THEGREENBOW

Windows Enterprise VPN Client 6.85

Deployment Guide

Latest update 29 March 2021

Table of Contents

1 Introduction

The Windows Enterprise VPN Client has been designed for easy deployment and management.

The software therefore includes many features that enable network administrators to preconfigure the installation prior to deployment, to install or update the software from a remote location, and even to centralize software and VPN security policy management.

The Windows Enterprise VPN Client is packaged in a Microsoft MSI installer that allows for the software to be deployed and updated using Microsoft Windows deployment functions and Group Policies (GPO). Furthermore, all the installation parameters can be placed in a file used by the software to configure itself automatically during deployment.

This document describes the various management and configuration options found in the Windows Enterprise VPN Client. Examples of how these options can be implemented are also provided. They illustrate how to manage the software.

Many features can be configured when the Windows Enterprise VPN Client software is installed:
- Software activation features: license number, activation email, hidden activation, etc.
- Display features: interface hidden from the user, menu customization, etc.
- PKI integration features: certificate, token or smart card reader specification, etc.
- VPN security policy to be deployed
- Installation features: hidden installation, etc.
- And more

Additional features can be used with the software itself once the installation is completed:
- VPN configuration management: import, export, signature, etc.
- Software management: start, stop, etc.
- VPN tunnel management: open, close, status
- And more

2 Security recommendations

2.1 Configuring the host workstation

The machine on which the Windows Enterprise VPN Client is installed and run must be clean and properly administered. More specifically:
1/ It must be equipped with an antivirus software with a regularly updated database.
2/ It must be protected by a firewall that controls the inbound and outbound communications of the workstation, which are not already going through the VPN Client.
3/ Its operating system is up to date with the various security patches.
4/ Its configuration is such that it is protected against local attacks (memory forensics, patch or binary corruption).

Configuration recommendations to strengthen the workstation are available (in French) on the ANSSI website, such as the following (the list is non-exhaustive):

- Computer health guide (Guide d'hygiène informatique, document only available in French)
- Configuration guide (Guide de configuration, document only available in French)
- Security updates (Mises à jour de sécurité, document only available in French)
- Password (Mot de passe, document only available in French)

We recommend that you install the Windows Enterprise VPN Client on a machine that has no previous version of the software installed. If there already is a previous version of the software installed on the machine, we therefore recommended that you uninstall it before installing this version. We also recommended that you execute the installation from an empty directory, especially for customized installations that use additional configuration files.

2.2 Execution rights

The Windows Enterprise VPN Client is designed to be installed with "administrator" rights and then to be used with "user" privileges only, regardless of the Windows OS used.

Since some features are inhibited in "user" mode (e.g. uninstalling the software), we strongly recommended that you follow these guidelines during deployment:

- Installation in "administrator" mode
- Use in "user" mode

2.3 Configuring for the end user

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

The entire interface of the software can be customized so that the number of features available to the end user is very limited (open and close a VPN tunnel).

In a similar fashion, the software can be entirely customized from the moment of the installation or deployment so that access to the VPN security policies is solely restricted to the administrator.

The software configuration options described further down below in this document make such restrictions possible so that the VPN Client is run in the most secure and reliable manner.

2.4 Managing multiple users

The Windows Enterprise VPN Client will apply the same VPN configuration (security policy) to all users of a multiple-user workstation. Consequently, we recommend running the software on a dedicated workstation (for instance by keeping an administrator account and a user account, as mentioned above).

2.5 Managing VPN security policies

The Windows Enterprise VPN Client features a standard set of command-line options to import, export, replace, or add new VPN security policies.

These options are intended to be used with software deployment scripts, for update or remote maintenance tasks or for various automated tasks such as automatically opening and closing VPN tunnels.

This document explains how to use these various command-line options without jeopardizing the integrity or confidentiality of the VPN security policies.

2.6 User authentication

As detailed in the “Windows Enterprise VPN Client User Guide” (tgbvpn_ug_en.pdf), we recommend using certificates, preferably stored on a token or smart card, to ensure strong authentication of the user when opening a VPN tunnel.

Software configuration options relative to this function are detailed in a separate document entitled “Management of PKI, certificates, tokens and smart cards” (tgbvpn_ug_pki_smartcard_en.pdf).

2.7 Protecting sensitive data

As described in the “The Windows Enterprise VPN Client User Guide” (tgbvpn_ug_en.pdf), we recommend that you do not store any sensitive data in the VPN configuration file: X-Auth login/password, pre-shared key or certificate.

2.8 Resetting

The Windows environment allows you to uninstall and then re-install the software.
The security policy is deleted during uninstallation. This procedure essentially restores the software’s initial configuration.

2.9 Deprecation of the CSP API for IKEv2 and SSL

Starting from the current version, the Microsoft Cryptographic Service Providers (CSP) API to use tokens/smart cards has been deprecated and is no longer available for IKEv2 or SSL. It has been replaced with the new Microsoft Cryptography API: Next Generation (CNG) API. use of the PKCS#11 API can still be forced (see section 7.8.2).

Note: When importing a certificate into the Windows certificate store, there is an option to determine which API will be used to access it: CSP or CNG. However, in Windows 10, the CSP API is still used by default to import RSA certificates. Use the following administrator command to force the use of the CNG API for a certificate:

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

Note: The CSP API is the only one available for IKEv1.

3 Deploying the VPN Client

3.1 Introduction

The deployment of the software mostly relies on the fact that it can be installed in a silent manner, i.e. without any user interaction (prompts or warnings).

All the software configuration options can therefore be transmitted to the installation, either through initialization files or the command-line options.

We strongly recommend restricting access to the VPN security policies to administrators only (default behavior).

3.2 Silent installation

A “silent” installation is an installation that is carried out without any user interaction, without any questions or warnings. The installation is carried out in an entirely transparent manner.

