THEGREENBOW

www.thegreenbow.com

Windows Enterprise VPN Client 6.87

Administrator's Guide

Latest update: 17 February 2022
Document: 20220217_AG_VPE_6.8_EN_1.6

Table of contents

1 Overview

1.1 Introduction

This guide is intended for administrators of the Windows Enterprise VPN Client.
It contains all the information required to implement and configure the software so that secure VPN tunnels can be opened.

A complementary document dedicated to the software's deployment, called "Deployment Guide", is also available on TheGreenBow's website.

1.2 Important information

1.2.1 Encrypted configuration files

VPN configuration files from versions of the Windows Standard VPN Client prior to 6.8 cannot be imported into the Configuration Panel.

During a software update, the installer will convert the existing configuration before it automatically imports the file into the Configuration Panel.

1.2.2 Check Gateway Certificate

By default, the gateway certificate will be checked each time a tunnel is opened. It may be necessary to import the complete chain of certification authorities (CA) to authenticate the gateway, either into the Windows store or into the VPN configuration file.

You can change this default behavior, though we do not recommend doing so (Options menu -> PKI Options).

1.2.3 End of support for "weak" algorithms

For security reasons, this version no longer supports the following algorithms: DES, 3DES, MD-5, SHA-1, DH 1-2, DH 5. If a previous configuration contains one of these algorithms, the installer will convert them to "auto" (automatic negotiation with the gateway).

If the gateway only supports this type of algorithm, you will not be able to establish a connection with this version of the VPN client.

1.3 What's new in release 6.8

1.3.1 TrustedConnect interface

- New TrustedConnect user interface with a simple and intuitive design
- Trusted Network Detection (TND) feature that allows you to automatically open a tunnel if the workstation is outside the trusted network, based on the DNS suffixes and on beacon identification
- Always-On feature which ensures that the connection remains secure whenever the network interface changes, for example, between Ethernet, Wi-Fi, and 4G

1.3.2 Installation, configuration, and deployment

- Use of a Microsoft Windows Installer (MSI) to facilitate deployment and software updates using GPOs, offering numerous installation options to meet all kinds of integration requirements (graphical interface, certificates, smart cards, tokens, etc.)
- The entire software is compiled in 64-bit mode for Windows 10 & 11 for optimized performance and security
- Access to the VPN configuration can be restricted to Windows administrators

1.3.3 Cryptography

- Support for RFC 4304 Extended Sequence Numbers (ESNs) and RFC 6023 (Childless IKE Initiation) for enhanced security
- Support for the following digital signature authentication algorithms for strong certificate authentication:
  - Method 9: ECDSA "secp256r1" with SHA-256 on the P-256 curve [RFC4754]
  - Method 10: ECDSA "secp384r1" with SHA-384 on the P-384 curve [RFC4754]
  - Method 11: ECDSA "secp521r1" with SHA-512 on the P-521 curve [RFC4754]
  - Method 14: Digital Signature Authentication PKCS1-v1.5 [RFC7427]
- The following algorithms, which are known to be vulnerable, are no longer supported in version 6.8 and higher: DES, 3DES, SHA, DH 1-2, DH 5
- Reinforced encryption and integrity of the VPN configuration

1.3.4 Smart cards and tokens

- Support for the Microsoft CNG API (Cryptography API: Next Generation) allows for the latest generation of smart cards and tokens to be used
- Microsoft has deprecated the Cryptographic Service Providers (CSP) API, it is no longer supported for IKEv2 as of version 6.8

1.3.5 SSL/TLS

- Support for Lz4 compression

2 Installing the software

2.1 Introduction

The Windows Enterprise VPN Client is installed by executing the program that can be downloaded from TheGreenBow's website.

The default installation procedure, run by double-clicking the icon of the downloaded program, opens a window that allows you to customize the installation.

The installation of the software can be customized using a set of command-line options and VPN configuration files. These options and features are detailed in the document entitled "Deployment Guide" available on TheGreenBow's website.

☞ Refer to section 2.2 Installation procedure.

2.1.1 Installation conditions

The Windows Enterprise VPN Client is available for the 64-bit version of Windows 10 & 11.

The minimum system requirements to install the software are as follows:

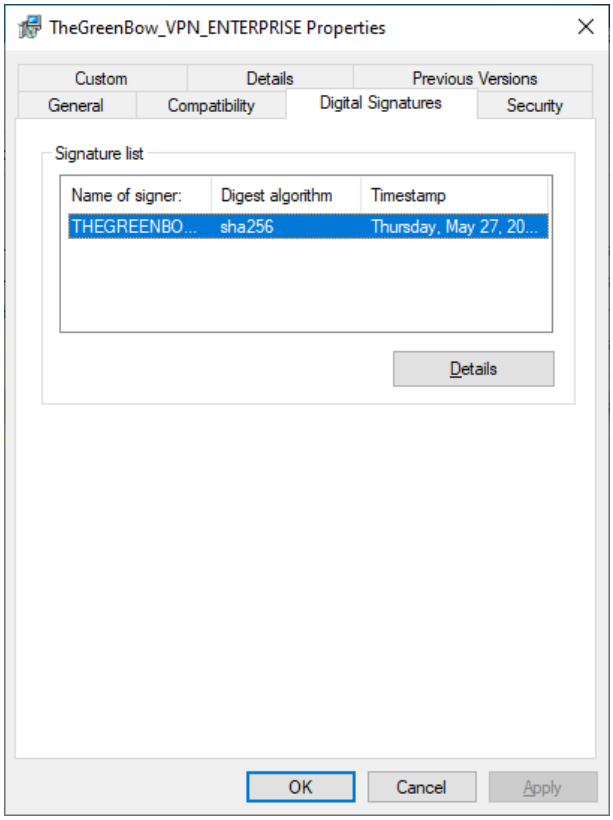
- Processor: 1 gigahertz (GHz) or faster processor
- RAM: 2 GB
- Hard disk space available: 40 MB

When the software is not installed from an administrator account, a window opens, prompting you for the username and password of an administrator account on the machine.

2.1.2 Digital signature and version

The installer software for the Windows Enterprise VPN Client is signed with a certificate issued for "THEGREENBOW SA". This allows the person performing the installation or the user to verify the integrity of the installation program at any time.

You can verify the authenticity of the software by displaying the program's properties (right-click MSI installer) and then selecting the "Digital signatures" tab.



Users can check the version number of the Windows Enterprise VPN Client in the "About…" window of the software.

2.1.3 Vulnerabilities

Moreover, users of the Windows Enterprise VPN Client who send an e-mail with their contact details to referent@thegreenbow.com will be warned of any vulnerabilities identified in the software and receive information on the means to remedy them (new version, update, available patches, workarounds, etc.).

See also our security recommendations.

2.2 Installation procedure

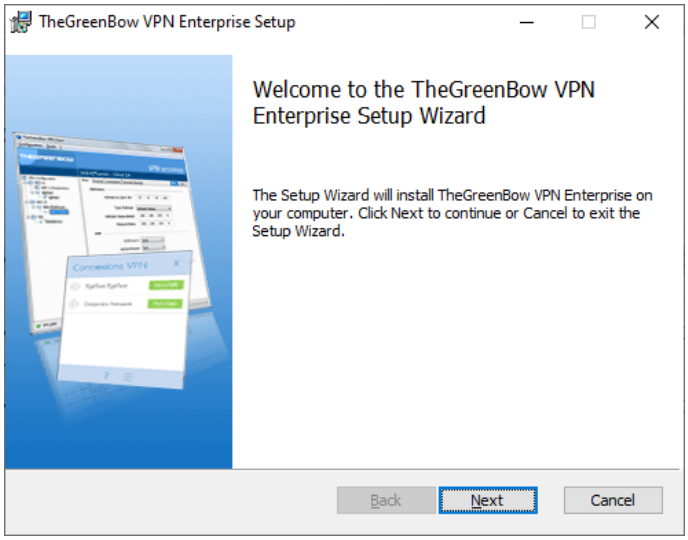
Once you have downloaded the Windows Enterprise VPN Client installation program and verified its authenticity (see section 2.1.2 Digital signature and version above), you can proceed with its installation by following the steps described below.

You can only update the software if your subscription is still valid (see section 4.1 How to get an update).

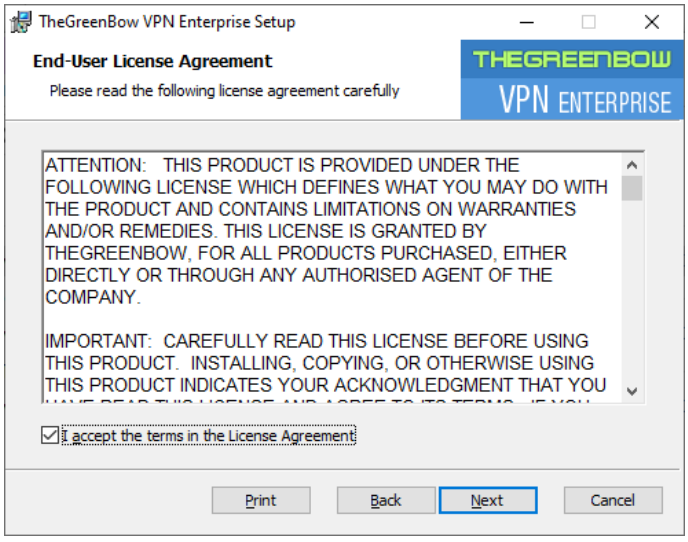
The installation procedure is the same whether it is an initial installation or an update (see chapter 4 Updating the software). When performing an update, the software settings, the existing VPN configuration, and the license are preserved.

If you want to perform a silent installation, pass specific parameters during installation or perform a large-scale deployment, refer to the "Deployment Guide".

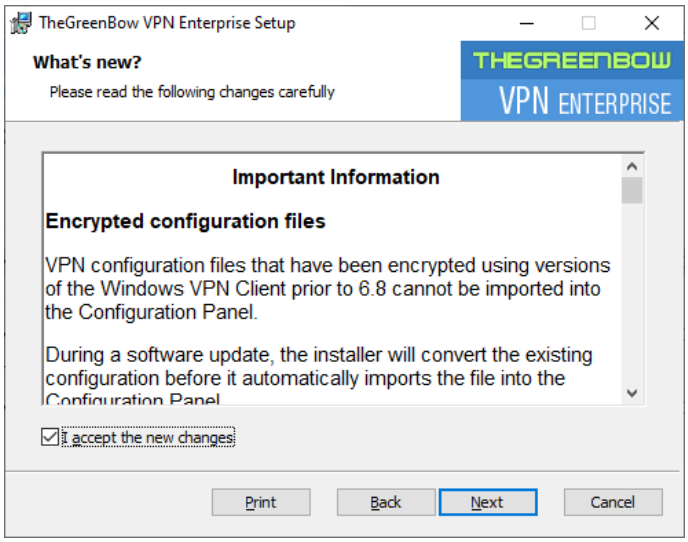
1/ Double-click the installation program you downloaded. The following window is displayed:



2/ Click "Next". The following window is displayed:



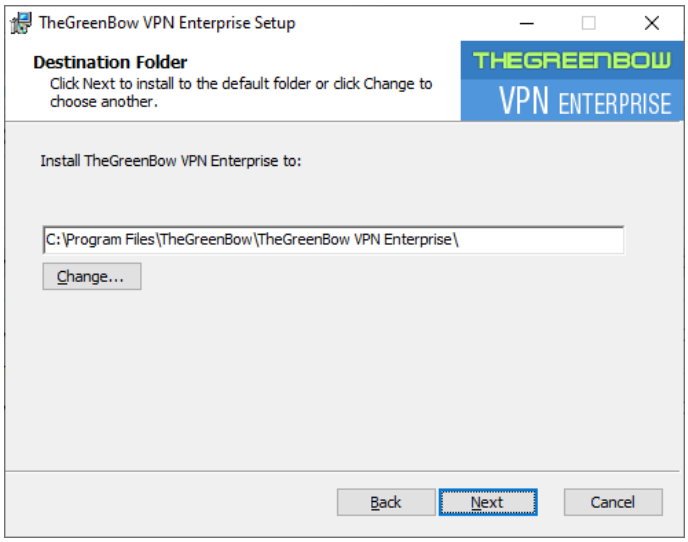
3/ Read the End User License Agreement (EULA) carefully. If you accept all the terms of the agreement, select the "I accept the terms of the license agreement" checkbox, and then click "Next". Otherwise, you will not be able to continue installing the Windows Enterprise VPN Client. The following window is displayed:



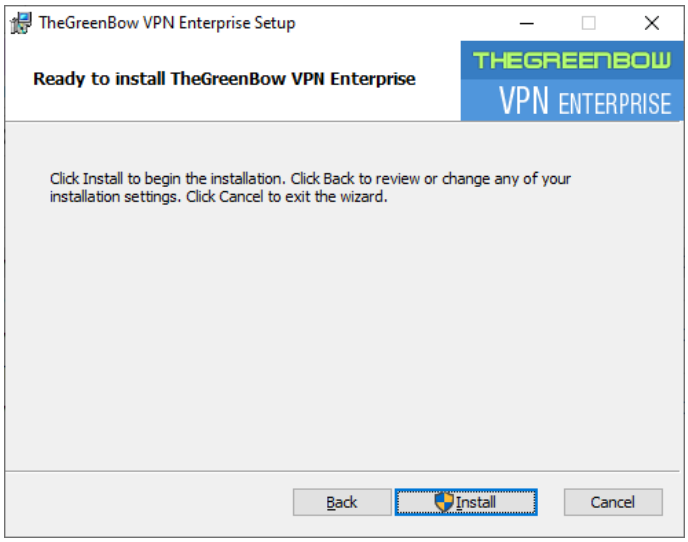
4/ Carefully read the information about what's new and the note about how the existing VPN configuration will be converted during an update.

⚠ Once the installation is complete, you will not be able to revert to an earlier version of the software without manual intervention. If in doubt, back up your VPN configuration to a separate folder or to a removable storage medium.

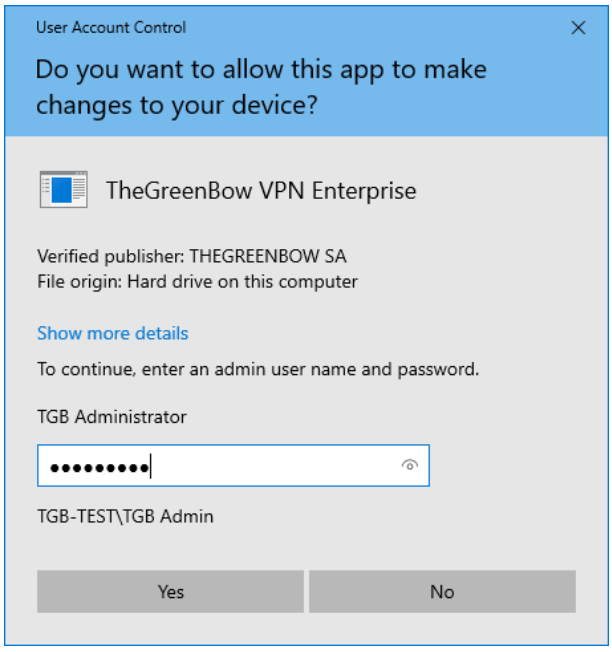
If you accept all the terms of the agreement, select the "I accept the new changes" checkbox, and then click "Next". The following window is displayed:



5/ If you want to install the Windows Enterprise VPN Client in a specific directory, click "Change…" and select the desired directory. Otherwise, you can keep the default directory. Then, click « Next ». The following window is displayed:



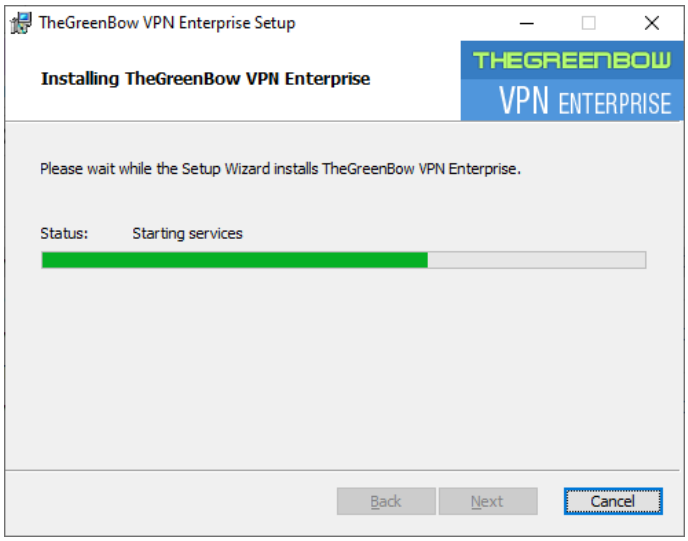
6/ The program is ready to install. If you want to go back to check or change your installation settings, click "Back". Otherwise, click "Install". If you are installing from an account that does not have administrator rights, the following window is displayed:



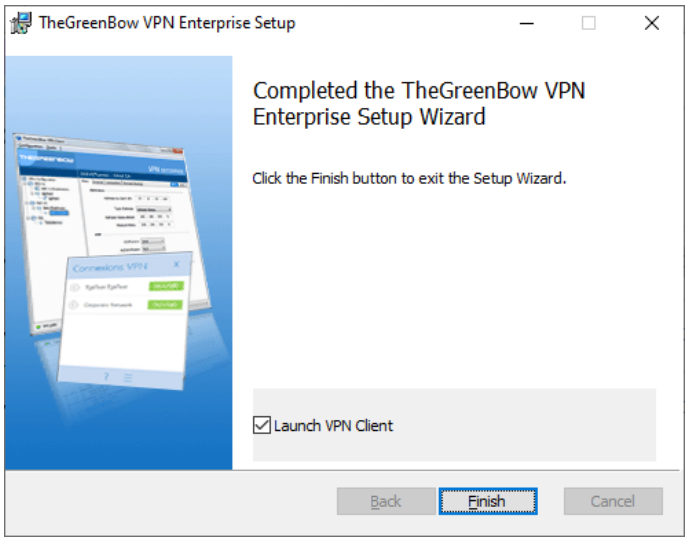
7/ To proceed with the installation, you must enter an administrator name and password to allow the installation program to make changes to your computer. Otherwise, the software will not be installed.

If you are installing from an administrator account, you do not need to enter a password. Simply confirm that you allow the app to make changes to your device.

8/ Installation begins and the following window is displayed:



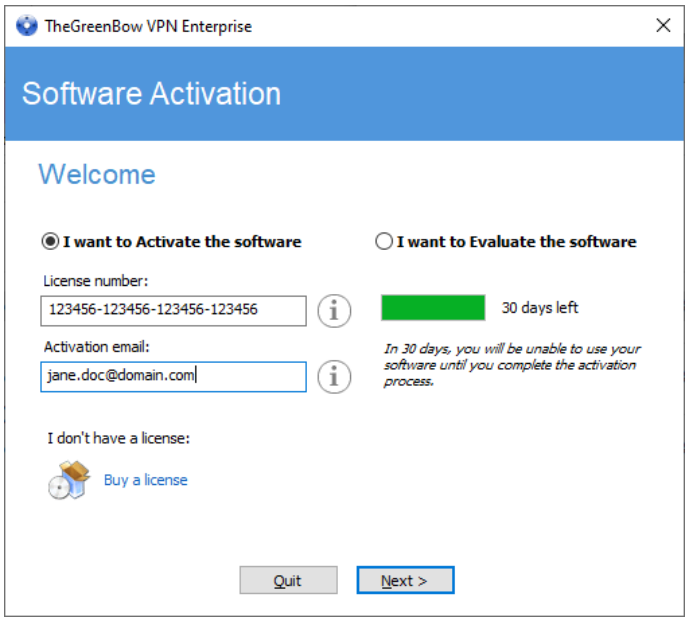
9/ Wait for the installation of the Windows Enterprise VPN Client including all its components to complete. If installation has succeeded, the following window is displayed:



10/ If you do not want to launch the VPN Client immediately, uncheck the corresponding box. To exit the setup wizard, click "Finish".

If you have performed an update, the software is launched directly in the taskbar. You can test your installation by opening the test tunnel (see section 6.3 Opening a test VPN tunnel from the Connection Panel).

Otherwise, the activation screen is displayed:



11/ The Windows Enterprise VPN Client is now installed on your workstation.

If you already own a license for the Windows Enterprise VPN Client:

- Select "I want to Activate the software"
- Enter the license number and activation email
- Then, click "Next"

For further details on the activation procedure, refer to chapter 3 Activation.

If you want to try the Windows Enterprise VPN Client:

- Select "I want to Evaluate the software"
- Then, click "Next"

You will then be able to use the software for a 30-day trial period. For further details on the trial period, refer to section 2.4 Trial period.

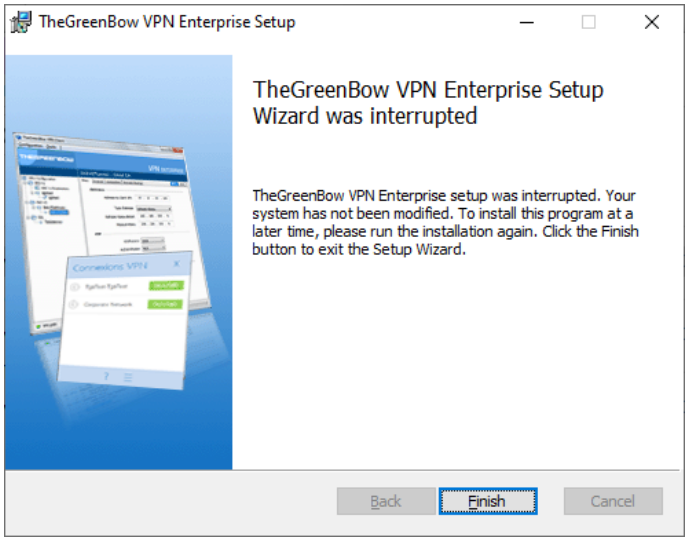
If you do not have a license and want to buy one, click "Buy a license". TheGreenBow online store is displayed in a browser window. Here, you can buy one or several licenses. For further details on the activation procedure, refer to chapter 3 Activation.

You are now ready to use the software. You can continue with the following steps:

- To start using the Windows Enterprise VPN Client immediately, refer to chapter 6 Getting started with the software.
- To use the configuration wizard to quickly create a VPN connection, refer to chapter 7 Configuration wizard.
- To import a TheGreenBow VPN configuration compatible with this version of the software, refer to section 12.1 Importing a VPN configuration.
- For a detailed presentation of the available interfaces, refer to chapters 8 Connection Panel, 9 Configuration Panel, and 10 TrustedConnect Panel.
- For a comprehensive explanation of all VPN tunnel configuration options, refer to chapter 13 Configuring a VPN tunnel.
- To uninstall the Windows Enterprise VPN Client, refer to chapter 5 Uninstalling the software.

2.3 Canceling installation

If you cancel the setup wizard before clicking the "Install" button, the following window is displayed:

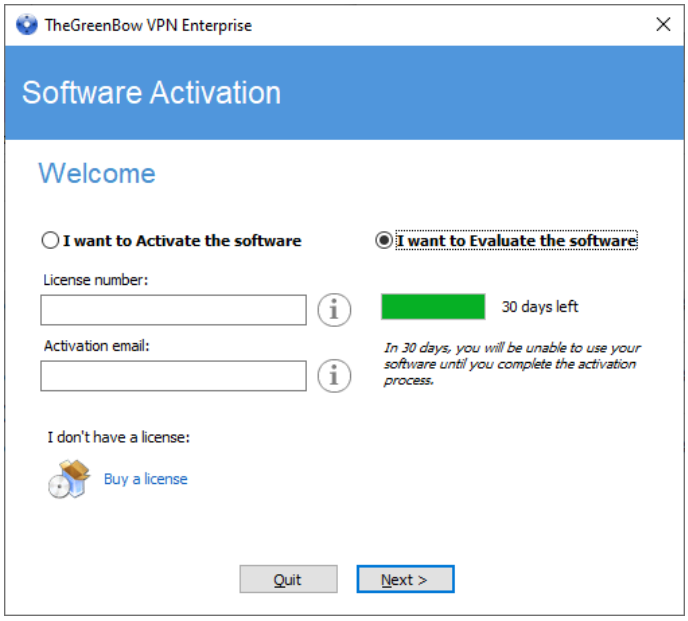


Your system has not been modified and you can resume installation at a later time.

2.4 Trial period

The first time the software is installed on a workstation, if no license key is provided to the installer, the VPN Client will enter a 30-day trial period. During this trial period, the VPN Client is fully operational, and all functions are unlocked.

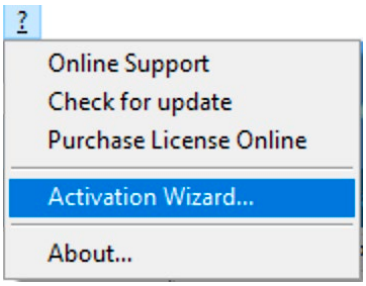
The activation window will be displayed every time the software is started during the trial period. It shows the number of days remaining in the trial period.



Select "I want to Evaluate the software", then click "Next >" to run the software.

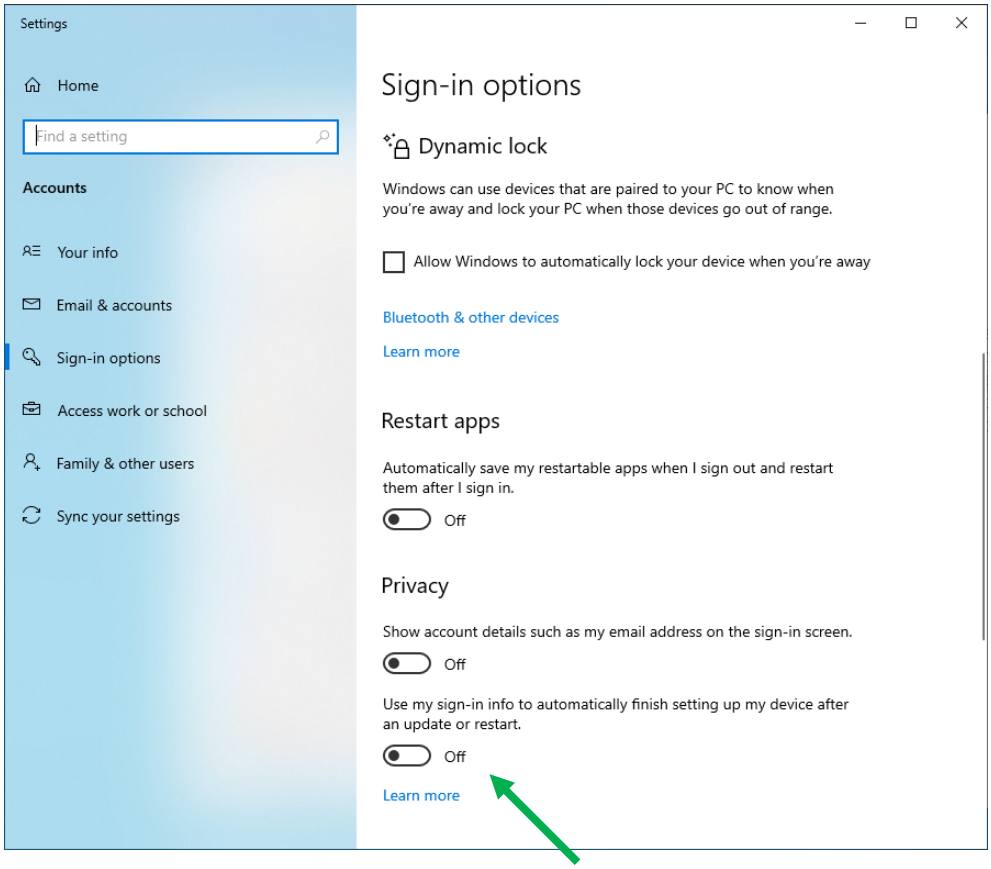
During the trial period, the "About…" window will display the number of days remaining until the trial ends.

During the trial period, the activation window can be accessed at any time using the "? > Activation Wizard…" menu item in the main interface (Configuration Panel).



2.5 Configuring Windows

Once you have completed installation, make sure the Windows privacy option "Use my sign-in info to automatically finish setting up my device after an update or restart", found under the "Sign-in options" in the Windows Settings, is disabled, as shown in the screenshot of the Windows 10 Settings below:



The same option is available in the Windows 11 Settings.

3 Activation

If the software has not been activated during its silent installation (refer to the "Deployment Guide"), the VPN Client must be activated to continue to work beyond the trial period.

The activation procedure can be accessed every time the software is launched or using the "? > Activation Wizard…" menu item in the main interface.

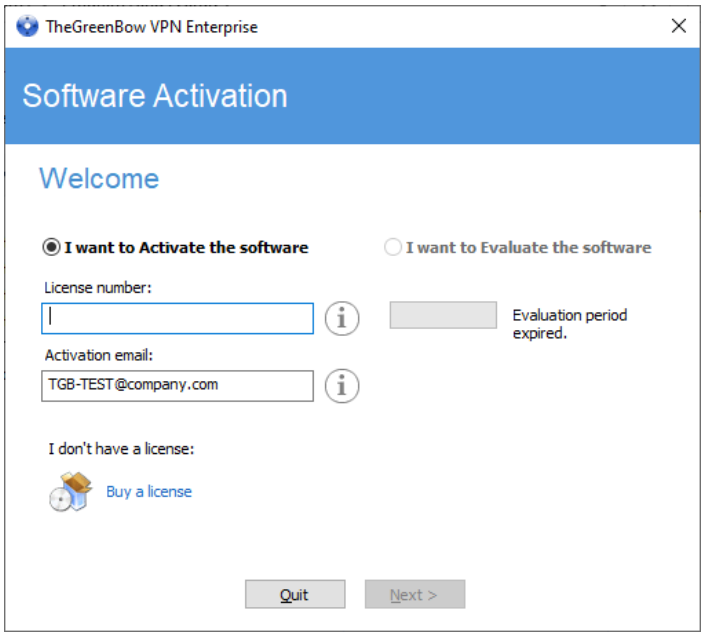
3.1 Step 1

If you do not yet have a license, click on "Buy a license". The TheGreenBow online store is displayed in a browser window. Follow the instructions to buy one or several licenses.

In the "License number" field, enter the license number you received by email.

The license number can be copy-pasted directly from the purchase confirmation email into this field.
The license number consists of the characters [0..9] and [A..F], possibly grouped 6 by 6 and separated by hyphens.

In the "Activation email" field, enter the email address used to identify your activation. This information is used for recovering the activation information if it is lost.



The "Activation email" field is filled by default with the username of the workstation on which the software is installed (as follows: "username@company.com"). This allows administrators of a "master" software license to individually identify all activated workstations. It allows them to manage software activations and deactivations in a deterministic way.

3.2 Step 2

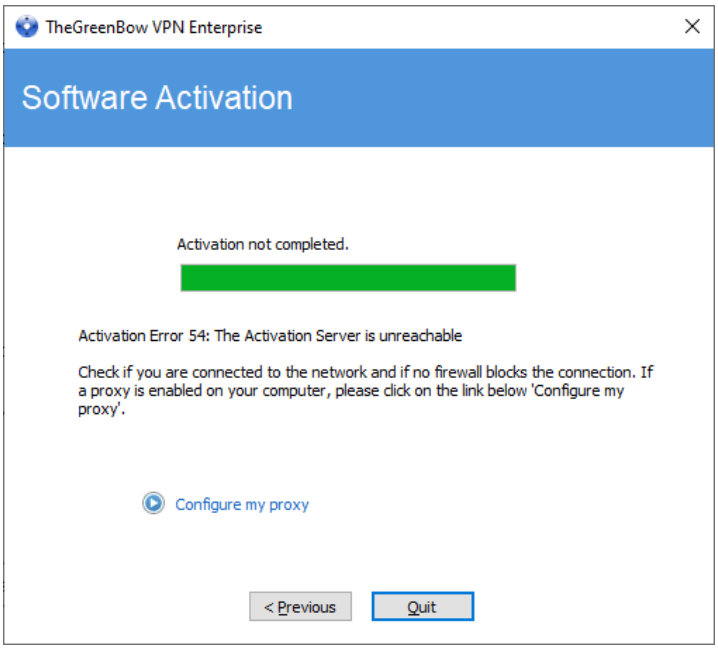
Click "Next >". The online activation process will run automatically.

Once the activation has been carried out successfully, click "Run" to run the software.

The software activation is linked to the workstation on which the software has been installed. Consequently, a license number allowing a single activation cannot be reused on another workstation once it is activated.
Conversely, a license number activation can be canceled by simply uninstalling the software.

3.3 Activation errors

Software activation may fail for various reasons. The error is always displayed in the activation window. It is sometimes followed by a link that displays more information about the error or suggests actions to solve the problem.



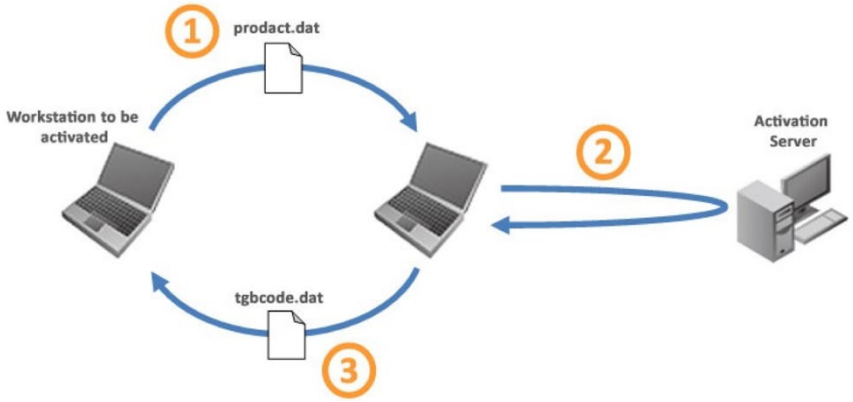
TheGreenBow lists all activation errors and procedures for solving activation issues on its website.

The following are the most common activation errors:

#	Meaning	Troubleshooting
31	Wrong license number	Check license number
33	The license number is already activated on a different workstation	Uninstall the software on the workstation with the activated license or contact TheGreenBow's Sales department
53, 54	Communication with the activation server is impossible	Ensure that the workstation is connected to the internet. Check that communication is not blocked by a firewall or proxy. Configure the firewall to let the communication through or the proxy to reroute it properly.

