

TheGreenBow  
VPN Client

Deployment Guide

## Table of Contents

|     |   |    |
|-----|---|----|
| 1   | Introduction.....   | 3  |
| 1.1 | Deployment and management facilities.....                         | 3  |
| 1.2 | Deployment tools .....  | 3  |
| 1.3 | VPN Standard and VPN Premium .....                                | 3  |
| 1.4 | Older version .....   | 3  |
| 2   | Security recommendations .....                                    | 4  |
| 2.1 | User right .....  | 4  |
| 2.2 | Configuration for the end-user .....                              | 4  |
| 2.3 | User authentication .....   | 4  |
| 3   | VPN Client Software Deployment .....                              | 5  |
| 3.1 | "Silent" setup .....  | 5  |
| 3.2 | How to create a "silent" VPN Client Setup? .....                  | 5  |
| 3.3 | Deploy a VPN Client Setup from an USB Drive or CD-Rom.....        | 6  |
| 3.4 | Run a VPN Client Setup from a shortcut or a network drive.....    | 6  |
| 3.5 | Deploy a VPN Client Setup using Batch script .....                | 7  |
| 3.6 | Deploy a VPN Client Software Update.....                          | 7  |
| 4   | VPN Client software customized for end-users.....                 | 8  |
| 4.1 | Introduction .....  | 8  |
| 4.2 | Limit VPN Client usage to Connection Panel .....                  | 8  |
| 4.3 | Limit VPN Client usage from the setup.....                        | 9  |
| 5   | VPN Configuration deployment .....                                | 10 |
| 5.1 | Embed a specific VPN Configuration into the VPN Client setup..... | 10 |
| 5.2 | Protect and deploy a new VPN Configuration .....                  | 10 |
| 5.3 | Protect a VPN security policy before it is deployed .....         | 10 |
| 6   | VPN automations.....  | 12 |
| 6.1 | Batch/script to open or close a tunnel .....                      | 12 |
| 6.2 | Automatically open a web page when tunnel opens .....             | 12 |
| 6.3 | Open a tunnel with a double-click on a desktop icon .....         | 13 |
| 6.4 | Difference between "import", "importance", "add", "replace" ..... | 13 |
| 7   | Reference Manual .....  | 15 |
| 7.1 | VPN Client Setup command line options.....                        | 15 |
| 7.2 | VPN Client Software command line options .....                    | 19 |
| 8   | Contact .....   | 24 |
| 8.1 | Information.....  | 24 |
| 8.2 | Sales .....   | 24 |
| 8.3 | Support .....   | 24 |

# 1 Introduction

## 1.1 Deployment and management facilities

TheGreenBow VPN Client software is designed to be easily deployed and managed. It implements several functionalities which enable the IT Manager to pre-configure the setup before deployment, to remotely install or upgrade the software, and to centrally manage VPN Configurations.

This document describes the management and configuration options of TheGreenBow VPN Client. It especially describes a set of use cases which illustrate the way to manage the software. These use cases are described in "How to" items, summarized below.

Various options can be configured during the installation process of TheGreenBow VPN Client:

- Software activation options: license number, activation email, hidden activation, etc.
- Graphical properties: hidden user interface, menus or functions customization, etc.
- PKI integration options: certificate or storage media characterisation, etc.
- VPN Security Policy to be deployed
- Setup properties: hidden installation, etc.
- Etc.

Additional options can be used with the software itself, for example, once the installation is completed:

- VPN Configuration management: import, export, signature, etc.
- Software management: start, stop, etc.
- VPN Tunnel management: open, close, status
- Etc.

## 1.2 Deployment tools

This document also describes the different way to deploy the VPN Client installation package:

- Network drive: users can download and install the VPN Client with a double-click on an icon
- CD-ROM/DVD: users have just to insert the media and the VPN Client installation will run automatically
- USB Drive: IT manager can carry the installation package on an USB drive, insert the USB drive into user laptop and the VPN Client will run automatically

## 1.3 VPN Standard and VPN Premium

The deployment and management features described in this document are all available with the PREMIUM VPN Client, but only a part of them are available with the (standard) VPN Client. The reference "Premium VPN only" is specified whenever the function is not available in the standard version.