The installation parameters are, in this case, configured through the set of command-line options or through the “vpnsetup.ini” initialization file that comes with the installation (see section 9).

In order to start the installation in silent mode, use the command-line option “/S”.

1/ Download the TheGreenBow_VPN_ENTERPRISE.msi installation program from http://www.thegreenbow.com
2/ Open the Windows command prompt and enter the command line:

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet (for additional options, see sect. 7)
```

Example:

```
[download_dir]/TheGreenBow_VPN_ENTERPRISE.msi /quiet LICENSE=[license_num]
```

[download_dir] is directory to which the installer has been downloaded.

3.3 Deploying an update

Deploying a Windows Enterprise VPN Client update is done in the exact same way as deploying a new installation.

When performing a silent update, the entire update process is silent (back up parameters, uninstall previous version, install new version, restore parameters).
When the installed version is older than version 6.8 and password-protected, this password must be entered in the update command line.

Example: If the previous version installed with the password `Tgb@dM1Npwd!`, the update command line will be as follows:

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

Note: Windows Enterprise VPN Client version 6.8 and higher is no longer password-protected, but uses privilege elevation instead (executing the software with administrator privileges).

Any older version of the Certified, Premium or Enterprise edition higher than or equal to 6.5 can be replaced. This update preserves the VPN configuration.

Note: However, no version whatsoever of the Standard edition can be updated. This edition requires the prior version to be uninstalled. Moreover, the VPN configurations are not compatible.

3.4 Repairing

The repair function of the MSI installer is currently not supported.

3.5 Uninstalling

3.5.1 Uninstalling from the Windows Control Panel

The software can be uninstalled from the “Programs and Features” tab in the Windows Control Panel or by right clicking the TheGreenBow Enterprise VPN icon in the Start menu and choosing “Uninstall”.

3.5.2 Uninstalling from the command line

The software can also be uninstalled using the Windows msiexec utility.

Example of the command line to use:

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

Refer to the documentation of the msiexec utility for further information.

4 Deploying the software's activation

4.1 Activation parameters

TheGreenBow software must be activated in order to be able to use it beyond the trial period.

By default, software activation is performed by submitting a request to the TheGreenBow activation server, which is accessible over the internet.
For customers who deploy TheGreenBow software on a network which has no Internet connection, TheGreenBow provides a Corporate Activation Server: the TheGreenBow Activation Server (TAS server) which can be installed on the customer's network.

The activation parameters can be configured to be automatically applied during the software installation and deployment process, either from the command line or in the vpnsetup.ini configuration file. These methods are described in the following sections below.

4.2 Deploying and automating activation

Using activation parameters, the software's activation can be fully integrated in the deployment process. This allows for the activation process to be automated and performed in a manner that is entirely transparent for the end user (no interaction required).

In order for the activation to be executed automatically and in a manner that is transparent for the user, use the installer's command-line options: "AUTOACTIV" (which automates activation) and "NOACTIVWIN" (which hides the activation window), together with the "LICENSE" and "ACTIVMAIL" parameters as described in section 7.5.

Command line for automated and silent activation:

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

When the software is activated through a TAS server ("TheGreenBow Activation Server", activation server installed on the Client's infrastructure), the parameters of this server can be specified in the VpnSetup.ini file added to the installer at the time of installation (see section 9
for details about the parameters) or use the MSI properties "OSAURL", "OSAPORT" and "OSACERT" in the command line.

Example of a command line for activating on a TAS server:

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

Example of a vpnsetup.ini file for activating on a TAS server:

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

4.3 Activating “within the tunnel”

The Windows Enterprise VPN Client implements the tunnel activation function as standard (all versions).
As soon as the “AUTOACTIV” and “NOACTIVWIN” properties are configured (as described in the previous section), the software automatically checks its activation within the VPN tunnel it just opened and performs an update when required.

This automation enables the software, when it is in a subscription mode, to automatically check and update its activation when the subscription is renewed. It also enables the software to automatically re-activate following an update, in a transparent manner for the end user.

4.4 Identifying activations

During automated software deployment, the identification of the workstation on which the activation is processed can also be automated. This allows for easy activation/deactivation of the installed licenses.

Workstation identification can be achieved by using the “activation email” field during the installation process to enter the name of the activated workstation.

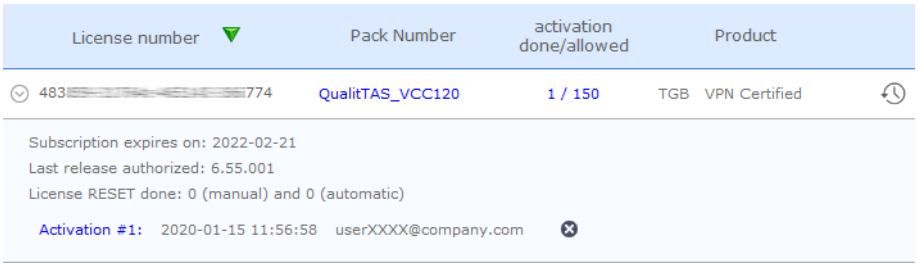
Automatic installation script with a workstation identifier:

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

PowerShell batch for an automatic installation with a workstation identifier:

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

The %ComputerName% identifier is automatically filled by the OS during the installation process. It is then automatically used by the activation process, and ultimately it is displayed in the visualization pages available on TheGreenBow or TAS activation servers.



Caution: The value of the “ACTIVMAIL” property must always be formatted according to the email address syntax, i.e. it must always contain the characters “@” and “.” (dot). If this is not the case, activation will fail.

5 Deploying VPN security policies

5.1 Integrity of an exported VPN security policy

The protection of an exported VPN security policy's integrity is a function that can be activated using the "SIGNFILE" property.

Example:

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

5.2 Including a VPN security policy in the installation

A preconfigured VPN security policy (VPN configuration) can be included in the installation of the Windows Enterprise VPN Client. This security policy will be automatically imported and applied during software installation. It will therefore be immediately operational for the end user, as soon as the VPN Client has been started for the first time.

The steps to create such an installation are as follows:

1/ Create the VPN security policy (VPN Configuration) intended for the target workstation.
2/ Export the VPN security policy ("Configuration" menu > "Export", refer to the Windows Enterprise VPN Client User Guide) and protect it with a password, if desired.
3/ Transfer the setup program and the VPN security policy to the target workstation.
4/ Execute the installation of the VPN Client by specifying the "TGBCONF_PATH" and "TGBCONF_PASSWORD" properties (if the security policy is password-protected). When the installation is completed, the VPN Client will have been installed with the imported VPN security policy applied.

Example:

```
TheGreenBow_VPN_ENTERPRISE.msi /quiet TGBCONF_PATH=C:\Users\Public\conf.tgb TGBCONF_PASSWORD=
[password]
```

From a deployment security perspective, this method relies on the integrity check function in VPN security policies, if it is activated. If this is the case, the function ensures that the security policy imported during installation has not been corrupted.

5.3 Deploying a new VPN security policy

5.3.1 Procedure

1/ Create the VPN security policy (VPN Configuration) intended for the target workstation.
2/ Export the security policy ("Configuration" menu > "Export", refer to the Windows Enterprise VPN Client User Guide). It can be encrypted with a password.
3/ Transfer this VPN security policy to the workstation to be updated (e-mail, file sharing, etc.).
4/ On the target workstation, run vpnconf.exe in the command line and, where applicable, specify the password used to protect the exported configuration (refer to the /import and /pwd options described in detail in section 6.2).

5.3.2 Difference between "import", "importonce", "add" and "replace"

The "/import" option is used to import a VPN security policy (VPN Configuration) and simultaneously start the VPN Client software, if it is not already running.

The “/importonce” option is used to import a VPN security policy (VPN Configuration) without starting the VPN Client software.

When the VPN Client software is already running, both options simply import the VPN security policy.

When the existing VPN security policy (prior to import) of the VPN Client software is not empty, both options will display a pop-up asking the user whether to “Add or replace”, i.e. add the new VPN security policy or replace the old policy with new one.
The “/add” and “/replace” options are used to prevent showing the user prompt: The “/add” option will always add the VPN security policy, while the “/replace” option will always replace the existing policy with the one being imported.

Option	Prompt to “Add or replace”	Starts the client if it is not already running
/import	Yes	Yes
/importonce	Yes	No
/add	No: adds the VPN security policy	No
/replace	No: replaces the VPN security policy	No

Note: If the VPN security policy is empty, both the “`/import`” and the “`/importonce`” options will not ask the user anything and simply “add” the VPN security policy.

5.4 Protecting the VPN security policy

If access to the Configuration Panel is restricted to administrators (default installation option), the command line interpreter (cmd, powershell, etc.) must be started with administrator privileges to be able to use the import or export commands: “/import”, “/importonce”, “/add”, “/replace”, “/export”, “/exportonce”.

From a security standpoint, we recommend using the “/importonce”, “/add” and “/replace” options for maintenance tasks (and not “/import”), since they quit the software immediately after their execution.

5.5 Exporting the security policy

The “`/export`” option is used to export a VPN security policy (VPN Configuration) and simultaneously start the VPN Client software, if it is not already running.

The “`/exportonce`” option is used to export a VPN security policy (VPN Configuration) without starting the VPN Client software.

When the VPN Client software is already running, both options simply export the VPN security policy.

6 Running vpnconf in the command line

6.1 Introduction

The Windows Enterprise VPN Client comes equipped with a standard set of command-line options that can be used in scripts or batch files. These options are used to perform various tasks, such as opening or closing a VPN tunnel, importing or exporting a VPN security policy, etc.

The syntax of these command-line options always remains the same:

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

- [directory] is the directory in which the “vpnconf.exe” executable file is located (typically the VPN Client installation directory).
- If the value contains blank spaces (e.g. a directory name), it must be placed between quotation marks.
- All available options are detailed below.

Several examples illustrating how these command-line options are implemented can be found on the TheGreenBow website at the following URL: www.thegreenbow.fr/vpn_tool.html

6.2 Importing

/import

Syntax:	/import:[ConfigFileName]
Usage:	This option is used to import a VPN configuration when the VPN Client is started. This option can be used to start the VPN Client with a specific VPN configuration. If the VPN Client is already running, this option will import and update the VPN configuration without stopping the software. [ConfigFileName] is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Example:	vpnconf.exe /import:"c:\my documents\myvpnconf.tgb"

Note: If the imported VPN configuration is password-protected, then /import must be used with the /pwd option (see below).

Note: If the current VPN configuration is not empty, the software will display a window asking the user whether to add the imported VPN configuration or replace the existing configuration with the one being imported. Use “/add” or “/replace” to avoid displaying this window. See below.

/importonce

Syntax:	/importonce:[ConfigFileName]
Usage:	This option is used to import a VPN configuration without starting the VPN Client.

	It can, for example, be used in an installation or update script. If the VPN Client is already running, this option will import and update the VPN configuration without stopping the software. [ConfigFileName] is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Return:	Refer to the note on the return code below. 0: command has been executed successfully 1: file not found 2: error in the file signature 3: wrong password (the configuration is protected) 4: a password is required and couldn't be obtained (password prompt window canceled)
Example:	vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb"

Note: If the current VPN configuration is not empty, the software will display a window asking the user whether to add the imported VPN configuration or replace the existing configuration with the one being imported. Use "/add" or "/replace" to avoid displaying this window. See below.

Note: The /importonce command is preemptive and will pause the rest of the command line until it has been successfully completed.
An error code will be returned in the ERRORLEVEL variable (see return codes below).
