TheGreenBow VPN Certified

Deployment Guide

Website : http://www.thegreenbow.com
Contact : support@thegreenbow.com

Table of Contents

1 Introduction

TheGreenBow VPN Client is a VPN Client software which can be used with all Windows OS.

TheGreenBow VPN Client is designed to be easily deployed and easily managed.
The software implements several functions which enable the IT manager or the network administrator to pre-configure the setup before deployment, install or update remotely the software or centrally manage the VPN Security Policies.

This document describes the management options and the configuration options of TheGreenBow VPN Client.
It also gives a set of examples for each option, in order to illustrate the way the software can be managed.

1.1 Installation and deployment method

TheGreenBow VPN Client is especially designed to enable installation and deployment from various media, and in varous matter:
1/ Silent mode installation
2/ Installation from a network drive
3/ Installation from a CD-ROM or from a removable drive (e.g. USB drive)

1.2 Installation options

Installation options are applied during the VPN Client installation process:

- License number
- VPN Client starting mode
- Software interface hidden mode
- PKI options management
- etc...

1.3 Setting options

Settings options are applied during the launch (sometimes the first launch) of the VPN Client:

- Import of a VPN Security Policy
- Start mode
- Tunnel opening
- etc...

All the options described in this document are available from TheGreenBow VPN Client version 4.2 and further.
For previous versions, please refer to the documents available on TheGreenBow website:
http://www.thegreenbow.com/vpn_doc.html

1.4 Documentation

This document refers to the following documentation, available on TheGreenBow website:

Intitulé	Référence
TheGreenBow VPN Client User Guide	tgbvpn_ug_en.pdf
PKI Deployment Guide	tgbvpn_ug_deployment_pki_en.pdf

2 Security considerations

2.1 Host configuration

The computer on which is running the TheGreenBow VPN Client software must be clean and correctly managed.
1/ It is running an anti-virus with an updated database
2/ It is protected with a firewall. This firewall is used to control and protect incoming and outgoing communications outside the VPN Tunnels,
3/ Its operating system is updated with the latest updates, patch or service pack
4/ It is configured to avoid local attacks (memory analysis, patch or binary corruption).

Several configuration recommendations, dedicated to the security improvement of a host machine, are available on the ANSSI website:

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

The administrator can also check the following Microsoft documentation if he does install the software on a Windows 7 platform:
Common Criteria Security Target, Windows 7 and Windows Server 2008 R2

2.2 Usage rights

TheGreenBow VPN Client requires “administrator” rights to be installed.
Then, it can be fully used with “user” rights, regardless of the platform used.

As some software operations are not allowed with “user” rights (e.g. software uninstallation), it is strongly recommended to deploy the software according to the following use of rights:
1/ Installation with "administrator" mode
2/ Software usage in “User” mode

2.3 End-user configuration

TheGreenBow VPN Client is designed to be used simultaneously and separately by an administrator (installation, initial configuration, personalization) and an end-user.

The User Interface can be configured to only show a restricted set of available options to the end-user (open/close a tunnel for example).

The software can also be configured, as soon it is installed or deployed, to restrict the access to the VPN Security Policy to the sole administrator.

The software configuration options described further in this document specifically allows to implement this partitioning, in order to implement the VPN client in the best possible safety and reliability.

2.4 Multi-users management

TheGreenBow VPN Client uses the same VPN Security Policy (VPN Configuration) for all users of a multi-users platform. Thus, it is recommended to install the software on a dedicated platform, with a single-user and optionally an administrator account as described previously.

2.5 VPN Security Policy Management

TheGreenBow VPN Client implements a set of command line options which enables import / export of new VPN Security Policies.

These options can be used by deployment scripts, remote maintenance updates, or various automatic mechanisms such as opening or closing automatically a tunnel.

This document describes the different ways to use the command line options, in order to not jeopardize the integrity or confidentiality of VPN Security Policies

2.6 User authentication

It is recommended to use certificate for VPN Tunnel configuration. It is recommended to store certificate on token or smartcard, in order to ensure a strong user authentication when the tunnel opens.

Configuration options concerning certificate usage and management are detailed in the administrator guide: “TheGreenBow VPN Client Deployment Guide PKI Options “ (tgbvpn_ug_deployment_pki_en.pdf).

2.7 Sensitive data protection

It is recommended to not store any sensitive data in the VPN Configuration file (VPN Security Policy) : login / password X-Auth, pre-shared key or certificate.
Specific precautions for sensitive data protection are described in the TheGreenBow VPN Client User Guide (tgbvpn_ug_en.pdf)

2.8 Reinitialization

Windows environment enables to uninstall then re-install the software.
During the uninstall process, the VPN Security Policy is removed. This procedure enables to reinitialize the software with its initial configuration.

3 VPN Client Software Deployment

VPN Client software deployment mainly uses the capability of the setup to be run "silently", which means without any questions to the user during installation.

To improve the transparency of the installation, the VPN Client Setup enables the use of command line options, which may be used to customize this installation. These command line options are fully detailed in the annexe, and are also described in the following various use cases.