## 1.4 Older version

**Note:** All features described in this document are applicable to TheGreenBow VPN Client 4.2 and further. For previous software release, look on our website for a previous version of this document.

## 2 Security recommendations

### 2.1 User right

TheGreenBow VPN Client is designed to be installed with the "Administrator" rights and then be used with struct "User" rights, whatever the Windows platform used.

Some operations are prohibited in "User" mode (e.g. uninstalling the software). It is strongly recommended that you deploy the software according to the use of rights:

- 1/ Installation in "Administrator" mode
- 2/ Use in "User" mode

### 2.2 Configuration for the end-user

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

All software graphical interface can be set to restrict the end user with a limited number of available operations (open or close a VPN tunnel).

Similarly, the software can be fully configured upon installation or deployment to allow VPN security policies access to the administrator only (masking functions, password access control, etc ...)

The configuration options of the software described in this document provide details about the way to do it.

### 2.3 User authentication

As detailed in TheGreenBow VPN Client User's Guide (tgbvpn\_ug\_en.pdf), it is recommended to use certificate possibly stored on token or smart card, to ensure strong user authentication when opening the VPN tunnel.

TheGreenBow VPN Client also implements a set of PKI and certificate management options, which are described in the "Deployment Guide - PKI Options" available on TheGreenBow website (documentation tab of the VPN Client product description or on the url: [http://www.thegreenbow.com/vpn\\_token.html](http://www.thegreenbow.com/vpn_token.html)). These options are available for the VPN Premium only.

## 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 known 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.

The following chapters describe the way to configure the installation configuration file and the meaning of each available command line options.

### 3.2 How to create a "silent" VPN Client Setup?

Download TheGreenBow\_VPN\_Client.exe setup from <http://www.thegreenbow.com>

To create a silent installation, open a command window, then enter the following command line:

**Syntax:** [software path]setup.exe /S --license=123456789 /D=[install path] (+  
command line options, see section "[setup command line options](#)")

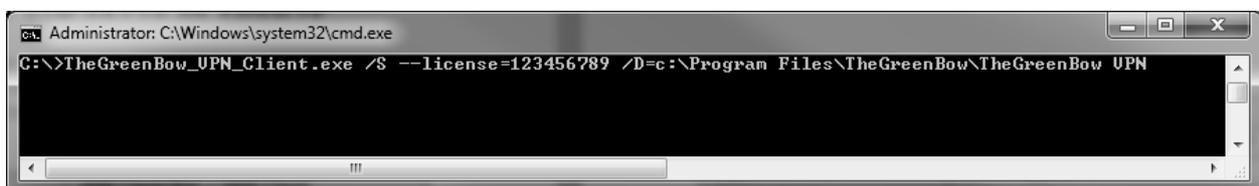
**Where:**

[software path] is the path to the setup software.

[install path] is the path to the directory where the software must be installed.

**Usage:** Enables a silent installation: no dialog is displayed to the user during the installation.

**Example:** C:\Users\bob\Downloads\TheGreenBow\_VPN\_Client.exe /S --license=123456789  
/D=c:\Program Files\TheGreenBow\TheGreenBow VPN



**Note:** The directory specified after the /D switch must be specified entirely. This switch doesn't recognize a relative directory. The /D switch MUST be the last switch in the command line.

**Note:** Command-line options that require a parameter must be specified with no space between the option and its parameter. Quotation marks around an option's parameter are required only if the parameter contains spaces, except for [install path] which do not need quote if there are spaces in the path.

### 3.3 Deploy a VPN Client Setup from an USB Drive or CD-Rom

Create a "silent" VPN Client Setup (see section 3.2)

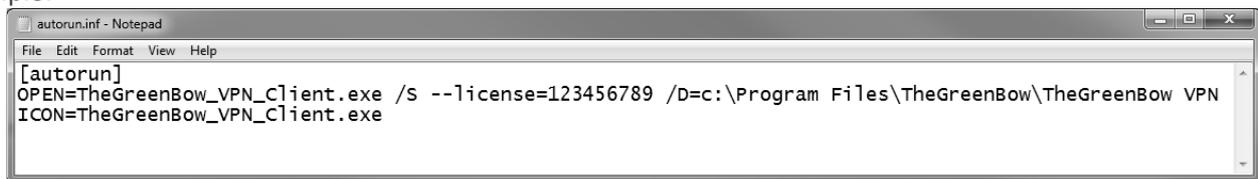
Create an "autorun" file

Create a text file called "autorun.inf". This file is used by the system, upon CD-Rom insertion, to automatically run TheGreenBow VPN Client software installation.