3.4 Manual activation

When activation fails because of a communication issue with the activation server, the software can be activated manually on TheGreenBow's website. The procedure is as follows:

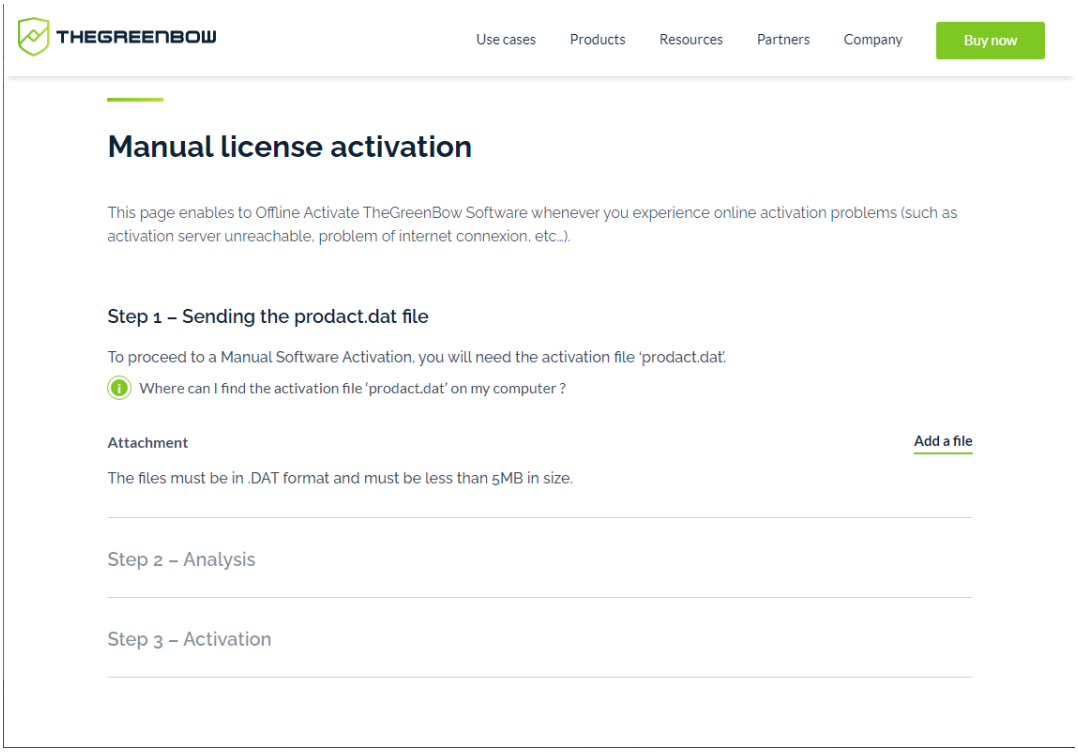


1	`prodact.dat` file	Retrieve the `prodact.dat` file from the "My Documents" directory in Windows on the workstation that you want to activate. (1)
2	Activation	On a workstation that is connected to the activation server (2), open the manual activation page (3), and post the `prodact.dat` file. Let the server automatically create the `tgbcode` before downloading it.
3	`tgbcode` file	Copy the `tgbcode` file to the "My Documents" directory in Windows on the workstation that you want to activate. Start the software; it will be activated.

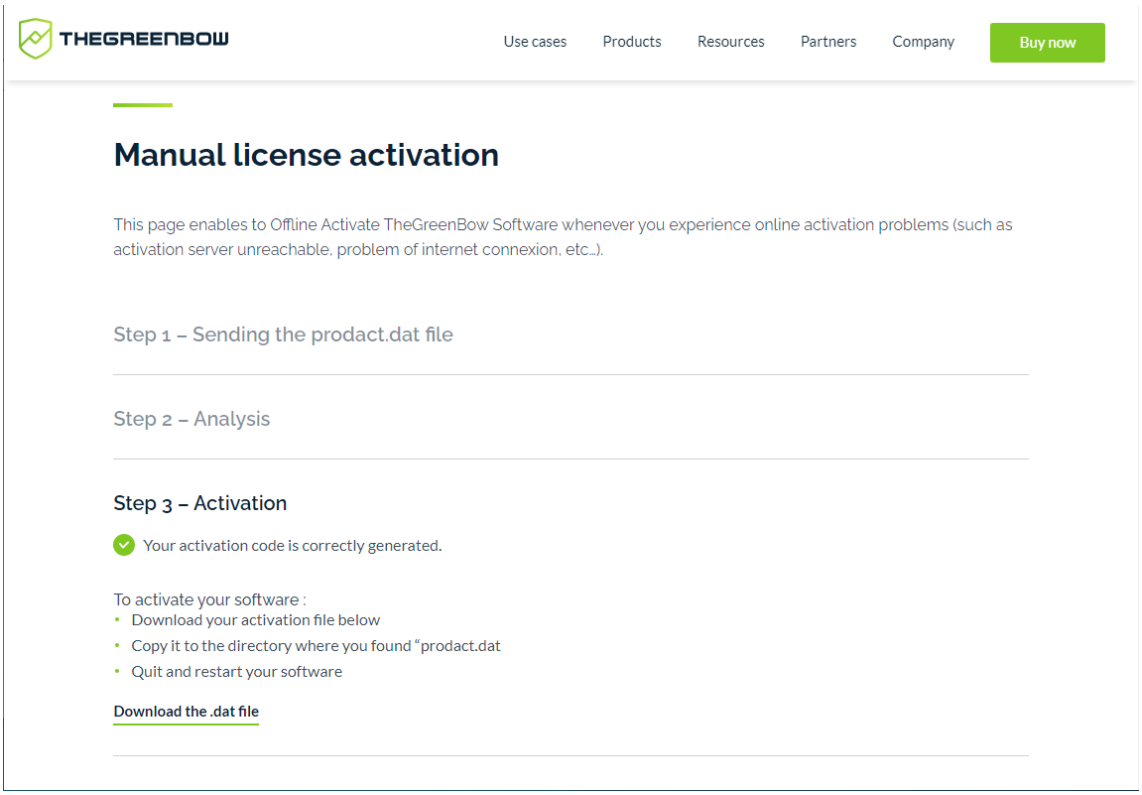
(1) The `prodact.dat` file is a text file that contains the workstation information used for the activation. If this file cannot be found in the "My Documents" directory, carry out the software activation steps on the workstation. This will generate the file even if activation fails.
(2) The activation server is the TheGreenBow server, which can be accessed on the internet.
(3) Refer to the detailed procedure below.

To proceed with manual activation, follow the steps below:

1/ On a workstation connected to TheGreenBow's website, open the following webpage:
https://www.thegreenbow.com/en/support/license-management/manual-license-activation/



2/ Click "Add a file" and open the `prodact.dat` file created on the workstation that you want to activate.
3/ Click "Submit". The activation server will check the validity of the information contained in the `prodact.dat` file.
4/ Click "Proceed". The activation server will provide a link to download a file containing the activation code for the workstation to be activated.



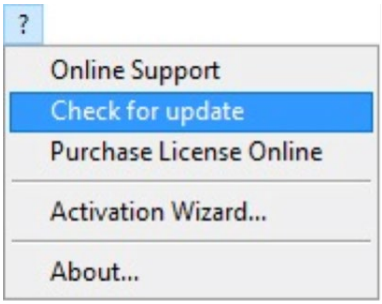
The file name has the following format: `tgbcode_[date]_[code].dat` (e.g. `tgbcode__20210615_1029.dat`).

3.5 License and activated software

Once the software is activated, the license and email used for activation can be viewed in the "About…" window of the software.

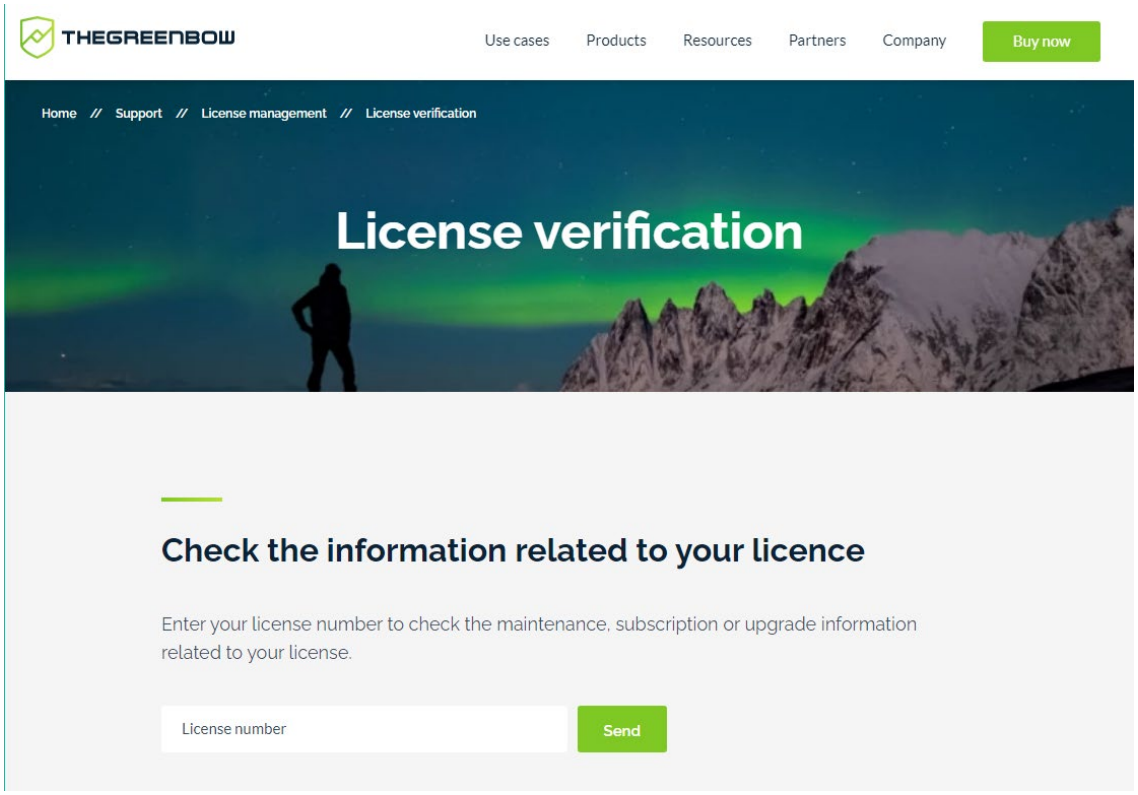
4 Updating the software

You can also check whether an update is available for the software at any time using the main interface menu "? > Check for update".



This menu opens the web page used to check for updates. This page will display whether an update is available and can be activated, depending on the type of license you have purchased and the type of maintenance or subscription you have chosen. To get this information, you must enter the license number in the corresponding field on the verification page, which can also be viewed directly under the following link: https://www.thegreenbow.com/en/support/license-management/checking-license/.

Example:



4.1 How to get an update

Software updates are provided according to the following rules:

Ongoing subscription (1)	All updates can be installed
No subscription	The software cannot be used or updated

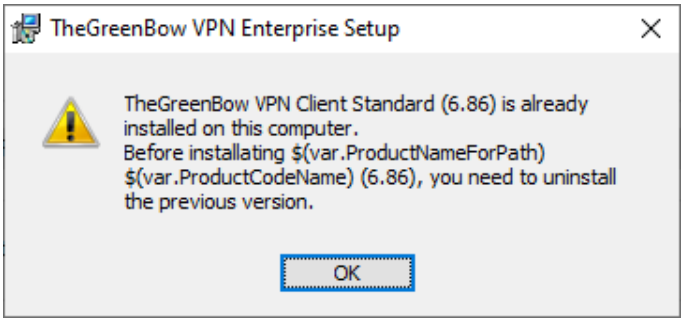
(1) The subscription starts on the date of purchase of the software.

⚠ Performing an update from a Standard edition to an Enterprise edition and vice versa is not allowed. However, you can update from any previous version of the Enterprise VPN Client (including Premium and Certified).

4.2 Update procedure

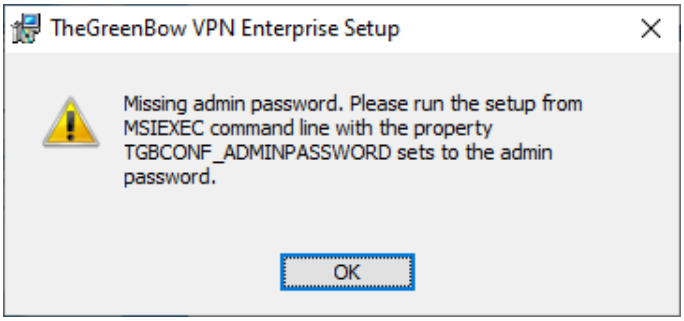
Updating the Windows Enterprise VPN Client allows you to upgrade to a newer version of the software while preserving the settings, the VPN configuration, and the license. It is performed in the same way as a normal installation (see section 2.2 Installation procedure) except in the following two cases:

1/ If the license of the installed product is not compatible with the Windows Enterprise VPN Client 6.8, updating will not be possible and the following screen is displayed:



In this case, you will need to uninstall the previous version of the software before you install the new one.

2/ If access to the Configuration Panel is protected by a password on the version that is already installed, the update cannot be performed using the graphical interface of the installation program. In this case, the following screen is displayed:



Password protection for access to the Configuration Panel has been replaced in version 6.8 of the Windows Enterprise VPN Client by a more secure mechanism. It consists in limiting access to the Configuration Panel to Windows administrators only. This option is enabled by default but can be disabled as described in section 24.1 Displaying/hiding the interface, check the "Restrict access to Configuration Panel to administrator" option.

You can either delete the password protecting access to the Configuration Panel, then proceed with the update, or perform the update in the command line using the `TGBCONF_ADMINPASSWORD` property (refer to the "Deployment Guide").

4.3 Updating the VPN configuration

The VPN configuration is automatically backed up and restored during an update.

If access to the Configuration Panel is password-protected, you must enter the password during the update to authorize configuration restoral.

4.4 Automation

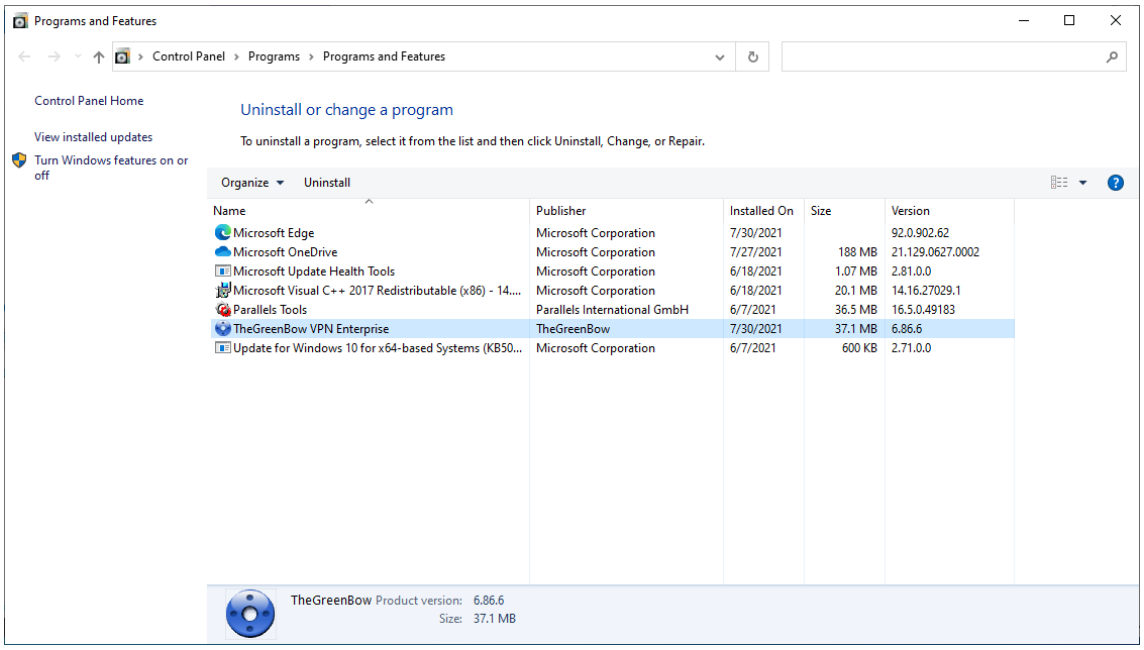
The way an update is carried out can be customized by a series of command-line options or an initialization file.

These options are described in the document entitled "Deployment Guide".

5 Uninstalling the software

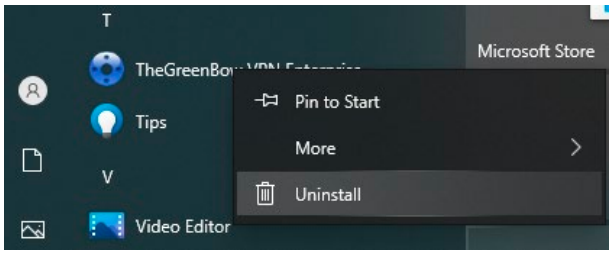
To uninstall the VPN Client, proceed as follows:

1/ Open the Windows Control Panel.
2/ Select « Uninstall a program ».
3/ Select "TheGreenBow VPN Enterprise" in the list of programs.
4/ Click "Uninstall" and follow the instructions to uninstall the program.



OR

1/ Open the Windows "Start" menu.
2/ Right-click the "TheGreenBow VPN Enterprise" program, then select "Uninstall".



3/ The Windows Control Panel is displayed. Select "TheGreenBow VPN Enterprise" in the list of programs.
4/ Click "Uninstall" and follow the instructions to uninstall the program.

Administrator privileges are required to install or uninstall the program on the workstation.

6 Getting started with the software

6.1 Introduction

The Windows Enterprise VPN Client graphical interface allows you to perform the following actions:

1/ Configure the software (startup mode, language, access control, etc.)
2/ Manage VPN tunnel configurations, certificates, imports, exports, etc.
3/ Use VPN tunnels (open, close, identify incidents, etc.)
4/ Switch to TrustedConnect mode (automatically open a tunnel when no trusted network is detected)

The graphical interface includes the following elements:

- The Connection Panel (list of VPN tunnels to open)
- The Configuration Panel, which can be displayed from the Connection Panel or using the icon in the taskbar and consists of the following items:
  - A set of menus for VPN configuration and software management
  - The VPN tunnel tree
  - VPN tunnel configuration tabs
  - A status bar
- The TrustedConnect Panel to use the Always-On and TND features (specific executable file)
- An icon on the taskbar and the associated menu, which is different for the TrustedConnect Panel and for the Connection/Configuration Panel

6.2 Starting the software

Once the installation or update is complete, if you have not unchecked the "Launch VPN Client" box and you have not activated the software, the activation window is displayed (see chapter 3 Activation). When the software has been activated or if you choose to try it out, the Windows Enterprise VPN Client will start minimized and the TheGreenBow VPN Enterprise icon will appear in the taskbar. The taskbar icon is described in detail in the paragraph entitled Taskbar icon below.

If you have unchecked the "Launch VPN Client" checkbox at the end of the installation or update procedure, or if you want to use the test tunnel after having installed or updated the software, to start the Windows Enterprise VPN Client, you can either double-click the corresponding desktop icon or open the Windows "Start" menu and then select the program in the list.

Starting the VPN Client using the shortcut on the desktop

During the installation of the software, a shortcut to run the application is created on the Windows desktop.

The Windows Enterprise VPN Client can be started directly by double-clicking on this icon.

The VPN Client will start minimized and the TheGreenBow VPN Enterprise icon will appear in the taskbar (see paragraph entitled Taskbar icon below).

Starting the VPN Client using the Windows Start menu

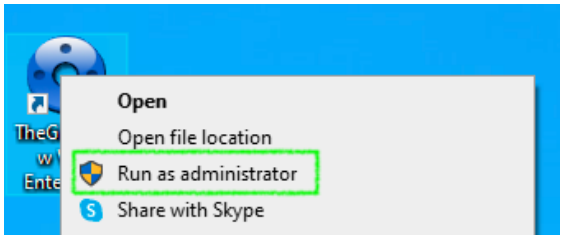
Once the installation is complete, you can start the Windows Enterprise VPN Client by clicking the program name in the Windows "Start" menu.

The VPN Client will start minimized and the TheGreenBow VPN Enterprise icon will appear in the taskbar (see paragraph entitled Taskbar icon below).

Starting the VPN Client as administrator

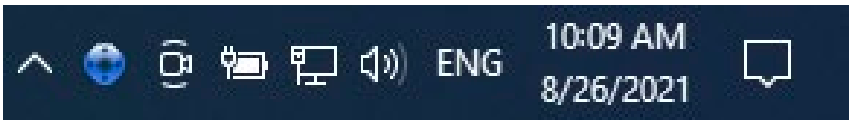
By default, access to the Configuration Panel is restricted to Windows administrators only.

To start the VPN Client in administrator mode and be able to access the Configuration Panel, right-click the TheGreenBow VPN Enterprise icon and then select "Run as administrator".



Taskbar icon

Under normal operating conditions, the taskbar icon shows the status of the Windows Enterprise VPN Client Connection Panel/Configuration Panel.



The color of the icon changes when a VPN tunnel is open:

Blue icon: no VPN tunnel open

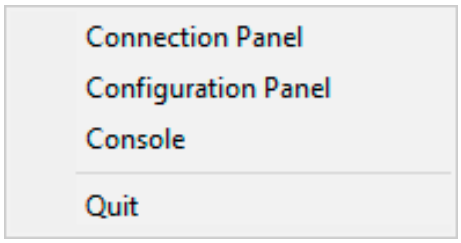
Green icon: at least one VPN tunnel is open

The tooltip for the icon always shows the software status:

- "VPN Tunnel opened" if one or several tunnels are open
- "TheGreenBow VPN Enterprise" when the VPN Client is running, but no tunnels are open

Left-clicking the icon opens the Connection Panel.

Right clicking the VPN Client icon in the taskbar opens the contextual menu associated with the icon:



The administrator can limit the options displayed in the menu (see section 24.1 Displaying/hiding the interface). The contextual menu contains the following items:

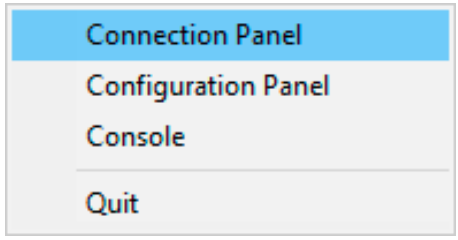
1/ Connection Panel: opens the Connection Panel
2/ Configuration Panel: opens the Configuration Panel
3/ Console: opens the VPN traces window
4/ Quit: closes all open VPN tunnels and quits the software

If the software has not been run as administrator and the "Restrict access to Configuration Panel to administrator" option has not been disabled, when the user selects the "Configuration Panel" option, a message is displayed indicating that the software must be run as administrator to access the Configuration Panel (see paragraph Running the VPN Client as administrator above).

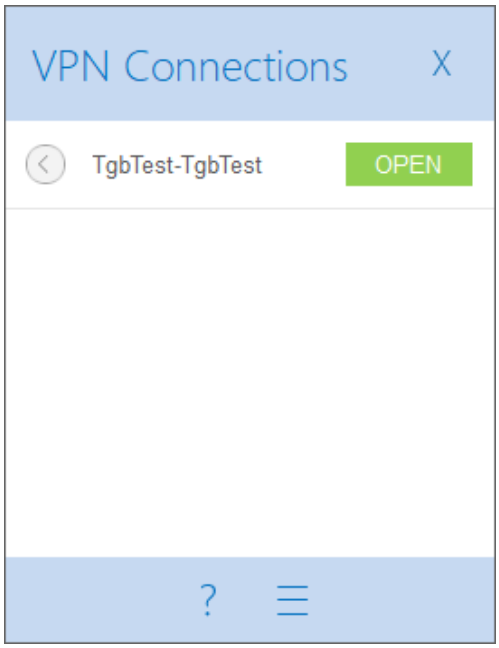
6.3 Opening a test VPN tunnel from the Connection Panel

The Windows Enterprise VPN Client comes equipped with a VPN configuration containing a VPN test tunnel named "TgbTest-TgbTest".

To open the Connection Panel, right-click the taskbar icon (see the paragraph entitled Taskbar icon above), and then select the "Connection Panel" menu item. The Connection Panel is described in chapter 8 Connection Panel.



In the Connection Panel, click the "OPEN" button next to the "TgbTest-TgbTest" tunnel.



When the software has not been run as administrator and the "Restrict access to Configuration Panel to administrator" option has not been disabled, the button with the three horizontal bars to the right of the question mark, which gives access to the Configuration Panel, is not displayed.

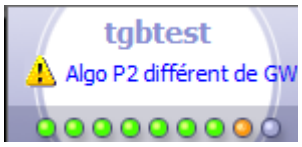
When opening or closing a VPN tunnel, a fade-out pop-up window appears above the VPN Client icon in the taskbar. This window shows the tunnel status when it is being opened or closed and automatically fades out unless the mouse cursor is placed directly over it:

Tunnel is being opened

Tunnel is open

Tunnel is closed

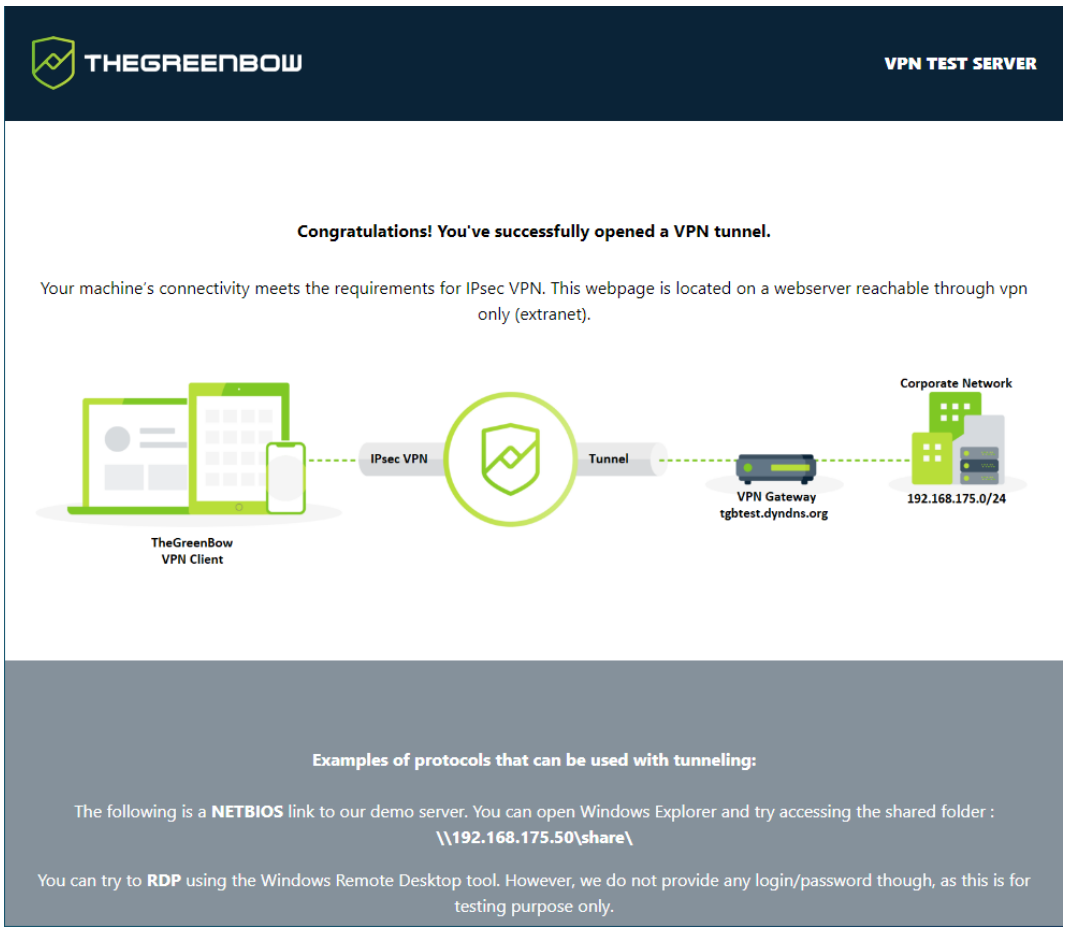
Failed to open the tunnel: the window will briefly explain what happened and provide a hyperlink for more information about the incident.



The fade-out window can be disabled. To do so, in the "Tools" menu select "Options", access the "View" tab, and then check the "Don't show the systray sliding popup" option.

The tunnel opens and the following confirmation window is briefly displayed:

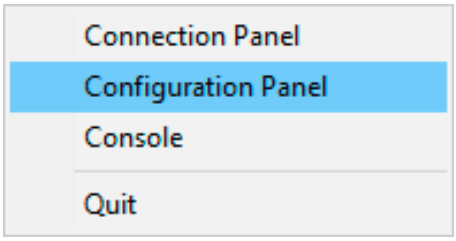
The TheGreenBow test website is then displayed in a browser window:



You can also open a test tunnel from the Configuration Panel (see chapter 9 Configuration Panel).

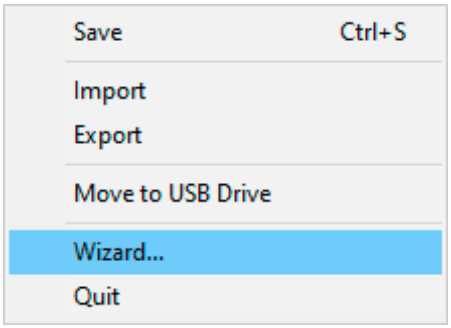
6.4 Configuring a VPN tunnel

To open the Configuration Panel, you must first have started the VPN Client as administrator (see paragraph Starting the VPN Client as administrator above). If this is not the case, quit and restart the VPN Client as administrator. If it is, right-click the taskbar icon (see the paragraph entitled Taskbar icon above), and then select the "Configuration Panel" menu item. The Configuration Panel is described in chapter 9 Configuration Panel.



When the "Restrict access to Configuration Panel to administrator" option is disabled (see section 24.1 Displaying/hiding the interface), you do not need to run the VPN Client as administrator to be able to access the Configuration Panel.

Then, open the configuration wizard by selecting the "Configuration > Wizard…" menu item.



On our website, you will find many configuration guides for most VPN firewalls/routers/gateways: https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-routers/.

Use the wizard as described in chapter 7 Configuration wizard below.

6.5 Automating the opening of a VPN tunnel

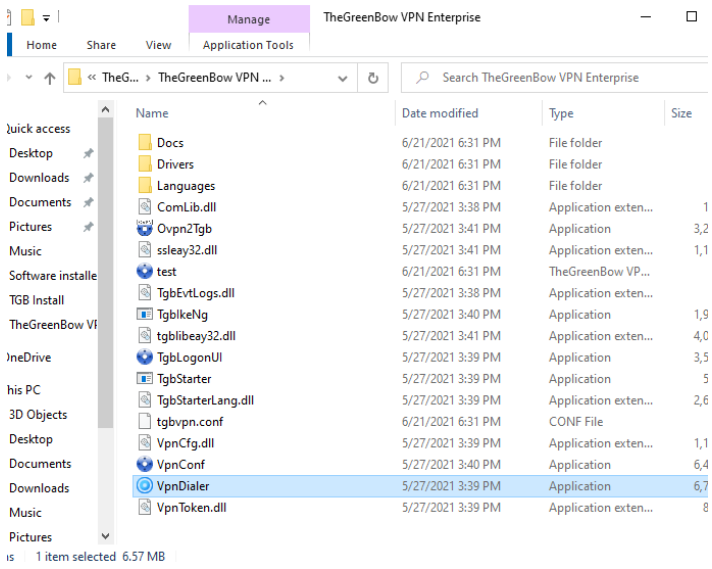
The Windows Enterprise VPN Client allows you to automate the opening of a VPN tunnel. It can be opened automatically in the following ways:

1/ When Windows is started, before or after logging on
2/ When traffic to the remote network is detected (see section 15 Automation)
3/ When inserting a USB drive containing the relevant VPN configuration (see section 22 USB mode)
4/ When inserting the smart card or token containing the certificate used for this tunnel (see section 18.8 Using a certificate stored on a smart card or token)
5/ When the TrustedConnect Panel is used, if the VPN Client detects that the workstation is not located in the trusted network (see section 21 Managing the TrustedConnect Panel)

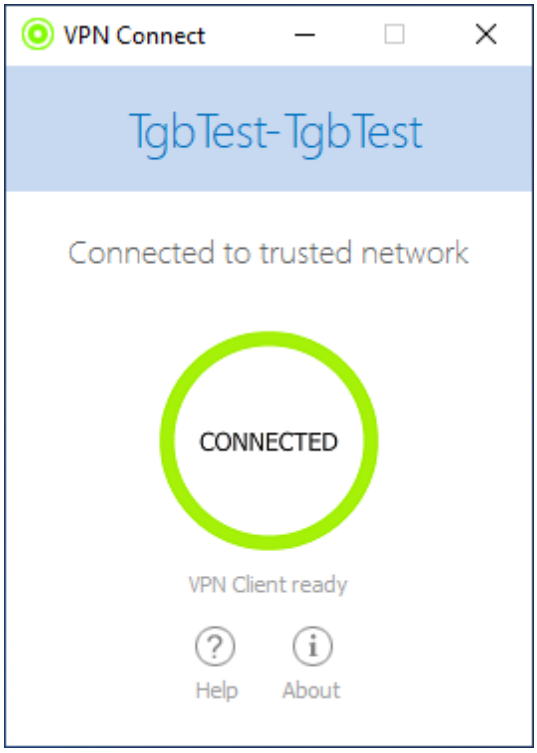
6.6 Opening a VPN tunnel from the TrustedConnect Panel

The TrustedConnect Panel is described in chapter 10 TrustedConnect Panel. It is used to automate the opening of a VPN connection when the workstation is located outside the trusted network and keep the connection open even if the network interface changes.

Start the TrustedConnect Panel using the `VpnDialer.exe` executable file located in `C:\Program Files\TheGreenBow\TheGreenBow VPN Enterprise` by default.



The tunnel "TgbTest-TgbTest" should open automatically.



The TrustedConnect Panel is started from a different executable file than the one for the Configuration Panel. If the TrustedConnect Panel is not launched automatically when the session starts, it can be executed from the VPN Client's installation folder: the executable file is named `VpnDialer.exe` (no desktop shortcut is created for this application during software installation).