3.1 "Silent" setup

A "silent" VPN Setup, also know as "silent" installation, is an installation which is processed automatically without any questions/inputs from the user. TheGreenBow VPN Client Setup is designed to be installed silently.

A silent installation uses a set of installation parameters which are provided via command line options, or via the initialization file "VpnSetup.ini" which may come together the setup.

Note: Depending on the security policy set on the target computer, a Windows notification may be displayed. Please contact our support to avoid this notification to be displayed.

3.1.1 How to create a "silent" VPN Client setup ?

TheGreenBow VPN Client setup is running in "silent" mode when the option "/S" is added to the command line of the setup program:

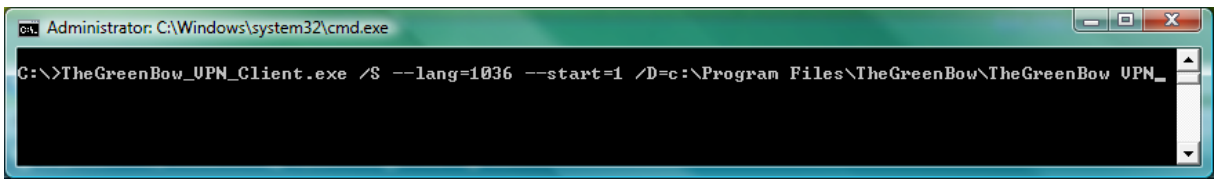
```
TheGreenBow_VPN_Client.exe /S (more options)
```

3.1.2 Example

Command line setup ran from a command window.
1/ Download TheGreenBow VPN Client froms http://www.thegreenbow.com/vpn
2/ Open a command window
3/ Enter the following command line:

```
[download_dir]\TheGreenBow_VPN_Client.exe /S --lang=1036 /D=[install_dir]
```

[download_dir] is the directory where TheGreenBow VPN Client is downloaded.
[rép_installation] is the directory where the software must be installed (this directory is by default: "C:\Program Files\TheGreenBow\TheGreenBow VPN")
The option "/D" must bé used at the end of the command line, without any space character between the option, the "=" character and the value.
The option "--lang" is detailed below.



Note: Refer to the chapter 7.1 for any detail about the options syntax rules.

3.2 How to deploy from a script

1/ Create a text file called "vpn_setup.bat"
2/ Edit this file (right-click and choose "Modify"")
3/ Enter the command line to be ran
4/ Deploy this batch file together with the setup TheGreenBow_VPN_Client.exe

Example:

```
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
```

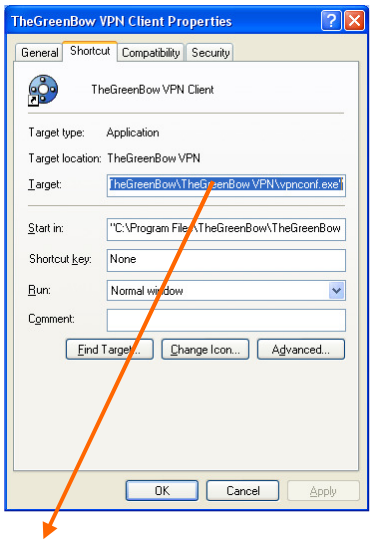
In this example:
- The setup directory is called "setup". It is located under the directory containing the batch file.
- This setup ends with the import of the security policy "myvpnconfig.tgb".

Note: Refer to chapter 7.1 for any detail about the options syntax rules.

3.3 How to deploy from a network drive or a shortcut

1/ Download TheGreenBow VPN Client froms http://www.thegreenbow.com/vpn
2/ Right-click on the "setup.exe" file in the setup directory
3/ select "Create Shortcut"
4/ Right-click on the new shortcut
5/ select "Properties"
6/ In the "**Target**" field of the "**Shortcut**" tab, add the install options to the command line. Make sure to keep spaces between each argument.
7/ Move the shortcut where it can be clicked by the end user (e.g. on the desktop)

Example:



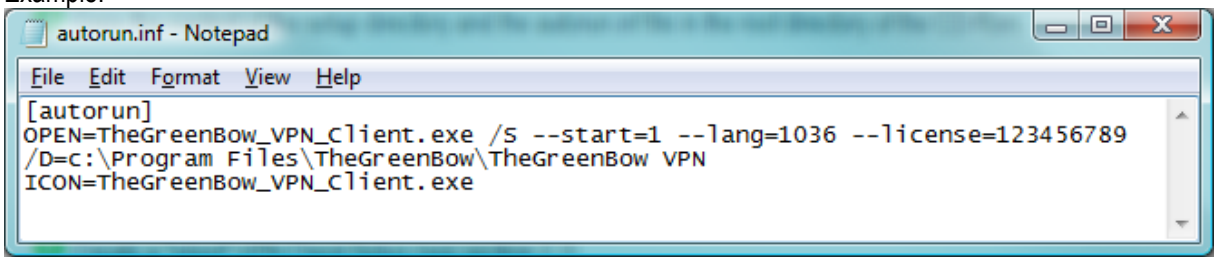

```
"F:\TheGreenBow_VPN_Client.exe /S --start=1 --lang=1036 /D=C:\Program
Files\TheGreenBow\TheGreenBow VPN"
```