The "autorun.inf" file shall have the following content:

```
[autorun]
OPEN=[cdpath\]TheGreenBow_VPN_Client.exe /S /D=c:\Program
Files\TheGreenBow\TheGreenBow VPN (+ command line options see sections below)
ICON=[cdpath\]TheGreenBow_VPN_Client.exe
```

Example:



Copy the content of the setup directory and the autorun.inf file in the root directory of the CD-Rom.

**Note:** See section below for details about the available command line options.

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>).

### 3.4 Run a VPN Client Setup from a shortcut or a network drive

1/ Create a "silent" VPN Client Setup (see previous section)

2/ Right-click on the "setup.exe" file in the setup directory, and from the pop-up menu, select "Create Shortcut".

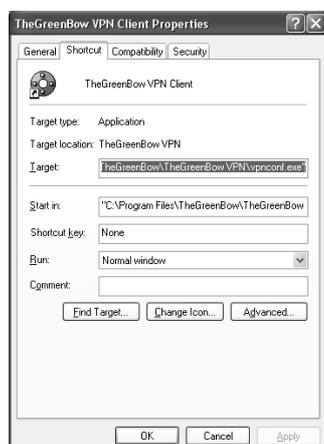
This will create a shortcut to "setup.exe" in the setup directory.

3/ Right-click on the new shortcut, and from the pop-up menu, select Properties.

4/ In the Target field, add the following options to the command line /S --license=123456789 /D=[install path] (see details on section 3.2).

5/ Move the shortcut where it can be clicked by the user (e.g. on the desktop)

Example :



"C:\Users\bob\Downloads\TheGreenBow\_VPN\_Client.exe /S --license=123456789 /D=c:\Program Files\TheGreenBow\TheGreenBow VPN"

**Important:** Make sure to place space characters between each argument

## 3.5 Deploy a VPN Client Setup using Batch script

- 1/ Create a "silent" VPN Client Setup (see section 3.2)
- 2/ Create a text file with a ".bat" extension (e.g. "VPN Client Setup.bat") and edit this file (right-click on the file and select "modify") with the command line you want to be processed.

### Example:

---

```
cd .\setup
setup.exe /S
cd ..
copy myvpnconfig.tgb C:\Program Files\TheGreenBow\TheGreenBow VPN
cd C:\Program Files\TheGreenBow\TheGreenBow VPN
vpnconf.exe /import:myvpnconfig.tgb
```

---

### In this example:

- the setup directory is called "setup" and is located under the directory containing the batch file.
- a VPN Configuration is imported at the end of the installation. See further sections for details about the import capabilities of the VPN Client Software.

Deploy this file (from a server or on an USB drive) together with the setup directory to the users.

## 3.6 Deploy a VPN Client Software Update

The deployment of a TheGreenBow VPN Client update is similar to the deployment of a new installation.

As part of a silent update, the entire process of updating is silent: backup of 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 VPN Client 4.2: the uninstallation 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 customized for end-users

## 4.1 Introduction

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

- 1/ The Configuration Panel: This interface enables the IT manager to create, modify, import or export the VPN security policy. It can be hidden or protected by a password.
- 2/ The Connection Panel: This interface enables the end-user 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 give access to the main functions of the software, such as quit, open the connection panel or the configuration panel, etc.

The Configuration Panel enables to manage the VPN security policy. It is recommended to protect or to hide this VPN configuration management facility, in order to show a very simple interface to end-users, while preventing mis-use of the VPN configuration from end-users.

The Connexion Panel and the systray menu can also be limited in order to show a simple interface to the end-user. For example, the whole software interface can be limited to the unique "open and close tunnel" function for the end-user.

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

## 4.2 Limit VPN Client usage to Connection Panel

The Configuration Panel can be hidden or protected with a password. The items of the systray menu can be limited. These limitations can be configured via the Configuration Panel, as described in the VPN Client User Guide (reference: `tgvpn_ug_en`).