The TrustedConnect Panel (run from the `VpnDialer.exe` executable file) cannot be run at the same time as the Configuration Panel or the Connection Panel (both run from the `VpnConf.exe` executable file, the desktop shortcut, or the Start menu).

When `VpnConf.exe` is running and you are running `VpnDialer.exe`, all tunnels opened in `VpnConf.exe` will be closed and `VpnDialer.exe` (TrustedConnect) will attempt to automatically launch the configured tunnel.

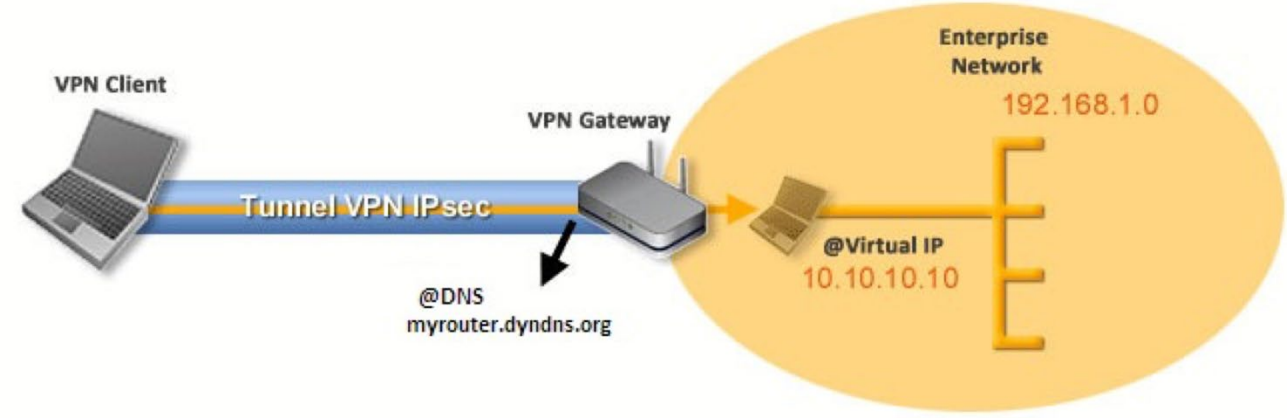
However, when `VpnDialer.exe` (TrustedConnect) is running, you cannot run `VpnConf.exe` immediately. You must first quit `VpnDialer.exe` before you can run `VpnConf.exe`.

7 Configuration wizard

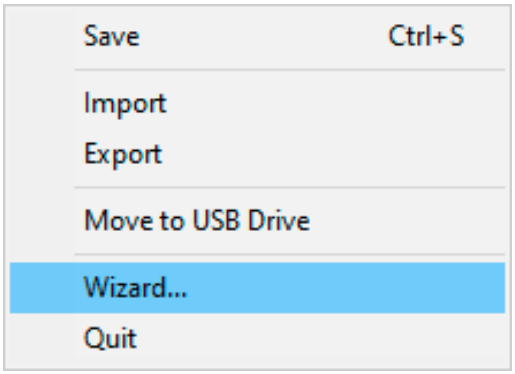
The Configuration wizard is used to configure a VPN tunnel in three easy steps.

The way the Configuration wizard works is illustrated in the example below:

- The tunnel is open between a workstation and a VPN gateway that has been assigned the DNS address "myrouter.dyndns.org"
- The company's local network is 192.168.1.0 (it may, for example, include machines that have been assigned the IP addresses 192.168.1.3, 192.168.1.4, etc.)
- Once the tunnel is open, the remote workstation will have the following IP address on the company's network: 10.10.10.10



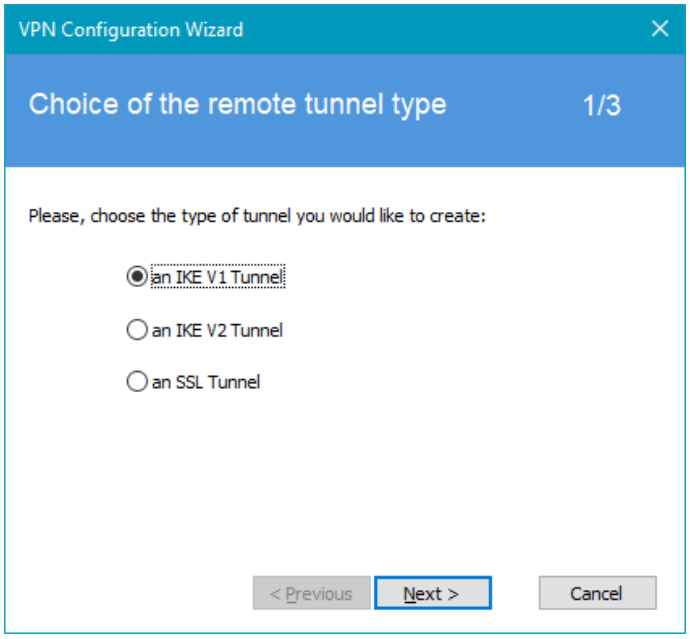
In the main interface, open the VPN configuration wizard: "Configuration > Configuration Wizard…".



Security recommendation: We recommend configuring IKEv2 tunnels with a certificate.
Refer to chapter 26 Security recommendations.

7.1 Step 1

Choose the VPN protocol to be used for the tunnel: IKEv1, IKEv2 or SSL.

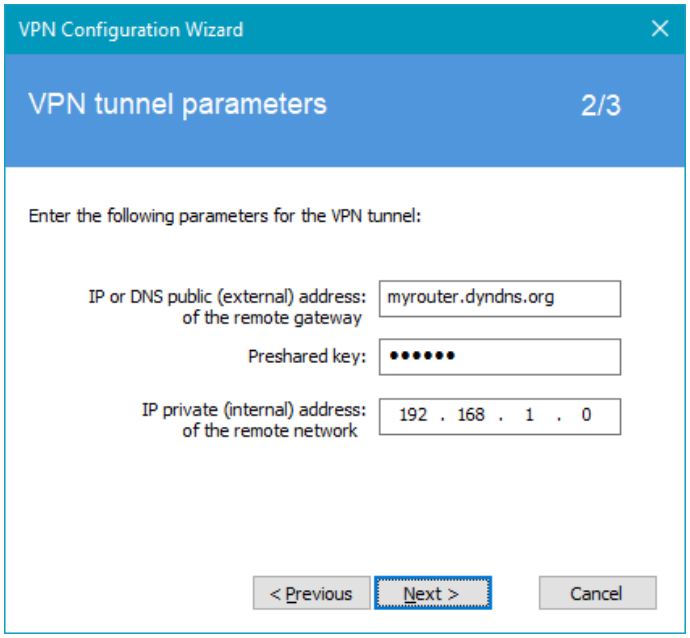


7.2 Step 2

7.2.1 For an IKEv1 VPN tunnel

Enter the following values:

- The IP or DNS address on the internet network side of the VPN gateway (e.g. myrouter.dyndns.org)
- A preshared key that must be configured identically on the gateway
- The IP Address of the corporate network (e.g. 192.168.1.0). (1)

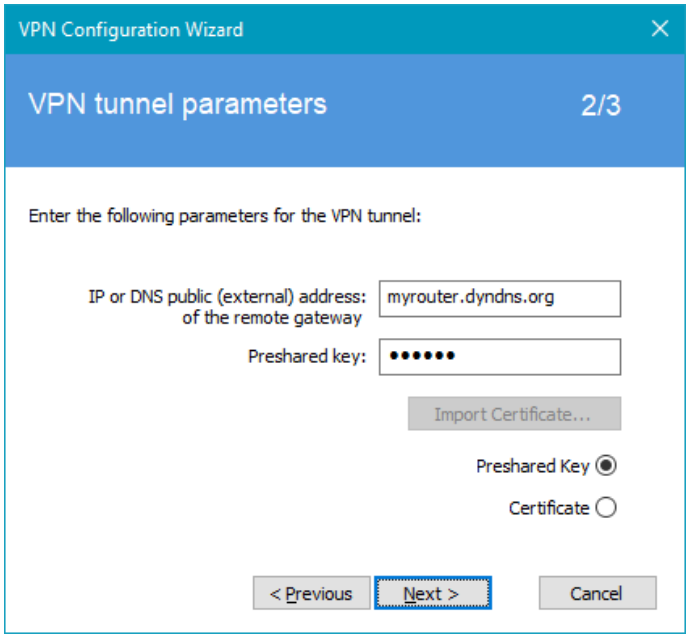


(1) By default, the remote network address used has a prefix length of 24. This value can be modified at a later stage.

7.2.2 For an IKEv2 VPN tunnel

Enter the following values:

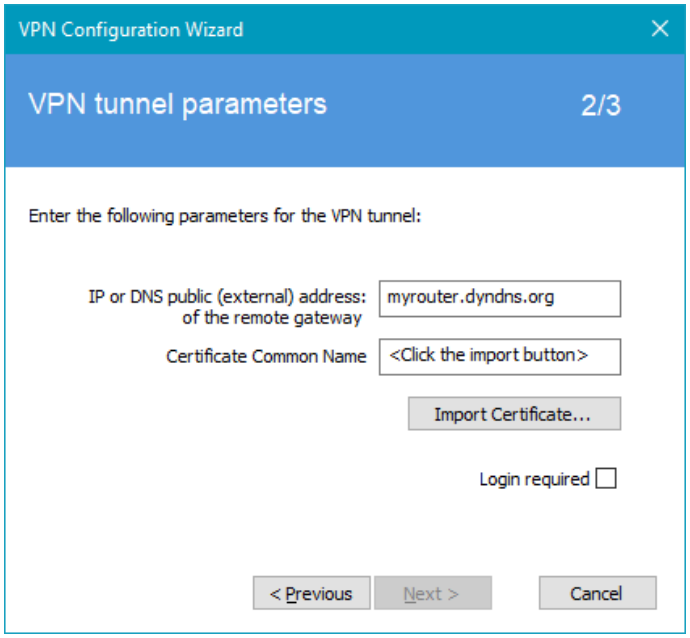
- The IP or DNS address on the internet network side of the VPN gateway (e.g. myrouter.dyndns.org)
- A preshared key that must be configured identically on the gateway
- OR: A certificate that must be imported using the "Import Certificate…" button (see section 18.3 Importing a certificate)



7.2.3 For an SSL tunnel (OpenVPN)

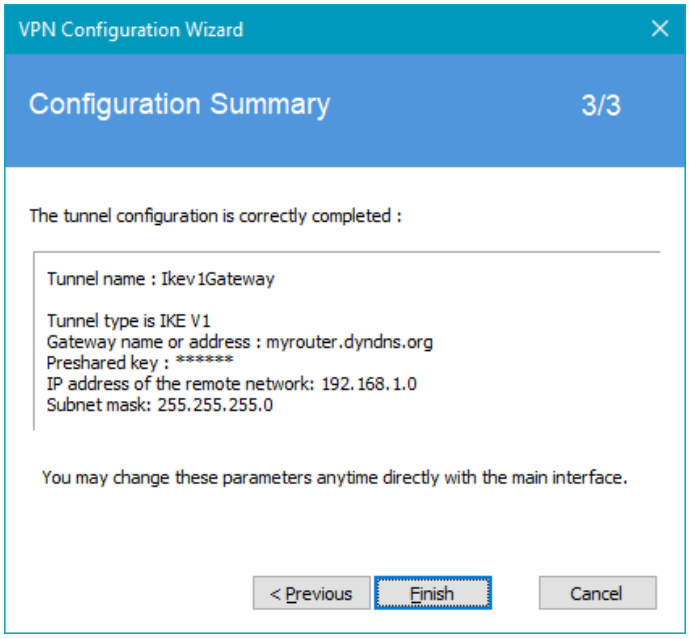
Enter the following values:

- The IP or DNS address on the internet network side of the VPN gateway (e.g. myrouter.dyndns.org)
- A certificate that must be imported using the "Import Certificate…" button (see section 18.3 Importing a certificate)



7.3 Step 3

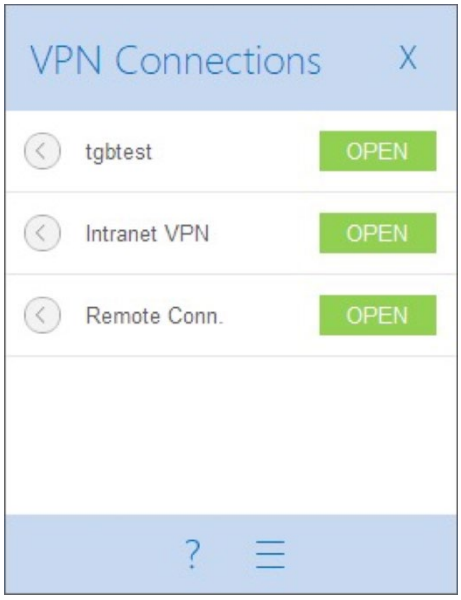
Review the Summary window to check whether the configuration is correct and then click "Finish".



The tunnel that has just been configured now appears in the tunnel tree of the main interface.
Double-click the tunnel to open it or use the tabs of the main interface for further configuration.

8 Connection Panel

The Connection Panel allows you to easily open and close the configured VPN connections:



The Connection Panel can be customized. You can select the VPN connections to be shown. You can also rename or sort the VPN connections.

Refer to chapter 20 Configuring the Connection Panel.

To open a VPN connection, simply click the relevant "OPEN" button.
The icon to the left of the connection name indicates the status of the connection:

Connection closed. Click this icon to open the VPN configuration for this connection in the Configuration Panel.
Caution: Access to the Configuration Panel may be restricted (see section 24.1 Displaying/hiding the interface).

Connection being opened or closed.

Connection open. When there is traffic on this connection, the color intensity of the disk at the center of the icon changes.

The connection experienced an incident while opening or closing. Clicking the warning icon will open a pop-up window giving detailed or additional information about the incident.

The Connection Panel buttons are used to perform the following actions:

? Open the "About…" window

Open the Configuration Panel
Caution: Access to the Configuration Panel may be restricted (see section 24.1 Displaying/hiding the interface).

X Close the Connection Panel

The following keyboard shortcuts are available for the Connection Panel:

- ESC (or ALT+F4) closes the window
- CTRL+ENTER opens the Configuration Panel (main interface)
- CTRL+O opens the selected VPN connection
- CTRL+W closes the selected VPN connection
- The Up and Down arrow keys can be used to navigate up or down the VPN connection list

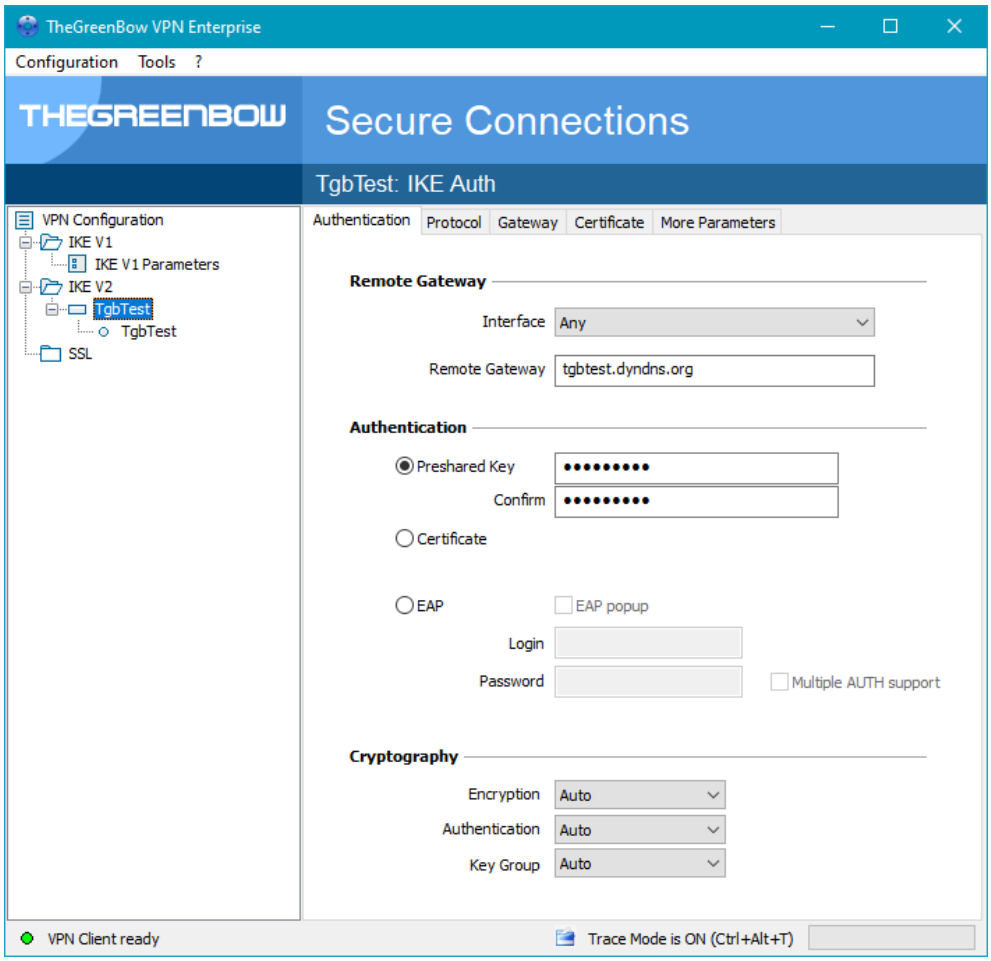
9 Configuration Panel

The Configuration Panel is the administrator's interface of the Windows Enterprise VPN Client.

It is only accessible if the VPN Client has been started as Windows administrator (see paragraph Starting the VPN Client as administrator in section 6.2 Starting the software above), or for any user if the option "Restrict access to the Configuration Panel to administrator" has been unchecked (not recommended).

It includes the following items:

- A set of menus for VPN configuration and software management
- The VPN tunnel tree
- VPN tunnel configuration tabs
- A status bar



9.1 Menus

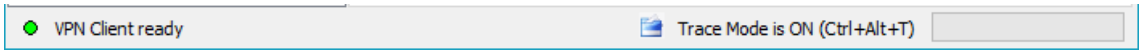
The following menus are available in the Configuration Panel:

- Configuration
  - Save
  - Import: Import a VPN configuration
  - Export: Export a VPN configuration
  - Move to a USB drive: USB mode
  - Configuration Wizard
  - Quit: Close all open VPN tunnels and quit the software

- Tools
  - Connection Panel
  - Connections Configuration
  - Console: IKE connection traces window
  - Reset IKE: Restart the IKE service
  - Options: Protection, display, startup, language management, PKI management options
- ?
  - Online support: Access to online support
  - Update: Check for available updates
  - Purchase license online: Access the online store
  - Activation Wizard…
  - About…

9.2 Status bar

The status bar at the bottom of the main interface displays multiple items:



- The "LED" on the left edge is green when all the software's services are operational (IKE service)
- The text on the left shows the software status ("VPN Client ready", "Saving configuration", "Applying configuration", etc.)
- When the trace mode is enabled, the text "Trace Mode is ON" is shown in the middle of the status bar.
- The icon, which appears to the left of this text, is a clickable icon that opens the folder containing the log files generated by the trace mode.
- The progress bar on the right side of the status bar shows the progress when saving a configuration.

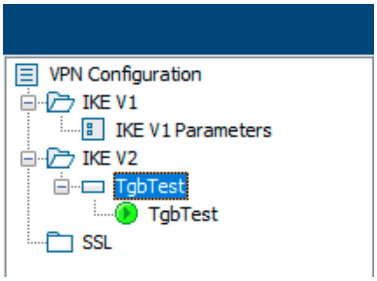
9.3 Shortcuts

CTRL+S	Save the VPN configuration
CTRL+ENTER	Switch to the Connection Panel
CTRL+D	Open the VPN log "Console" window
CTRL+ALT+R	Restart the IKE service
CTRL+ALT+T	Enable the trace mode (log generation)

9.4 VPN tunnel tree

9.4.1 Usage

The left side of the Configuration Panel is the tree structure of the VPN configuration. The tree can contain an infinite number of tunnels.



Under the root called "VPN Configuration", there are three levels that allow you to create the following respectively:

- IPsec IKEv1 tunnels, specified by a Phase 1 and a Phase 2, knowing that each Phase 1 can contain more than one Phase 2
- IPsec IKEv2 tunnels, specified by an IKE Auth and a Child SA, knowing that each IKE Auth can contain more than one Child SA
- SSL/TLS tunnels

Clicking on a Phase 1, Phase 2, IKE Auth, Child SA, or TLS will open the corresponding VPN configuration tabs on the right-hand side of the Configuration Panel. See the following sections for further details:

1. IPsec IKEv1 VPN tunnel
   IKEv1 (Phase 1): Authentication
   IKEv1 (Phase 2): IPsec

2. IPsec IKEv2 VPN tunnel
   IKEv2 (IKE Auth): Authentication
   IKEv2 (Child SA): IPsec

3. SSL VPN tunnel
   SSL: TLS

An icon is associated with each tunnel (Phase 2, Child SA, or TLS). This icon shows the status of the VPN tunnel:

- Tunnel is closed
- Tunnel is being opened
- Tunnel is open
- Incident when opening or closing the tunnel

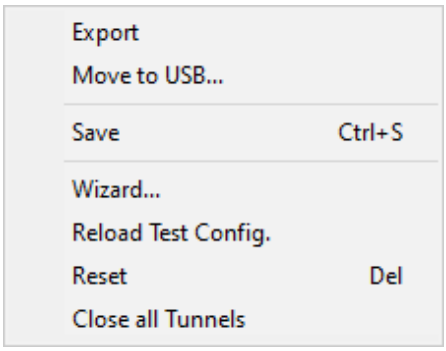
You can edit and change the name of any item in the tree by clicking twice in a row on it, without double-clicking.
If there are any unsaved changes in the VPN configuration, the modified item is shown in bold. As soon as the tree is saved, all text formatting is removed.

Two items in the tree cannot have the same name. The software displays a message to the user if the name entered is already in use.

9.4.2 Contextual menus

1. VPN configuration

Right clicking the VPN configuration (root of the tree) displays the following contextual menu:



Export	Used to export the complete VPN configuration.
Move to USB drive…	Moves the VPN configuration to a USB drive and initiates USB mode.
Save	Used to save the VPN configuration.
Configuration Wizard	Opens the VPN Configuration Wizard.
Reload default configuration	The Windows Enterprise VPN Client comes with a default VPN configuration that can be used to test opening a VPN tunnel. This menu is used to reload the default configuration at any time.
Reset	Resets the VPN configuration following confirmation by the user.
Close all tunnels	Closes all open tunnels.

2. IKEv1, IKEv2, SSL

Right-clicking the IKEv1, IKEv2 or SSL items will display the following contextual menu, which allows you to export, save, create, or paste a Phase 1/IKE Auth/SSL:

IKEv1 menu

IKEv2 menu

SSL menu

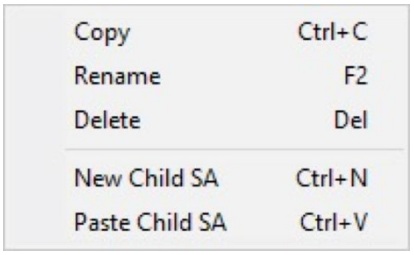
Export	Used to export all IKEv1 tunnels (resp. all IKEv2 tunnels)
Save	Used to save all IKEv1 tunnels (resp. all IKEv2 tunnels)
New Phase 1 New IKE Auth New TLS	Used to create a new Phase 1/IKE Auth/TLS. The parameters of this new Phase 1/IKE Auth/TLS will be filled in with default values.

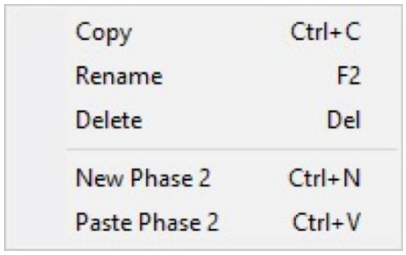
Paste Phase 1 Paste IKE Auth Paste TLS	Adds a Phase 1/IKE Auth/TLS that has been previously copied to the clipboard.

(1) This choice will be shown when a Phase 1/IKE Auth/TLS has been copied to the clipboard using the contextual menu associated with the Phase 1/IKE Auth/TLS (see below).

3. Phase 1 or IKE Auth

Right clicking a Phase 1 or IKE Auth displays the following contextual menu:





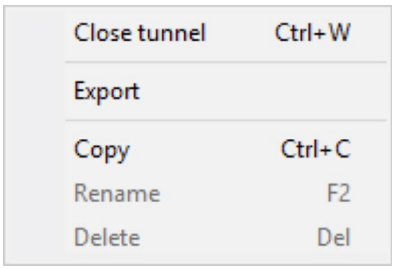
Copy	Copies the selected Phase 1 or IKE Auth to the clipboard.
Rename (1)	Used to rename the Phase 1/IKE Auth.
Delete (1)	Used to delete the selected Phase 1 or IKE Auth following confirmation by the user, including every corresponding Phase 2 (resp. Child SA).
New Phase 2 New Child SA	Adds a new Phase 2/Child SA to the selected Phase 1/IKE Auth.
Paste Phase 2 (2) Paste Child SA	Adds the Phase 2/Child SA that has been copied to the clipboard to the Phase 1/IKE Auth.

(1) This menu is disabled as long as one of the tunnels of the relevant Phase 1/IKE Auth is open.
(2) This choice will be shown when a Phase 2/Child SA has been copied to the clipboard using the contextual menu associated with the Phase 2/Child SA (see below).

4. Phase 2, Child SA, or TLS

Right clicking a Phase 2, Child SA, or TLS displays the following contextual menu:

Menu with tunnel closed



Menu with tunnel open

Open tunnel	Displayed if the VPN tunnel is closed and is used to open the selected tunnel (Phase 2, Child SA, or TLS)

Close tunnel	Displayed if the VPN tunnel is open and is used to close the selected tunnel (Phase 2, Child SA, or TLS)
Export (1)	Used to export the selected Phase 2, Child SA, or TLS
Copy	Used to copy the selected Phase 2, Child SA, or TLS
Rename (2)	Used to rename the selected Phase 2, Child SA, or TLS
Delete (2)	Used to delete the selected Phase 2, Child SA, or TLS following confirmation by the user

(1) This function allows users to export the entire tunnel, i.e. both the Phase 2 and the corresponding Phase 1 (resp. Child SA and its associated IKE Auth, or TLS), and thus to create a fully operational, single-tunnel VPN configuration (which becomes immediately functional when imported).
(2) This menu is disabled while the tunnel is open.

9.4.3 Shortcuts

The following shortcuts are available for tree management:

F2	Used to edit the name of the selected Phase
DEL	Used to delete a selected phase, following confirmation by the user. If the actual VPN configuration is selected (root of the tree), the software asks whether a full reset of the configuration should be performed.
CTRL+O	Opens the corresponding VPN tunnel if a Phase 2/Child SA/TLS is selected.
CTRL+W	Closes the corresponding VPN tunnel if a Phase 2/Child SA/TLS is selected.
CTRL+C	Copies the selected phase to the clipboard.
CTRL+V	Pastes (adds) the phase that has previously been copied to the clipboard.
CTRL+N	If the VPN configuration is selected, creates a new Phase 1/IKE Auth. If a Phase 1/IKE Auth is selected, creates a Phase 2/Child SA/TLS.
CTRL+S	Saves the VPN configuration.

10 TrustedConnect Panel

10.1 Introduction

The TrustedConnect Panel allows you to permanently keep a secure connection to the trusted network thanks to the following features:

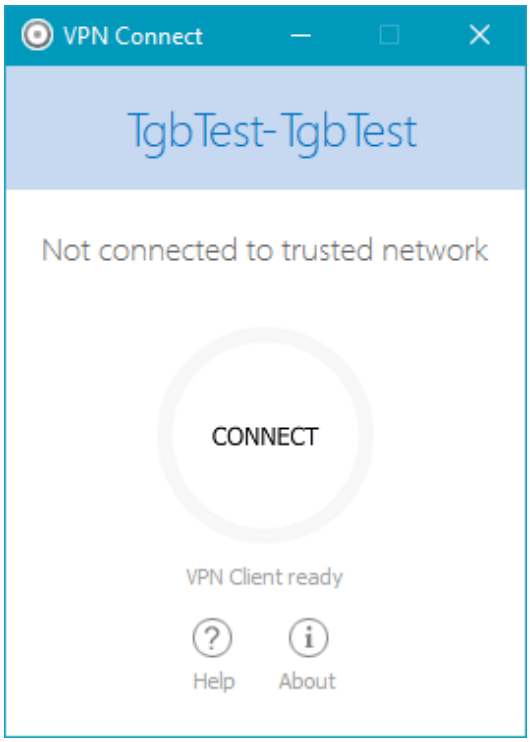
- **Trusted Network Detection (TND)**: Used to determine whether the workstation is within the trusted network based on the DNS suffixes and on beacon identification
- **Always-On**: Ensures that the connection remains secure whenever the network interface changes, for example, between Ethernet, Wi-Fi and 4G/5G

10.2 Interface

When it is used for the first time, the TrustedConnect Panel is displayed in the center of the screen.
For subsequent uses, the TrustedConnect Panel memorizes the place to which the user has moved it.

The interface of the TrustedConnect Panel includes the following items:

- A title that identifies the name of the connection being managed
- An information message about the connection status
- A Connect button
- A message that indicates the current status of the software and displays possible error codes
- A help button that gives access to a document with help for the user
- An information button that displays essential information about the software
- A set of icons whose color reflects the connection status



You can minimize the TrustedConnect Panel at any time either to the taskbar, by clicking the "minimize" button in the title bar, or to the notification area, by clicking on the "Close" button in the title bar.

Conversely, you can display the TrustedConnect Panel at any time by clicking the TrustedConnect icon in the taskbar or in the notification area.

You can quit the software by right clicking the TrustedConnect icon in the notification area and then selecting "Quit".

10.3 Taskbar icon and color codes

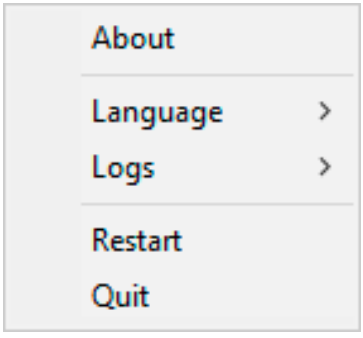
The taskbar icon of the TrustedConnect Panel application is slightly different from that of the Windows Enterprise VPN Client Configuration Panel/Connection Panel.

The various icons in the TrustedConnect Panel have the following meaning:

	This state means that the TrustedConnect Panel is not managing any connection on the workstation. Generally, this state is encountered when the user explicitly requests the VPN connection to be closed.
	This state means that the workstation is directly connected to the corporate network, which is considered as a trusted network.
	This state means that the workstation is connected to the corporate network through a VPN connection. The workstation thus is physically located on a network that is not considered as trusted.
	This state means that the VPN connection could not be established.

10.4 Contextual menus

Right clicking the TrustedConnect Panel icon in the taskbar opens the contextual menu associated with the icon:



The contextual menu contains the following items:

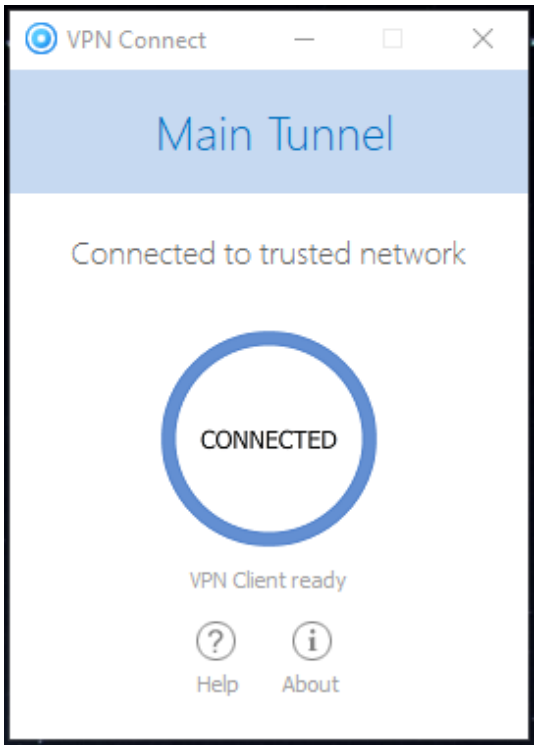
1/ About…: Opens the "About…" window
1/ Language: Used to switch between French and English
2/ Logs: Used to start logging. Once logging is started, two additional options are shown to display the logs and stop logging.
3/ Restart: Used to restart the tunnel
4/ Quit: Closes the VPN tunnel and quits the software

10.5 Usage

There are two types of use depending on whether the workstation is already connected to the corporate network or not.

10.5.1 Workstation connected to corporate network

The TrustedConnect Panel switches to the "CONNECTED" status after having detected trusted networks:



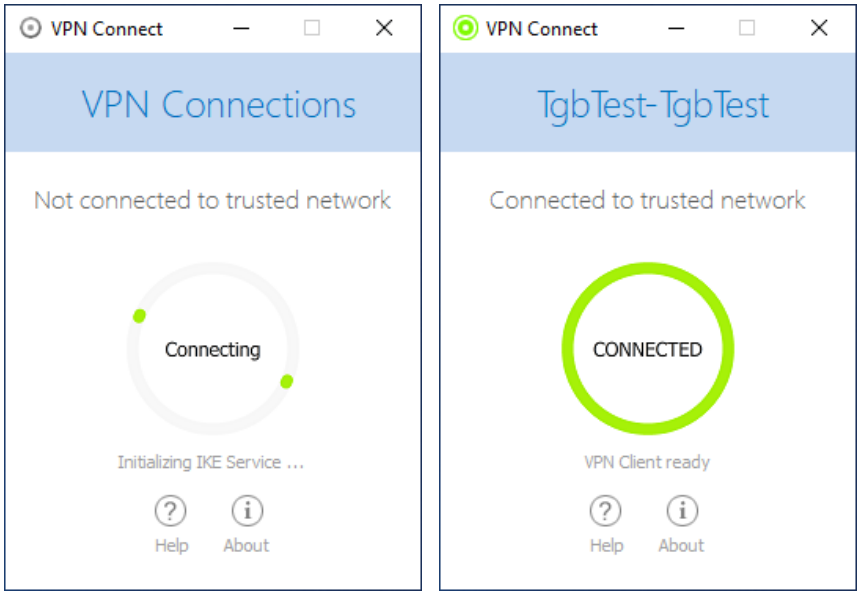
The window of the TrustedConnect Panel then automatically minimizes either to the taskbar or to the notification area, depending on the behavior that the administrator has configured.
☞ Refer to the "Deployment Guide".