3.4 How to deploy from a CD-ROM

1/ Create a file called "autorun.inf" with the following content:

```
[autorun]
OPEN=TheGreenBow_VPN_Client.exe /S /D=c:\Program Files\TheGreenBow\TheGreenBow VPN
(+ more options, Cf. chapitre 7.1)
ICON=TheGreenBow_VPN_Client.exe
```

Example:



2/ copy in the root directory of the CD-ROM
- the file "autorun.inf"
- the file "TheGreenBow_VPN_Client.exe"

Upon CD-Rom insertion, the setup will be run automatically silently.

Note: Refer to chapter 7.1 for any detail about the options syntax rules.

Note : See also 'Enabling and Disabling AutoRun' for some Windows versions (i.e. http://msdn.microsoft.com/en-us/library/windows/desktop/cc144204%28v=vs.85%29.aspx#floppy).

3.5 How to deploy a VPN Client Software Update

Deploying TheGreenBow VPN Client update runs exactly as the deployment of a new installation.

As part of a silent update, the entire process of updating is silent: backup of the VPN security policy of the previous version, install the new version, restore the VPN security policy of the former version.

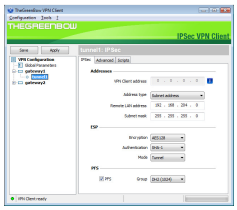
Restriction: Upgrade from any software release prior to TheGreenBow IPSec VPN Client 4.2: the un-installation can NOT be silent and the user will have to click on 'Accept un-installation' and 'Close' (without reboot) at the end of un-installation. The rest of upgrade installation will be silent.

4 VPN Client software customization for end-users

4.1 Software user interfaces

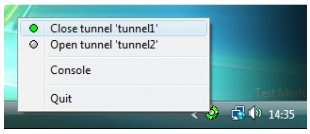
TheGreenBow VPN Client software may be used by end-users through three graphical user interfaces:

1/ Configuration Panel
This interface is used to configure the VPN security policy.
It allows all the VPN security policy management operations: creation, modification, save, export and import.
This interface can be hidden or protected by a password.



2/ The Connection Panel
This interface enables to open/close tunnels and to collect simple warning messages on VPN connection troubles. This interface can also be hidden

3/ The systray menu
This interface is used to open and close VPN tunnels. It is also used to open the other interfaces. The items of the systray menu may be hidden (the tunnels are always shown).



As the Configuration Panel enables to modify, save, import export and apply any new VPN security policy, it is strongly recommended its access is controlled (protected by a password) and reserved to the sole administrator.

The Connection Panel and the systray menu can also be limited, in order to restrict the interface for the end-user. Thus, it is possible to configure the setup of the VPN Client for the end-user only being allowed to open or close VPN tunnel.

Note: As the VPN Security Policy is signed and encrypted, any manual editing of the file disables the VPN Security Policy.

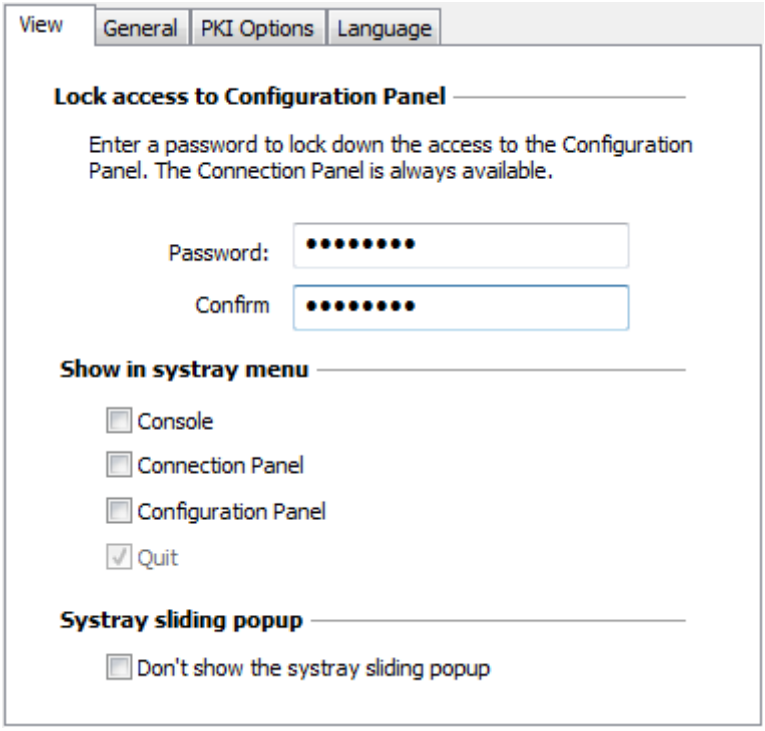
This section describes the VPN Client setup or VPN Client software options which enable to hide or limit the interface of the software.