If /importonce is not specified with a password, but a password is required, a dialog box opens.

Note: If the user cancels the Add/Replace prompt, a return code set to 1 will be written in ERRORLEVEL (users are not supposed to use /importonce in a script if the execution should be silent).

/add

Syntax:	/add:[ConfigFileName]
Usage:	Used to add a VPN security policy. [ConfigFileName] is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Return:	Refer to the note on the return code below. 0: command has been executed successfully 1: file not found 2: error in the file signature 3: wrong password (the configuration is protected) 4: a password is required and couldn't be obtained (password prompt window canceled)
Example:	vpnconf.exe /add:"c:\my documents\myvpnconf.tgb"

Note: If the imported VPN configuration is password-protected, then /add must be used with the /pwd option (see below).

Note: The /add command is preemptive and will pause the rest of the command line until it has been successfully completed.
An error code will be returned in the ERRORLEVEL variable (see return codes below).
If /add is not specified with a password, but a password is required, a dialog box will open.

/replace

Syntax:	/replace:[ConfigFileName]
Usage:	Used to add a VPN security policy.

	[ConfigFileName] is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.
Return:	Refer to the note on the return code below. 0: command has been executed successfully 1: file not found 2: error in the file signature 3: wrong password (the configuration is protected) 4: a password is required and couldn't be obtained (password prompt window canceled)
Example:	vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb"

Note: If the imported VPN configuration is password-protected, then /replace must be used with the /pwd option (see below).

Note: The /replace command is preemptive and will pause the rest of the command line until it has been successfully completed.
An error code will be returned in the ERRORLEVEL variable (see return codes below).
If /replace is not specified with a password, but a password is required, a dialog box will open.

/pwd

Syntax:	/pwd:[password]
Usage:	Used to specify a password for importing and exporting VPN security policies. This option is used with the following options: "/import", "/importonce", "/add", "/replace", "/export" and "/exportonce". In the command line, the "/pwd" option must be specified after the import or export options.
Example:	vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd=mypwd

6.3 Exporting

/export

Syntax:	/export:[ConfigFileName]
Usage:	Used to export a VPN security policy when starting the VPN Client software. If the software is already running, the /export option will export the VPN configuration without stopping it. [ConfigFileName] is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after. /export can be used with /pwd in order to export a VPN security policy and protect it with a password.
Example:	vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" vpnconf.exe /export:"c:\my documents\myvpnconf.tgb" /pwd:gq1aRe7

/exportonce

Syntax:	/exportonce:[ConfigFileName]
Usage:	Used to export a VPN security policy without starting the VPN Client software. If the software is already running, the /exportonce option will export the VPN configuration without stopping it. [ConfigFileName] is the complete path to the file to be imported. If the path contains blank spaces, quotation marks must be added before and after.

	/exportonce can be used with /pwd in order to export a VPN security policy and protect it with a password.
Example:	vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb" /pwd: gq1aRe7

6.4 Opening/closing a VPN tunnel

/stop

Syntax:	/stop
Usage:	Closes all VPN tunnels currently open and quits VPN Client.
Example:	vpnconf.exe /stop

/open

Syntax:	/open:[TunnelName(1)]
Usage:	Used to open a VPN tunnel from a command line.
Return:	0: Tunnel is still closed 2: Tunnel is now open Other: See the list of return codes below.

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

/status

Syntax:	/status:[TunnelName(1)]
Usage:	Used to get the status of a VPN tunnel from a command line.
Return:	0: VPN tunnel is closed 1: VPN tunnel is being opened 2: VPN tunnel is open 3: VPN tunnel is being closed 4: Error while opening VPN tunnel Other: See the list of return codes below.

Example:	`"C:\Program Files\TheGreenBow\TheGreenBow VPN\vpnconf" /status:tgbtest-tgbtest`
	`@echo return = %ERRORLEVEL%`
	`pause`

/close

Syntax:	/close:[TunnelName(1)]
Usage:	Used to close a VPN tunnel from a command line.
Return:	0: VPN tunnel is closed Other: See the list of return codes below.

Example:	`vpnconf.exe /close:"Home gateway-cnx1"` (quotation marks are required, because the tunnel name contains blank spaces)

/closeall

Syntax:	vpnconf.exe /closeall
Usage:	Used to close all currently open VPN tunnels.
Return:	0: All VPN tunnels are closed Other: See the list of return codes below.
Example:	vpnconf.exe /closeall

6.5 Restarting

/resetike

Syntax:	vpnconf.exe /resetike
Usage:	Used to restart the IKE service from a command line.
Return:	0: IKE service has restarted Other: See the list of return codes below.
Example:	vpnconf.exe /resetike

6.6 Further details

TunnelName

(1) In this section, the tunnel name consists of the following:

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

Return codes for command-line options

Several command-line options (/open, /close, /status, /closeall, /resetike) may return the following codes:

-1, -2, -3:	Cannot find the VPN Client instance that should execute the command.
100 to 199:	Command execution timeout.
200 to 299:	Command execution timeout: software is not responding.
300:	Internal error.
500:	Cannot find the specified VPN tunnel.
1000 to 1999:	An issue occurred while opening the VPN tunnel.
> 10000:	Internal error.

7 Parameters of the MSI installer

7.1 Introduction

The installer of the Windows Enterprise VPN Client is in Microsoft Installer (MSI) format. It can be configured using command-line parameters and “properties”.

To install the Windows Enterprise VPN Client, we recommend starting the MSIEXEC command line from an admin shell with the /i and /q options as well as any other suitable properties for your deployment.

Example