To display the window again, select the application in the taskbar. When connected to the corporate network, users cannot perform any action on the connection status.

10.5.2 Workstation not connected to corporate network

When switching to a network that is not considered as trusted, the TrustedConnect Panel will automatically open the VPN tunnel.

The button's animation shows the progress of the connection being established until it is established.

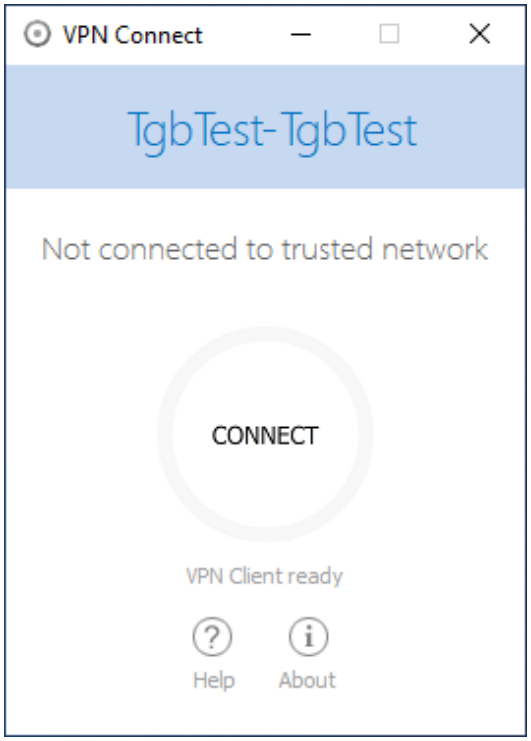


Once the connection is established, the window of the TrustedConnect Panel automatically minimizes either to the taskbar or to the notification area, depending on the behavior that the administrator has configured.

The connection may not be established for various reasons. The information message below the button provides a first level of information. The various possible cases of connection failure are detailed in the next section.

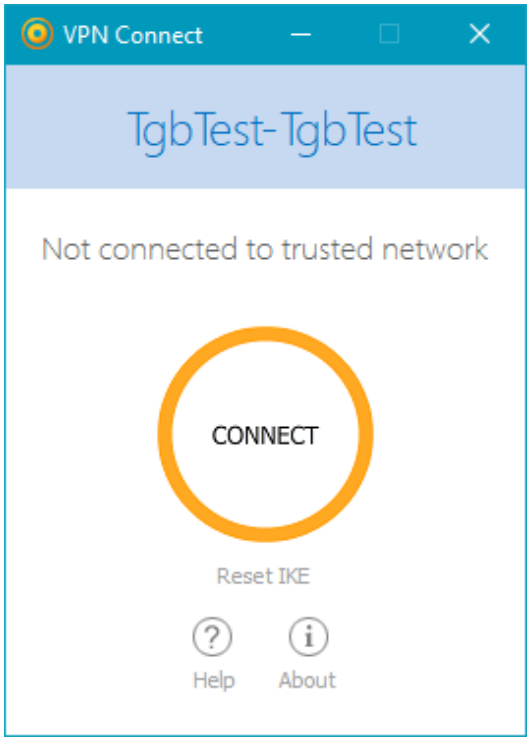
When the tunnel is mounted and the workstation is shown as being on the corporate network, you can click inside the connection status indicator ring to stop the tunnel.

The application then switches to the state "Not connected" and you can click the button to manually open the tunnel again:



10.6 Error cases

An orange Connect button, an error code, and a brief message describing the error are shown in the TrustedConnect Panel interface to identify the main error cases.

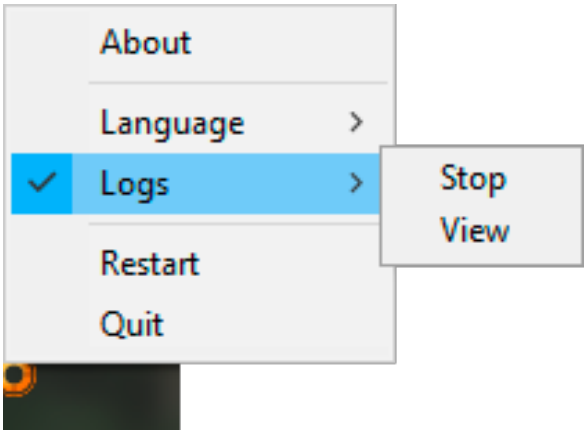


Contact the network administrator to resolve the issue. The error code shown may provide some indication or explanation as to the issue encountered. If the administrator requests the logs, refer to the procedure described in the next section.

The list of error codes is provided in the appendix of this document (see section 27.3 TrustedConnect Panel diagnostics.

10.7 Generating logs

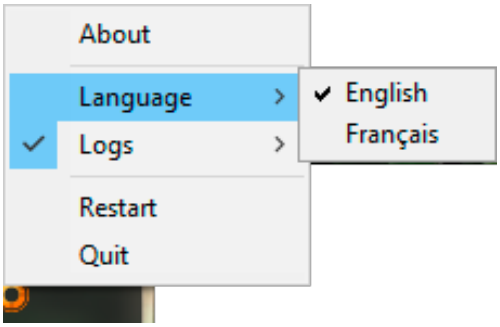
The TrustedConnect Panel allows you to create and view logs.
To initiate the creation of log files, right click the TrustedConnect icon in the notification area, select "Logs". A check mark next to the menu item indicates that logging is enabled:



To view the logs, access the system menu and select the item "Access logs". A window with the log folder is shown with a certain number of files. You can send these files to the administrator when you encounter any issues.

10.8 Selecting the language

The TrustedConnect Panel allows you to select the software's display language: French or English. To select the language, access the menu and select the "Languages" item. In the submenu, select "English" or "Français":



10.9 Current limitations

The TrustedConnect Panel (run from the `VpnDialer.exe` executable file) cannot be run at the same time as the Configuration Panel or the Connection Panel (both run from the `VpnConf.exe` executable file, the desktop shortcut, or the Start menu).

When `VpnConf.exe` is running and you are running `VpnDialer.exe`, all tunnels opened in `VpnConf.exe` will be closed and `VpnDialer.exe` (TrustedConnect) will attempt to automatically launch the configured tunnel.

However, when `VpnDialer.exe` (TrustedConnect) is running, you cannot run `VpnConf.exe` immediately. You must first quit `VpnDialer.exe` before you can run `VpnConf.exe`.

The TrustedConnect Panel (`VpnDialer.exe`) is currently only available in French and English.

11 "About…" window

The "About…" window can be accessed as follows:

- Click the "?" menu in the Configuration Panel and choose "About…"
- Use the system menu in the Configuration Panel
- Click the [?] button in the Connection Panel
- Click the [?] button in the TrustedConnect Panel

The "About…" window displays the following information:

- The name and version number of the software
- A web link to TheGreenBow's website
- When the software is activated, the license number and email used for activation
- During the software trial period, the number of days remaining before the trial period expires
- The version numbers of all software components (1)

(1) You can select and copy the contents of the entire list of version numbers (right-click on the list and choose "Select all"), for example to send the information for analysis purposes. When the "About" window is open, if the Windows Enterprise VPN Client has not been activated, the software tries to connect to the activation server to validate the license.

12 Importing and exporting the VPN configuration

12.1 Importing a VPN configuration

The Windows Enterprise VPN Client allows you to import a VPN configuration in various ways:

- From the "Configuration" menu in the Configuration Panel (main interface), choose "Import"
- From the command line, use the `/import` option (1)

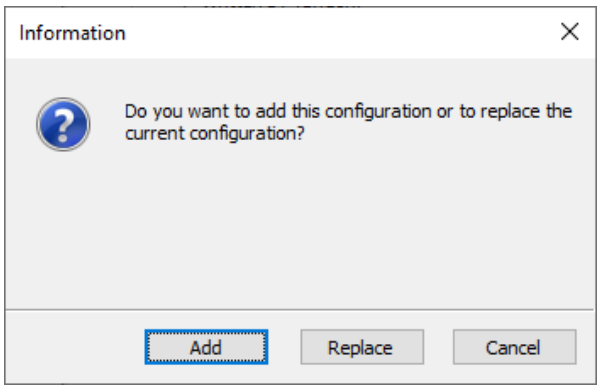
(1) The use of command-line options within the software is covered in the "Deployment Guide".
In particular, it details all the options available for importing a VPN configuration: `/import`, `/add`, `/replace` or `/importonce`.

As of version 6.8 of the Windows Enterprise VPN Client, dragging and dropping a VPN configuration file (`.tgb` file) onto the Configuration Panel is no longer supported, because privilege elevation is now required to manage VPN configurations.

As of version 6.8 of the Windows Enterprise VPN Client, the function that allows you to double-click on a VPN configuration file to import it is no longer available.

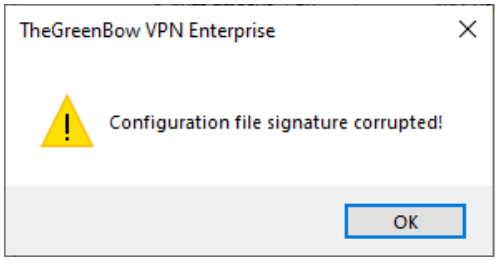
The Windows Enterprise VPN Client does not monitor VPN configuration file integrity. In this case, a signature is generated during export and the integrity of the file is checked during import.

When importing a VPN configuration, users are prompted to specify whether they want to add the new VPN configuration to the current one or replace (overwrite) the current configuration with the new one:

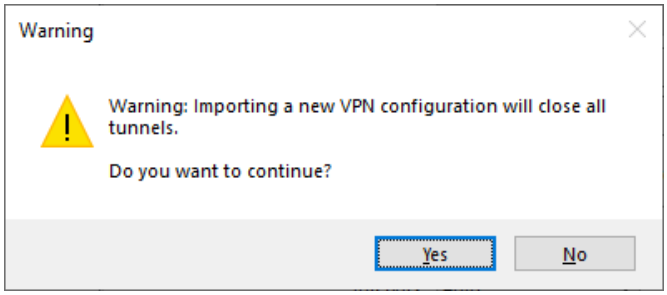


If the imported VPN configuration has been exported with a password protection (see section 12.2 Exporting a VPN configuration below), users will have to provide the password.

If the VPN configuration is exported with an integrity check (see section 12.2 Exporting a VPN configuration below) and it has been corrupted, a warning will be displayed to the user and the software will not import the configuration.



If one or several tunnels are open when importing, the following information window will be displayed to let you know that the import will close all open tunnels:



Once this message has been confirmed and the import has been completed, you will need to reopen the tunnels.

If some of the VPN tunnels added have the same name as certain tunnels in the current configuration, they are automatically renamed during import (an increment will be added between brackets).

Importing IKEv1 parameters

If the user chooses "Replace" during an import or if the current configuration is empty, the IKEv1 parameters of the imported VPN configuration will replace the IKEv1 parameters of the current configuration.
If the user chooses "Add" during an import, the IKEv1 parameters of the current VPN configuration are preserved.

User's choice during import	Current VPN configuration is empty	Current VPN configuration is not empty
Add	IKEv1 parameters are replaced with the new ones	IKEv1 parameters are preserved
Replace	IKEv1 parameters are replaced with the new ones	IKEv1 parameters are replaced with the new ones

12.2 Exporting a VPN configuration

The Windows Enterprise VPN Client allows you to export a VPN configuration in various ways:

1/ From the "Configuration" menu, choose "Export": The complete VPN configuration is exported.
2/ Contextual menu at the root of the VPN tree > Export: The complete VPN configuration is exported.
3/ Contextual menu associated with a Phase 1 (IKEv1) or an IKE Auth (IKEv2) > Export: The entire Phase 1/IKE Auth (including all Phase 2/Child SA it contains) is exported.
4/ Contextual menu associated with a Phase 2 (IKEv1) or a Child SA (IKEv2) > Export: The Phase 2/Child SA is exported along with the Phase 1/IKE Auth with which it is associated.
5/ Contextual menu associated with a TLS > Export: The TLS is exported.
6/ Using the `/export` option in the command line. (1)

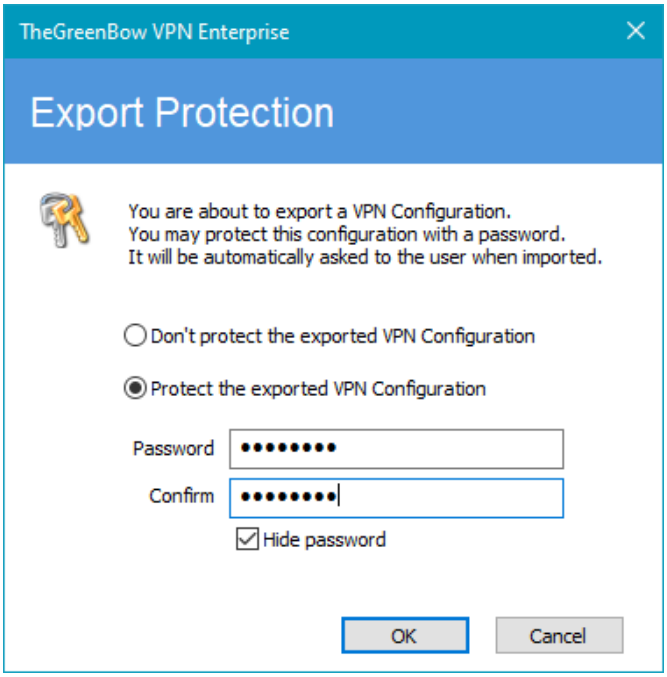
(1) The use of command-line options within the software is covered in the "Deployment Guide". In particular, it details all the options available for exporting a VPN configuration: `/export` or `/exportonce`.

By default, the extension of exported VPN configuration files is `.tgb`.

Regardless of the method used, the export starts with the choice of protection for the exported VPN configuration: it can be exported with (encryption) or without (clear text) password protection. If a password has been set, users will be required to enter it when importing.

Whether it is exported with or without encryption, the exported VPN configuration can benefit from integrity protection.

Protecting the integrity of a VPN configuration when it is exported is a feature that can be enabled using an MSI installer property. This function is covered in the "Deployment Guide".



We recommend that you always export VPN configurations with a password protection (encrypted).

If an exported VPN configuration is integrity-protected, but is corrupted subsequently, a warning will be displayed to the user during the import and the software will not import the configuration (see section 12.1 Importing a VPN configuration above).

12.3 Merging VPN configurations

Several configurations can be merged by successively importing all VPN configurations and choosing "Add" each time (see section 12.1 Importing a VPN configuration above).

12.4 Splitting a VPN configuration

Using the various export options available (exporting a Phase 1/IKE Auth/TLS with all the corresponding Phase 2/Child SA/TLS or exporting a single tunnel), a VPN configuration can be split into as many "sub-configurations" as desired (see section 12.2 Exporting a VPN configuration above).

This method can be used to deploy the configurations for a pool of workstations: derive the VPN configurations for each individual workstation from a common VPN configuration prior to sending them to each user for import.

13 Configuring a VPN tunnel

13.1 IPsec IKEv1, IPsec IKEv2 or SSL VPN

The Windows Enterprise VPN Client allows you to create and configure several types of VPN tunnels.
It also allows you to open them simultaneously.

The Windows Enterprise VPN Client allows you to configure the following types of tunnels:

- IPsec IKEv1
- IPsec IKEv2
- SSL

The procedure used to create a new VPN tunnel is described in the previous sections: 7 Configuration wizard and 9.4.2 Contextual menus.

Security recommendation: We recommend configuring IKEv2 tunnels with a certificate.
Refer to chapter 26 Security recommendations.

13.2 Editing and saving a VPN configuration

The Windows Enterprise VPN Client allows you to modify the VPN tunnels and test these modifications "on-the-fly" without saving the VPN configuration.
All unsaved changes in the VPN configuration are clearly shown in the tree, as the name of modified items appears in bold.

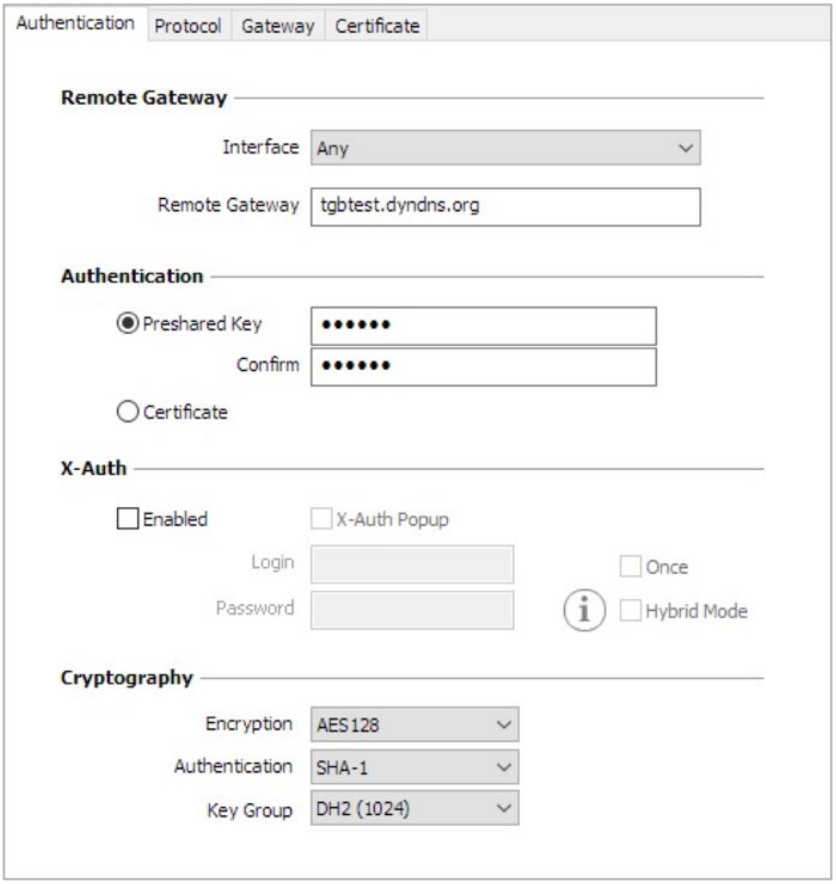
The VPN configuration can be saved at any time using either of the following:

- CTRL+S shortcut
- "Configuration > Save" menu item

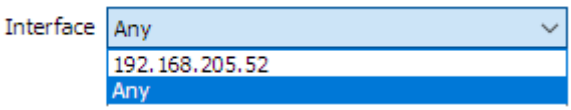
A warning will be displayed if a VPN configuration has been changed and the user tries to quit the software without saving.

13.3 Configuring an IPsec IKEv1 tunnel

13.3.1 Phase 1: Authentication



Addresses

Interface	IP address of the network interface on which the VPN connection is open. You can let the software automatically decide which interface to use by selecting "Any".  We recommend choosing this option if the tunnel being configured is to be deployed on a different workstation.
Remote Gateway	IP address (IPv4 or IPv6) or DNS address of the remote VPN gateway. This field is mandatory.

Authentication

Preshared key	Password or key shared by the remote gateway.

> The preshared key is an easy way to configure a VPN tunnel. However, it is less flexible in terms of security management than the use of certificates.
> Refer to chapter 26 Security recommendations.

Certificate	Use of certificates for VPN connection authentication.

> Using Certificate strengthens the security in terms of VPN connection management (mutual authentication, verification of validity periods, revocation, etc.)
> Refer to chapter 26 Security recommendations.

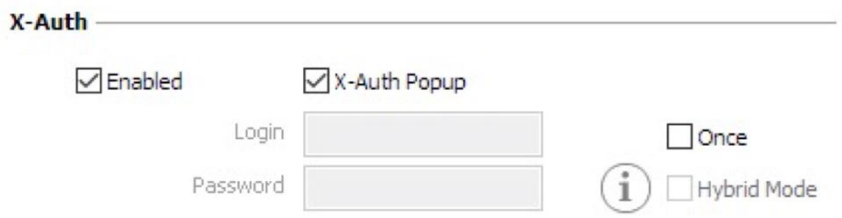
Refer to the dedicated chapter: 18 Managing certificates.

X-Auth management

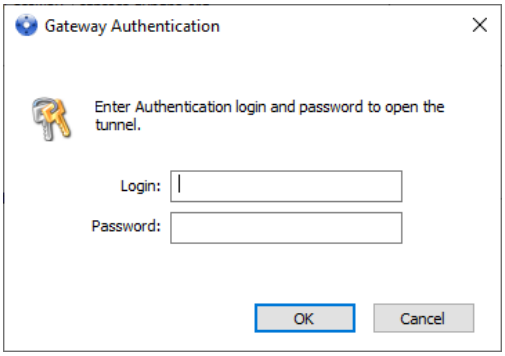
X-Auth is an extension of the IKE protocol (Internet Key Exchange).

The X-Auth function is used to force the entry of a login name and password to open a VPN tunnel.

> This requires a similar configuration to be set up on the VPN gateway.

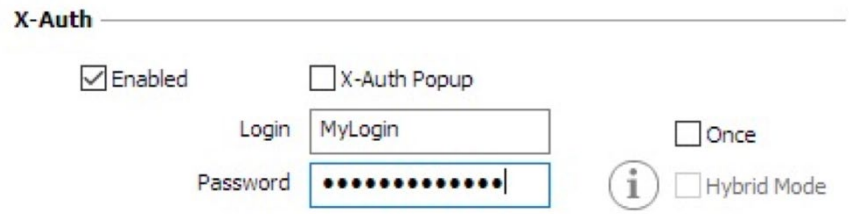


If the "X-Auth Popup" box is checked, a popup window prompting the user to enter a login name and authentication password will be shown each time a VPN tunnel is opened (the window prompting for a login name and password will have the same name as the tunnel to avoid any confusion).



This window has a timeout limit (which can be set in the IKEv1 parameters). When the timeout expires, a warning is displayed prompting the user to re-open the tunnel.

The VPN Client can store the X-Auth login name and password in the VPN configuration. If this is the case, the login name and password will be automatically sent to the VPN gateway when the tunnel is opened.



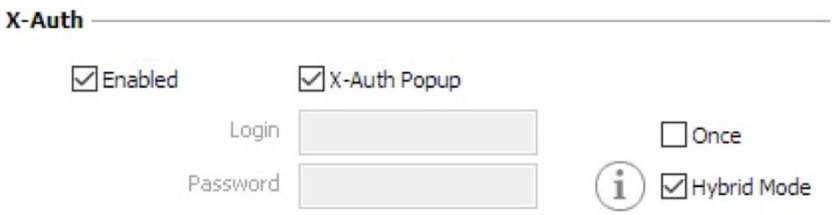
This option facilitates the use and deployment of the software. However, it is considered a less secure option than displaying a dynamic X-Auth login window.

We recommend that you do not store the X-Auth login and password in the VPN configuration. Refer to chapter 26 Security recommendations.

Check the "Once" option to avoid having to enter the password again during a Phase 1 renegotiation.

The Hybrid mode "mixes" two different types of authentication: standard VPN gateway authentication and X-Auth authentication for the VPN Client.

To activate the Hybrid mode, the tunnel must be associated with a certificate (see chapter 18 Managing certificates) and the X-Auth function must be configured.



Cryptography

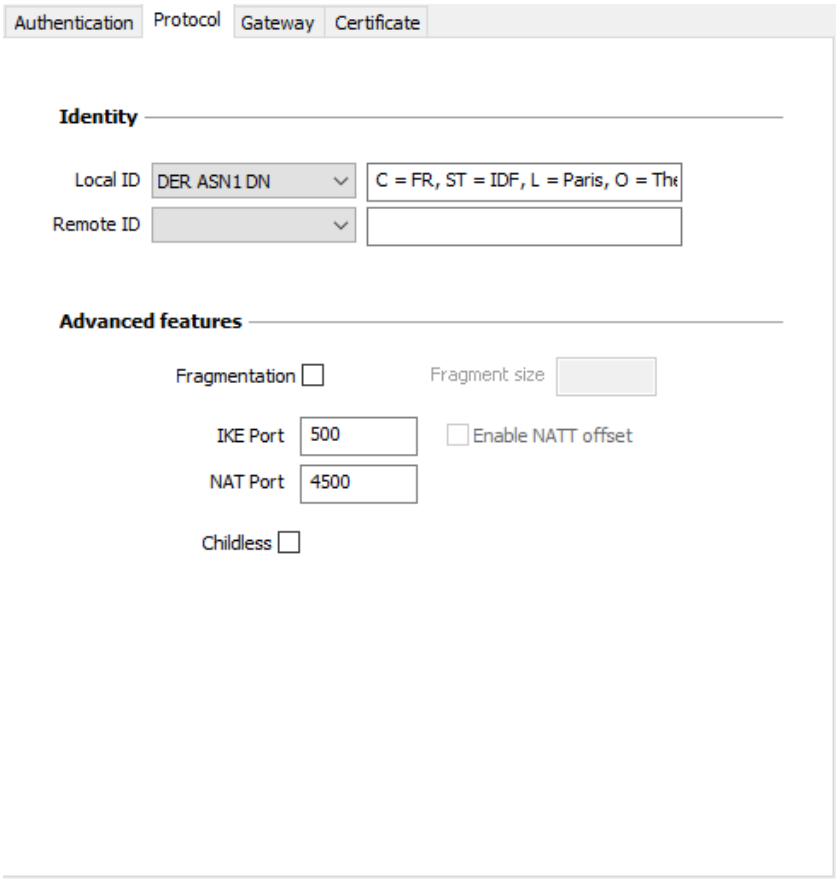
Encryption	Encryption algorithm negotiated during the authentication phase (1): Auto (2), AES-128, AES-192, AES-256.
Authentication	Authentication algorithm negotiated during the authentication phase (1): Auto (2), SHA2-256, SHA2-384, SHA2-512.
Key group	Length of Diffie-Hellman key (1): Auto (2), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)

(1) Refer to chapter 26 Security recommendations on the choice of algorithm.

(2) Auto means that the VPN Client automatically adapts to the gateway parameters. When "Auto" is selected, the following algorithms (and their various combinations) are supported:
- Encryption: AES-128, AES-192
- Authentication: SHA2-256, SHA2-384, SHA2-512
- Key group: DH14 (2048), DH15 (3072), DH16 (4096)

If the gateway has been configured using a different algorithm, then the "Auto" mode cannot be used. The algorithm must be specified explicitly in the VPN Client.

13.3.2 Phase 1: Protocol



Identity

Local ID	"Local ID" is the authentication phase (Phase 1) identifier that the VPN Client sends to the remote VPN gateway. According to the type selected, this identifier can be any of the following: - IP address: an IPv4 address (type = IPV4 ADDR), e.g. 195.100.205.101 - DNS: a domain name (type = FQDN), e.g. gw.mydomain.net - KEY ID: a character string (type = KEY ID), e.g. 123456 - Email: an email address (type = USER FQDN), e.g. support@thegreenbow.com - DER ASN1 DN: the X.509 subject of a certificate (type = DER ASN1 DN) - X509 subject: this field is automatically filled in with the subject of an X.509 certificate when the tunnel is associated with a user certificate (see chapter 18 Managing certificates) If this parameter is not set, the VPN Client's IP address is used by default.
Remote ID	"Remote ID" is the identifier that the VPN Client expects to receive from the VPN gateway. According to the type selected, this identifier can be any of the following: - IP address: an IP address (type = IPV4 ADDR), e.g. 80.2.3.4 - DNS: a domain name (type = FQDN), e.g. router.mydomain.com - KEY ID: a character string (type = KEY ID), e.g. 123456 - Email: an email address (type = USER FQDN), e.g. admin@mydomain.com - DER ASN1 DN: the X.509 subject of a certificate (type = DER ASN1 DN) This setting is required since version 6.8 for security reasons.

Advanced features

Fragmentation/ Fragment size	This function enables IKE fragmentation, which prevents packets from becoming fragmented (and potentially blocked) by the IP network they're passing through. We recommend that you enable this option (both on the gateway and on the VPN Client) in case the internet service provider has set up carrier-grade NAT (CGN), which prevents fragmentation from working at the IP level. The fragment size must generally be set to a value that is smaller by 200 bytes than the MTU of the physical interface, e.g. 1300 bytes for a typical 1500-byte MTU.
IKE port	IKE Phase 1 (Authentication) exchanges use the UDP protocol and port 500 by default. IKE port configuration can bypass the networking hardware (firewall, routers) that filter port 500.  The remote VPN gateway must also be able to perform the IKE Phase 1 exchanges on a port other than 500.

NAT port	IKE Phase 2 (IPsec) exchanges use the UDP protocol and port 4500 by default. NAT port configuration can bypass the networking hardware (firewall, routers) that filter port 4500. The remote VPN gateway must also be able to perform the IKE Phase 2 exchanges on a port other than 4500.
Enable NATT offset	When the IKE port is different from 500, it may be necessary to check this option for the gateway to accept the connection.
Mode Config	Once it is activated, Mode Config enables the VPN Client to get the configuration data required to open the VPN tunnel from the VPN gateway. See the following paragraph below: Managing Mode Config.
Aggressive mode	The VPN Client uses the Aggressive mode to connect to the VPN gateway.
NAT-T	"NAT-Traversal" mode. The VPN Client can handle three types of NAT-T modes:

Disabled	Prevents the VPN Client and the VPN gateway to switch to NAT-Traversal mode.
Automatic	Lets the VPN Client and the VPN gateway negotiate the NAT-Traversal mode.
Forced	The VPN Client will force the NAT-T mode by systematically encapsulating IPsec packets into UDP frames. This will solve NAT-Traversal issues using intermediate routers.

Managing Mode Config

Once it is activated, Mode Config enables the VPN Client to get the configuration data required to open the VPN tunnel from the VPN gateway:

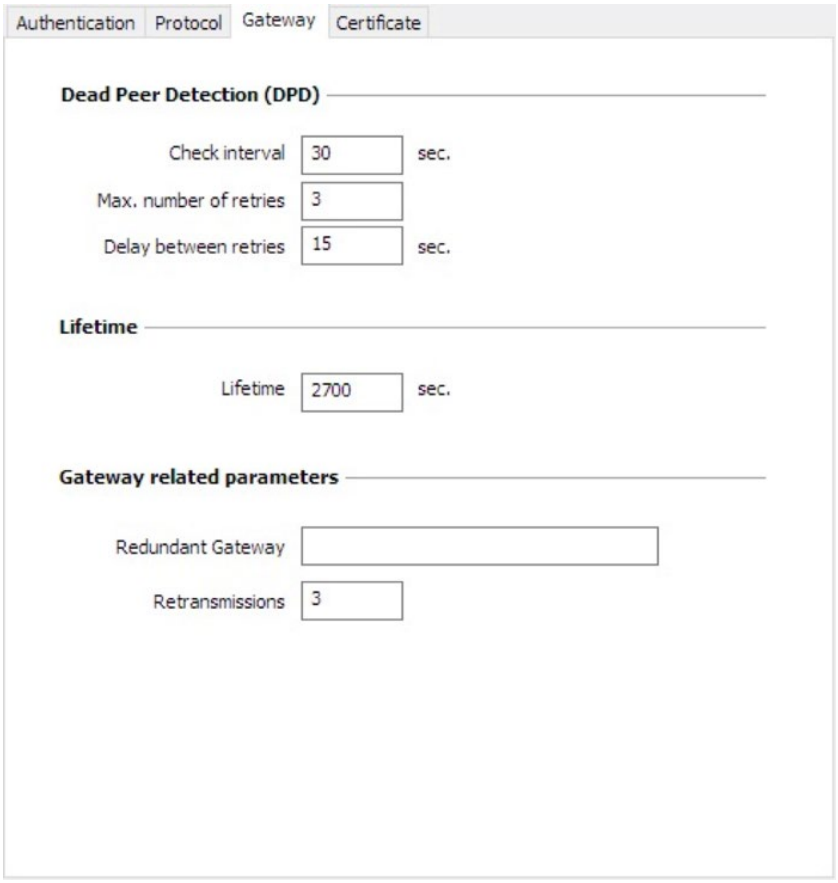
- Virtual IP address of the VPN Client
- DNS server address (optional)
- WINS server address (optional)

Mode Config will only be operational if the VPN gateway supports it.

When Mode Config is disabled, the three items "VPN Client address", "DNS server" and "WINS server" can be configured manually in the VPN Client (see sections 13.3.6 Phase 2: IPsec and 13.3.7 Phase 2: Advanced).

Similarly, when Mode Config is enabled, the Phase 2 fields "VPN Client address", "DNS server" and "WINS server" will be automatically filled in when a VPN tunnel is opened. Therefore, no data can be entered in them (they are grayed out).

13.3.3 Phase 1: Gateway



Dead Peer Detection (DPD)

Dead Peer Detection	The Dead Peer Detection (DPD) function enables the VPN Client to detect whether the VPN gateway has become unreachable or inactive. (1) - Check interval: Time interval between two DPD check messages, expressed in seconds. - Max. number of retries: Number of consecutive unsuccessful attempts before concluding that the VPN gateway is unreachable. - Delay between retries: Time between two DPD messages when the VPN gateway is not responding, expressed in seconds.

(1) The DPD function is activated once the tunnel is open (phase 1 established). When linked to a redundant gateway, DPD allows the VPN Client to automatically switch between gateways when one of them is unavailable.

Lifetime

Lifetime	Lifetimes are negotiated when the tunnel is established. (1) When the lifetime is reached, the Phase 1 will be renegotiated. The default value for the lifetime of the Phase 1 is 2700 s (45 min).

(1) Lifetimes are negotiated between the VPN Client and the VPN gateway. However, some gateways simply return the lifetime value suggested by the VPN Client. Regardless of the method used, the VPN Client will always apply the lifetime value sent by the VPN gateway.

Gateway-related parameters

Redundant gateway	Defines the address of a spare VPN gateway that the VPN Client will switch to when the initial gateway is unavailable or unreachable. The address of the redundant VPN gateway can be either an IP or a DNS address. ☞ Refer to chapter 14 Redundant gateway.
Retransmissions	Number of IKE protocol message resent when the gateway is not responding. Once this number of retransmission attempts is reached, the tunnel is declared as failing.

13.3.4 Phase 1: Certificate

☞ Refer to chapter 18 Managing certificates.