4.2 End-user interface limitation

4.2.1 Via the Configuration Panel

The Configuration Panel may be hidden or protected by a password. The systray menu items may be limited. These limitations can be configured via the Configuration Panel, as described in the "TheGreenBow VPN Client User Guide" (Ref: tgbvpn_ug_en)

Example:
In the Configuration Panel, go to the menu "Tools > Options", select the tab "View"
Enter a password and confirm
Uncheck the option "Console", "Connection Panel" and "Configuration Panel"
Validate and close the software interface ("Close" button on the upper right corner)



From now on, the VPN Client can only be used:
1/ via the systray menu, which only allows to open/close the VPN Tunnels
2/ via a left-click on the systray icon which displays the password popup, required to access the Configuration Panel

In this mode, no operation is available on the VPN Security Policy for the end-user.

4.2.2 Via the install options

The install option "**`--guidefs=user`** " enable the VPN Client to start with the Connection Panel (rather than the Configuration Panel).

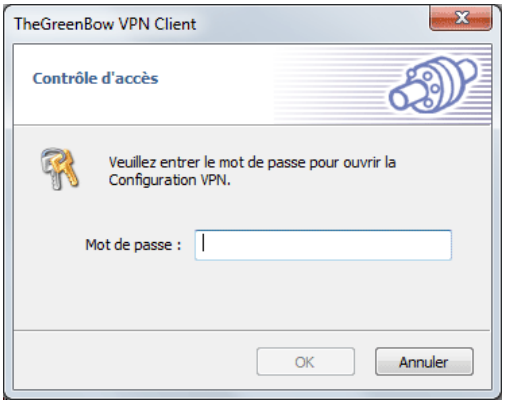
```
TheGreenBow_VPN_Client.exe --guidefs=user
```

The install option "**`--guidefs=hidden`** " enables the VPN Client to display no interface when it starts. The display is limited to the systray icon.

```
TheGreenBow_VPN_Client.exe --guidefs=hidden
```

The install option "**`--password=mypassword`** " enables to protect the Configuration Panel with a password.

```
TheGreenBow_VPN_Client.exe --guidefs=hidden --password=Adm1#
```



TheGreenBow IPSec VPN Client will start only showing the systray icon after the installation reboot, and the user won't be able to open the Configuration Panel, nor the Connection Panel, which are protected by the password. It will only be able to open/close VPN tunnels via the systray menu.

This Configuration is recommended as it securizes the access to the VPN Security Policy.

4.2.3 Via le paramétrage de la base de registre

Le Client VPN TheGreenBow offre, en standard, un mode dit "mode USB", qui permet de stocker une politique de sécurité sur clé USB, et de monter le tunnel VPN associé à cette politique automatiquement sur insertion de cette clé USB.
Ce mode peut être désactivé en positionnant la clé suivante en base de registre :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\TgbIke.exe
NoUSBMode = 1 (binary)
```

5 VPN Configuration Deployment

5.1 How to embed a specific VPN configuration into the VPN Client Setup

The VPN Client Setup enables the IT Manager to embed a pre-configured VPN Configuration. This VPN Configuration will be automatically used by the VPN Client during the installation process.

5.1.1 Procedure

1/ Create a VPN Configuration with TheGreenBow VPN Client. This step doesn't need to be done on the target computer and may be processed on any computer where the VPN Client software has been installed, from which the configuration is exported

2/ Export the VPN Configuration (menu "Configuration > Export") and rename your configuration into conf.tgb.

Important: The exported VPN Configuration must not be protected with a password

3/ Add the VPN Configuration (duly configured "conf.tgb" file) to the directory where you intend to put setup on the target computer (i.e. where software will be installed). In case you intend to deploy software on an USB drive, copy the VPN Configuration onto the USB drive together with the setup software

4/ Deploy the package to the user (the ".tgb" VPN Configuration is imported during the setup)

5/ Execute the setup: At the end of the installation, the VPN Client is installed with the VPN Security Policy imported and applied.

From the point of view of security deployment, this method uses the control of integrity of VPN security policies (standard feature of the VPN Client). This feature ensures that the imported security policy at the time of installation has not been corrupted.

5.2 How to deploy a new VPN Configuration

5.2.1 Procedure

1/ Create a VPN Configuration with TheGreenBow VPN Client. This step doesn't need to be done on the target computer

2/ Export the VPN Configuration (menu "Configuration > Export"). The exported VPN configuration may be protected with a password.

3/ Give the VPN Configuration to the end-user, either by email, or through file-sharing

4/ When the user opens the VPN Configuration (e.g. he opens the email attachment), he will be automatically asked for the password, and as the password is correctly entered, the VPN Configuration will be automatically imported and applied by TheGreenBow VPN Client.

Note: Opening a "tgb" file with a double-click on the file is not allowed with the "VPN Client Certified 2013". Nevertheless, it is possible to import a new VPN Security Policy:
- via the Configuration Panel menu: "Configuration > Import",
- or via the command line option "/import", together with the password used for the protection of the exported configuration, when it's required. (Cf. options /import and /pwd detailed in chapter **Erreur ! Source du renvoi introuvable.**)

5.3 How to protect a VPN Configuration before deployment

A VPN Security Policy can be exported from TheGreenBow VPN Client in order to be deployed to all end-users in the company.
1/ Select the menu "Configuration > Export".
2/ Select "Protect the exported VPN Configuration" and enter a password, then click on "Ok".

The exported VPN Configuration is encrypted. When the user will open it, he will be automatically asked for the password.

5.3.1 Integrity of an exported VPN Security Policy

The automatic integrity protection of a VPN Security Policy can be activated through a registry key:

- Windows XP :
  `HKEY_LOCAL_MACHINE\SOFTWARE\TheGreenBow\TheGreenBow VPN\SignFile = 1 (binary)`
- Windows x64 :
  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TheGreenBow\TheGreenBow VPN\SignFile = 1 (binary)`

5.3.2 Procedure

1/ Create the VPN Security Policy (VPN Configuration) for the target host machine

2/ Export this VPN Security Policy (menu "Configuration > Export", Cf. TheGreenBow VPN Client User Guide) with a password protection.

3/ Install the VPN Client on the host machine

4/ Once the software is installed, move the VPN Security Policy on the host machine to be equipped.

5/ Import the VPN Security Policy (either with the command line or with the Configuration Panel menu "Configuration > Import"). The protection password is asked.

Note: Opening a "tgb" file with a double-click on the file is not allowed with the "VPN Client Certified 2013". Nevertheless, it is possible to import a new VPN Security Policy:
- via the Configuration Panel menu: "Configuration > Import",
- or via the command line option "/import", together with the password used for the protection of the exported configuration, when it's required. (Cf. options /import and /pwd detailed in chapter **Erreur ! Source du renvoi introuvable.**)

6 VPN Automations

6.1 How to create a batch/script that automatically opens or closes a tunnel

From software release 4.1 and further, your batch/script can use a simple command line as followed:

```
vpnconf.exe /open:[NomPhase1-NomPhase2]
vpnconf.exe /close:[NomPhase1-NomPhase2]
```

Before software release 4.1 (included), process as follows:

1/ Create a VPN Security Policy with "Open automatically when Client starts" selected for the relevant Phase 2 (Advanced Phase2 dialog).

2/ Export the VPN Configuration in a file (e.g. "MyTunnel.tgb")

3/ Add to your script the following command line: `vpnconf.exe /import:MyTunnel.tgb`

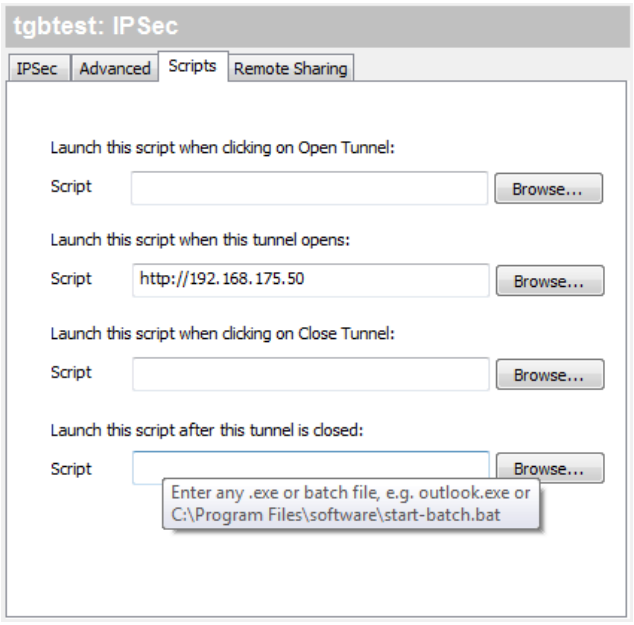
This script will start the VPN Client software with "MyTunnel" VPN Configuration, and will automatically open the tunnel.
To close a tunnel, the command line is: `vpnconf.exe /stop`
This command line will quit the VPN Client while closing all the opened tunnels.

6.2 How to automatically open a web page when the VPN tunnel opens

1/ Create a VPN Security Policy (VPN Configuration)

2/ Open the "Scripts" tab of the relevant VPN tunnel

3/ Enter the url of the web page to open (internet web page or intranet portal) in the field: "Launch this script when this tunnel opens:"



4/ Save the configuration and open the tunnel: the web page is automatically opened as soon as the tunnel is open.

6.3 How to open a tunnel with a double-clic on a desktop icon

It is possible to open a tunnel with a double-clic on a desktop icon. This icon has just to be associated with a VPN Configuration.

1/ Create a VPN Security Policy with "Open automatically when Client starts" selected for the relevant Phase 2 (Advanced Phase2 dialog).

2/ Export the VPN Configuration in a file (e.g. "MyTunnel.tgb"),

3/ Copy, move or shortcut this file on the desktop

A double-click (open) on the desktop icon will run the VPN Client software with the VPN Configuration "MyTunnel", which will automatically open the tunnel.

Note: This function is not allowed with the "VPN Client Certified 2013" version.

6.4 Options "/import", "/importonce", "/add" et "/replace"

The option `"/import"` enables to import a VPN Configuration and start the VPN Client software if it is not already running.

The option `"/importonce"` enables to import a VPN Configuration without starting the VPN Client.

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

When the current VPN security policy (before import) of VPN Client is not empty, these two options require the user if he wants to `"Add or replace"` the new VPN security policy.
Options `"/add"` and `"/replace"` can avoid to ask the user. The option `"/add"` adds the VPN security policy, the `"/replace"` replaces the VPN security polic.

Option	Ask the user "Add or replace"	Starts the VPN Client if it's not already started
/import	Yes	Yes
/importonce	Yes	No
/add	No: Add the VPN Security Policy	No
/replace	No: Replace the VPN Security Policy	No

Note: When the VPN security policy is empty, the options `"/import"` and `"/importonce"` do not request anything from the user and "add" the VPN security policy.

6.4.1 Protection of VPN Security Policy

These options can be combined with the administrator password:

When access to the Configuration Panel is protected by password (called "administrator password"), it is mandatory to add this password on the command line using the `"/pwd"` to all commands `"/import"`, `"/importonce"`, `"/add"`, `"/replace "`, `"/export"`, `"/exportonce"`.

If the password "admin" is not specified in the command line, the import or export is denied.

Note: This security feature implies that when access to the Configuration Panel is protected by a password, the import or export of a security policy encrypted by password is not possible via command line. It is possible by using the menus in the Configuration Panel.

From a security point of view, it is recommended to prefer the options "/importonce", "/add" et "/replace" for maintenance operation (versus the "/import" option) as the software is quitted immediately after their execution.

6.5 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.

6.5.1 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 protégée 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.

7 Reference Manual

7.1 VPN Client Setup command line options

A set of command line options are available to customize the VPN Client setup.

Syntax rules

1/ Command-line options that require a parameter must be specified with no space between the option and its parameter.

2/ Quotation marks around an option's parameter are required only if the parameter contains spaces

7.1.1 /S

Syntax: `/S` (S must be uppercase and preceded by only one slash)
Usage: Enables a silent installation (no dialog are displayed to the user during the installation)
Example: `TheGreenBow_VPN_Client.exe /S`

7.1.2 /D

Syntax: `/D=[rep install]` (D must be uppercase and preceded by only one slash)
Usage: `[rep install]` is the path where to install the software.
Example: `TheGreenBow_VPN_Client.exe /S /D=C:\mon repertoire\vpn`

Attention : [rep install] No quotation marks is required even if space in the path when this option is located at the end of the command line.

Note : The path should be full as relative path does not work (e.g. "../../myrep")

By default, the install directory of the software is: "C:\Program Files\TheGreenBow\TheGreenBow VPN".

7.1.3 --license

Syntax: `--license=[license_number]` ("license" must be preceded by 2 dashes)
Usage: Enables to configure the license number. The license number can be a set of 24 or 20 hexadecimal characters, depending of the software release.