### Exemple

- 1/ In the Configuration Panel, go to the menu "Tools > Options > View", enter and confirm a password. It is also possible to limit the number of items in the systray menu.
- 2/ Switch to the "Connection Panel" (Ctrl + ENTER)
- 3/ Optionally close the Connection Panel.

The screenshot shows the 'Options PKI' tab in the 'Affichage' section of the VPN Client configuration panel. It contains three main sections:

- Bloquer l'accès à l'interface**: A section for password protection. It includes a text box for 'Mot de passe' and a 'Confirmer' text box, both containing masked characters (dots).
- Visualiser en menu de barre des tâches**: A list of checkboxes for items to be shown in the taskbar:
  - Console
  - Panneau des Connexions
  - Panneau de Configuration
  - Quitter
- Popup de barre des tâches**: A checkbox for 'Ne pas afficher la popup de barre des tâches' which is currently unchecked.

From now on, the configuration panel cannot be open from the systray menu, and the access to the configuration panel from the connexion panel is protected with a password.

## 4.3 Limit VPN Client usage from the setup

The software interface can be limited during the software installation, via the following command line options:

The option "`--guidefs=user`" enables to limit the interface to the connection panel (see details section 7).

The option "`--guidefs=hidden`" enables to limit the interface to the systray menu. No interface (configuration panel or connection panel) is visible from the end-user. Only the systray icon of the software is visible. Since the list of tunnel isn't displayed in the systray menu from version 6.4, the end-user cannot manually open or close a tunnel. This operation has to be handled automatically (see the various automatisms enabled with the software in the VPN Client user guide or further in this document).

The option "`--password=[password]`" enables specifying a password to protect the access to the configuration panel, in order to prevent any unauthorized VPN security policy modification.

# 5 VPN Configuration deployment

## 5.1 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.

The process to create such setup is the following:

- 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 and execute the setup: the ".tgb" VPN Configuration is imported during the setup

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 Protect and deploy a new VPN Configuration

A VPN Configuration can be exported from TheGreenBow VPN Client, in order to be deployed to all employees in the company

- 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").
- 3/ Select "Protect the exported VPN configuration", enter a password then click on "Ok".
- 4/ Give the VPN Configuration to the end-user, either by email, or through file-sharing.

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



## 5.3 Protect a VPN security policy before it is deployed

The VPN Client software checks the integrity of the VPN security policy when it is imported or exported. It is also possible to protect the exported VPN security policy with a password. This password is asked when the VPN security policy is imported.

### 5.3.1 VPN security policy integrity

The VPN Client always checks the integrity of a VPN security policy when it is imported. Conversely the software doesn't systematically process the integrity calculation on a VPN security policy when it is exported. It is possible to force the software to systematically apply the integrity calculation on an exported VPN security policy with the following registry key:

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

### 5.3.2 Procedure

- 1/ Create the VPN security policy (VPN Configuration) for the target computer
- 2/ Export this VPN security policy ("Configuration > Export") protected with a password
- 3/ Run the VPN Client setup on the target computer
- 4/ Once the software is installed, transfer the VPN security policy on the target computer
- 5/ Import the VPN security policy, either by opening the ".tgb" file or via the command line /import and /pwd detailed in chapter 7.

## 6 VPN automations

### 6.1 Batch/script to open or close a tunnel

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

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

TunnelName is composed as follows:

|       | Tunnel Name:    |
|-------|-----------------|
| IKEv1 | Phase1-Phase2   |
| IKEv2 | IKEAuth-ChildSA |
| SSL   | TLS             |

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

- 1/ Create a VPN Configuration 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`

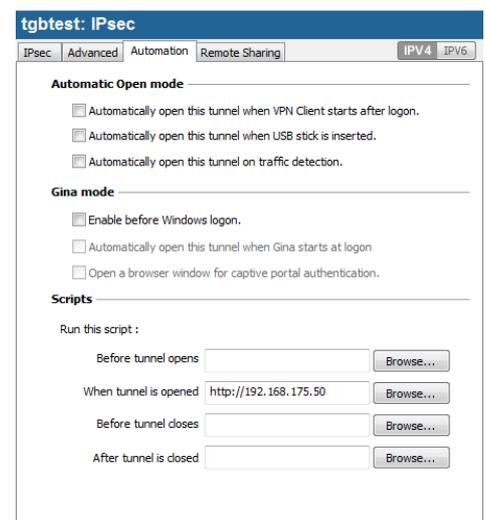
This script will start the VPN Client software with "MyTunnel" VPN Configuration, and will automatically open the tunnel.