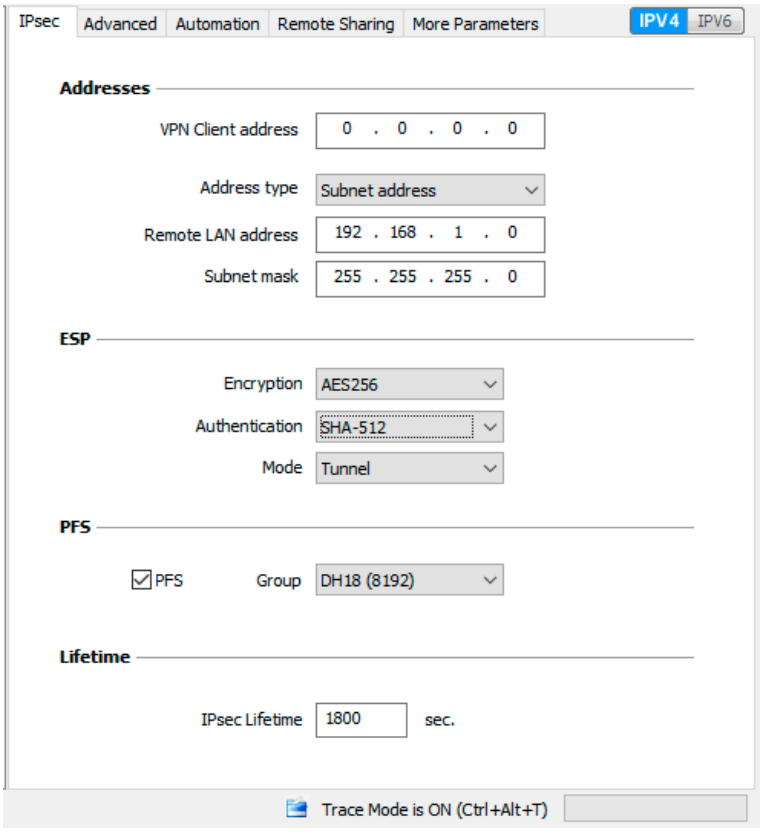
13.3.5 Phase 2

Phase 2 of a VPN tunnel is the IPsec phase. The purpose of this Phase is to negotiate the security parameters that will be applied to the data going through the VPN tunnel.

In order to configure the Phase 2 parameters, select the relevant Phase 2 in the Configuration Panel VPN tree. The parameters can be configured in the right-hand tabs of the Configuration Panel.

If any changes are made to a tunnel, it will appear in bold in the VPN tree. You do not need to save a VPN configuration for it to be taken into account. The tunnel can be tested with the modified configuration immediately.

13.3.6 Phase 2: IPsec



Addresses

VPN Client address	"Virtual" IP address of the workstation, the way it will be "seen" on the remote network. From a technical standpoint, it is the source IP address of the IP packets going through the IPsec tunnel. When the field is set to "0.0.0.0" the software will use the workstation's physical IP address automatically for the virtual IP address provided to the gateway.
	When Mode Config is enabled, this field will be grayed out (uneditable). It is automatically filled in when the tunnel is opened with the value sent by the VPN gateway during the Mode Config exchange.
Address type	The endpoint of the tunnel can be a network or a remote workstation. ☞ To find out how to configure the address type, refer to the paragraph entitled **Configuring the Address type** below.

ESP

Encryption	Encryption algorithm negotiated during the IPsec phase (1): Auto (2), AES-128, AES-192, AES-256.
Authentication	Authentication algorithm negotiated during the IPsec phase (1): Auto (2), SHA2-256, SHA2-384, SHA2-512.
Mode	IPsec encapsulation mode: Tunnel or Transport (1)

(1) Refer to chapter 26 Security recommendations on the choice of algorithm.

(2) Auto means that the VPN Client automatically adapts to the gateway parameters.

PFS

PFS - Group	Can be enabled or disabled. Length of Diffie-Hellman key: DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192)
	IKEv1 does not have an automatic mode for the DH group. It must be specified beforehand. Refer to chapter 26 Security recommendations on the choice of algorithm.

Lifetime

Lifetime	Lifetimes are negotiated when the tunnel is established. (1) When the lifetime is reached, the Phase 2 will be renegotiated. The default value for the lifetime of Phase 2 is 1800 s (30 min).

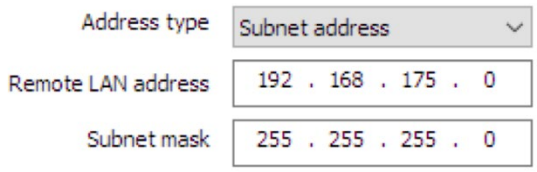
(1) Lifetimes are negotiated between the VPN Client and the VPN gateway. However, some gateways simply return the lifetime value suggested by the VPN Client. Regardless of the method used, the VPN Client will always apply the lifetime value sent by the VPN gateway.

IPv4/IPv6

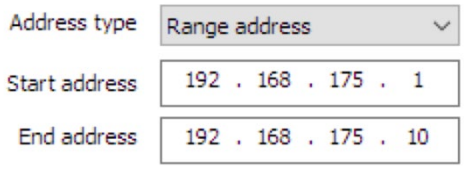
IPv4-IPv6	Refer to chapter 17 IPv4 and IPv6.

Configuring the Address type

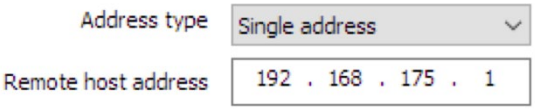
If the endpoint of the tunnel is a network, choose the "Subnet address" type and then enter the Remote LAN address and Subnet mask:



As an alternative, you can also select "Range address" and enter the Start and End addresses:



If the endpoint of the tunnel is a workstation, choose the "Single address" type and then enter the Remote host address:



The function "Automatically open this tunnel on traffic detection" is used to automatically open a tunnel when traffic with one of the addresses specified in the address range is detected (provided that this address range is authorized in the VPN gateway configuration).

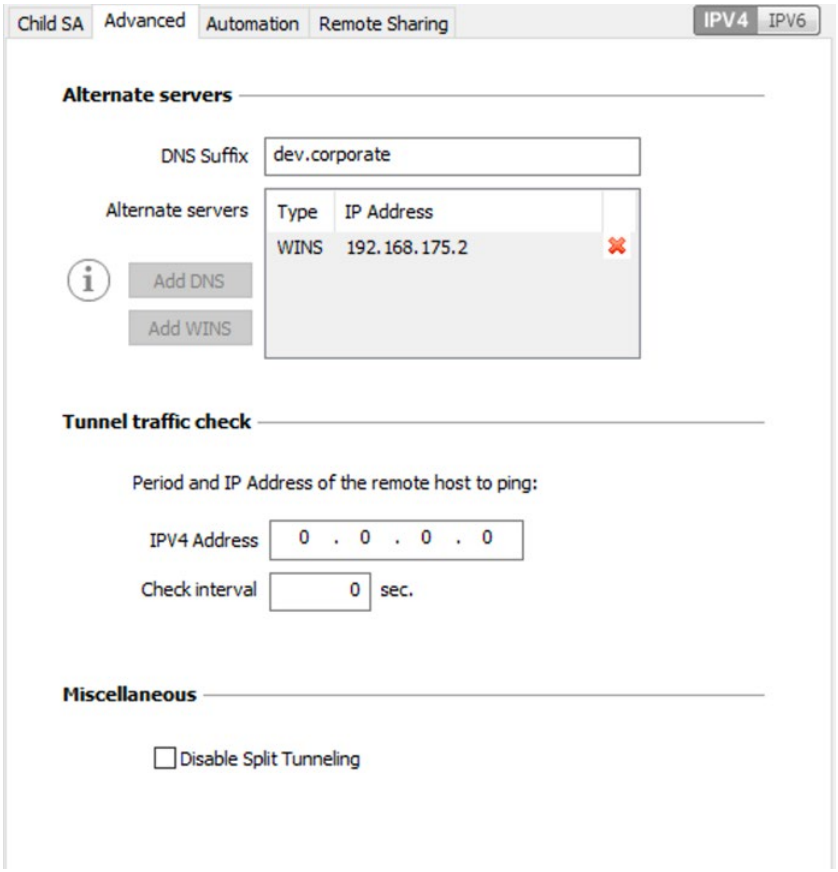
If the IP address of the VPN Client workstation is included in the address range for a remote network (e.g. @workstation IP=192.168.10.2 and @remote network=192.168.10.x), then opening a tunnel will prevent the workstation from communicating on the local network. All communications will go through the VPN tunnel.

"All traffic through the VPN tunnel" configuration

The VPN Client can be configured so that all the workstation's outbound traffic goes through the VPN tunnel. To implement this function, select "Subnet address" as the address type and enter "0.0.0.0" as the Remote LAN address and Subnet mask.

Several VPN Client configuration guides for various VPN gateways are available on our website at: https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-routers/.

13.3.7 Phase 2: Advanced



Alternate servers

DNS Suffix	Domain extension added to each machine name, for example: "mozart.dev.corporate". This is an optional parameter: When it is specified, the VPN Client will try to translate the machine address without adding the DNS suffix. However, if translation fails, the DNS suffix will be added, and the Client will try to translate the address again.
Alternate servers	Table containing the IP addresses of the DNS (maximum 2) and WINS (maximum 2) servers available on the remote network. The IP addresses will be IPv4 or IPv6 addresses depending on the network type configured in the "IPsec" tab.

When Mode Config is enabled, these fields will be grayed out (uneditable). They are automatically filled in when the tunnel is opened with the values sent by the VPN gateway during the Mode Config exchange.

Tunnel traffic check

IP address	The VPN Client can be configured so that connectivity to the remote network is checked on a regular basis. If connectivity has been lost, the VPN Client will automatically close the tunnel and attempt to open it again. The IPv4/IPv6 field is the address of a machine within the remote network, which should reply to pings sent by VPN Client. If a ping goes unanswered, the connection is considered lost. If the tunnel is configured in IPv4 (see the button at the top right of the tab), then the IPv4 field is displayed. If the tunnel is configured in IPv6, then the IPv6 field is displayed.
Check interval	The "Check interval" indicates the time interval in seconds between two pings sent by the VPN Client to the machine with the IP address specified above.

13.3.8 Phase 2: Automation

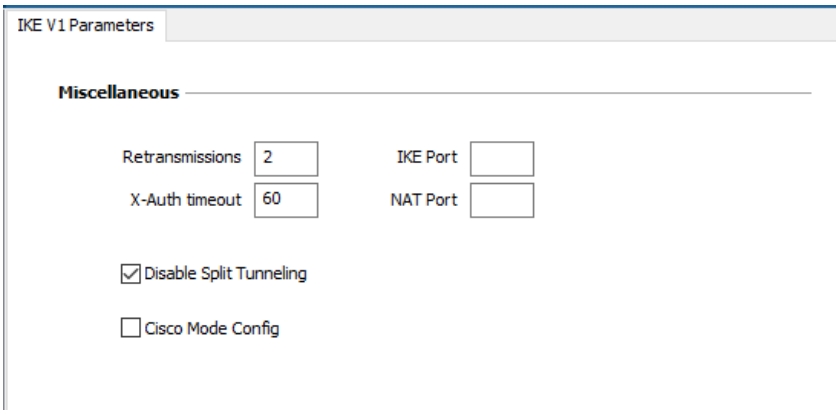
Refer to chapter 15 Automation.

13.3.9 Phase 2: Remote sharing

Refer to chapter 19 Remote Desktop Sharing.

13.3.10 IKEv1 parameters

IKEv1 parameters are common to all IKEv1 tunnels (every Phase 1 and every Phase 2).



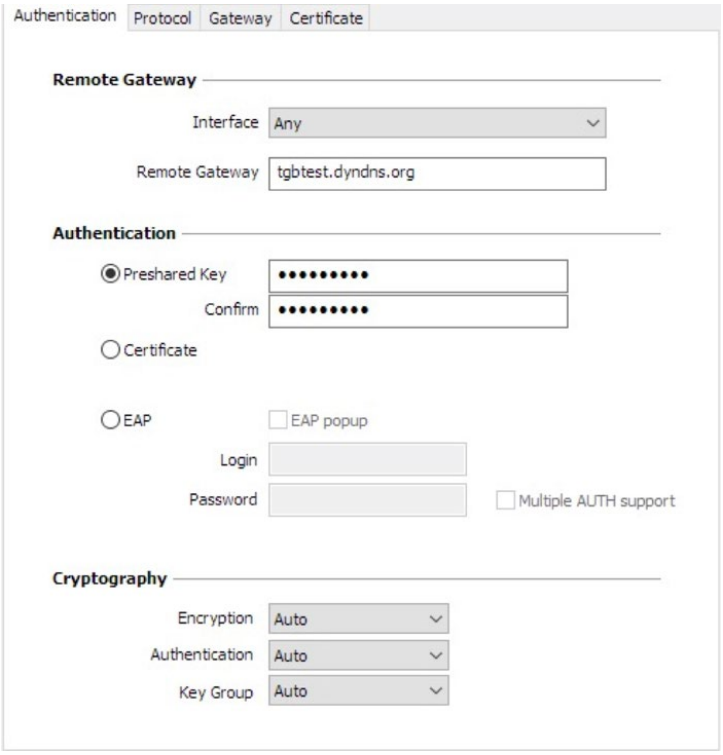
Miscellaneous

Retransmissions	Number of IKE protocol message resends before failure.
X-Auth timeout	Time allowed to enter X-Auth login/password
IKE port	This field is used to configure the IKE port for all IKEv1 tunnels.  The IKE ports that can be configured in every tunnel have the priority over this parameter.
NAT port	This field is used to configure the NAT port for all IKEv1 tunnels.  NAT ports that can be configured in every tunnel have the priority over this parameter.
Disable Split Tunneling	When this option is selected, only the traffic going through the tunnel is authorized. ☞ See note (1) below.
Cisco Mode Config	This box must be checked to ensure compatibility with Cisco ASA-type gateways

(1) The "Disable Split Tunneling" configuration option increases the "leakproofness" of the workstation, provided that the VPN tunnel is open. More specifically, this function eliminates the risk of incoming data flows that do not go through the VPN tunnel.
Combined with the "All traffic through the VPN tunnel" Configuration (see section 13.3.6 Phase 2: IPsec), this option guarantees the complete leakproofness of the workstation provided the VPN tunnel is open.

13.4 Configuring an IPsec IKEv2 tunnel

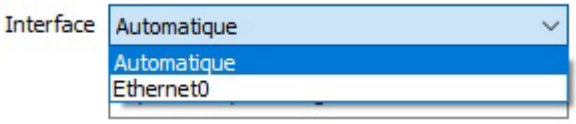
13.4.1 IKE Auth: IKE SA



Addresses

Interface

Name of the network interface on which the VPN connection is open.
You can let the software automatically decide which interface to use by selecting "Any".



We recommend choosing this option if the tunnel being configured is to be deployed on a different workstation.

In case several IP addresses are assigned to the network interface, you can specify a specific IP address or subnet to be used. To do this, add the "local_subnet" dynamic parameter on the "IKE Auth" tab (see Displaying more parameters in section 24.2 General) and define its value to the IP address of the desired suubnet using the aaa.bbb.ccc.ddd/xx format, e.g. 192.168.0.0/24 to specify the 192.168.0.1 – 192.168.0.255 subnet. To specify a single IP address, use the value 32 for the subnet mask, e.g. 192.168.0.2/32 to specify the IP address 192.168.0.2.

This last feature is only available for IPv4.

Remote Gateway	IP (IPv4 or IPv6) or DNS address of the remote VPN gateway. This field is mandatory.

Authentication

Preshared key	Password or key shared by the remote gateway. The preshared key is an easy way to configure a VPN tunnel. However, it is less flexible in terms of security management than the use of certificates. Refer to chapter 26 Security recommendations.
Certificate	Use of certificates for VPN connection authentication. Using Certificate strengthens the security in terms of VPN connection management (mutual authentication, verification of validity periods, revocation, etc.) Refer to chapter 26 Security recommendations. Refer to the dedicated chapter: 18 Managing certificates.
EAP	The Extensible Authentication Protocol (EAP) mode is used to authenticate the user based on a login name and password. When the EAP mode is selected, a popup window will prompt the user to enter a login name and password every time the tunnel is opened. When the EAP mode is selected, you can choose to display a prompt for the EAP login name and password every time the tunnel is opened (using the "EAP popup" checkbox) or to store them in the VPN configuration by entering them in the Login and Password fields. We recommend not to use the latter mode (see chapter 26 Security recommendations).
Multiple AUTH support	Enables the combination of certificate and EAP authentications. (1)

(1) The VPN Client supports "Certificate then EAP" double authentication.
The VPN Client does not support "EAP then Certificate" double authentication.

Cryptography

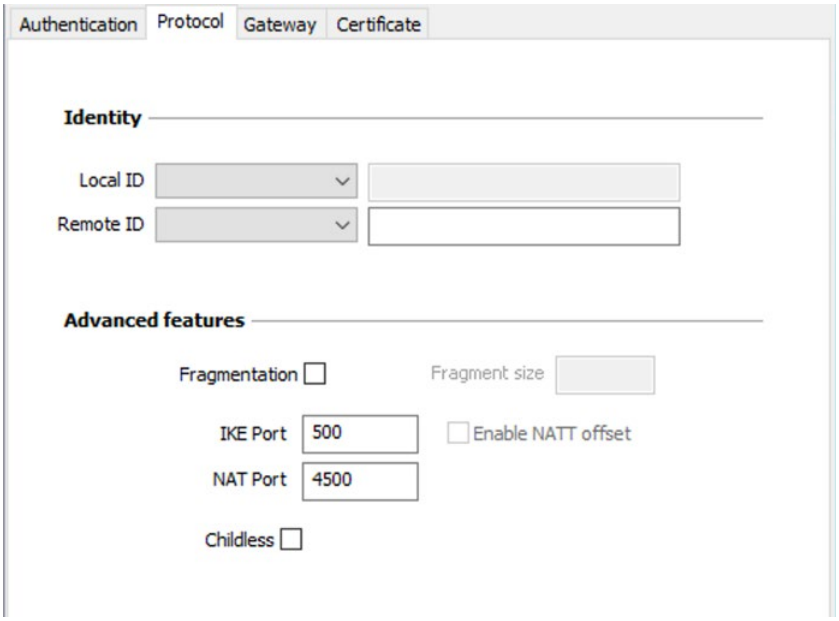
Encryption	Encryption algorithm negotiated during the authentication phase (1): Auto (2), AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Authentication	Authentication algorithm negotiated during the authentication phase (1): Auto (2), SHA2 256, SHA2 384, SHA2 512.

Key group	Length of Diffie-Hellman key (1): Auto (2), DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521).

(1) Refer to chapter 26 Security recommendations on the choice of algorithm.

(2) Auto means that the VPN Client automatically adapts to the gateway parameters.

13.4.2 IKE Auth: Protocol



Identity

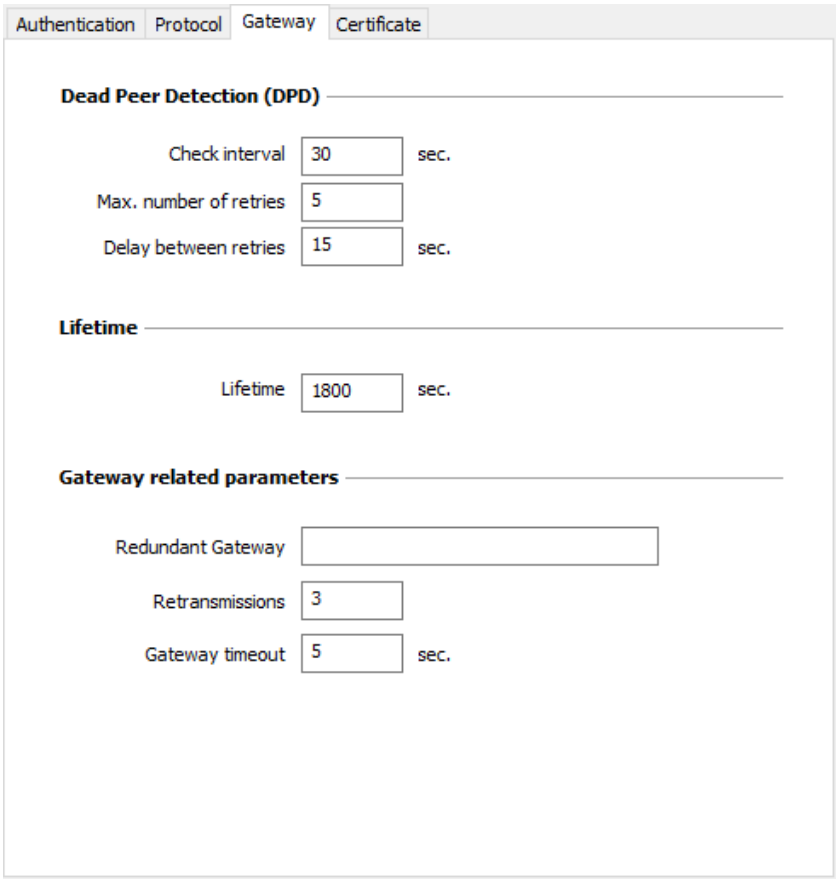
Local ID	"Local ID" is the identifier that the VPN Client sends to the remote VPN gateway during the authentication phase. According to the type selected, this identifier can be any of the following: - IP address: an IPv4 address (type = IPV4 ADDR), e.g. 195.100.205.101 - DNS: a domain name (type = FQDN), e.g. gw.mydomain.net - KEY ID: a character string (type = KEY ID), e.g. 123456 - Email: an email address (type = USER FQDN), e.g. support@thegreenbow.com - DER ASN1 DN: the X.509 subject of a certificate (type = DER ASN1 DN) - X509 subject: this field is automatically filled in with the subject of an X.509 certificate when the tunnel is associated with a user certificate (see chapter 18 Managing certificates) If this parameter is not set, the VPN Client's IP address is used by default.

Remote ID	"Remote ID" is the identifier that the VPN Client expects to receive from the VPN gateway. According to the type selected, this identifier can be any of the following: - IP address: an IP address (type = IPV4 ADDR), e.g. 80.2.3.4 - DNS: a domain name (type = FQDN), e.g. router.mydomain.com - KEY ID: a character string (type = KEY ID), e.g. 123456 - Email: an email address (type = USER FQDN), e.g. admin@mydomain.com - DER ASN1 DN: the X.509 subject of a certificate (type = DER ASN1 DN) This setting is required since version 6.8 for security reasons.

Advanced features

IKEv2 fragmentation	Enables IKEv2 packet fragmentation in accordance with RFC 7383. This function prevents IKEv2 packets from being fragmented by the IP network they're passing through. The fragment size must generally be set to a value that is smaller by 200 than the MTU of the physical interface, e.g. 1300 bytes for a typical MTU of 1500.
IKE port	IKE Auth (Authentication) exchanges use the UDP protocol and port 500 by default. IKE port configuration can bypass the networking hardware (firewall, routers) that filter port 500. The remote VPN gateway must also be able to perform the IKE Auth exchanges on a port other than 500.
NAT port	IKE Child SA (IPsec) exchanges use the UDP protocol and port 4500 by default. NAT port configuration can bypass the networking hardware (firewall, routers) that filter port 4500. The remote VPN gateway must also be able to perform the IKE Child SA exchanges on a port other than 4500. To connect to certain firewalls/gateways configured in "D" mode, NAT-T must be forced from end to end, and the VPN Client must not send the NAT discovery payloads. To do this, add the dynamic parameter "NoNATTNegotiation" with the value set to "true" on the "IKE Auth" tab (refer to the paragraph entitled Displaying more parameters in section 24.2 General).
Enable NATT offset	When the IKE port is different from 500, it may be necessary to check this option for the gateway to accept the connection.
Childless	When this mode is enabled, the VPN Client will attempt to initiate IKE exchanges without creating any Child SA in accordance with RFC 6023. We recommend using this mode.

13.4.3 IKE Auth: Gateway



Dead Peer Detection (DPD)

Check interval	The Dead Peer Detection (DPD) function enables the VPN Client to detect whether the VPN gateway has become unreachable or inactive. (1) The check interval is the time period between two consecutive DPD check messages sent, expressed in seconds.
Max. number of retries	Number of consecutive unsuccessful attempts before concluding that the VPN gateway is unreachable.
Delay between retries	Time between two DPD messages when the VPN gateway is not responding, expressed in seconds.

(1) The DPD function is enabled upon opening the tunnel (after the authentication phase). When linked to a redundant gateway, DPD allows the VPN Client to automatically switch between gateways when one of them is unavailable.

Lifetime

Lifetime	Lifetime of the IKE Authentication phase. The lifetime is expressed in seconds. The default value is 1800 seconds.

Gateway-related parameters

Redundant gateway	Used to define the address of a spare VPN gateway that the VPN Client will switch to when the initial gateway is unavailable or unreachable. The address of the redundant VPN gateway can be either an IP or a DNS address. ☞ Refer to chapter 14 Redundant gateway.
Retransmissions	Number of IKE protocol message resends before failure.
Gateway timeout	Delay between two retransmissions

13.4.4 IKE Auth: Certificate

☞ Refer to chapter: 18 Managing certificates.

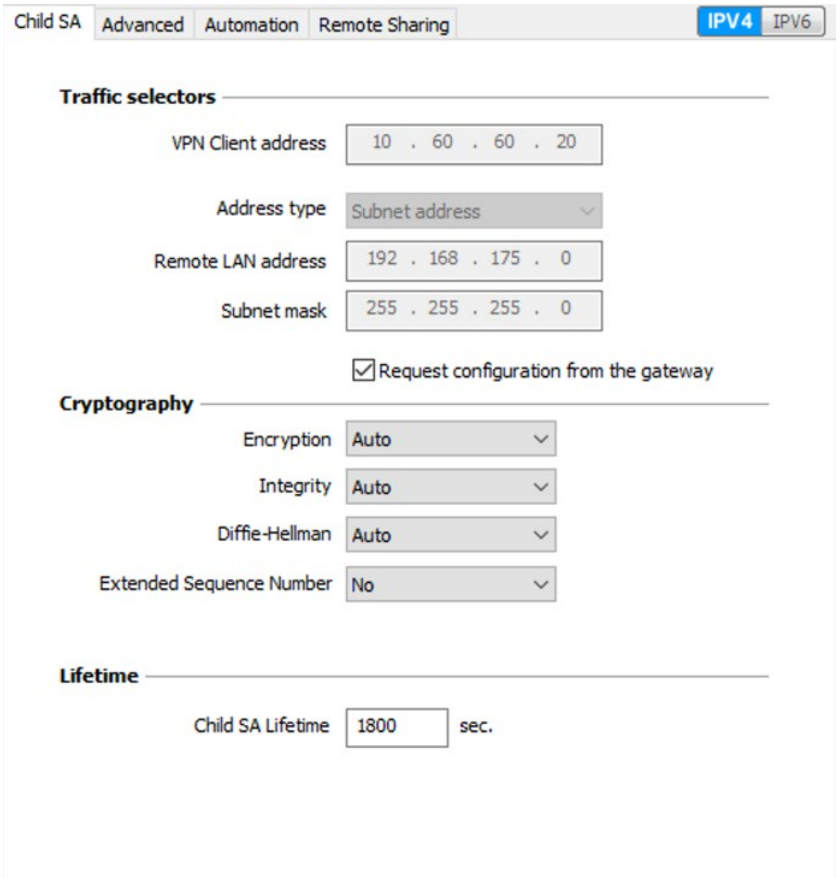
13.4.5 Child SA: Overview

The "Child SA" of a VPN tunnel is the IPsec phase. The purpose of this Phase is to negotiate the security parameters that will be applied to the data going through the VPN tunnel.

To configure Child SA parameters, select the Child SA in the Configuration Panel VPN tree. The parameters can be configured in the right-hand tabs of the Configuration Panel.

If any changes are made to a tunnel, it will appear in bold in the VPN tree. You do not need to save a VPN configuration for it to be taken into account. The tunnel can be tested with the modified configuration immediately.

13.4.6 Child SA: Child SA



Traffic selectors

VPN Client address	"Virtual" IP address of the workstation, the way it will be "seen" on the remote network. From a technical standpoint, it is the source IP address of the IP packets going through the IPsec tunnel.
Address type	The endpoint of the tunnel can be a network or a remote workstation. ☞ To find out how to configure the address type, refer to the paragraph entitled **Configuring the Address type** below.
Request configuration from the gateway	This option (also called "Configuration Payload" or "Mode CP") lets the VPN Client get all the information required for the VPN connection from the gateway: VPN Client addresses, remote network address, subnet mask and DNS addresses. When this option is checked, all corresponding fields are disabled (uneditable). They are filled in dynamically as the tunnel is opened with the values sent by the VPN gateway during the Mode CP exchange.

Cryptography

Encryption	Encryption algorithm negotiated during the IPsec phase (1): Auto (2), AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).

Integrity	Authentication algorithm negotiated during the IPsec phase (1): Auto (2), SHA2 256, SHA2 384, SHA2 512.
Diffie-Hellman	Length of Diffie-Hellman key (1): Auto (2), DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521), No Diffie-Hellman.
Extended Sequence Number	Allows you to use 64-bit extended sequence numbers (see RFC 4304): Auto (2), No, Yes. We recommend using this mode.

(1) Refer to chapter 26 Security recommendations on the choice of algorithm.

(2) Auto means that the VPN Client automatically adapts to the gateway parameters.

Lifetime

Child SA Lifetime	Time interval, expressed in seconds, between two renegotiations. The default value for the Child SA lifetime is 1800 s (30 min).

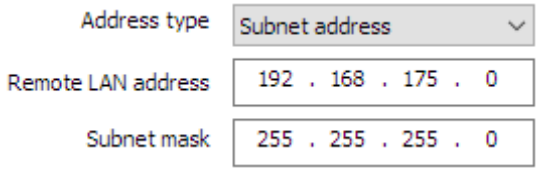
As opposed to IKEv1, in IKEv2 lifetimes are not negotiated between the VPN Client and the gateway. This means that the lifetime of the tunnel will be exactly the lifetime configured in VPN Client.

IPv4/IPv6

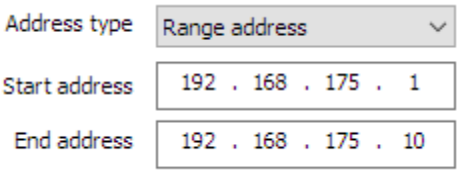
IPv4/IPv6	Refer to chapter 17 IPv4 and IPv6.

Configuring the Address type

If the endpoint of the tunnel is a network, choose the "Subnet address" type and then enter the Remote LAN address and Subnet mask:



As an alternative, you can also select "Range address" and enter the Start and End addresses:



If the endpoint of the tunnel is a workstation, choose the "Single address" type and then enter the Remote host address:

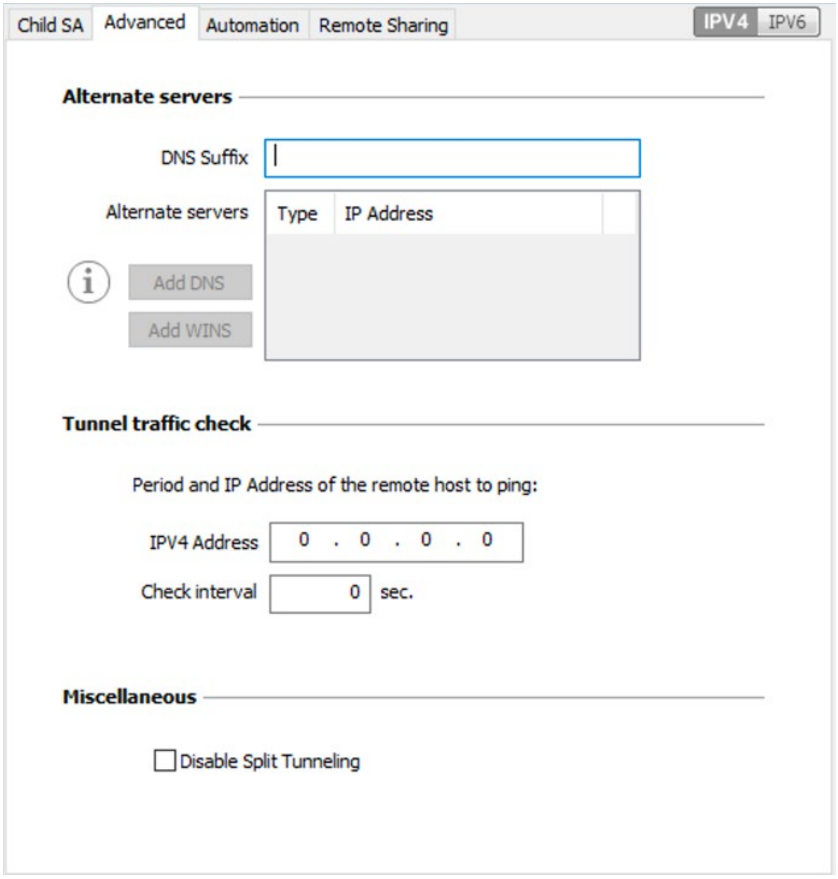
The function "Automatically open this tunnel on traffic detection" is used to automatically open a tunnel when traffic with one of the addresses specified in the address range is detected (provided that this address range is authorized in the VPN gateway configuration).

If the IP address of the VPN Client workstation is included in the address range for a remote network (e.g. @workstation IP=192.168.10.2 and @remote network=192.168.10.x), then opening a tunnel will prevent the workstation from communicating on the local network. All communications will go through the VPN tunnel.

"All traffic through the VPN tunnel" configuration
The VPN Client can be configured so that all the workstation's outbound traffic goes through the VPN tunnel. To implement this function, select "Subnet address" as the address type and specify "0.0.0.0" as the Remote LAN address and Subnet mask.

Several VPN Client configuration guides for various VPN gateways are available on our website at: https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-routers/.

13.4.7 Child SA: Advanced



Alternate servers

DNS Suffix	Domain suffix to be added to all machine names, e.g. "mozart.dev.thegreenbow". This is an optional parameter: When it is specified, the VPN Client will try to translate the machine address without adding the DNS suffix. However, if translation fails, the DNS suffix will be added, and the Client will try to translate the address again.
Alternate servers	Table containing the IP addresses of the DNS (maximum 2) and WINS (maximum 2) servers available on the remote network. The IP addresses will be IPv4 or IPv6 addresses depending on the network type configured in the "Child SA" tab.

When Mode CP is enabled (see the "Request configuration from the gateway" parameter in the "Child SA" tab), these fields will be grayed out (uneditable). They are automatically filled in as the tunnel is opened with the values sent by the VPN gateway during the Mode CP exchange.