Example: `TheGreenBow_VPN_Client.exe --license=1234567890ABCDEF12345678`

7.1.4 --activmail

Syntax: `--activmail=[activation_email]` ("activmail" must be preceded by 2 dashes)
Usage: Enables to force the email used for activation confirmation. During the activation process, the edit box used for entering this email will be disabled.
Example: `TheGreenBow_VPN_Client.exe --activmail=sales@company.com`

7.1.5 --autoactiv

Syntax: `--autoactiv=1` ("autoactiv" must be preceded by 2 dashes)
Usage: In case of software upgrade (i.e. license number and activation email have already been entered in previous installation) and --autoactiv=1 option is added, the software will try to activate software

automatically when starting if network is available or when requesting to open a tunnel if network was not available at startup.

Example: `TheGreenBow_VPN_Client.exe --autoactiv=1`

Note: The option `--autoactiv` must be the last option in the command line.

7.1.6 --noactiv

Syntax: `--noactiv=1` ("noactiv" must be preceded by 2 dashes)

Usage: Disable the "Activation window" displayed when the software starts.
This option is typically associated to the option: "`--autoactiv=1`"

Example: `TheGreenBow_VPN_Client.exe --noactiv=1 --autoactiv=1`

7.1.7 --start

Syntax: `--start=[1|2]` ("start" must be preceded by 2 dashes)

Usage: Enables to configure the start mode for the VPN Client: after the logon windows [1], or manually [2]. Default is [1].

Example: `TheGreenBow_VPN_Client.exe --start=2`

7.1.8 --reboot

Syntax: `--reboot=1` ("reboot" must be preceded by 2 dashes)

Usage: Allows to reboot automatically after a silent installation. Default is [1]..
When this option is not specified, a silent install doesn't end with a reboot.
Note: This option is typically dedicated to Windows XP OS which require a reboot after this installation. It is not required for Windows Vista, Windows 7 and further OS.

Example: `TheGreenBow_VPN_Client.exe --reboot=1`

7.1.9 --password

Syntax: `--password=[password]` ("password" must be preceded by 2 dashes)

Usage: Enables to control the access to the VPN Client Configuration Panel with a password. Thus, this option enables the protection of the VPN Security Policy. The user will be asked for the password when he clicks or double-clicks on the VPN systray icon, or when he wants to switch from the Connection Panel to the Configuration Panel.

Example: `TheGreenBow_VPN_Client.exe --password=adm253q`

7.1.10 --guidefs

Syntax: `--guidefs=[full|user|hidden]` ("guidefs" must be preceded by 2 dashes)

Usage: Enables to define the GUI appearance when the VPN Client software starts.
"`full`" : The Configuration Panel is displayed
"`user`" : The Connection Panel is displayed
"`hidden`" : ": The Configuration Panel and Connection Panel cannot be displayed, the systray menu is limited to the tunnels and the items "Quit" and "Console".
By default, the Configuration Panel is displayed.

Example: `TheGreenBow_VPN_Client.exe --guidefs=hidden`

7.1.11 --menuitem

Syntax: `--menuitem=[0..31]` ("menuitem" must be preceded by 2 dashes)
Usage: Enables to configure the items of the systray menu. The value is a bitfield, where each bit defines a menuitem:
1 (1st bit) = Quit,
2 (2nd bit) = Connection Panel,
4 (3rd bit) = Console,
8 (4th bit) = Save and Apply (*obsolee from version 5*)
16 (5th bit) = Configuration Panel
Default is 31 (1F): All menus are displayed.
Example: `"TheGreenBow_VPN_Client.exe --menuitem=3"` affichera seulement les items "Quitter" et "Panneau des Connexions".

Note 1: The tunnels are always shown in the systray menu, and can always be opened and closed from this systray menu.

Note 2: `"--menuitem"` might override `"--guidefs=hidden"`.
By default, `"--guidefs=hidden"` set the systray menu to Quit + Console. (The items Save & Apply and Connection Panel are not visible). But `"--menuitem"` overrides `"--guidefs"`. That means the following options: `"--guidefs=hidden --menuitem=1"` will set a systray menu with only the "Quit" item.

7.1.12 --pkicheck

See the " PKI Deployment Guide" (tgbvpn_ug_deployment_pki_en.pdf)

7.1.13 -- smartcardroaming

See the " PKI Deployment Guide" (tgbvpn_ug_deployment_pki_en.pdf)

7.1.14 --lang

Syntax: `--lang=[language code]` ("lang" must be preceded by 2 dashes)
Usage: This option specifies the language for the TheGreenBow IPSec VPN Client software and installation software. Available languages are listed below.
Example: `TheGreenBow_VPN_Client.exe --lang=1040` will start software in Italian.

Code	Langue	Nom français	Code ISO 639-2
1033 (default)	English	English	EN
1036	Français	French	FR
1034	Español	Spanish	ES
2070	Português	Portuguese	PT
1031	Deutsch	German	DE
1043	Nederlands	Dutch	NL
1040	Italiano	Italian	IT
2052	简化字	Chinese simplified	ZH
1060	Slovenscina	Slovenian	SL
1055	Türkçe	Turkish	TR
1045	Polski	Polish	PL
1032	ελληνικά	Greek	EL

1049	Русский	Russian	RU
1041	日本語	Japanese	JA
1035	Suomi	Finnish	FI
2074	српски језик	Serbian	SR
1054	ภาษาไทย	Thai	TH
1025	عـربي	Arabic	AR
1081	हिन्दी	Hindi	HI
1030	Danske	Danish	DK
1029	Český	Czech	CZ
1038	Magyar nyelv	Hungarian	HU
1044	Bokmål	Norwegian	NO
1065	ىفـارس	Farsi	FA
1042	한국어	Corean	KO

7.2 VPN Client software command line options

TheGreenBow IPSec VPN Client enables to run command line options, used to open/close a tunnel, import a new VPN Configuration, etc... A command line can be used in batch files, in scripts or in setup "inf" files as detailed in previous chapters.

The syntax of a command line option is always the same:

```
[dir]\vpnconf.exe [/option[:value]]
```

"dir" is the directory where the file "vpnconf.exe" is located, typically the installation directory.

If "value" contains space characters, it must be enclosed in double quotes.

7.2.1 /import

Syntax: `/import:[ConfigFileName]`

Usage: Enables the VPN Client to import a VPN Security Policy. If the VPN Client software is not running, it is automatically started by this option. Thus, this option may be used to start the VPN Client with a given VPN Security Policy.
If the VPN Client software is running, this option imports and updates the VPN Security Policy without stopping the software

[ConfigFileName] is the full path of the file to be imported. It must be enclosed in double-quotes if it contains space characters.

"/import" can be used with "/pwd" to import a VPN Security Policy which is protected with a password (see "/pwd" below and chapter **Erreur ! Source du renvoi introuvable.** for details about protection of the VPN Security Policy)

See chapter 6.4 for differences between "/import", "/importonce", "/add" and "/replace"

Example:
```
vpnconf.exe /import:"c:\my documents\myvpnconf.tgb"
vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd:gq1a
```

7.2.2 /importonce

Syntax: `/importonce:[ConfigFileName]`

Usage: Enables the VPN Client to import a VPN Security Policy. If the VPN Client software is not running, it won't be started by this option. Thus, this option may be used to import a given VPN Security Policy without starting the VPN Client, for example within an installation script.
If the VPN Client software is running, this option imports and updates the VPN Security Policy without stopping the software.

[ConfigFileName] is the full path of the file to be imported. It must be enclosed in double-quotes if it contains space characters.

"/importonce" can be used with "/pwd" to import a VPN Security Policy which is protected with a password (see "/pwd" below and chapter **Erreur ! Source du renvoi introuvable.** for details about protection of the VPN Security Policy)

See chapter 6.4 for differences between "/import", "/importonce", "/add" and "/replace"

Example:
```
vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb"
vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb" /pwd:gq1a
```

7.2.3 /add

Syntax: `/add:[ConfigFileName]`

Usage: Enables to add a VPN Security Policy to the current configuration. This feature is available in software release 4.1 and further, and may be used instead of the /importonce option.

[ConfigFileName] is the full path of the file to be added. It must be enclosed in double-quotes if it contains space characters.

"/add" can be used with "/pwd" to add a VPN Security Policy which is protected with a password (see "/pwd" below and chapter **Erreur ! Source du renvoi introuvable.** for details about protection of the VPN Security Policy)

See chapter 6.4 for differences between "/import", "/importonce", "/add" and "/replace"

Example:
```
vpnconf.exe /add:"c:\my documents\myvpnconf.tgb"
vpnconf.exe /add:"c:\my documents\myvpnconf.tgb" /pwd:gq1a
```

7.2.4 /replace

Syntax: `/replace:[ConfigFileName]`

Usage: Enables to replace the current configuration by a new VPN Security Policy. This feature is available in software release 4.1 and further, and may be used instead of the /importonce option.

[ConfigFileName] is the full path of the file to be replaced. It must be enclosed in double-quotes if it contains space characters.

"/replace" can be used with "/pwd" to replace a VPN Security Policy which is protected with a password (see "/pwd" below and chapter **Erreur ! Source du renvoi introuvable.** for details about protection of the VPN Security Policy)

See chapter 6.4 for differences between "/import", "/importonce", "/add" and "/replace"

Example:
```
vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb"
```