```
msiexec /q /i [path_to_installer]
```

Syntax rules: Options that call for a specific value must be entered without any blank spaces between the option and the value assigned to it. Values that contain blank spaces, such as directory names, must be placed between quotation marks.

7.2 Running MSI parameters in the command line

/i

Syntax: `msiexec /i [path_to_installer]`

Usage: Installs the Windows Enterprise VPN Client software

Example: `msiexec /i TheGreenBow_VPN_ENTERPRISE.msi`

/x

Syntax: `msiexec /x [path_to_installer]`

Usage: Uninstalls the Windows Enterprise VPN software

Example: `msiexec /x TheGreenBow_VPN_ENTERPRISE.msi`

/quiet

Syntax: `msiexec /quiet` or `/q`

Usage: Configures the installation or uninstallation in silent mode (no messages or warnings to the user)

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

/L*V!

Syntax: `msiexec /L*V! <path_to_log_files>`

Usage: Activates logging and includes a detailed output in the output log file by specifying the location and name of the output log file.

Example:
```
msiexec -i TheGreenBow_VPN_ENTERPRISE.msi /L*v! "C:\install.log"
```

7.3 Installing

7.3.1 APPLICATIONROOTDIRECTORY

Syntax:
```
APPLICATIONROOTDIRECTORY=[install_dir]
```

Usage: [install_dir] is the directory where VPN Client is to be installed.
Quotation marks are required before and after [install_dir], if the directory name contains blank spaces.

Example:
```
msiexec /i TheGreenBow_VPN_ENTERPRISE.msi /q
APPLICATIONROOTDIRECTORY=”C:\my directory\vpn"
```

Note: “C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise” is the default installation directory.

7.3.2 TGBCONF_ADMINPASSWORD

Syntax:
```
TGBCONF_ADMINPASSWORD=[password]
```

Usage: Administrator password used to protect access to the configuration panel in version 6.8 and earlier, where appropriate. Used to update an earlier version in which the configuration panel was password protected.

7.4 TAS activation server

The parameters of the “Activation” section define the characteristics of the TAS activation server (“TheGreenBow Activation Server”, an activation server installed as an option on the user’s infrastructure).
These parameters include the following: server address, access port and activation authentication certificate.

Since these parameters are required for specific configurations, they are generally provided by TheGreenBow.

7.4.1 OSACERT

Syntax:
```
OSACERT=[certificate_contents]
```

Usage: Certificate used to authenticate to the TAS activation server.

7.4.2 OSAPORT

Syntax:
```
OSAPORT=[tas_port]
```

Usage: Port for TAS activation server.

7.4.3 OSAURL

Syntax: `OSAURL=[tas_url]`

Usage: URL for TAS activation server.

7.5 Activating the license

7.5.1 ACTIVMAIL

Syntax: `ACTIVMAIL=[activation_email]`

Usage: Used to configure the e-mail address use to activate the software. (Refer to the "Windows Enterprise VPN Client User Guide" for the characteristics of this email address).

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

7.5.2 AUTOACTIV

Syntax: `AUTOACTIV=1`

Usage: For an update (i.e. the license number and email address required for activation have already been specified in a previous installation), this property is used to automatically activate the software.

Example: `TheGreenBow_VPN_ENTERPRISE.msi AUTOACTIV=1`

7.5.3 LICENSE

Syntax: `LICENSE=[license_number]`

Usage: Used to configure the license number use to activate the software. (Refer to the "Windows Enterprise VPN Client User Guide" for the characteristics of this license number).

Example: `TheGreenBow_VPN_ENTERPRISE.msi LICENSE=1234567890ABCDEF12345678`

7.5.4 NOACTIVWIN

Syntax: `NOACTIVWIN=1`

Usage: This option is used to prevent displaying the activation window.
It can be combined with the "`AUTOACTIV=1`" option to deploy a non-activated software on the target user workstations and to automate its activation in an entirely transparent manner for the users.
Please bear in mind that the activation window will ultimately be displayed to the user at the end of the trial period if no activation has been carried out by that date.

7.6 VPN security policy

7.6.1 TGBCONF_PATH

Syntax: `TGBCONF_PATH=[path_to_conf_file]`

Usage: Full path to the VPN configuration file to be used for this installation.

7.6.2 TGBCONF_PASSWORD

Syntax: `TGBCONF_PASSWORD=[password]`

Usage: Password used to protect the VPN configuration entered as a parameter via `TGBCONF_PATH`.

7.7 TrustedConnect panel

This section is used to define the parameters of the TrustedConnect panel (user or GINA mode).

7.7.1 USEDIALERBYDEFAULT

Syntax: `USERDIALERBYDEFAULT=1`

Usage: The TrustedConnect Panel is used as user interface when this property is set to 1. The TrustedConnect Panel will start automatically when the Windows user session is started, unless the NOAUTORUN property is set to 1.

7.7.2 TNDSUFFIXES

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

Usage: This parameter defines the list of trusted DNS suffixes.

This list can be empty or contain several DNS suffixes.
The suffixes must be separated by a comma in the list, without any blank spaces.

7.7.3 TNDHTTPSERVERURL

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

Usage: This parameter defines the list of trusted server URLs.

The list of URLs can be empty: the VPN Client will then fall back to the list of DNS suffixes to determine whether the workstation is connected to the trusted network or not.
This list can contain several trusted server URLs. The VPN Client will then successively test all the URLs and all the certificates associated with each server until it finds one that is accessible and valid.
The URLs must be separated by a comma in the list, without any blank spaces.

There is no need to add the “https://” to an URL.

7.7.4 TNDHTTPSERVERPORT

Syntax: `TNDHTTPSERVERPORT=443`