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 Automatically open a web page when tunnel opens

- 1/ Create a VPN Configuration
- 2/ Open the "Automation" tab and set the url of the web page to open (internet or corporate intranet) in the field: "Run this script when tunnel is opened"
- 3/ Open the tunnel: the web page is automatically opened as soon as the tunnel is opened.



## 6.3 Open a tunnel with a double-click on a desktop icon

It is possible to open a tunnel with a double-click on a desktop icon.

### 6.3.1 Double-click on a ".tgb" file

1/ Create a VPN Configuration with "Open automatically when Client starts" selected for the relevant tunnel in the 'Automation' tab.

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

### 6.3.2 Script with a /open command

1/ Create the tunnel in the VPN Configuration.

2/ Create a batch file ("MyTunnel.bat" for example) which owns the tunnel opening command:

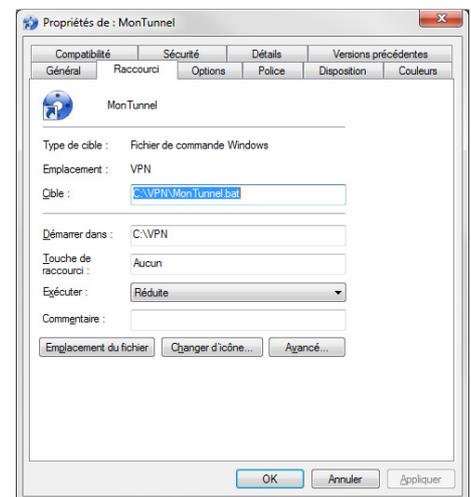
```
"C:\Program Files (x86)\TheGreenBow\TheGreenBow
VPN\vpnconf.exe" /open:tunnel_name
```

3/ Create a shortcut of this batch file on the windows desktop

4/ Modify the shortcut properties into run mode: "Minimized"

5/ Optionnaly modify the name and the icon of the shortcut..

A double-click on the icon on the windows desktop will automatically open the selected tunnel.



## 6.4 Difference between "import", "importance", "add", "replace"

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

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

Both options import and update a VPN Configuration when the VPN Client software is already running, without stopping it.

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 policy.

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

## 6.4.1 Protection of VPN security policy

When access to the Configuration Panel is protected by a 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.

The option `/pwd` is also used to import or export a VPN configuration protected with a password. This security function implies that, when the Configuration Panel is protected with a password, it is not possible to import or export a VPN configuration with a password different to the administrator password. This operation remains possible by using the menus in the Configuration Panel.

# 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.

**Note:** Command-line options that require a parameter must be specified with no space between the option and its parameter. Quotation marks around an option's parameter are required only if the parameter contains spaces.

### /S (case sensitive)

Syntaxe : /S ("S" must be preceded by only 1 slash)

Usage : Enables a silent installation (no dialog are displayed to the user during the installation)

Exemple : TheGreenBow\_VPN\_Client.exe /S

### /D

Syntaxe : /D=[install path] ("D" must be preceded by only 1 slash)

Usage : [install path] is the path where to install the software. No quotation marks even if space in the path. The path should be full as relative path does not work (e.g. ".././myrep").

Exemple : The /D option MUST be the last one in the command line if several options provided.

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

### --license

Syntaxe : --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.

Exemple : TheGreenBow\_VPN\_Client.exe --license=1234567890ABCDEF12345678

### --activmail

Syntaxe : --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.

Exemple : TheGreenBow\_VPN\_Client.exe --activmail=salesgroup@company.com

### --autoactiv

Syntaxe : --autoactiv=1

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.

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

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

## `--noactiv`

Syntaxe : `--noactiv=1`

Usage : No display of the 'Trial window' once software started until trial period ends. User doesn't know he is in trial period and software will be disabled at the end of trial period. It means that if the user tries to launch the software after the end of trial period, the software will start and open the 'Trial window' but the 'Evaluate' button will be disabled.