Tunnel traffic check

Traffic check when tunnel is opened	The VPN Client can be configured so that connectivity to the remote network is checked on a regular basis. If connectivity has been lost, the VPN Client will automatically close the tunnel and attempt to open it again. The IPv4/IPv6 field is the address of a machine within the remote network, which should reply to pings sent by VPN Client. If a ping goes unanswered, the connection is considered lost.

If the tunnel is configured in IPv4 (see the button at the top right of the tab), then the IPv4 field is displayed. If the tunnel is configured in IPv6, then the IPv6 field is displayed.

Check interval	The "Check interval" indicates the time interval in seconds between two pings sent by the VPN Client to the machine with the IP address specified above.

Miscellaneous

Disable Split Tunneling	When this option is selected, only the traffic going through the tunnel is authorized. See note (1) below.

(1) The "Disable Split Tunneling" configuration option increases the "leakproofness" of the workstation, provided that the VPN tunnel is open. More specifically, this function eliminates the risk of incoming data flows that do not go through the VPN tunnel.
Combined with the "All traffic through the VPN tunnel" configuration (see section 13.4.6 Child SA: Child SA), this option guarantees the complete leakproofness of the workstation, provided that the VPN tunnel is open.
We recommend using this mode.

13.4.8 Child SA: Automation

Refer to chapter 15 Automation.

13.4.9 Child SA: Remote sharing

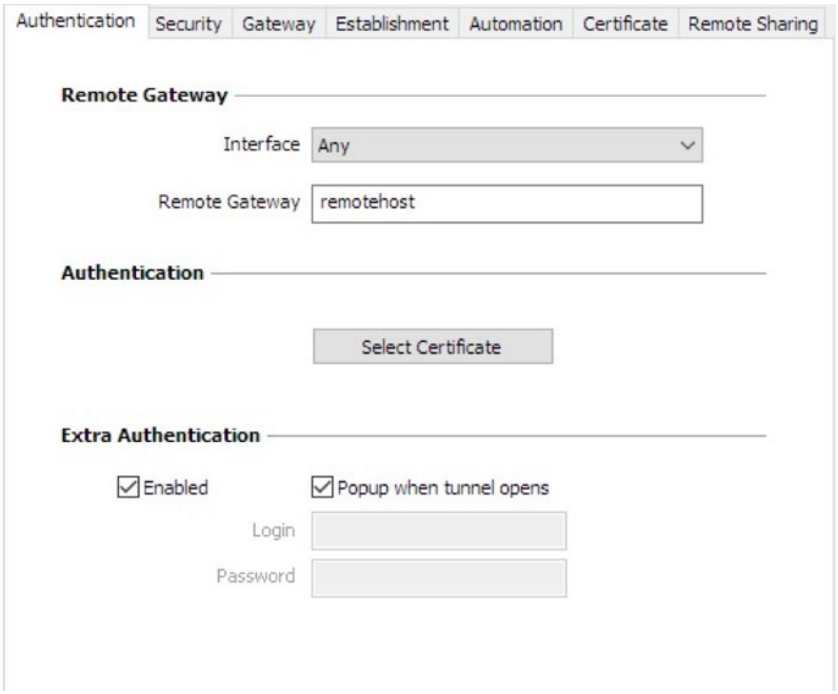
Refer to chapter 19 Remote Desktop Sharing.

13.5 Configuring an SSL VPN tunnel

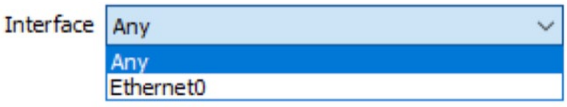
13.5.1 Introduction

Versions 6 and later of the Windows Enterprise VPN Client can be used to open SSL VPN tunnels.
SSL VPN tunnels established by the Windows Enterprise VPN Client are compatible with OpenVPN and can establish secure connections with all gateways implementing this protocol.

13.5.2 Main



Remote Gateway

Interface	Name of the network interface on which the VPN connection is open. You can let the software automatically decide which interface to use by selecting "Any".  We recommend choosing this option if the tunnel being configured is to be deployed on a different workstation.
Remote Gateway	IP (IPv4 or IPv6) or DNS address of the remote VPN gateway. This field is mandatory.

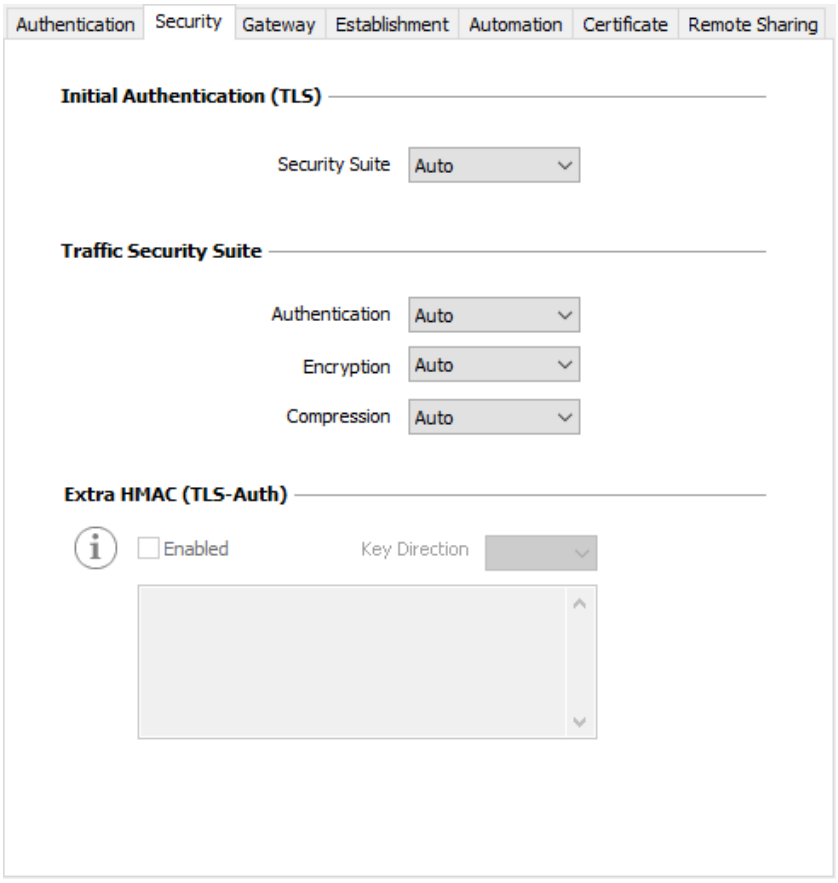
Authentication

Select Certificate	Choose a certificate for VPN connection authentication. Refer to the dedicated chapter: 18 Managing certificates.

Extra Authentication

Extra authentication	This option increases the security level by asking the user to enter a login name and password whenever a tunnel is opened. When the box "Popup when tunnel opens" is checked, users will be prompted for their login name and password whenever they open the tunnel. When it is unchecked, the login name and password must be entered here permanently. Users therefore will not need to enter them every time they open the tunnel.

13.5.3 Security



Initial Authentication (TLS)

Security Suite	This parameter is used to configure the security level of the authentication phase during the SSL exchange. - Auto: All cryptography suites (except null) are sent to the gateway, which will use the best fit. - Low: Only weak cryptography suites are sent to the gateway. In the current version, these are suites that use 64 or 56-bit encryption algorithms. - Normal: Only "medium" cryptography suites are sent to the gateway. In the current version, these are suites that use 128-bit encryption algorithms. - High: Only strong cryptography suites are sent to the gateway. In the current version, these are suites that use 128-bit or higher encryption algorithms. For further information: https://www.openssl.org/docs/man1.1.1/man1/ciphers.html

Traffic Security Suite

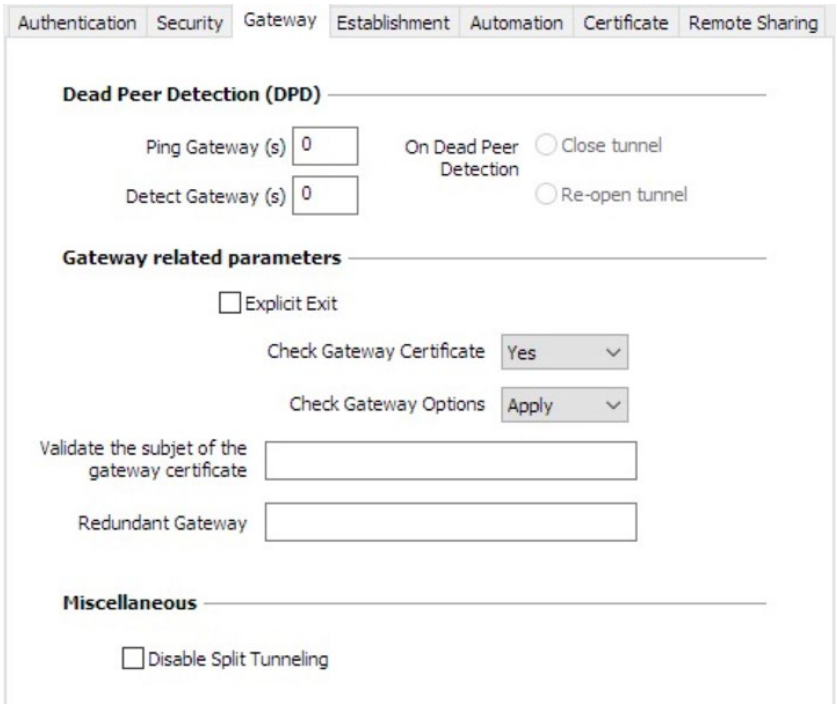
Authentication	Authentication algorithm negotiated for traffic: Auto (1), MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512. If the "Extra HMAC" option is enabled (see below), the authentication algorithm cannot be set to "Auto". It will have to be configured explicitly and must be identical to the one chosen at the gateway end.
Encryption	Traffic encryption algorithm: Auto (1), BF-CBC-128, AES-128-CBC, AES-192-CBC, AES-256-CBC.
Compression	Traffic compression: Auto (1), Lz0, No, Lz4.

(1) Auto means that the VPN Client automatically adapts to the gateway parameters.

Extra HMAC (TLS-Auth)

Extra HMAC	This option adds an authentication layer to the packets exchanged between the VPN Client and the VPN gateway. For this option to be fully operational, it must also be configured on the gateway (on gateways, this option is often referred to as "TLS-Auth"). If this option is enabled, a key must be entered in the field below the checked box. The same key must also be entered on the gateway. It consists of a string of hexadecimal characters, in the following format: -----BEGIN Static key----- 362722d4fbff4075853fbe6991689c36 b371f99aa7df0852ec70352122aee7be … 515354236503e382937d1b59618e5a4a cb488b5dd8ce9733055a3bdc17fb3d2d -----END Static key----- The "Key Direction" must also be defined: - BiDir: The specified key is used in both directions (default mode) - Client: The key direction must be defined as "Server" on the gateway - Server: The key direction must be defined as "Client" on the gateway

13.5.4 Gateway



Dead Peer Detection (DPD)

The Dead Peer Detection (DPD) function enables both endpoints of the tunnel to mutually make sure the other one is active. (1)

Ping Gateway	Period, expressed in seconds, between two pings sent by the VPN Client to the gateway. Sending this ping enables the gateway to determine whether the VPN Client is still active.
Detect Gateway	Time, expressed in seconds, after which the gateway is considered down if no ping has been received.
On Dead Peer Detection	When the gateway is detected as unavailable (i.e. once the "Detect Gateway" time has expired), the tunnel can be closed, or the VPN Client may try to open it again.

(1) The DPD function is enabled once the tunnel is open. When linked to a redundant gateway, DPD allows the VPN Client to automatically switch between gateways when one of them is unavailable.

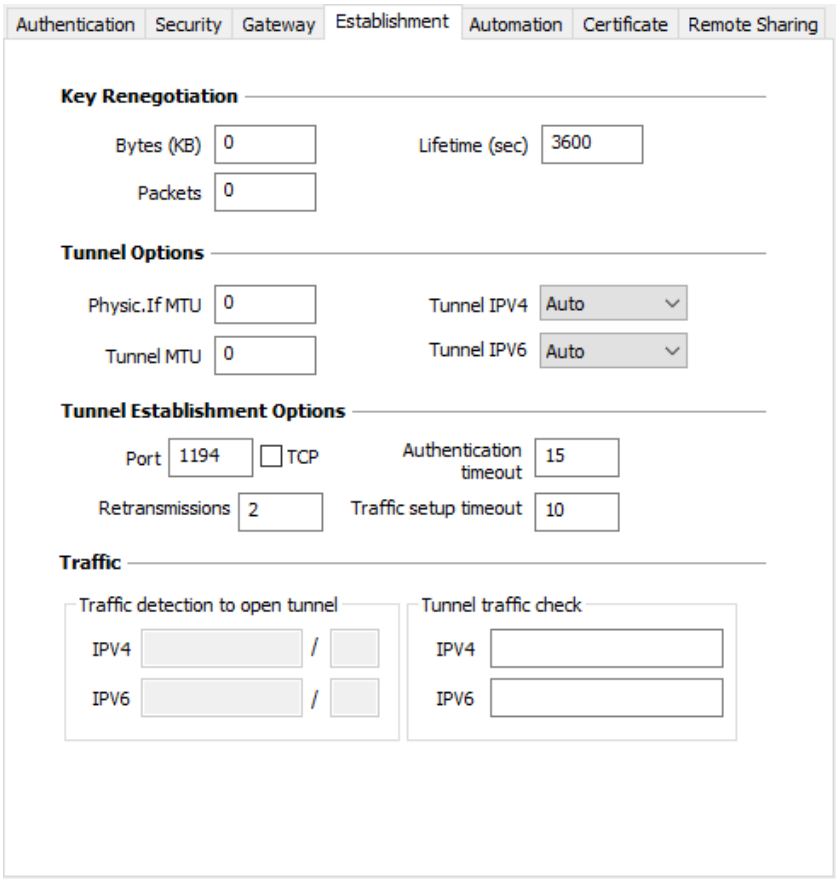
Gateway-related parameters

Explicit exit	This parameter configures the VPN Client to send a specific VPN tunnel closing frame to the gateway when closing the tunnel. If this option is not selected, the gateway will use DPD to close the tunnel at its end, which is less effective.
Check Gateway Certificate	Specifies the control level applied to the gateway's certificate. In the current version, two levels are available: - Yes (the validity of the certificate is verified) - No (the validity of the certificate is not verified) The "Lite" option is reserved for future use and, in the current version, it is equivalent to "Yes". If the "Check gateway certificate signature" option is enabled in the PKI Options (cf. section 24.4 PKI options), the present option on the "Gateway" tab is grayed out and the option is set to "Yes".
Check Gateway Options	Used to determine the coherence level between the VPN tunnel and gateway parameters (encryption algorithms, compression, etc.). - Yes: Coherence is verified for all VPN parameters. The VPN tunnel will not open if any parameter is different. - No: Coherence is not verified before opening the tunnel. The VPN tunnel will try to open, even though no traffic may pass through because certain parameters are not consistent. - Lite: Consistency between the VPN Client and the gateway is only verified for essential parameters. - Apply: Gateway parameters will be applied.
Validate the subject of the gateway certificate	If this field is filled in, the VPN Client will check that the subject of the certificate received from the gateway is, indeed, the one specified.
Redundant gateway	Defines the address of a spare VPN gateway that the VPN Client will switch to when the initial gateway is unavailable or unreachable. The address of the redundant VPN gateway can be either an IP or a DNS address. ☞ Refer to chapter 14 Redundant gateway.

Miscellaneous

Disable Split Tunneling	When this option is selected, only the traffic going through the tunnel is authorized. The "Disable Split Tunneling" configuration option increases the "leakproofness" of the workstation, provided that the VPN tunnel is open. More specifically, this function eliminates the risk of incoming data flows that do not go through the VPN tunnel.

13.5.5 Establishment



Key Renegotiation

Bytes, Packets, Lifetime	Keys can be renegotiated when any of the three criteria (which can be combined) expire: - Traffic volume, expressed in KB - Quantity of packets, expressed in number of packets - Lifetime, expressed in seconds If more than one criterion is set, keys will be renegotiated when the first of these expires.

Tunnel Options

Physical interface MTU	Maximum size of OpenVPN packets. Used to set a packet size so that OpenVPN frames are not fragmented at the network level. The default value for MTU is 0, meaning that the software will use the MTU value of the physical interface.

Tunnel MTU	Virtual interface MTU. When values have been entered, we recommend setting a lower value for the tunnel MTU than that of the physical interface MTU. By default, the MTU is set to 0, meaning that the software will use the MTU value of the physical interface less one fixed delta value.
Tunnel IPv4	Defines the VPN Client's behavior when it receives an IPv4 configuration from the gateway: - Auto: Accepts the information sent by the gateway - Yes: Checks whether the information sent by the gateway matches the configured behavior. If this is not the case, a warning message is displayed on the console and the tunnel is not established. - No: Ignore Please make sure that the "Tunnel IPv4" and "Tunnel IPv6" options are not both set to "No".
Tunnel IPv6	Defines the VPN Client's behavior when it receives an IPv6 configuration from the gateway: - Auto: Accepts the information sent by the gateway - Yes: Checks whether the information sent by the gateway matches the configured behavior. If this is not the case, a warning message is displayed on the console and the tunnel is not established. - No: Ignore Please make sure that the "Tunnel IPv4" and "Tunnel IPv6" options are not both set to "No".

Tunnel Establishment Options

Port/TCP	Port number used to establish the tunnel. The default port value is set to 1194. The tunnel will use UDP by default. The "TCP" option is used to transport the tunnel over TCP.
Authentication Timeout	Time allowed to establish the authentication phase. When this time expires, it is assumed that the tunnel will not open. When this timeout expires, the tunnel is closed.
Retransmissions	Number of retries for sending a protocol message. If there is no response by the time the defined number of retries is reached, the tunnel is closed.
Traffic setup timeout	Tunnel establishment phase: time after which the tunnel is closed, if not all the steps have been completed.

Traffic

Traffic detection to open the tunnel	With OpenVPN, the remote network's details are not configured (they are automatically obtained during the tunnel opening exchange with the gateway). To implement traffic detection with OpenVPN, the remote network's details must therefore be stated explicitly. That is the purpose of the IPv4 and IPv6 fields. It is not mandatory to fill in both fields. The IP field is a sub-network address, configured as an IP address and a prefix length. Example: IP = 192.168.1.0 / 24: the first 24 bits of the IP address are taken into account, i.e. the network: 192.168.1.x These parameters are linked to the traffic detection function. The "Automatically open this tunnel on traffic detection" box must be checked on the "Automation" tab for the IPv4 and IPv6 fields to be enabled.
Tunnel traffic check	If these fields are filled in, the VPN Client will try to ping these addresses after opening the VPN tunnel. The connection status (reply to pings or no reply to pings) is shown in the console. It is not mandatory to fill in both fields. No particular steps are taken if the ping goes unanswered.

13.5.6 Automation

Refer to chapter 15 Automation.

13.5.7 Certificate

Refer to chapter 18 Managing certificates.

13.5.8 Remote sharing

Refer to chapter 19 Remote Desktop Sharing.

14 Redundant gateway

The Windows Enterprise VPN Client can be used to manage a redundant VPN gateway.

When combined with Dead Peer Detection (DPD) settings, this function allows the VPN Client to automatically switch to the redundant gateway as soon as the main gateway is detected as being down or unavailable.

If the DPD is lost and a redundant gateway has been configured, the tunnel will automatically try to open again. You can configure a redundant gateway that is identical to the main one, in order to benefit from the automatic reopening mode without actually having to use two gateways.

The algorithm for taking into account the redundant gateway is as follows:

The VPN Client contacts the initial gateway to open the VPN tunnel.
If the tunnel cannot be opened after N attempts,
the VPN Client contacts the redundant gateway.

The same algorithm applies to the redundant gateway:

If the redundant gateway is unavailable,
the VPN Client will try to open the VPN tunnel with the initial gateway.

The VPN Client will not try to contact the redundant gateway if the initial gateway can be reached, but issues are experienced when opening the tunnel.

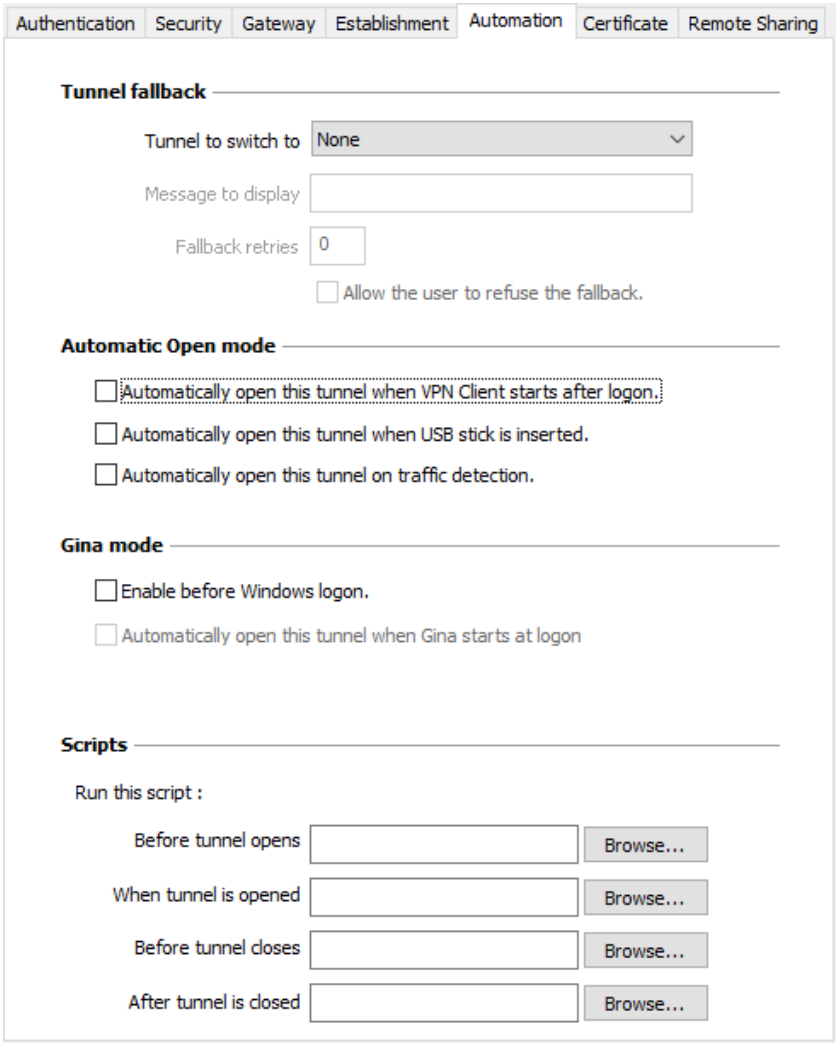
The VPN Client will not try to contact the redundant gateway if the initial gateway cannot be reached due to a DNS resolution issue.

15 Automation

The Windows Enterprise VPN Client can perform automated actions for each VPN tunnel, such as switching to a fallback tunnel, opening the tunnel automatically if certain criteria are met, running batches or scripts at various stages while opening or closing a tunnel, etc.

These automated actions can be performed on any type of tunnel: IKEv1, IKEv2 and SSL.

These automated actions are configured for each tunnel type on the "Automation" tab of the corresponding tunnel: Phase 2 (IKEv1), Child SA (IKEv2) or TLS (SSL).



Tunnel fallback

Refer to chapter 16 Fallback tunnel.

Automatic Open mode

Automatically open this tunnel when VPN Client starts after logon.	The tunnel will automatically open when the VPN Client is started.

Automatically open this tunnel when USB stick is inserted.	If the tunnel is part of a configuration on a USB drive (see chapter 22 USB mode), it will automatically be opened when the USB drive is inserted. If the tunnel is configured with a certificate stored on a smart card or token, it will automatically be opened when the smart card or token is inserted.
Automatically open this tunnel on traffic detection.	The tunnel will automatically open when traffic is detected that is heading towards an IP address on the remote network.

GINA mode

Enable before Windows logon	This option specifies that the VPN connection can be opened before the Windows logon: It appears in the GINA connections window (refer to chapter 23 GINA mode below).
Automatically open this tunnel when GINA starts at logon	When this option is enabled, the tunnel will automatically open before the Windows logon. This option is enabled if the option "Enable before Windows logon" is selected.

Scripts

Before tunnel opens	The specified command line is executed before the tunnel opens.
When tunnel is opened	The specified command line is executed as soon as the tunnel is open.
Before tunnel closes	The specified command line is executed before the tunnel closes.
After tunnel is closed	The specified command line is executed as soon as the tunnel is closed.

The command lines can be as follows:

- Calling a "batch" file, e.g. `C:\vpn\batch\script.bat`
- Running a program, e.g. `C:\Windows\notepad.exe`
- Opening a web page, e.g. `https://my.site`
- etc.

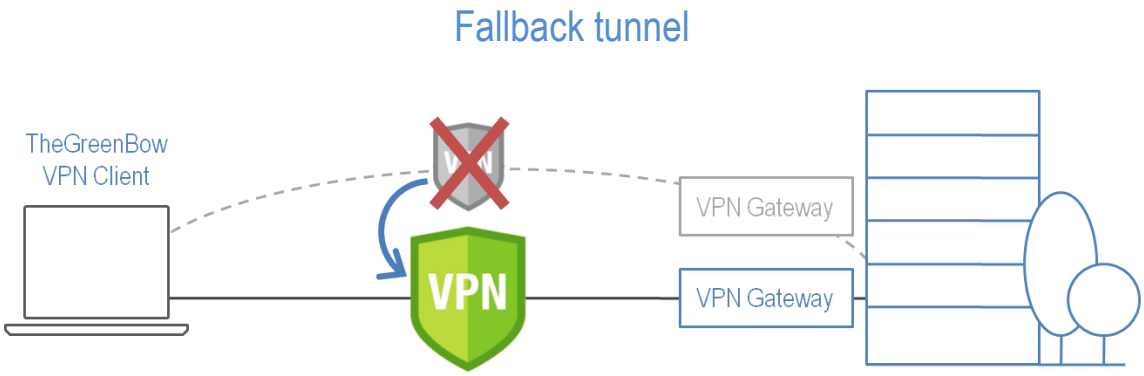
There are many possible applications, such as the following:

- Creating a semaphore file when the tunnel is open, so that a third-party application can detect the instant when the tunnel is open
- Opening one of the company's intranet servers automatically once the tunnel is open
- Cleaning or checking a configuration before opening the tunnel
- Checking the workstation (antivirus is up-to-date, correct versions of applications, etc.) before opening the tunnel
- Automatic cleaning (file deletion) of a workspace on the workstation before closing the tunnel
- Application for counting openings, closings, and durations of VPN tunnels
- Changing the network configuration, once the tunnel has been opened, then restoring the initial network configuration once the tunnel has been closed
- etc.

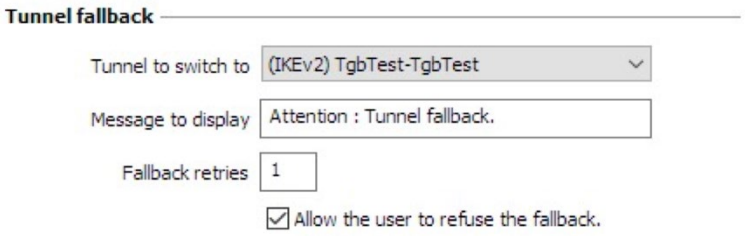
Scripts cannot be configured for a tunnel configured in GINA mode. Data entry fields are disabled.

16 Fallback tunnel

The Windows Enterprise VPN Client is equipped with a fallback tunnel function, which automatically attempts to open a second tunnel if the first one cannot be opened.



This function can be configured on the "Automation" tab of each tunnel (IKEv1, IKEv2 or SSL).



Tunnel to switch to	This field displays the list of tunnels to which the software can automatically switch if the current tunnel is unavailable.
Message to display	As this function can automatically switch from one tunnel to another, with the second being, for example, less secure than the first, this option is used to display a warning message to the user. This message will be displayed every time the connection switches to the fallback tunnel.
Max. number of retries	The number of fallback attempts is set to avoid infinite switching loops (tunnel 1 falling back to tunnel 2 falling back in turn to tunnel 1).
Allow the user to refuse the fallback	Used to configure the fallback function so that the user gets to decide whether to fall back from one tunnel to another.

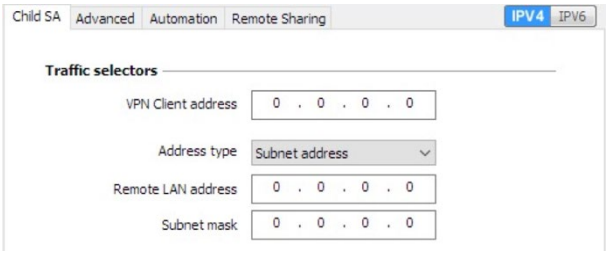
17 IPv4 and IPv6

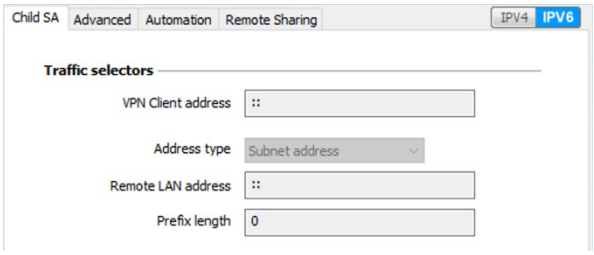
The Windows Enterprise VPN Client is compatible with IPv4 and IPv6 protocols, both for communicating with the gateway and with the remote network. The VPN Client allows you to combine the use of IPv4 and IPv6, for example to open a secure IPv4 connection in a VPN tunnel transported over IPv6.

The choice between IPv4 and IPv6 is made either based on the IP address if it is digital or based on the DNS resolution. In the latter case, the resolution of the gateway name will provide an IPv4 or IPv6 IP address, or both. If both are provided, preference is given to the IPv4 address.

For IKEv1 and IKEv2 VPN tunnels, the IPv4 or IPv6 protocol configuration can be accessed in the top-right corner of the IPsec (for Phases 2 of IKEv1 tunnels) or Child SA (for Child SA of IKEv2 tunnels) tab.

The IP protocol configured using the IPv4/IPv6 button is exactly the same as the protocol used on the remote network.





Choosing between IPv4 and IPv6 has an impact on the settings of the tunnel's other configuration tabs. The IPv4/IPv6 selection button therefore still is shown on the top-right corner of these other tabs, but it is disabled.

For SSL tunnels, the protocol configuration is detected automatically. No configuration is required. Moreover, an SSL tunnel can manage IPv4 and IPv6 traffic simultaneously inside the same tunnel. Unlike for IKEv1 or IKEv2, it is not necessary to configure two separate tunnels.

18 Managing certificates

The Windows Enterprise VPN Client is the VPN connection software for which the innovations in terms of PKI integration are the most advanced on the market. The Windows Enterprise VPN Client is compatible with every PKI on the market in a flexible, scalable, vastly customizable manner, with many automated actions available.

The Windows Enterprise VPN Client includes an unparalleled selection of interfacing functions with all types of certificates, issued by any PKI, and on any type of storage device, such as smart card, token, certificate store, etc.

More specifically, the Windows Enterprise VPN Client implements the following functions and features:

- Use of any type of certificates storage medium: smart card, token, certificate store, file, VPN configuration, USB drive
- Specification of the certificate storage medium to be used: automatic selection between several competing media
- PKCS#11, CSP (IKEv1 only), and CNG access to tokens and smart cards
- Support for X.509 certificate formats: PKCS#12, PEM, PFX
- Select certificates to be used according to multiple criteria: subject, key usage, etc.
- Management of certificates on user's side (the VPN Client's side), such as VPN gateway certificates, including validity dates, certificate chains, root certificates, and CRL management
- Certification authority management (Certificate Authority: CA)
- Validation of client and gateway certificates: mutual authentication with identical or different certification authorities (import specific CAs)
- Possible pre-configuration of all PKI parameters for an automatic integration during installation

The Windows Enterprise VPN Client provides additional security features for PKI management, such as automatically opening or closing a tunnel upon insertion or removal of a smart card or token, or even the ability to configure the PKI interface in the software setup file in order to automate deployment.

The list of smart cards and tokens compatible with the Windows Enterprise VPN Client is available on TheGreenBow's website at: https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-tokens/.

The certificates to be used are configured and specified in the "Certificate" tab of the relevant tunnel: Phase 1 (IKEv1), IKE Auth (IKEv2) or TLS (SSL).

18.1 Selecting a certificate ("Certificate" tab)

The VPN Client can assign a user certificate to a VPN tunnel.
There can only be one certificate per tunnel, but each tunnel can have its own certificate.

The VPN Client allows you to choose a stored certificate:

- In the VPN configuration file (see below "Importing a certificate")
- In the Windows Certificate Store (see below "Windows Certificate Store")
- On a smart card or token (see below "Using a certificate stored on a smart card or token")

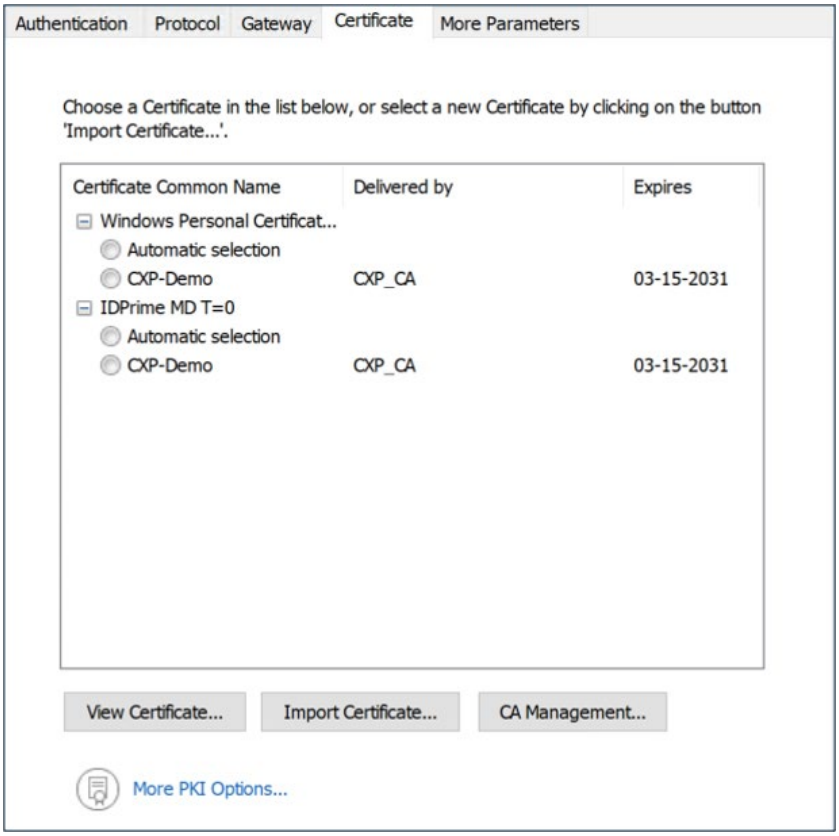
The "Certificate" tab for the relevant tunnel lists all accessible storage media that contain certificates.