Usage: This parameter defines the port to be used to reach trusted servers.

Only one port that will be used for all URLs can be configured.
If the parameter 1.1.1 TNDHTTPSERVERPORT is not configured, the VPN Client will use the port 443 by default.

7.7.5 TNDLATENCY

Syntax: `TNDLATENCY=3000`

Usage: The time required to take into account a new network interface varies from one system to the next. If it is too long, it may interfere with the TND mechanism, which may lead the VPN Client to attempt establishing a VPN connection even though the workstation is connected to the trusted network.
To avoid this issue, the TNDLATENCY property is used to delay the triggering of the TND mechanism.

It is expressed in milliseconds. If the default value needs to be changed, we recommend specifying a value greater than or equal to 3000 ms.
By default, the value is equal to 0 and the TND mechanism is started immediately, which is suitable in most cases.

7.7.6 AONITFPASSOVER

Syntax: `AONITFPASSOVER=HYBER-V`

Usage: Network interfaces can be excluded from Always On monitoring.
An interface is excluded using the “description” property (visible with ipconfig /all).

The value of this parameter must contain part or all of the “description” field of the network interface to be excluded. If the value only contains part of the description, then any interface whose “description” field contains the value defined will be excluded from monitoring.

You can also specify several network interfaces to exclude by specifying the parts of their respective descriptions separated by a comma.

Example: To exclude any interface whose description field contains the character string “Hyper-V”, use `AONITFPASSOVER=Hyper-V`.

7.7.7 DIALERMINIMIZE

Syntax: `DIALERMINIMIZE=5000`

Usage: Configure the time delay before the VPN Client's HMI is minimized, when the workstation has been detected as being connected to the trusted network (either physically or through the VPN tunnel).

This time delay is configured in milliseconds.
If the value is set to 0, the feature is disabled: the HMI is no longer automatically minimized.
If the time delay is not configured, the default time delay is 2000 ms (2 seconds).

7.7.8 DIALERDEFS

Syntax: `DIALERDEFS="01 00 00 00"`

Usage: In addition to the minimization time delay, the type of minimization can also be configured: the TrustedConnect Panel can be minimized to the taskbar or to the notification area (systray or system tray).
To minimize the TrustedConnect Panel to the taskbar, enter the value "01 00 00 00".
If the property is not specified, the TrustedConnect Panel is minimized to the notification area (systray or system tray) by default.
Reminder: The time delay and minimization type only apply to automatic minimization of the TrustedConnect Panel upon detection of a connection to the trusted network.

7.7.9 VPNLOGPURGE

Syntax: `VPNLOGPURGE=3`

Usage: This feature is used to configure the number of days log files are kept.
The value is expressed in number of days.
The default value is 10 days.
If the value is set to 0, the purging of log files is disabled.

7.7.10 TOKENOUTHANDLE

Syntax: `TOKENOUTHANDLE=30`

Usage: This parameter is used to configure the behavior of the TrustedConnect Panel when the token/smart card is removed from the reader while a VPN tunnel is open.

The following three modes are available for this event:

- Mode 1: The tunnel is closed immediately as soon as the token/smart card is removed (default behavior).
- Mode 2: The tunnel remains open for the configured time period.
- Mode 3: The tunnel remains open indefinitely.
  Note: In this mode, if the token/smart card is required to open the VPN tunnel, the next renegotiation will fail.

By default, if nothing has been configured, mode 1 is enabled.

TokenOutHandle=00 => tunnel is not closed when the token/smart card is removed (Mode 3)
TokenOutHandle=NN => time in seconds before the tunnel is closed once the token/smart card is removed (Mode 2)

7.7.11 GINABEHAVES

Syntax: `GINABEHAVES=01`

Usage: This parameter is used to make the TrustedConnect Panel visible in GINA mode (lock session user).

Note: The “Enable before Windows logon” field in the automation section of the configuration panel (refer to User Guide) does not apply to the TrustedConnect Panel. This parameter must therefore be used to use the GINA mode with the TrustedConnect Panel.

The default value is 0 (i.e. the TrustedConnect Panel is not visible in GINA mode).

7.8 Tokens and smart cards

7.8.1 SMARTCARDROAMING

Syntax: `SMARTCARDROAMING=01`

Usage: This parameter specifies the smart card reader to be used:

Undefined	Card reader configured in the VPN configuration Subject of the certificate in the VPN configuration
“01”	Card reader configured in the VPN configuration The subject of the certificate in the VPN configuration is not taken into account
“02”	Card reader configured in the VpnConf.ini file Subject of the certificate in the VPN configuration
“03”	Card reader configured in the VpnConf.ini file The subject of the certificate in the VPN configuration is not taken into account
“04”	1st card reader connected that contains a smart card Subject of the certificate in the VPN configuration
“05”	1st card reader connected that contains a smart card The subject of the certificate in the VPN configuration is not taken into account

7.8.2 PKCS11ONLY

Syntax: `PKCS11ONLY=01`

Usage: This parameter specifies the smart card/token access mode:

Undefined	The CNG mode (Cryptography API: Next Generation) is used (default value)
"01"	Forces the VPN Client to use the PKCS#11 mode

7.8.3 KEYUSAGE

Syntax: `KEYUSAGE=01`

Usage: This parameter specifies the type of certificate used: if it is specified, the software searches for an “Authentication” certificate. If this parameter is not specified, the certificate type is not checked.