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

## `--start`

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

Usage : Enables to configure the start mode for the VPN Client:  
1: (default) automatically after the logon windows (with the user session)  
2: manually (e.g.: by double click on the desktop VPN Client icon)  
By default, the VPN Client starts automatically with the Windows logon (mode=1)

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

## `--password`

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

Usage : Enables to control the access to the VPN Client Configuration Panel with a password.  
The user will be asked for the password:  
- when the user selects the Configuration Panel item from the systray VPN menu.  
- when the user wants to switch from the Connection panel to the Configuration panel.

The password must not contain a space character.  
The maximum length of the password is 15 characters.

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

## `--guidefs`

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

Usage : Enables to define the GUI appearance when the VPN Client software starts.  
"user": Limits the software GUI to the Connection Panel.  
"hidden": The Configuration Panel and Connection Panel cannot be displayed. Only the systray icon is visible. The end-user cannot open or close manually a tunnel. This function has to be configured via the VPN automatism. (See the VPN Client User Guide for more details)

Exemple : TheGreenBow\_VPN\_Client.exe --guidefs=hidden

Warning : It is mandatory the "--guidefs=user" option comes together with the "--password" option, which enables to define a passord for access control to the Configuration Panel.

## --menuitem

Syntaxe : --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 (1<sup>st</sup> bit)=Quit

2 (2<sup>nd</sup> bit)=Connection panel

4 (3<sup>rd</sup> bit)=Console

8 (4<sup>th</sup> bit)=Save&Apply (obsolete from version 5)

16 (5<sup>th</sup> bit)=Configuration panel

Default is 31 (1F): All menus.

Exemple : TheGreenBow\_VPN\_Client.exe --menuitem=3 will only show the "Quit" and "Connection Panel" menu items.

0 doesn't display the systray menu

1 displays "Quit"

2 displays "Connection Panel"

3 displays "Connection Panel" and "Quit"

4 Displays "Console"

5 Displays "Console" and "Quit"

6 Displays "Connection Panel" and "Console"

7 Displays "Connection Panel", "Console" and "Quit"

Etc.

Note : "--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.

## --pkicheck

Syntaxe : --pkicheck=1

Usage : **VPN Premium only**

This parameter is either set to 1 or not set at all.

Force the VPN Client to check the Certificate Root Authority of the certificate received from the VPN gateway.

Exemple : TheGreenBow\_VPN\_Client.exe --pkicheck=1

## --smartcardroaming

Syntaxe : --smartcardroaming=1

Usage : **VPN Premium only**

This option can be set to 0, 1, 2, 3, 4 or 5.

It enables to configure the way the VPN Client handles tokens, smartcards, certificate storage and

certificates received from the gateway. This option enables to deploy the software among computers equipped with various tokens or smartcard readers.

This option and its different values are detailed in the document "PKI, Certificate, smartcard and token management guide" available on the TheGreenBow website.

## --lang

Syntaxe : --lang=[language code]

Usage : This option specifies the language for the TheGreenBow VPN Client software.  
Available languages are listed below.

Exemple : TheGreenBow\_VPN\_Client.exe --lang=1040 will start software in Italian.

|    | ISO 639-2 code | Language code  | Native name  | English name       |
|----|----------------|----------------|--------------|--------------------|
| 1  | EN             | 1033 (default) | English      | English            |
| 2  | FR             | 1036           | Français     | French             |
| 3  | ES             | 1034           | Español      | Spanish            |
| 4  | PT             | 2070           | Português    | Portuguese         |
| 5  | DE             | 1031           | Deutsch      | German             |
| 6  | NL             | 1043           | Nederlands   | Dutch              |
| 7  | IT             | 1040           | Italiano     | Italian            |
| 8  | ZH             | 2052           | 简化字          | Chinese simplified |
| 9  | SL             | 1060           | Slovenscina  | Slovenian          |
| 10 | TR             | 1055           | Türkçe       | Turkish            |
| 11 | PL             | 1045           | Polski       | Polish             |
| 12 | EL             | 1032           | ελληνικά     | Greek              |
| 13 | RU             | 1049           | Русский      | Russian            |
| 14 | JA             | 1041           | 日本語          | Japanese           |
| 15 | FI             | 1035           | Suomi        | Finnish            |
| 16 | SR             | 2074           | српски језик | Serbian            |
| 17 | TH             | 1054           | ภาษาไทย      | Thai               |
| 18 | AR             | 1025           | عربي         | Arabic             |
| 19 | HI             | 1081           | हिन्दी       | Hindi              |
| 20 | DK             | 1030           | Danske       | Danish             |
| 21 | CZ             | 1029           | Český        | Czech              |
| 22 | HU             | 1038           | Magyar nyelv | Hungarian          |
| 23 | NO             | 1044           | Bokmål       | Norwegian          |
| 24 | FA             | 1065           | فارسی        | Farsi              |
| 25 | KO             | 1042           | 한국어          | Corean             |