- The smart card or token is compatible with CNG, CSP (IKEv1 only), or PKCS#11
- The smart card or token middleware is correctly installed on the computer
- Where appropriate, the smart card is correctly inserted into the corresponding reader

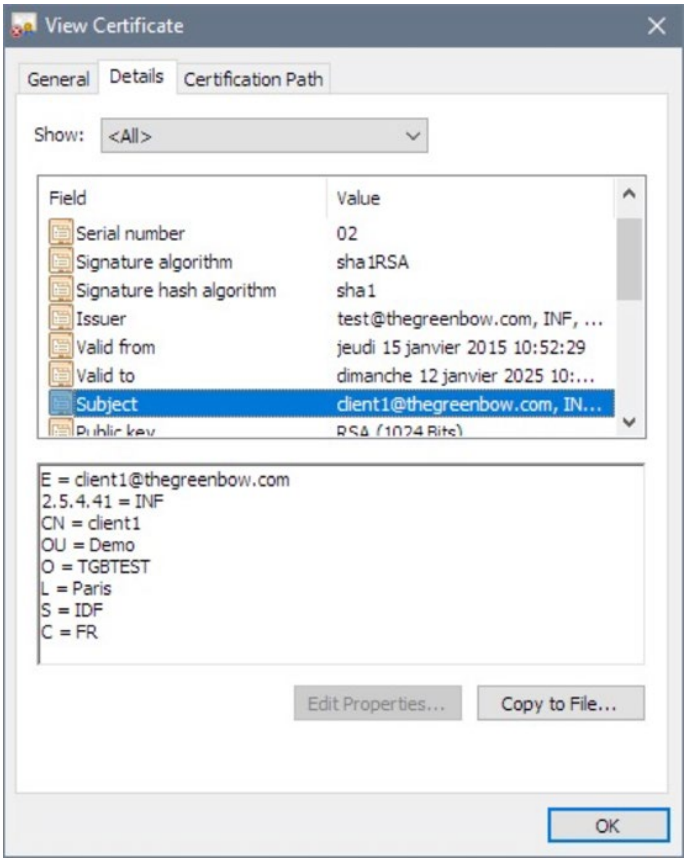
If a medium does not contain any certificates, it simply will not appear in the list (e.g. if the VPN configuration file does not contain any certificates, it will not appear in the list).
Clicking the desired medium displays the list of certificates it contains.
Click the desired certificate to assign it to the VPN tunnel.

For smart cards readers, the reader is displayed with a warning icon in front, if the smart card is not inserted.

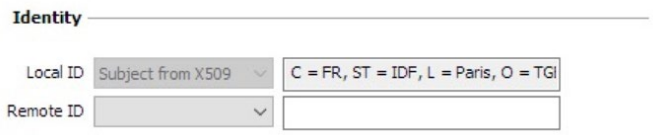
Only available certificates that have not expired are displayed.



Once a certificate has been selected, the "View Certificate" button will show detailed information about the certificate.



Once a certificate has been selected, the tunnel's Local ID type will automatically switch to "X509 subject" or "DER ASN1 DN" and the certificate's subject will be used as the default value of this "Local ID".



18.2 Selecting the certificate automatically

On the "Certificate" tab of the relevant tunnel, you can choose the "Automatic selection" button for certificates stored in the Windows Certificate Store or on a token/smart card. In this case, the VPN Client will automatically select the certificate on the corresponding medium based on either of the following:

- Global criteria defined on the "PKI Options" tab (see section 24.4 PKI options)
- Tunnel-specific criteria defined with dynamic parameters (see below)

You can combine the selection based on the key usage extension with the selection based on the subject.

18.2.1 Selection based on key usage extension

The dynamic parameter "user_cert_keyusage" is used to specify a certificate on a given medium and for a given tunnel based on the key usage extension.

To enable certificate selection based on the key usage extension, add the dynamic parameter "user_cert_keyusage" set to one of the values in the table below on the "IKE Auth" tab (refer to the paragraph entitled Displaying more parameters in section 24.2 General).

0 or undefined	Certificate is not selected based on the "key usage" extension.
1	The certificate whose "key usage" extension contains the value "digitalSignature" is selected.
2	The certificate whose "key usage" extension contains the values "digitalSignature » and "keyEncipherment is selected".
3	The certificate whose "key usage" extension contains the values "digitalSignature" and "clientAuthentication".

This dynamic parameter has the priority over the global setting "Only use authentication certificate" available in the PKI options (see section 24.4 PKI options) or defined with the MSI property KEYUSAGE (refer to the "Deployment Guide").

18.2.2 Selection based on subject

The dynamic parameter "user_cert_dnpattern" is used to specify a certificate on a given medium and for a given tunnel based on the certificate's subject (DN = Distinguished Name).

To enable certificate selection based on the subject, add the dynamic parameter "user_cert_dnpattern" with its value set to a pattern on the "IKE Auth" tab (refer to the paragraph entitled Displaying more parameters in section 24.2 General).

When the dynamic parameter is specified, the Windows Enterprise VPN Client will search for the certificate, whose subject contains the specified subject, on the token or smart card and in the Windows Certificate Store.

When this dynamic parameter is not defined, the VPN Client will search for the first certificate that matches the configured characteristics ("key usage" extension).

This dynamic parameter has the priority over any global setting possibly defined with the MSI property DNPATTERN (refer to the "Deployment Guide").

18.3 Importing a certificate

The Windows Enterprise VPN Client can import certificates in PEM or PKCS12 format to the VPN configuration. This solution is less secure than using the Windows Certificate Store, a smart card, or a token, but it makes it easier to transport certificates.

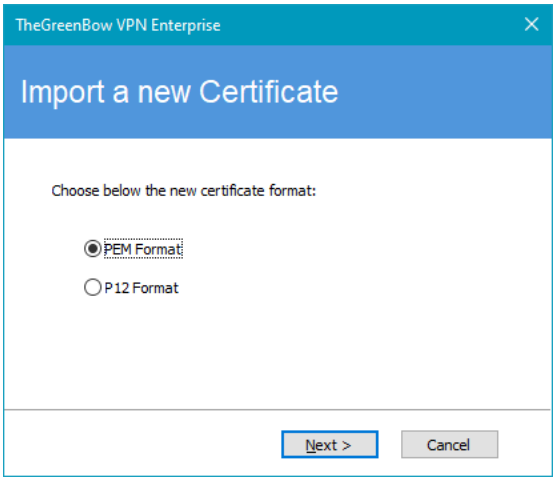
This solution has the advantage of combining the certificate (user-specific) and the VPN configuration (generic) in a single file, which can easily be sent to the user's workstation and imported into the VPN Client.

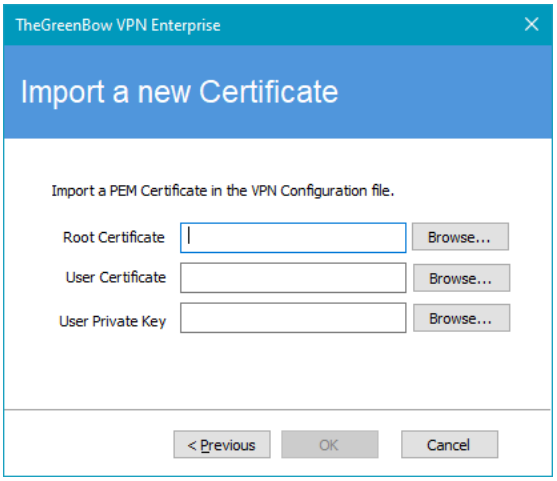
Nevertheless, the disadvantage of transporting certificates in a VPN configuration is that each configuration then becomes user-specific. We therefore do not recommend this solution for a substantial deployment.

Whenever you import a certificate into a VPN configuration, we strongly recommend that you protect the configuration file with a password when you export it (see section 12.2 Exporting a VPN configuration) so that the certificate does not become visible in clear text.

Importing a PEM certificate

1/ On the Certificate tab of a Phase 2, click "Import Certificate…".
2/ Choose "PEM Format".
3/ Click "Browse" to select the root and user certificates as well as the user's private key to import.
4/ Confirm.



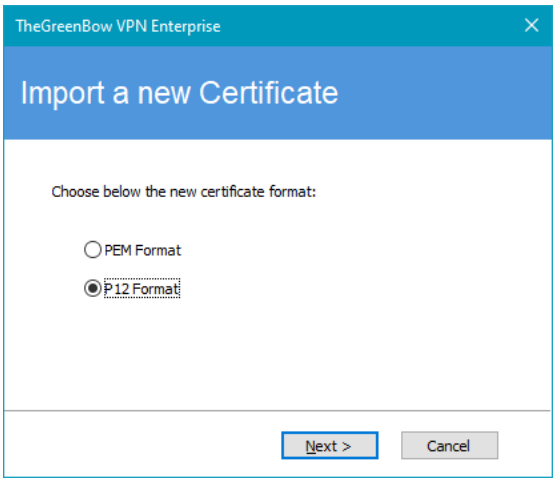


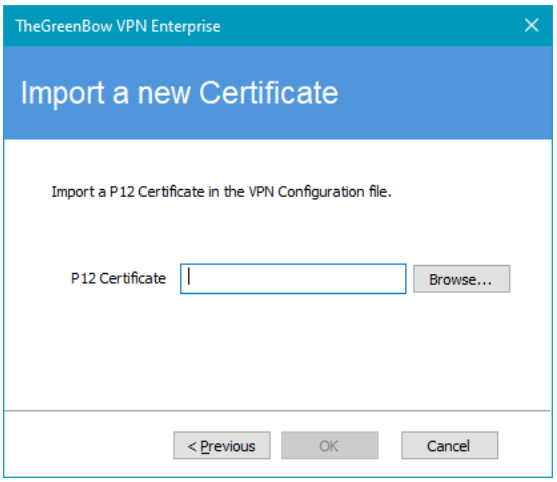
The certificate is shown and is selected in the certificate list displayed on the "Certificate" tab.
Save the VPN configuration: The certificate will be saved in the VPN configuration.

The file containing the private key may not be encrypted.

Importing a PKCS#12 certificate

1/ On the Certificate tab of a Phase 2, click "Import Certificate…".
2/ Choose "P12 Format".
3/ Click "Browse" to select the PKCS12 certificate to import.
4/ If it is password-protected, enter the password and confirm.





The certificate is shown and is selected in the certificate list displayed on the "Certificate" tab.
Save the VPN configuration: The certificate will be saved in the VPN configuration.

18.4 Windows Certificate Store

For the Windows Enterprise VPN Client to identify a certificate available in the Windows Certificate Store, the certificate must meet the following criteria:

- The certificate must be certified by a certification authority (which excludes self-signed certificates)
- The certificate must be located in the "Personal" Certificate Store (it represents the personal identity of the user who wants to open a VPN tunnel to the corporate network) To use the Windows Machine Certificate Store, the `MACHINESTORE` property must be set to 1 when installing the software.

☞ Refer to the "Deployment Guide" for the corresponding instructions.

Microsoft provides a standard management tool (certmgr.msc) to manage the certificates in the Windows Certificate Store. To run this tool, go to the Windows "Start" menu and then enter "certmgr.msc" in the "Search for programs or files" field.

18.5 PKI options: specifying the certificate and its storage device

The Windows Enterprise VPN Client provides several ways in which to specify the certificate to use, as well as to select the smart card reader or token that contains the certificate.

This feature is available under the "More PKI options" link at the bottom of the "Certificate" tab and on the "PKI options" tab of the Options configuration window.

18.6 VPN gateway certificate

We recommend forcing the Windows Enterprise VPN Client to check the certificate chain of the certificate received from the VPN gateway (default behavior).

☞ Refer to the paragraph entitled Checking certificates in section 24.4 PKI options.
To do this, you need to import the root certificate and all certificates in the certificate chain (root certification authority and intermediate certification authorities) to the configuration file.

If the option is checked, the VPN Client will also use the Certificate Revocation List (CRL) of the various certification authorities.
If these CRLs are not in the certificate store, or if these CRLs cannot be downloaded when the VPN tunnel is opened, the VPN Client will not be able to validate the gateway certificate.

Checking each item in the chain implies the following:

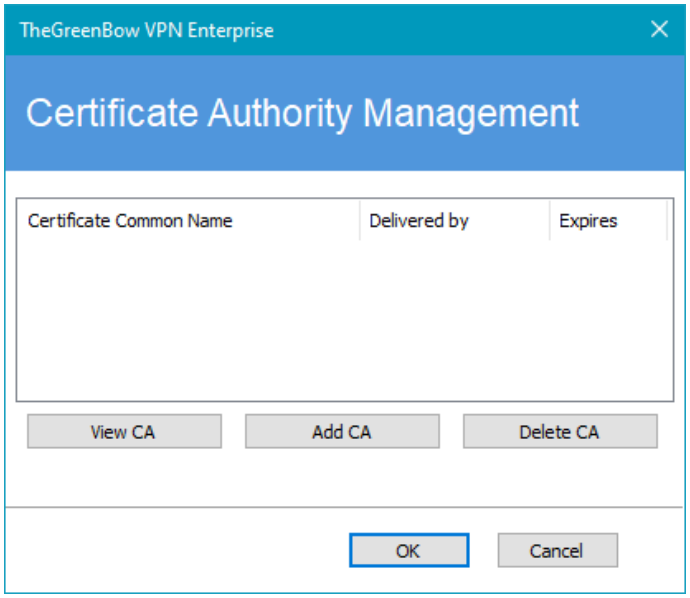
- Checking gateway certificate expiration date
- Checking certificate validity start date
- Checking signatures of all certificates in the certificate chain (including root certificate, intermediate certificates, and server certificate)
- Updating CRLs of all certificate issuers in the certificate chain
- Checking that none of the certificates concerned have been revoked in the corresponding CRL lists

18.7 Managing certification authorities

If the Windows Enterprise VPN Client is configured to check the client and gateway certificates, you may need to import Certification Authorities (CAs) in addition to the certificates used.
This is particularly the case any time the software is unable to find the gateway certificate's CA locally, i.e. in the following situations:

1/ The gateway certificate's CA is different from the client's, and this gateway CA is not available/accessible on the workstation.
2/ The gateway certificate's CA is the same as the client's, but the client's CA is stored on a smart card or token. In this case, the software cannot access it.
3/ The EAP mode is selected (this mode does not require a client certificate), and the gateway certificate's CA is not available/accessible on the workstation.

As of version 6.8 of the Windows Enterprise VPN Client, for security reasons, the Windows Certificate Store can no longer be used to access CAs.



1/ In the "Certificate Authority Management" window, click "Add CA".
2/ Choose the desired CA certificate type (PEM or DER).
3/ Select ("Browse") the CA to import.

In the current version of the Windows Enterprise VPN Client, you cannot add more than three CAs to a configuration.

18.8 Using a certificate stored on a smart card or token

When a VPN tunnel is configured to use a certificate stored on a smart card or token, users will be prompted for the PIN code required to access this smart card or token every time a tunnel is opened.

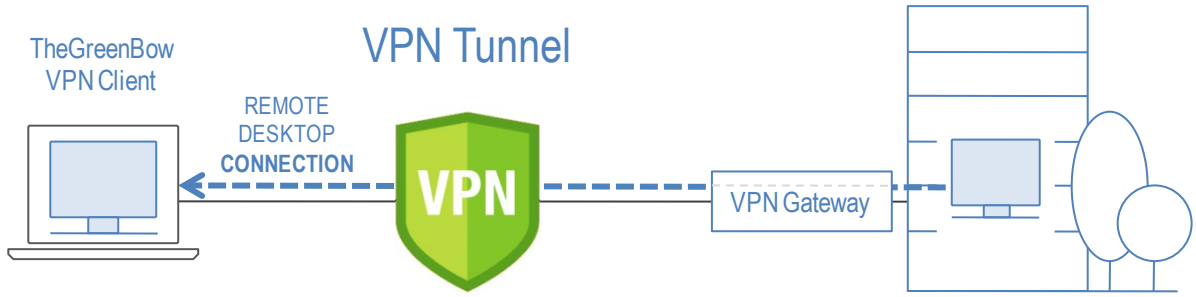
If the smart card is not inserted or the token cannot be accessed, the tunnel will not open.
If the certificate found does not meet the configured criteria (see section 18.5 PKI options: specifying the certificate and its storage device above), the tunnel will not open.
If an incorrect PIN code is entered, the Windows Enterprise VPN Client will show a warning, informing users that they only have three (in most cases) consecutive attempts to unlock the smart card or token.

The Windows Enterprise VPN Client implements a mechanism to automatically detect smart card insertion.
Tunnels that are associated with a certificate stored on a smart card will therefore be established automatically when the smart card is inserted. Likewise, removing the smart card will close all the corresponding tunnels.
To implement this function, check "Automatically open this tunnel when a USB stick is inserted" (see section 15 Automation).

19 Remote Desktop Sharing

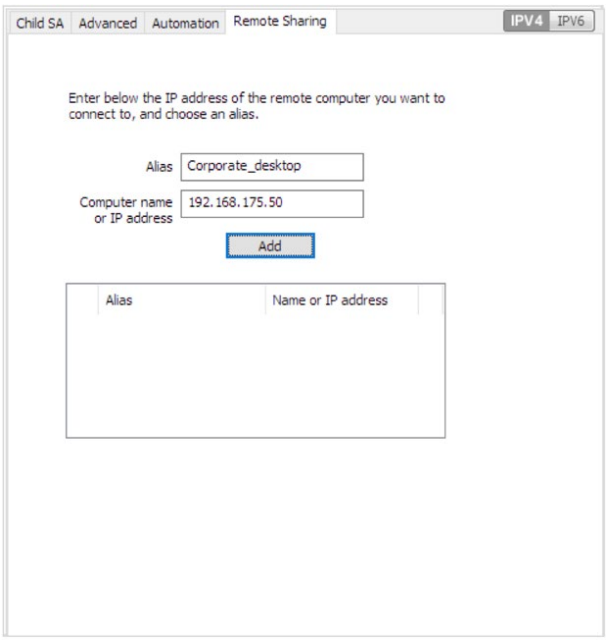
Opening a "Remote desktop" session on a Windows computer over the internet usually requires that you establish a secure connection and enter the connection parameters (address of the remote computer, etc.).

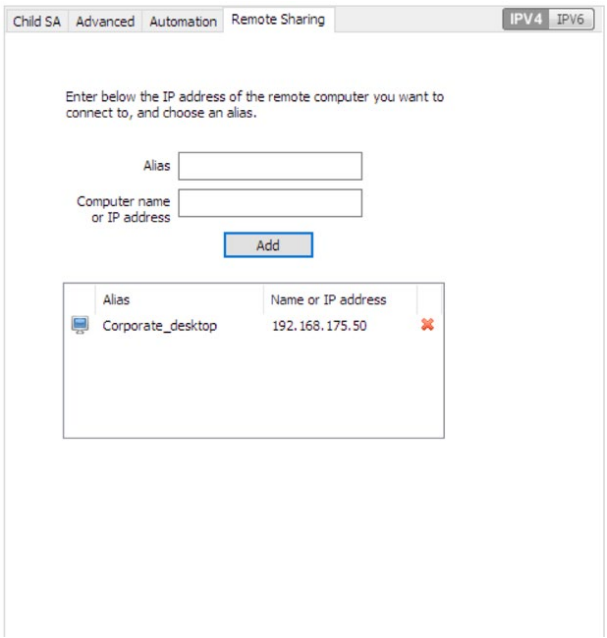
The Windows Enterprise VPN Client allows you to simplify and automatically secure the opening of a Remote Desktop session: The VPN connection to the remote workstation is established and the Remote Desktop Protocol (RDP) session automatically opens on this remote workstation with a single click.



To set up Remote Desktop Sharing, proceed as follows:

1/ Select the VPN tunnel (Phase 2, Child SA, or TLS) in which the "Remote desktop" session will be opened.
2/ Select the "Remote Sharing" tab.
3/ Enter an alias for the connection (the name will be used to identify the connection in the various software menus), then enter the IP address or the Windows name of the remote workstation.
4/ Click "Add". The Remote Desktop Sharing (RDP) session will be added to the list of sessions.

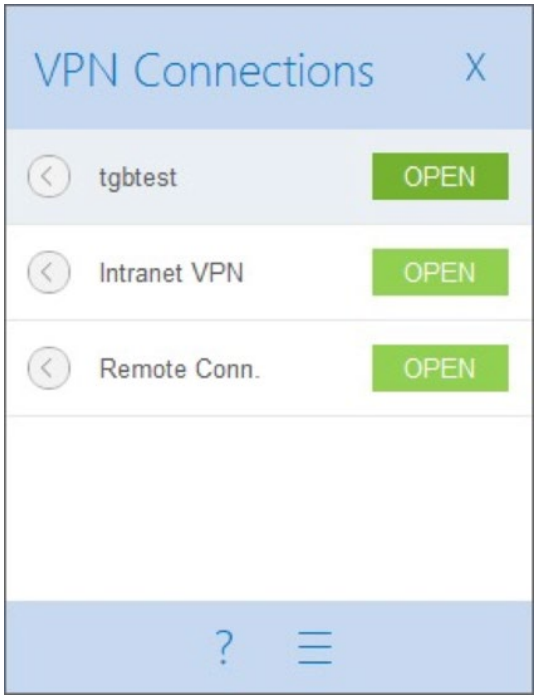




To open this RDP connection with a single click, we recommend displaying it specifically in the Connection Panel using the function described in detail in the section entitled "Configuring the Connection Panel" below.

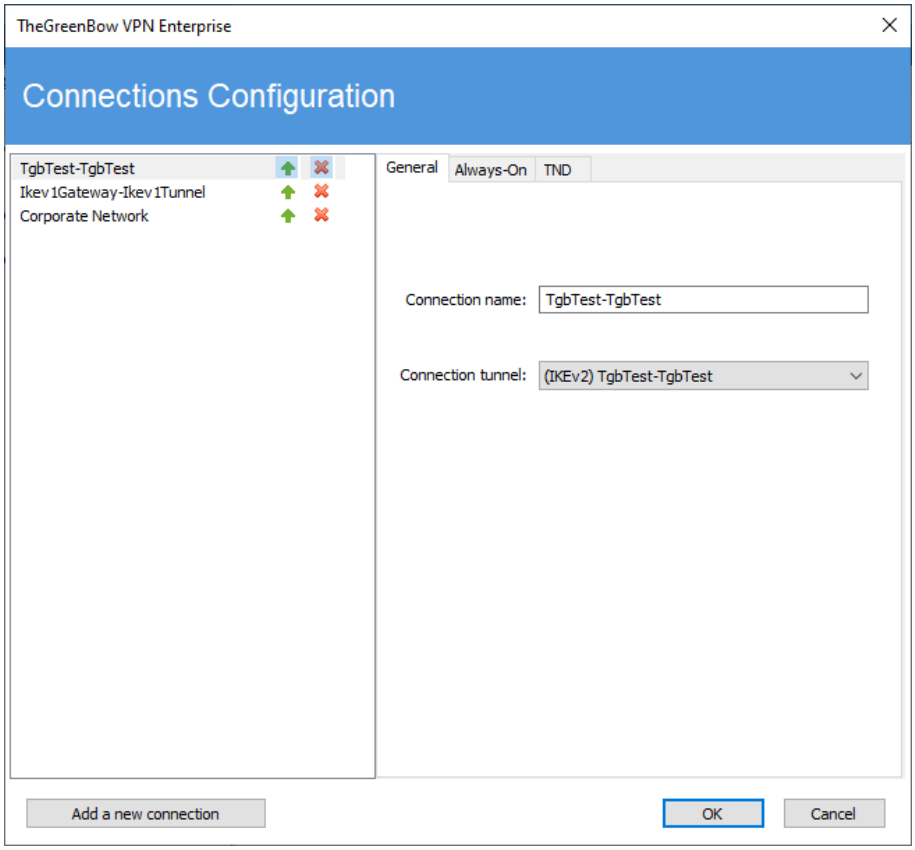
20 Configuring the Connection Panel

The Connection Panel of the Windows Enterprise VPN Client is entirely configurable.



VPN connections can be VPN tunnels or "Remote desktop" connections, i.e. a VPN tunnel for which the "Remote desktop" function has been specified.

A window that can be accessed from the "Tools > Connections Configuration" menu allows you to manage VPN connections in the Connection Panel, i.e. creating, naming, and sorting them.



The configuration window in the Connection Panel is used for the following actions:

- Choosing the VPN connections that are shown in the Connection Panel
- Creating and sorting VPN connections
- Renaming VPN connections
- Configure Always-On in the TrustedConnect Panel
- Configure Trusted Network Detection (TND) in the TrustedConnect Panel

The left side of the window shows the list of connections as they appear in the Connection Panel.

The right side contains the following three tabs:

- General
- Always-On
- TND

The General tab shows the parameters of each connection: its name, the associated VPN tunnel and possibly the Remote Desktop Sharing (RDP) connection, if it has been configured.

To create a new VPN connection, click "Add a new connection", choose a name and select the corresponding VPN tunnel. If a Remote Desktop Sharing connection is configured, an option used to select it automatically appears below the selected tunnel. Once they have been confirmed, changes made in the Connection Panel configuration window instantly appear in the Connection Panel.

The Always-On and TND tabs are described in the next chapter: Managing the TrustedConnect Panel.

The configuration of the Connection Panel is stored in the VPN configuration file. Therefore, it can be exported into `.tgb` files, which are useful for deploying an identical Connection Panel across all workstations.

21 Managing the TrustedConnect Panel

The TrustedConnect Panel is described in chapter 10 TrustedConnect Panel. It allows you to automatically open a VPN connection when you're outside the trusted network and keep the connection open even if the network interface changes.

For it to be taken into account, this VPN connection must meet the following conditions:

1/ The VPN connection must be the first VPN connection defined in the Connection Panel. To configure this first connection, refer to chapter 20 Configuring the Connection Panel below.
2/ The VPN connection must be configured in IKEv2.

The following functions of the TrustedConnect Panel can be configured:

- Exclude network interfaces from Always-On
- Detect the trusted network (TND)
- Manage token or smart card removal
- Manage scripts linked to the VPN tunnel
- Minimize the 'HMI
- Purge log files

21.1 Always-On

21.1.1 Operating principle

The Always-On feature, which is always enabled with the TrustedConnect Panel, ensures that the connection remains secure whenever the network interface changes.

The following network interfaces are supported:

- Virtual adapter (e.g. vmware)
- Wi-Fi
- Ethernet
- USB modem (i.e. smartphone)
- Bluetooth modem (i.e. smartphone)

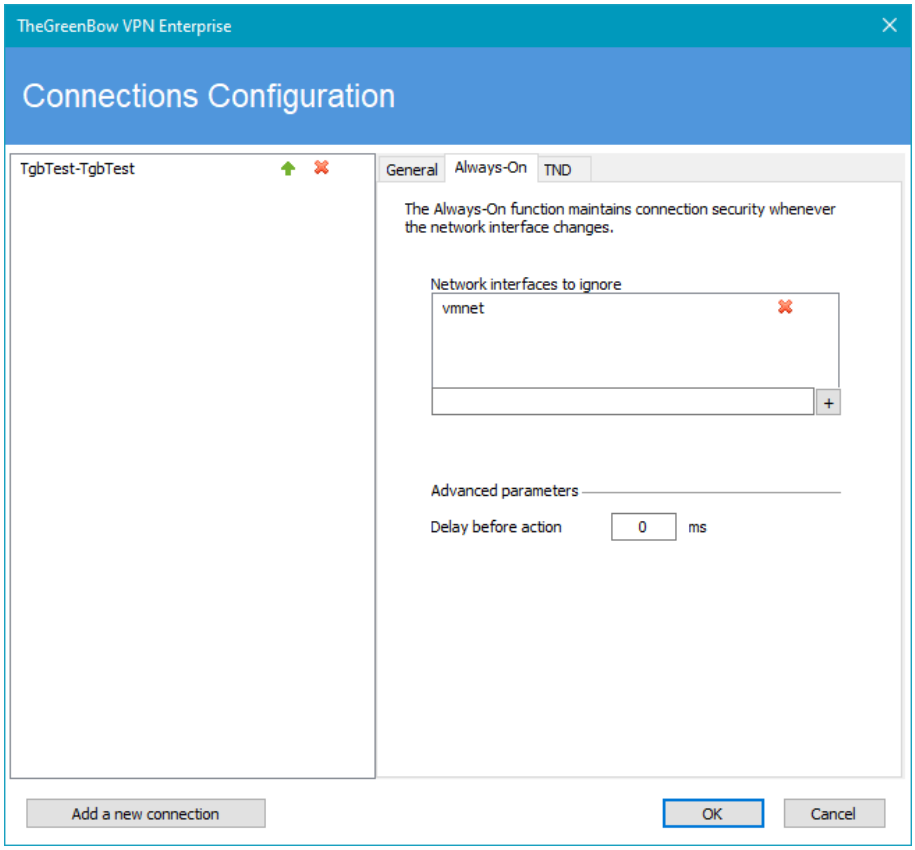
The following network events trigger automatic tunnel reconnection (and, where appropriate, detection of the trusted network), unless they have been explicitly excluded (see section 21.1.2 Configuring Always-On):

- Connection to a network (API addresses ignored)
- Disconnection from a network
- An adapter changes IP address or DHCP switches to static or vice versa
- ipconfig /release
- ipconfig /renew
- Switch to airplane mode

21.1.2 Configuring Always-On

The Always-On feature is enabled as soon as the TrustedConnect Panel is used for open a VPN tunnel. You can configure it to exclude certain network interfaces from automatic reconnection to the VPN tunnel.

The Always-On tab in the Connections Configuration window allows you to configure the settings for the Always-On feature:



Network interfaces to ignore	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. The values of this parameter are not case sensitive (all character strings are converted to lowercase before comparison). You can 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 strings `Hyper-V` and `vmnet`, enter `Hyper-V,vmnet`.
Delay before action	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, this parameter is used to delay the triggering of the TND mechanism (see next section). 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.

21.2 Trusted Network Detection (TND)

21.2.1 Operating principle

This feature consists in detecting whether the workstation is connected to the corporate network (trusted network) or not. When the VPN Client detects that workstation is not on the corporate network, the predefined tunnel is opened automatically. This feature is referred to as Trusted Network Detection (TND) in this document.

The TrustedConnect Panel uses the following two methods to detect whether the workstation is on a trusted network or not:

1/ It checks whether the DNS suffixes of the network interfaces available on the workstation are part of the list of trusted DNS suffixes (list configured in the software, see below).
2/ Automatically accesses a trusted web server in HTTPS mode and checks that its certificate is valid.

The two methods are used in combination to detect whether the workstation is on a trusted network: the VPN Client starts by testing whether a trusted DNS suffix is available; if none are found, the VPN Client does not continue the test and concludes that the workstation is not connected to the trusted network; if it does find one, it continues the test sequence by verifying the access to the trusted server and the validity of its certificate.

At the first accessible trusted server found whose certificate is valid, the VPN Client concludes that the workstation is connected to the trusted network.

In all of the following other cases, the VPN Client concludes that the workstation is not connected to the trusted network and automatically attempts to open the configured VPN connection:

- No DNS suffix has been found in the list of trusted DNS suffixes
- The list of trusted DNS suffixes is empty
- The list of trusted server URLs is empty
- No trusted server is accessible or none has a valid certificate

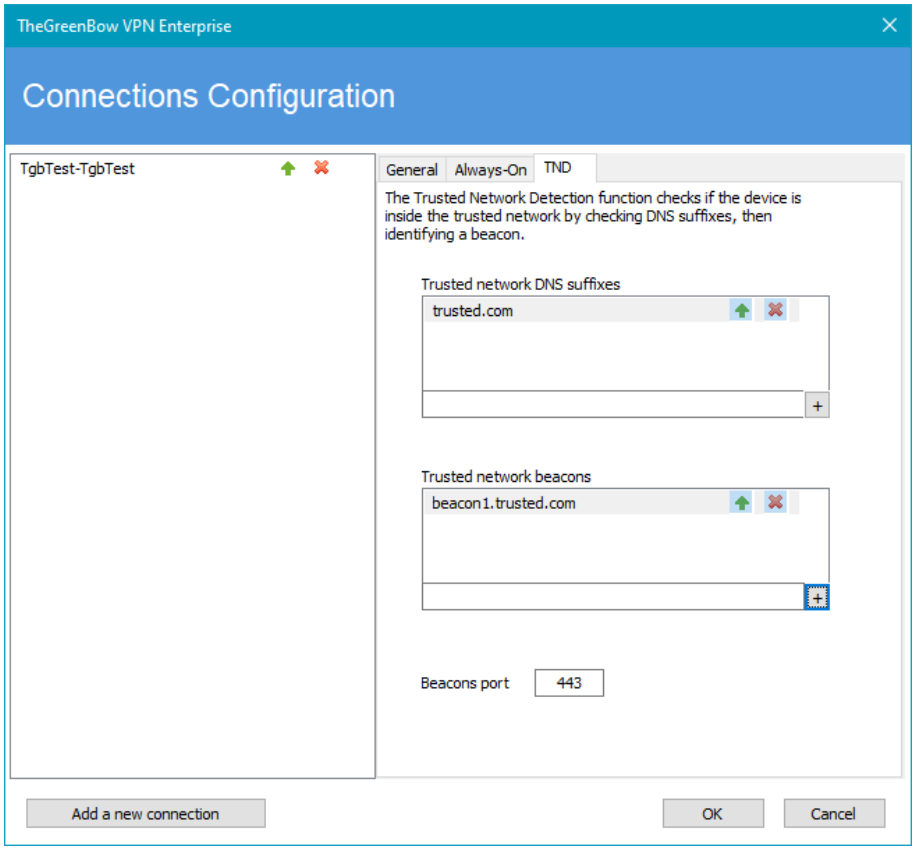
Therefore, to enable the Trusted Network Detection (TND) feature, the following parameters must be configured:

- A list of DNS suffixes
- A list of trusted server URLs

On some workstations, a few seconds are required before the interface is ready to transmit when a network interface appears. To mitigate this time delay, there is a "Delay before action" option on the "Always-On" tab (see previous section).