7.8.4 NOCACERTREQ

Syntax: `NOCACERTREQ=01`

Usage: This parameter configures the VPN Client to manage various Client/Gateway certification authorities (CAs). It must be specified if the Client and Gateway certificates come from different CAs (this can also be done using the software interface).

7.8.5 PKICHECK

Syntax: `PKICHECK=01`

Usage: This parameter is used to specify the way in which the VPN gateway certificate is checked:

Undefined	The VPN Gateway certificate is not checked.
“00”	The VPN Gateway certificate is not checked.
“01”	The following characteristics of the VPN gateway certificate are checked: validity date, certificate chain, signature and CRL of each certificate in the certificate chain.
“02”	The following characteristics of the VPN gateway certificate are checked: validity date, certificate chain, signature of each certificate in the certificate chain (not the CRLs).
“03”	Same as “01”.

7.8.6 X509DIRECTORYSTRING

Syntax: `X509DIRECTORYSTRING=14`

Usage: This parameter specifies the expected identifier for Remote ID:

Undefined	Expected identifier type: teletexString
“14”	Expected identifier type: teletexString
“13”	Expected identifier type: printableString
“1C”	Expected identifier type: universalString
“0C”	Expected identifier type: utf8String
“1E”	Expected identifier type: bmpString

Note: As of version 6.85 of the software, the characters “0x” must no longer be prefixed to the value of the X509DirectoryString parameter.

7.8.7 MACHINESTORE

Syntax: `MACHINESTORE=01`

Usage: This parameter is used to enable the use of the machine’s certificate store instead of the user’s. If it is not defined, the user’s store will be used by default.

7.8.8 DNPATTERN

Syntax: `DNPATTERN=[text]`

Usage: This parameter is used to specify the user certificate to be used: when specified, the VPN Client searches for the certificate whose subject contains the "`[text]`" pattern on the token, smart card or, as of version 6.5x, in the Windows certificate store.
If this parameter is not specified, the VPN Client searches for the first certificate that meets the other characteristics configured.

7.9 General parameters

7.9.1 MENUITEM

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

Usage: Used to determine which items appear in the taskbar menu.
The value assigned to menu item is a bit field, in which every bit represents one item of the taskbar menu:
1 (1st bit)=Quit
2 (2nd bit)=Connection panel
4 (3rd bit)=Console
8 (4th bit)=Save and Apply (obsolete since version 5)
16 (5th bit)=Configuration panel
By default, all items are displayed: value = 31 (1F hexa).

Example: `MENUITEM=3`
Will only display the "Connection panel" and "Quit" items.

0	Does not display the taskbar 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.

7.9.2 NOAUTORUN

Syntax: `NOAUTORUN=1`

Usage: This property is used to not start the VPN Client (regardless of the mode: Connection Panel, TrustedConnect) when Windows is started. Default value 0 (automatic startup).

7.9.3 RESTRICTCONFADMIN

Syntax: `RESTRICTCONFADMIN=0`

Usage: Used to restrict access to the connection configuration panel to administrators only. By default, the configuration panel is only accessible with administrator privileges.

7.9.4 NOSPLITTUNELLING

Syntax: `NOSPLITTUNELLING=01`

Usage: This parameter disables the default route of the physical interface when the tunnel is established. Only applies to tunnels configured with “All traffic through the tunnel”.

7.9.5 NOSPLITDNS

Syntax: `NOSPLITDNS=01`

Usage: This parameter ensures that the DNSs of the virtual interface also apply to the physical interface when the tunnel is established. Only applies to tunnels configured with “All traffic through the tunnel”.

7.9.6 NOPINCODE

Syntax: `NOPINCODE=01`

Usage: This parameter is used to prevent a PIN code from being requested for tokens that do not require it. For example, Ercom's microSD is one such token.

7.9.7 PINTIMEOUT

Syntax: `PINTIMEOUT=120`

Usage: Specifies a timeout value in seconds that is used to automatically close the “Pin Code” entry window when the timeout has expired.

7.9.8 NOCFGPKTID

Syntax: `NOCFGPKTID=01`

Usage: This parameter configures IKEv1 so that it becomes compatible with the Cisco ASA routers for the Mode Config function (IKEv1 accepts the “truncated” Mode Config data exchange of Cisco ASA routers).

7.9.9 PWDUTF8

Syntax: `PWDUTF8=01`

Usage: This parameter encodes the X-Auth password in UTF8 prior to sending it to the gateway. For example, this allows for accents to be used in X-Auth passwords (IKEv1 only).

7.9.10 ROUTINGMODE

Syntax: `ROUTINGMODE=01`

Usage: This parameter is used to prevent local traffic coming from the physical interface from going through the tunnel. Only the traffic coming from the virtual interface will be allowed through.

7.9.11 PKCS1V15SCHEME

Syntax: `PKCS1V15SCHEME=02`

Usage: This parameter is used to configure the authentication method when the tunnel is established.

Undefined	Method 14 is implemented
“01”	HASH_MD5
“02”	HASH_SHA1 (Method 1)
“03”	HASH_SHA2_224
“04”	HASH_SHA2_256
“05”	HASH_SHA2_384
“06”	HASH_SHA2_512
“07”	HASH_MD4
“08”	HASH_MD5_SHA1

7.9.12 FORCELOCALTRAFFICTOTUNNEL

Syntax: `FORCELOCALTRAFFICTOTUNNEL=01`

Usage: In “all through tunnel” mode, this parameter is used to route the local traffic coming from the physical interface through the tunnel. If this parameter is not included, by default, the mode will not be enabled.

Undefined	Mode disabled
“00”	Mode disabled
“01”	Mode enabled

7.9.13 IKESTART

Syntax: `IKESTART=1`

Usage: This parameter is used to start the IKE service independently of the software’s interface. If this parameter is not included, by default, the mode will not be enabled.

Undefined	The mode is not enabled
“1”	The mode is enabled