## 7.2 VPN Client Software command line options

TheGreenBow 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:

```
[directory]\vpnconf.exe [/option[:"value"]]
```

- "directory" is the directory where the file "vpnconf.exe" is located (typically the installation directory)
- "value" does not require double quote if there it does not contain space characters.
- All available command line "options" are detailed below.

Various examples of command line options usages are available on TheGreenBow website:

[www.thegrenbow.vom/vpn\\_tool.html](http://www.thegrenbow.vom/vpn_tool.html)

### /import

Syntax: /import:[ConfigFileName]

Usage: Enables the VPN Client to import a VPN Configuration. If the VPN Client software is not running, it is automatically started by this option. Thus, this option can be used to start the VPN Client with a given VPN Configuration.

If the VPN Client software is running, this option imports and updates the VPN Configuration without stopping the software.

[ConfigFileName] must be enclosed in double-quotes if it contains space characters.

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

Note: If the VPN Configuration to be imported is protected with a password or if the Configuration Panel is protected with a password, /import must be used with the /pwd option. See chapter 6.4.1 and option "/pwd" below for more details.

Note: When the current configuration is not empty, the software displays a window asking the user if he wants to add or replace the VPN configuration. To avoid this window, please use the options /add or /replace described below.

### /importonce

Syntax: /importonce:[ConfigFileName]

Usage: Enables the VPN Client to import a VPN Configuration. 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 Configuration 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 Configuration without stopping the software.

[ConfigFileName] must be enclosed in double-quotes if it contains space characters.

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

Note: If the VPN Configuration to be imported is protected with a password or if the Configuration Panel is protected with a password, `/importonce` must be used with the `/pwd` option. See chapter 6.4.1 and option `"/pwd"` below for more details.

Note: When the current configuration is not empty, the software displays a window asking the user if he wants to add or replace the VPN configuration. To avoid this window, please use the options `/add` or `/replace` described below.

## `/export`

Syntax: `/export:[ConfigFileName] /pwd:[Password]`

Usage: Enables the VPN Client to export a VPN Configuration. If the VPN Client software is not running, it is automatically started by this option. Please note that `/pwd:` is mandatory.  
If the VPN Client software is running, this option exports the VPN Configuration without stopping the software.  
[ConfigFileName] must be enclosed in double-quotes if it contains space characters.

Example: `vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" /pwd:gg1`

Note: If the Configuration Panel is protected with a password, `/export` must be used with the `/pwd` option. See chapter 6.4.1 and option `"/pwd"` below for more details.

## `/exportonce`

Syntax: `/exportonce:[ConfigFileName] /pwd:[Password]`

Usage: Enables the VPN Client to export a VPN Configuration. If the VPN Client software is not running, it won't be started by this option. Please note that `/pwd:` is mandatory.  
If the VPN Client software is running, this option exports the VPN Configuration without stopping the software.  
[ConfigFileName] must be enclosed in double-quotes if it contains space characters.

Example: `vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb" /pwd:gg1`

Note: If the Configuration Panel is protected with a password, `/exportonce` must be used with the `/pwd` option. See chapter 6.4.1 and option `"/pwd"` below for more details.

## `/add`

Syntax: `/add:[ConfigFileName]`

Usage: Enables to add a VPN Configuration to the current configuration.  
[ConfigFileName] must be enclosed in double-quotes if it contains space characters.

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

Note: If the VPN Configuration to be imported is protected with a password or if the Configuration Panel is protected with a password, `/importonce` must be used with the `/pwd` option. See chapter 6.4.1 and option `"/pwd"` below for more details.

## /replace

Syntax: /replace:[ConfigFileName]

Usage: Enables to replace the current configuration by a new VPN Configuration.  
[ConfigFileName] must be enclosed in double-quotes if it contains space characters.