```
vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb" /pwd:gq1a
```

7.2.5 /export

Syntax: `/export:[ConfigFileName]`

Usage: Enables the VPN Client to export a VPN Security Policy. If the VPN Client software is not running, it is automatically started by this option.
If the VPN Client software is running, this option exports the VPN Security Policy without stopping the software.

[ConfigFileName] is the full path of the file to be exported. It must be enclosed in double-quotes if it contains space characters.

"/export" can be used with "/pwd" to export a VPN Security Policy protected with a password (see "/pwd" below and chapter 6.5.1 for details about protection of the VPN Security Policy)

See below the difference with "/exportonce"

Example:
```
vpnconf.exe /export:"c:\my documents\myvpnconf.tgb"
vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" /pwd:gq1a
```

7.2.6 /exportonce

Syntax: `/exportonce:[ConfigFileName]`

Usage: Enables the VPN Client to export a VPN Security Policy. If the VPN Client software is not running, it won't be started by this option.
If the VPN Client software is running, this option exports the VPN Security Policy without stopping the software

[ConfigFileName] is the full path of the file to be exported. It must be enclosed in double-quotes if it contains space characters.

"/export" can be used with "/pwd" to export a VPN Security Policy protected with a password (see "/pwd" below and chapter 6.5.1 for details about protection of the VPN Security Policy)

See above the difference with "/export"

Example:
```
vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb"
vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb" /pwd:gq1a
```

7.2.7 /pwd

Syntax: `/pwd:[Password]`

Usage: Enables to set a password for import or export operations. This option can be used together with the /import, /importonce, /export, /exportonce, /add and /replace options.
In the command line, it always must be placed after those options.

See chapter **Erreur ! Source du renvoi introuvable.** for the protection of a VPN Security Policy..

Example:
```
vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd:gq1a
```

7.2.8 /stop

Syntax: `/stop`
Usage: Enables to close the opened VPN tunnels and to exit the VPN Client.
Example: `vpnconf.exe /stop`

7.2.9 /open

Syntax: `/open:[Phase1Name-Phase2Name]`
Usage: Enables to open a VPN tunnel.
Example: `vpnconf.exe /open:Corporate-gateway1`

7.2.10 /close

Syntax: `/close:[Phase1Name-Phase2Name]`
Usage: Enables to close a VPN tunnel.
Example: `vpnconf.exe /close:"Home gateway-cnx1"` (double quotes are required as the tunnel name contains a space character).

8 Support

Information and update are available at: http://www.thegreenbow.com

Technical support via email at: support@thegreenbow.com
Or on the website: http://www.thegreenbow.com/support.html

Sales via email at: sales@thegreenbow.com

Secure, Strong, Simple.

TheGreenBow Security Software