Other value	The mode is not enabled

7.9.14 SIGNFILE

Syntax: `SIGNFILE=1`

Usage: Used to force the integrity hash check for the VPN configuration file.
The default value is 0.

7.9.15 SYSTEMLOGOUTPUT

Syntax: `SYSTEMLOGOUTOUT=7`

Usage: This parameter is used to select the output of administrator logs. The outputs can be combined, e.g. use the value 7 to combine the 3 outputs.

0	No system logs
1	Log files
2	Syslog server
4	Windows event observer

7.9.16 SYSTEMLOGSYSLOGSERVER

Syntax: `SYSTEMLOSERVER=syslogserver.company.com`

Usage: This parameter is used to specify the machine's IP address or name to syslog servers.

7.9.17 SYSTEMLOGSYSLOGPORT

Syntax: `SYSTEMLOGSYSLOGPORT=5514`

Usage: This parameter is used to specify the port of the machine for the syslog servers. The default port is 514.

8 Automated actions in the VPN Client software

8.1 Batch/script to open or close a tunnel

The Windows Enterprise VPN Client allows you to open or close a tunnel using the following command lines, which can also be used in a script:

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

The Tunnel Name consists of the following:

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

A tunnel can also be opened or closed using a script, by following the steps below:

1/ Create a VPN security policy (VPN Configuration) with the “Automatically open this tunnel when VPN Client starts” option checked.
2/ Export the VPN security policy (VPN Configuration) to a file (e.g. “MyTunnel.tgb”).
3/ Create the script with the following command line: vpnconf.exe /import:MyTunnel.tgb.

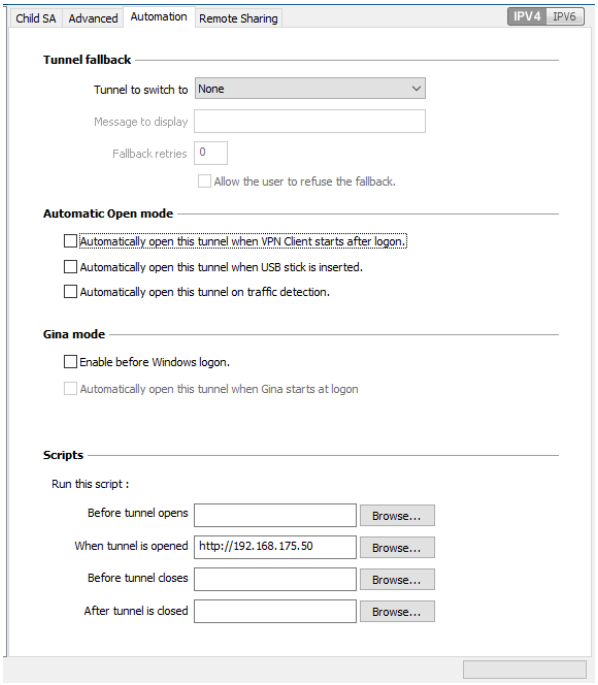
This script starts the Windows Enterprise VPN Client while importing the “MyTunnel.tgb” VPN security policy (VPN Configuration), and will automatically open the VPN tunnel.
In order to close the tunnel, use the vpnconf.exe /stop command line, which will close the VPN tunnel that has been opened prior to closing the software.

8.2 Automatically open a web page when the tunnel opens

1/ Create a VPN security policy (VPN Configuration).

2/ Open the “Automation” tab and enter the URL of the web page to be opened (e.g. on the company network) in the “Scripts / When the tunnel is opened” field .

3/ Open the tunnel: The specified web page will be automatically opened when the tunnel is established.



9 VpnSetup.ini file

9.1 Introduction

The VpnSetup.ini file is used to configure the installation of the Windows Enterprise VPN Client from a file, rather than using MSI command line properties.

Caution: Due to Microsoft MSI installer constraints, as opposed to previous versions of the software, the VpnSetup.ini file may no longer be located in the same directory as the installer, but should be in the C:\Windows folder.

The VpnSetup.ini file is used to define the following parameters:

- Software activation parameters
- Parameters of the TrustedConnect Panel
- PKI parameters for token, smart card reader and certificate management
- General operating parameters
- System log parameters
- Other parameters

The names of the parameters for the VpnSetup.ini file are identical to those of the msiexec installer's properties (see section Parameters of the MSI installer), the only difference being that they are not case-sensitive (no difference is made between lowercase and uppercase characters).

It can be edited using a standard text editor (e.g. Notepad). Just like any other "ini" file, it is organized into sections. The parameters must be entered in the appropriate section, as specified below.

Note: The MSI installer's installation and VPN security policy parameters have no equivalent in the VpnSetup.ini file.

9.2 [Activation] section

The [Activation] section uses the following parameters:

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

9.3 [Dialer] section

The [Dialer] section uses the following parameters:

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

- DialerDefs
- VpnLogPurge
- TokenOutHandle
- GinaBehaves

9.4 [PKIOptions] section

The parameters defined in the [PKIOptions] section are used to specify how the software should use smart cards, tokens, and certificates:

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

9.5 [AddRegKey] section

The [AddRegKey] section is used to define the general operating parameters:

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

9.6 [Config] section

The [Config] section uses the following parameter:

- SignFile

9.7 [Logs] section

The [Logs] section is used to define options for system logs: This section uses the following parameters:

- SystemLogOutput
- SystemLogSyslogServer
- SystemLogSyslogPort

9.8 Example of a vpnsetup.ini file

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

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


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

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

[Config]
SignFile=1

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

10 Contact

10.1 Information

All the information on TheGreenBow products is available on the following websites:
English: www.thegreenbow.com
French: www.thegreenbow.fr

10.2 Sales

Phone contact: +33.1.43.12.39.30
Email contact: sales@thegreenbow.com

10.3 Support

There are several pages related to the software's technical support on our websites:

Support

English: http://www.thegreenbow.com/support.html
French: http://www.thegreenbow.fr/support.html

Online help

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

FAQ

English: http://www.thegreenbow.com/vpn_faq.html
French: http://www.thegreenbow.fr/vpn_faq.html

Contact

Technical support can be reached using the forms available on our website or directly via email at the following address:
support@thegreenbow.com

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software