mot de passe, /add doit être accompagnée de l'option /pwd. Cf chapitre 7.4.1 et option "/pwd" 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 ou si l'accès à l'interface de configuration (Panneau de Configuration) est protégé par un mot de passe, /replace doit être accompagnée de l'option /pwd. Cf chapitre 7.4.1 et option "/pwd" 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

Note : Lorsque l'accès au panneau de configuration est protégé par un mot de passe, ce mot de passe doit être spécifié pour toute opération d'importation/exportation. C'est aussi l'option "/pwd" qui est utilisée pour spécifier ce mot de passe. Ceci implique que lorsque le panneau de configuration est protégé par un mot de passe, il n'est pas possible d'importer une configuration protégée par un mot de passe différent. Cf chapitre 7.4.1 pour le détail des opérations possibles.

/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 fermé 2 : Le tunnel est 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 fermés Autres : Voir la liste des codes retours ci-dessous
Exemple :	vpnconf.exe /closeall

/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

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: Timeout d'exécution de la commande.
200 à 299: Timeout 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

9 Contact

9.1 Information

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

9.2 Commercial

Téléphone : +33.1.43.12.39.30
Email : sales@thegreenbow.com

9.3 Support

Plusieurs liens concernant le support sont disponibles sur le site TheGreenBow :

Support

http://www.thegreenbow.fr/support.html

Aide en ligne

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

FAQ

http://www.thegreenbow.fr/vpn_faq.html

Contact

Le support technique est disponible via les formulaires en ligne ou à l'adresse mail : support@thegreenbow.com

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software