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

Note: If the VPN Configuration to be imported is protected with a password or if the Configuration Panel is protected with a password, /importonce must be used with the /pwd option. See chapter 6.4.1 and option "/pwd" below for more details.

## /pwd

Syntax: /pwd:[Password]

Usage: Enables to set a password for import operations. This option can be used together with the /import, /export, /add and /replace options but it must be placed after one of those options.  
In the command line, the option /pwd must be set at the end of the command line.

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

Note: When the Configuration Panel is protected with a password, this password must be specified in the command line for any import or export operation. Since this option is also used to specify the password protecting the VPN Configuration to be imported or exported, it implies that, when the Configuration Panel is protected with a password, it is not possible to import or export a VPN Configuration with a different password. See chapter 6.4.1 for the details of the possible operations.

## /stop

Syntax: /stop

Usage: Enables to close all opened VPN tunnels and exit the VPN Client.

Example: `vpnconf.exe /stop`

## /open

Syntax: /open:[TunnelName(1)]

Usage: Enables to open a VPN tunnel.  
Returns the following codes:  
- 0: Tunnel is closed  
- 2: Tunnel is opened  
- Other: See the return codes list below

---

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

---

## /status

Syntax: /status:[TunnelName(1)]

Usage: Enables to get the status of a VPN tunnel.  
Returns the following codes:  
- 0: Tunnel is closed  
- 1: Tunnel is opening (opening in progress)  
- 2: Tunnel is opened  
- 3: Tunnel is closing (closing in progress)  
- 4: Tunnel with an error  
- Other: See the return codes list below

---

Example: "C:\Program Files\TheGreenBow\TheGreenBow VPN\vpnconf" /status:tgptest-tgptest  
@echo retour = %ERRORLEVEL%  
Pause

---

## /close

Syntax: /close:[TunnelName(1)]

Usage: Enables to close a VPN tunnel.  
Returns the following codes:  
- 0: Tunnel is closed  
- Other: See the return codes list below

Example: vpnconf.exe /close:"Home gateway-cn1"  
(double quote is required because the tunnel name contains a space character)

## /closeall

Syntax: vpnconf.exe /closeall

Usage: Enables to close all opened VPN tunnels.  
Returns the following codes:  
- 0: All tunnels are closed  
- Other: See the return codes list below

Example: vpnconf.exe /closeall

## /resetike

Syntax: vpnconf.exe /resetike

Usage: Enables to restart the IKE daemon.  
Returns the following codes:  
- 0: IKE daemon is restarted  
- Other: See the return codes list below

Example: vpnconf.exe /resetike

## TunnelName

(1) In this chapter, TunnelName is composed as follows:

|       | Tunnel Name     |
|-------|-----------------|
| IKEv1 | Phase1-Phase2   |
| IKEv2 | IKEAuth-ChildSA |
| SSL   | TLS             |

## Command line return codes

Many command line options (/open, /close, /status, /closeall, /resetike) may return the following error code:

-1, -2, -3: Cannot find the main instance of the software which must execute the command.  
100 à 199: Execution timeout, identified by the main instance of the software  
200 à 299: Execution timeout: no answer from the software during 30 seconds  
300: Internal error  
500: Cannot find the tunnel  
1000 à 1999: Problem during the opening of the tunnel  
> 10000: Internal error

# 8 Contact

## 8.1 Information

All TheGreenBow products information are available on: [www.thegreenbow.com](http://www.thegreenbow.com)

## 8.2 Sales

Phone: +33.1.43.12.39.30

Email: [sales@thegreenbow.com](mailto:sales@thegreenbow.com)

## 8.3 Support

Different pages concerning the support are available on TheGreenBow website:

### Support

<http://www.thegreenbow.com/support.html>

### Online help

[http://www.thegreenbow.com/support\\_flow.html?product=vpn&lang=en](http://www.thegreenbow.com/support_flow.html?product=vpn&lang=en)

### FAQ

[http://www.thegreenbow.com/vpn\\_faq.html](http://www.thegreenbow.com/vpn_faq.html)

### Contact

Technical support is available through the inline forms or directly at: [support@thegreenbow.com](mailto:support@thegreenbow.com)

**THEGREENBOW**

**Secure, Strong, Simple**

TheGreenBow Security Software