21.2.2 Configuring TND

The TND tab in the Connections Configuration window allows you to configure the settings for the Trusted Network Detection feature:



Trusted network DNS suffixes	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.
Trusted network beacons	This parameter defines the list of trusted servers to use (e.g. www.server.com). The VPN Client will attempt to connect via https to the /index.html page of the servers in the list (e.g. https://www.server.com/index.html), until it finds a server that is accessible and has a valid certificate. The server list 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.
Beacons port	This parameter defines the port to be used to reach trusted servers. Only one port that will be used for all servers can be configured. If this parameter is not configured, the VPN Client will use port 443 by default.

Visually identify direct connection to the trusted network	This option adds a visual cue to the TrustedConnect Panel to indicate that the VPN Client is connected to the trusted network. If the box is checked, the taskbar icon and the color of the circle in the panel is blue when the machine is connected to the trusted network and green when a tunnel is open. If the box is unchecked, the taskbar icon and the color of the circle in the panel remains green in both cases. No distinction is made between the trusted network and an open tunnel.

21.3 Scripts

The TrustedConnect Panel can run scripts when a tunnel is opened or closed. To configure this feature, refer to chapter 15 Automation.

21.4 Minimizing the panel

By default, the TrustedConnect Panel is automatically minimized to the notification area (systray) after two seconds, when the workstation has been detected as being connected to the trusted network (either physically or through the VPN tunnel).

You can set the time delay before the VPN Client's HMI is minimized, as well as the type of minimization. The TrustedConnect Panel can be minimized to the taskbar or to the notification area (systray, by default).
These configurations must be made in the properties of the VPN Client installer.
☞ Refer to the "Deployment Guide" for the corresponding instructions.

The time delay and minimization type only apply to automatic minimization of the TrustedConnect Panel upon detection of a connection to the trusted network.

21.5 Purging logs

You can configure the number of days during which log files are kept.
The default value is 10 days.

This configuration must be made in the properties of the VPN Client installer.
☞ Refer to the "Deployment Guide" for the corresponding instructions.

21.6 Behavior when smart card or token is removed

You can configure the behavior of the TrustedConnect Panel when the smart card or token is removed from the reader while a VPN tunnel is open.

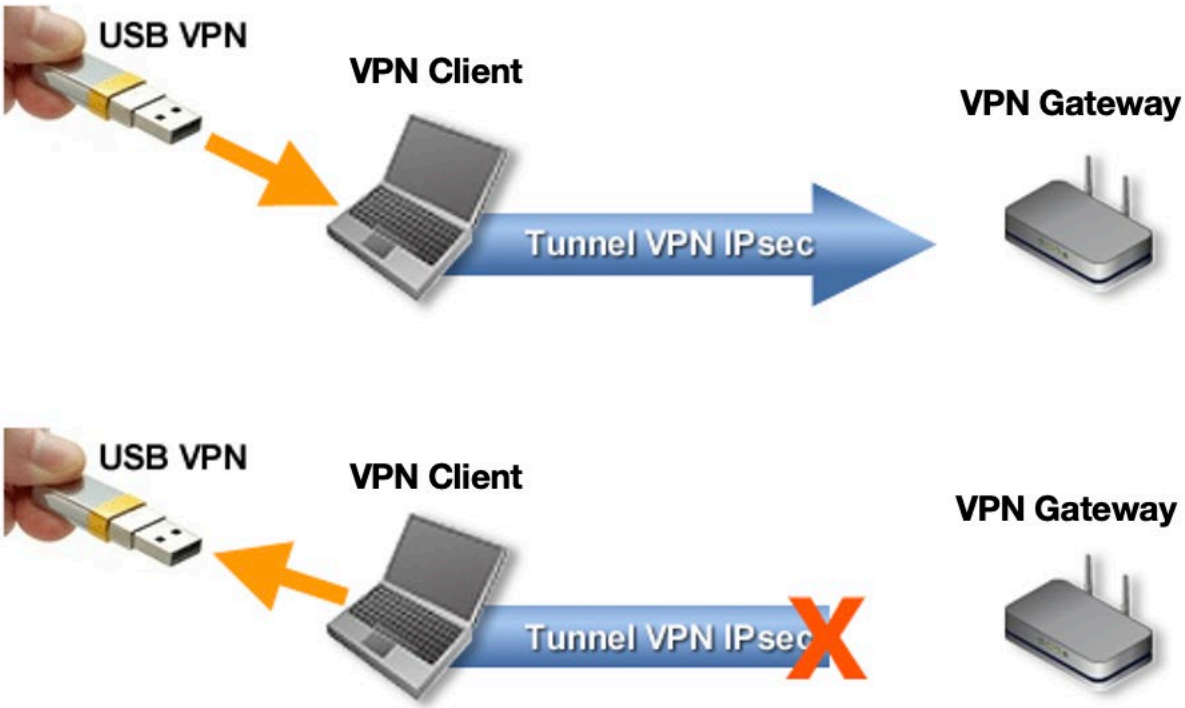
This configuration must be made in the properties of the VPN Client installer.
☞ Refer to the "Deployment Guide" for the corresponding instructions.

22 USB mode

22.1 Overview

The Windows Enterprise VPN Client features a unique VPN connection management mode known as the USB mode.

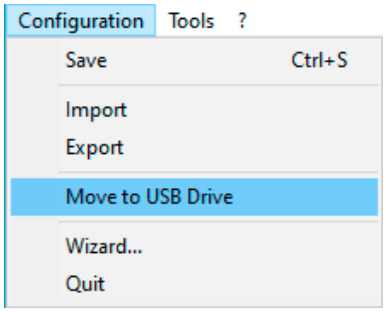
In this mode, the VPN configuration is securely stored on a removable storage device (USB drive). No VPN security elements are stored on the workstation from which the VPN connection is opened. The VPN connection is established automatically as soon as the USB drive is inserted and closed when the USB drive is removed.



Hereinafter, the USB drive containing the VPN configuration will be referred to as "VPN USB drive".

22.2 Configuring the USB mode

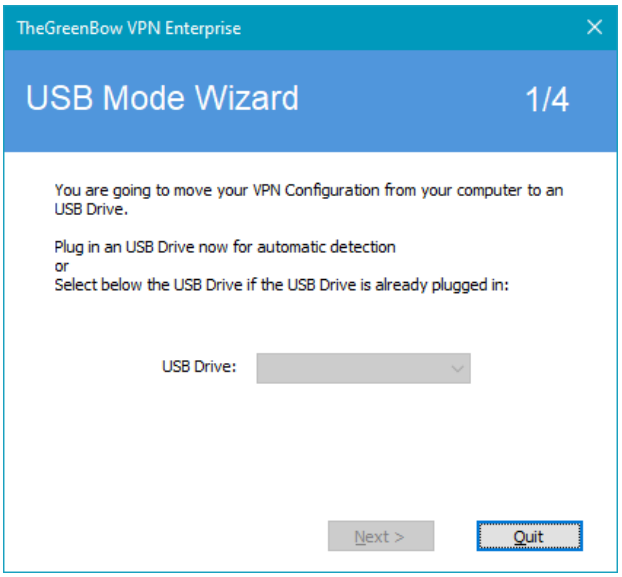
The USB mode is configured using the configuration wizard available from the "Configuration > Move to USB Drive" menu of the Configuration Panel.



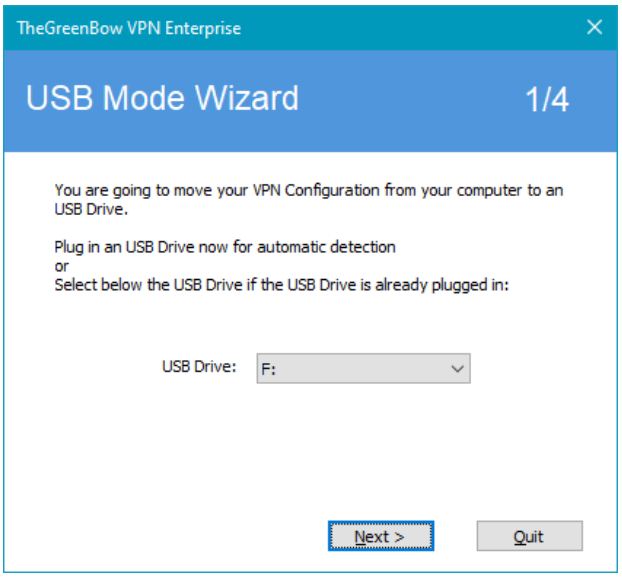
Step 1: Choosing a USB drive

Screen 1 allows you to choose the removable storage device (USB drive) to use to protect the VPN configuration.
If a drive is already inserted, it is automatically displayed in the list of available USB drives.
Otherwise, simply insert the selected USB drive at this stage. It will be detected automatically as soon as it is inserted.

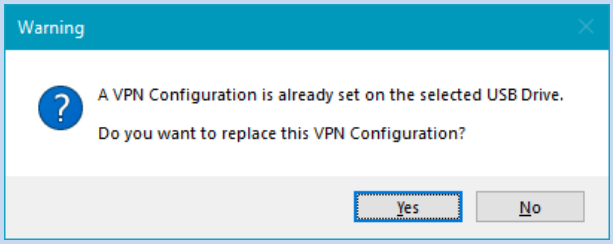
No USB drive inserted



USB drive already inserted



The USB mode only allows you to protect a single VPN configuration on a USB drive. If there already is a VPN configuration on the inserted USB drive, the following warning will be displayed:



If an empty USB drive is inserted and it is the only drive inserted into the workstation, the wizard will automatically proceed to step 2.

Step 2: Protecting the VPN configuration in USB mode

The following two protections are available:

1/ Pairing with the user's workstation:

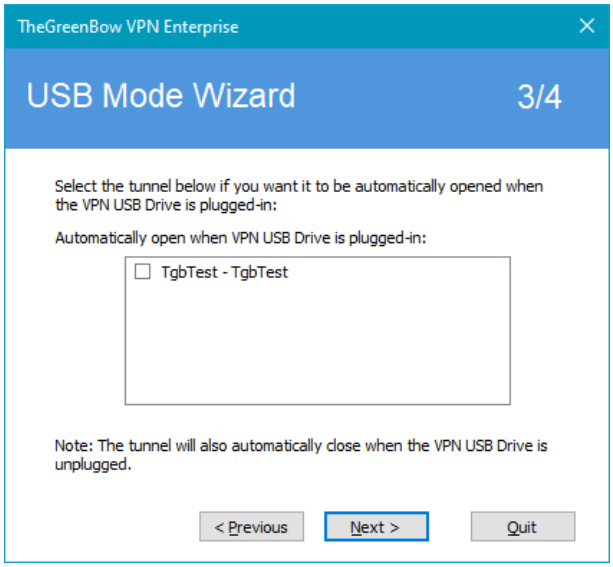
The USB VPN configuration can be uniquely paired to the workstation from which it originates.
In this case, the VPN USB drive can only be used on this workstation.
On the other hand, if the USB drive is not paired with a specific workstation, the VPN USB drive can be used on any workstation equipped with the VPN Client.

2/ Password protection:

The USB VPN configuration can be password-protected.
In this case, the password will be required every time the VPN USB drive is inserted.

Step 3: Automatically opening the tunnel

The wizard allows you to configure which VPN connections are opened automatically every time the VPN USB drive is inserted.



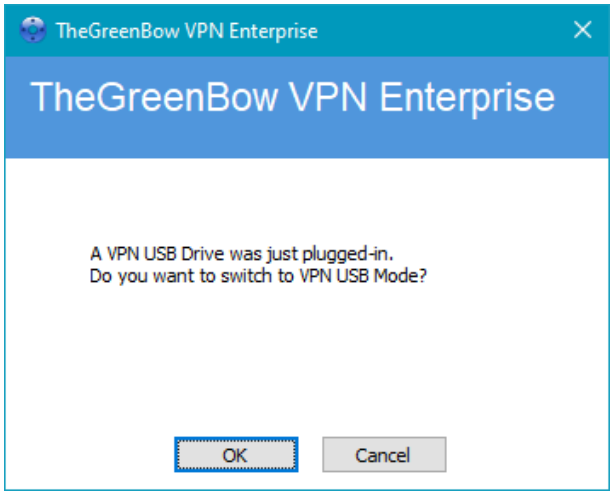
Step 4: Summary

The summary gives you the opportunity to check whether the VPN USB drive has been properly configured.

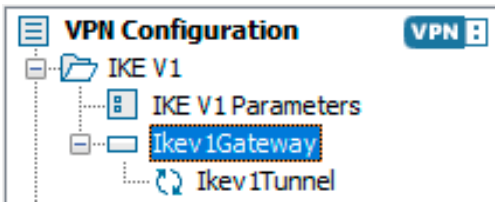
Once this final step is confirmed, the workstation's VPN configuration is transferred onto the USB drive.
It remains enabled for as long as the USB drive is inserted. When the VPN USB drive is removed, the VPN Client will revert to an empty VPN configuration.

22.3 Using the USB mode

After starting the Windows Enterprise VPN Client, regardless of whether a VPN configuration is loaded, insert the VPN USB drive. The following information window is automatically displayed:



Once the prompt has been confirmed, the USB VPN configuration is loaded automatically and, where appropriate, the corresponding tunnel(s) is (are) opened automatically. A "USB mode" icon is shown in the top-right corner of the tree on the Configuration Panel when the USB mode is enabled:



The VPN connections running in USB mode automatically close when the VPN USB drive is removed. The VPN configuration contained in the USB drive is removed from the workstation. (If a VPN configuration had already been set on the workstation before the USB drive was inserted, it will be restored in the software.)

The Windows Enterprise VPN Client can only take into account a single VPN USB drive at a time. As long as a VPN USB drive is inserted, any additional VPN USB drives that are inserted will not be taken into account

The import function is disabled in USB mode.

The VPN configuration can be edited in USB mode. Any changes made to the VPN configuration are saved to the VPN USB drive.

The VPN Client does not provide any function to directly change the password or the pairing with a workstation.

In order to change these parameters, follow the steps below:

1/ Insert the VPN USB drive.
2/ Export the VPN configuration.
3/ Remove the VPN USB drive.
4/ Import the VPN configuration exported in step 2.
5/ Reload the USB mode wizard with this configuration and the desired new parameters.

23 GINA mode

23.1 Overview

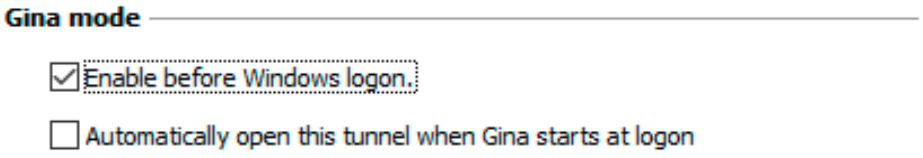
The GINA mode allows you to open VPN connections before the Windows logon.
This function can, for example, create a secure connection to an access rights management server so that the user workstation access rights can be obtained before opening a user session.

When a tunnel is configured "in GINA mode", the following two situations are possible:

1/ If the VPN Client is configured to start up in "TrustedConnect" mode (refer to section section 24.2 General), then the TrustedConnect Panel will be displayed on the Windows logon screen and the VPN Client tries to automatically connect to the trusted network.
2/ Otherwise, a window allowing you to open a tunnel that is similar to the Connection Panel will be displayed on the Windows logon screen. It allows you to open a VPN tunnel manually or automatically.

23.2 Configuring the GINA mode

Configuring the GINA mode for a VPN connection is done on the "Automation" tab of the relevant tunnel.
☞ Refer to chapter 15 Automation.



23.3 Using the GINA mode

When the VPN tunnel is configured in GINA mode, the window used to open GINA tunnels is displayed on the Windows logon screen. The tunnel will open automatically if it is configured accordingly.

A GINA-mode VPN tunnel can perfectly implement an EAP authentication (users must enter their login name and password) or a certificate-based authentication (users must enter the PIN code required to access the smart card or token).

⚠ If two tunnels are configured in GINA mode and one of the two is set to open automatically, it may happen that both tunnels will open automatically.

For the "Automatically open this tunnel on traffic detection" option to be operational after Windows logon, the "Enable before Windows logon" option must not be checked.

Limitation: Scripts and USB mode are not available for VPN tunnels configure in GINA mode.

A VPN tunnel configured with a certificate stored in the Windows User Certificate Store will not work in GINA mode. The reason for this is that the GINA mode is run before a Windows user is identified (prior to opening any session). Therefore, the software cannot identify the user store to use in the Windows Certificate Store.

Security considerations

A tunnel configured in GINA mode can be opened before Windows logon, i.e. by any user of the workstation. We therefore strongly recommend that you set up a strong authentication method that is certificate-based and, if possible, stored on a removable device.

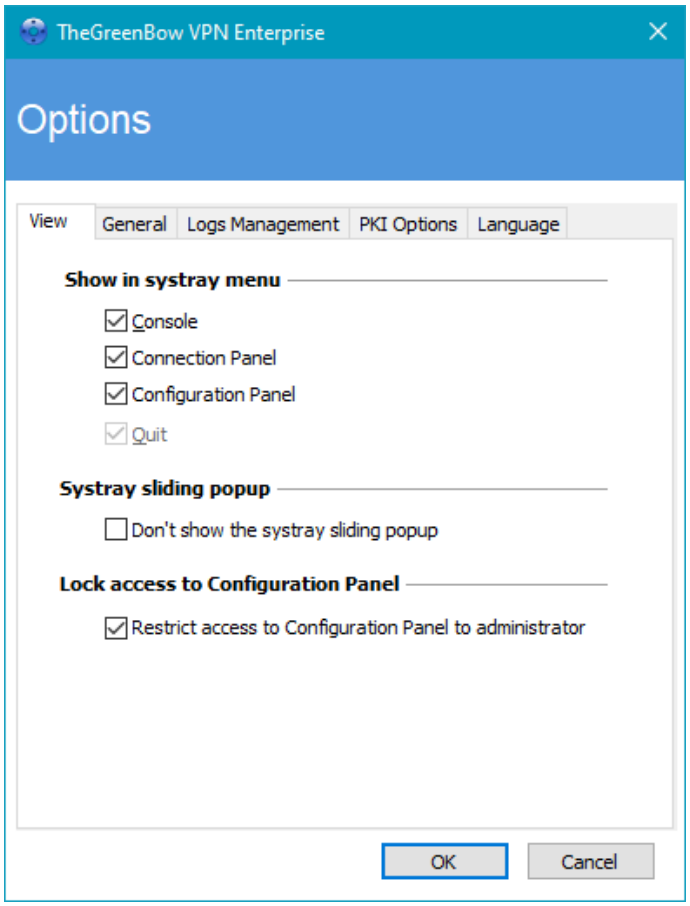
24 Options

24.1 Displaying/hiding the interface

Using the options listed in the "View" tab of the "Options" window, you can hide all the software's interfaces by removing the items "Console", "Connection Panel" and "Configuration Panel" from the taskbar menu. The taskbar menu can therefore be reduced to the single item "Quit".

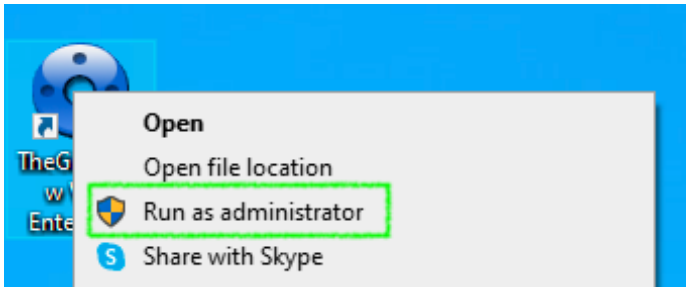
The taskbar menu's "Quit" item cannot be removed using the software. However, it can be deleted using the installation options (refer to the "Deployment Guide").

The pop-up window that appears when a tunnel is opened or closed can also be hidden ("Don't show the systray sliding popup" option).

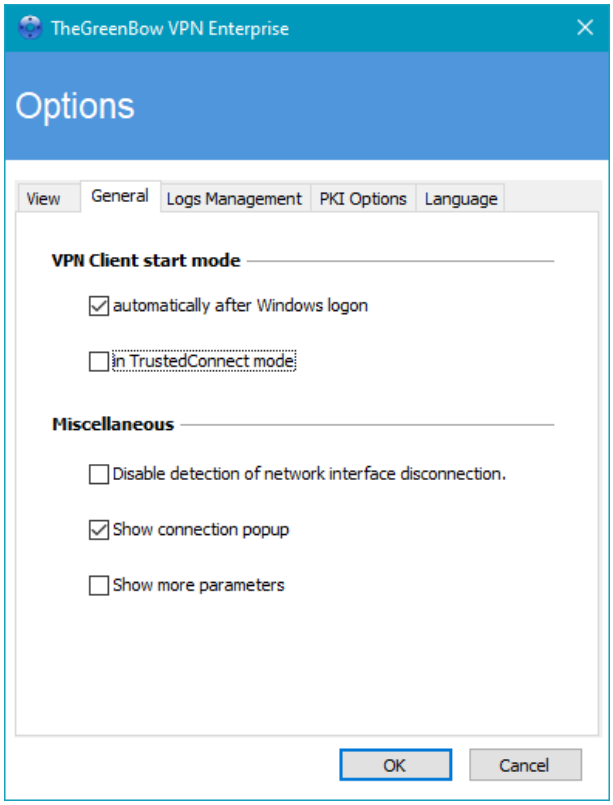


In the Windows Enterprise VPN Client, the interface of the Configuration Panel is restricted to administrators, by default. To give users access to the Configuration Panel, uncheck the "Restrict access to Configuration Panel to administrators" option.

To start the VPN Client in administrator mode, right-click the TheGreenBow VPN Enterprise icon and then select the "Run as administrator" menu item.



24.2 General



VPN Client startup mode

If the option "automatically after Windows logon" is checked, the VPN Client will start automatically when the user session is opened.

If the option is not checked, the user must start the VPN Client manually, either by double-clicking on the desktop icon or by selecting the software in the Windows "Start" menu.
☞ Refer to section 6.2 Starting the software.

If the "in TrustedConnect mode" option is also checked, the VPN Client will start up showing the TrustedConnect Panel. Otherwise, the VPN Client will start up showing the Connection Panel.

Disabling detection of network interface disconnection

The standard behavior of the VPN Client is to close the VPN tunnel at its end as soon as a communication issue is encountered on the remote VPN gateway.

For unreliable physical networks prone to frequent micro-disconnections, this function can have drawbacks (which can go as far as not being able to open a VPN tunnel).

When the "Disable detection of network interface disconnection" box is checked, the VPN Client will not close tunnels as soon as a disconnection is observed. This ensures greater stability of the VPN tunnel on unreliable physical networks, typically satellite networks.

We recommend that you do not enable this option in TrustedConnect mode (keep the box unchecked).

Show connection popup

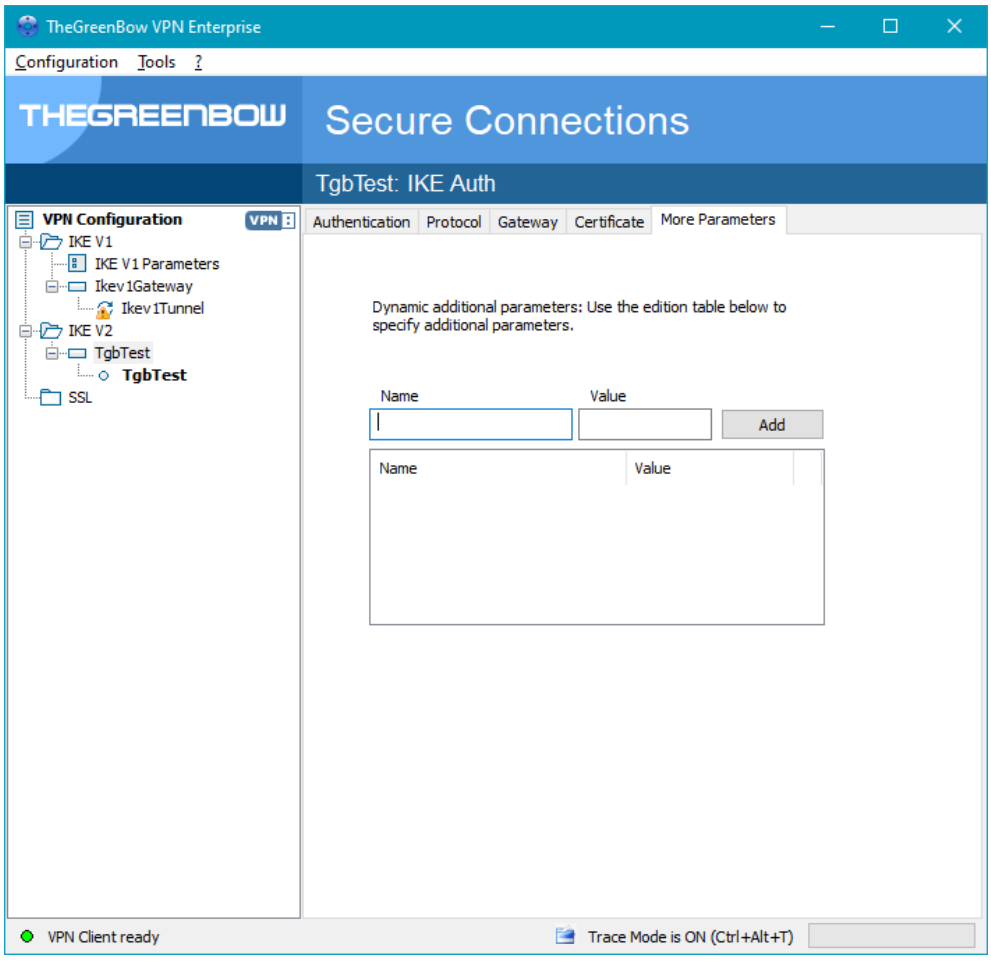
A connection window will be displayed automatically every time a VPN connection is established.
This feature can be disabled by unchecking the "Show connection popup" box.

Displaying more parameters

If required, the Windows Enterprise VPN Client allows you to configure additional parameters, which are not documented in this document.

Under certain circumstances, the TheGreenBow support team may offer to add additional parameters (Name, Value) that will allow you to manage specific use cases, either on the version of the installed software or in patches that will be provided to you.

To enable the "More Parameters" tab in the VPN tunnel configuration window as shown below, check the "Show more parameters" option.



24.3 Managing logs

Refer to section 25.1 Administrator logs.

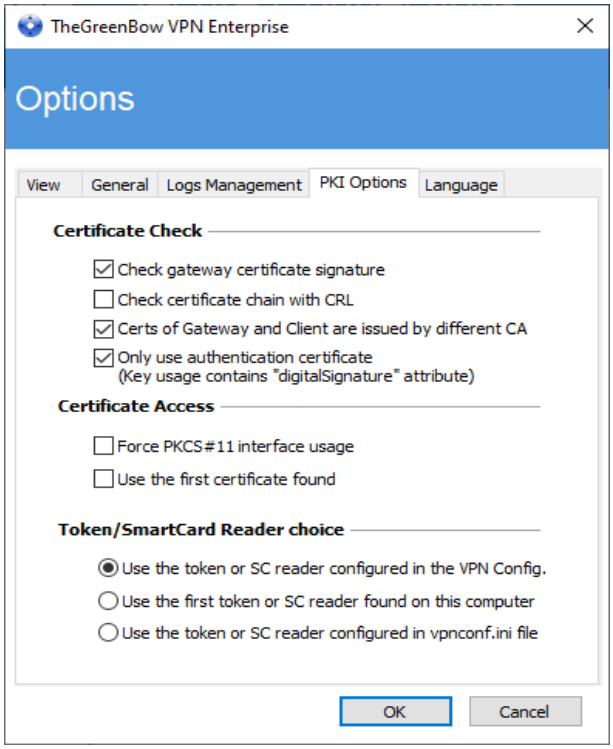
24.4 PKI options

The "PKI Options" tab is used to fine-tune smart card and token management and to further specify certificate access.

PKI options include the following:

- Configuring rules for gateway certificate verification (validity, CRL, key usage)
- Specifying the certificate that the VPN Client must use to open a VPN tunnel
- Defining the smart card reader or token to use on the user workstation

When deploying the software, all these options can be preconfigured when the Windows Enterprise VPN Client is installed. This mechanism is described in the document entitled "Deployment Guide".



Certificate Check

Check gateway certificate signature	When this option is selected, the VPN gateway certificate is checked (including its validity date), as well as all certificates in the certificate chain down to the root certificate.

Security advisory: When this option is selected, the subject of the gateway certificate must be entered in the Remote ID of the tunnel concerned to prevent vulnerability 2018_7293 from being exploited.

Check certificate chain with CRL	When this option is selected, the Certificate Revocation List (CRL) of the VPN gateway certificate is checked, as well as the CRL of all certificates in the certificate chain down to the root certificate. The root and intermediate certificates must be imported into the configuration or available in the Windows Certificate Store. Likewise, the CRLs must also be accessible, either in the Windows Certificate Store or available for download.
Certs of Gateway and Client are issued by different CA	If the VPN Client and the VPN gateway use certificates from a different certification authority, this box must be checked.
Only use authentication certificate	When this option is enabled, the VPN Client will only take into account "Authentication" certificates (i.e. certificates whose "key usage" extension contains the value "digitalSignature"). This function allows you to automatically select a certificate when several are stored on the same smart card or token. The checkbox is grayed out when the `KEYUSAGE` property is set to 2 or 3 during installation (refer to the "Deployment Guide").

This option is used to globally configure the specification of certificates for all the VPN Client's tunnels. To separately specify the certificates for each tunnel, you must use the dynamic parameters described in section 18.1 Selecting a certificate ("Certificate" tab).

Certificate Access

Force PKCS#11 interface usage	The VPN Client knows how to handle the PKCS#11 and CNG APIs in order to access the certificate for smart cards or tokens. When this option is checked, the VPN Client will only consider the PKCS#11 API to access the certificate for smart cards and tokens.
Use the first certificate found	When this option is checked, the VPN Client will use the first certificate found on the specified smart card reader or token.

Token/Smart Card Reader choice

Use the token/SC reader configured in the VPN Config.	The VPN Client uses the reader or token specified in the VPN configuration file to search for a certificate.
Use the first token or SC reader found on this computer	The VPN Client uses the first smart card or token found on the workstation to search for a certificate.
Use the token or SC reader configured in vpnconf.ini file	The VPN Client uses the `vpnconf.ini` configuration file to identify the smart card readers or tokens to use to search for a certificate. ☞ Refer to the "Deployment Guide".

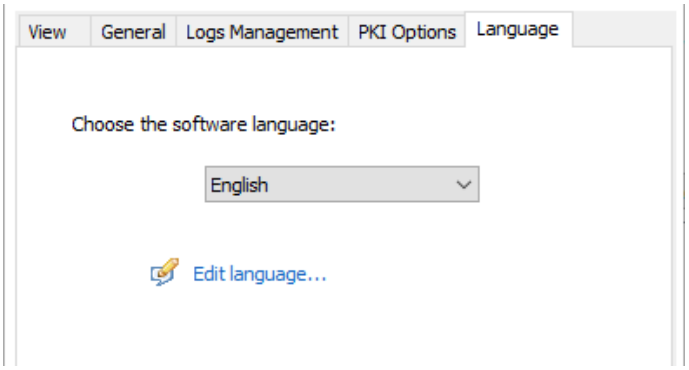
Since the use of the `vpnconf.ini` file only applies to the PKCS#11 interface, this option requires that the "Force PKCS#11 interface usage" option be selected.

24.5 Managing languages

24.5.1 Choosing a language

The Windows Enterprise VPN Client can run in several languages.
You can change languages while running the software.

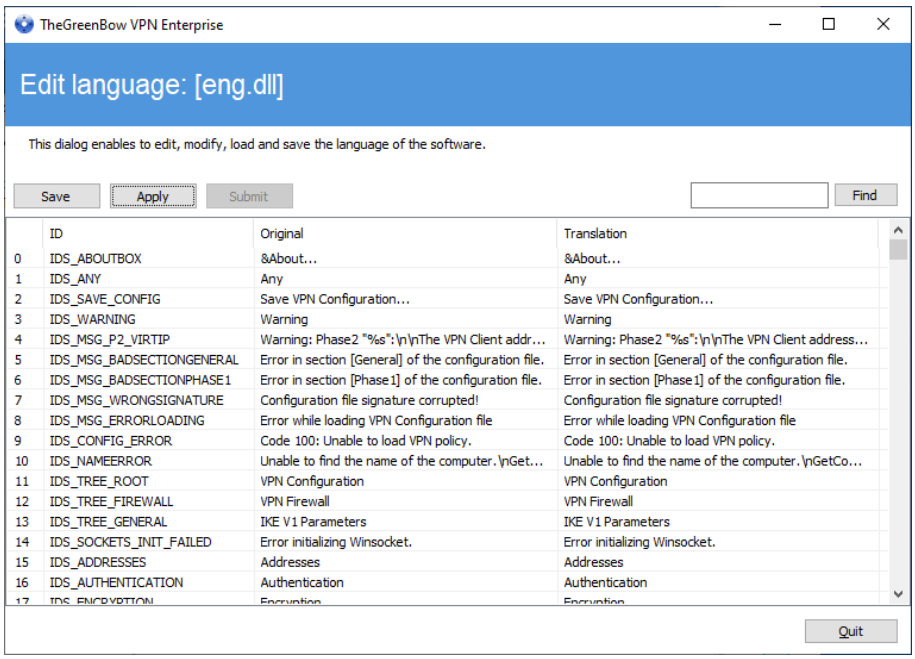
To choose another language, open the "Tools > Options" menu, then select the "Language" tab.
Choose the desired language in the drop-down menu:



The list of languages available in the standard version of the software is provided in an appendix in section 27.4 Windows Enterprise VPN Client technical data.

24.5.2 Editing or creating a language

The Windows Enterprise VPN Client lets you create new translations or edit the language used, then test these changes dynamically through an integrated translation tool.
In the "Language" tab, click the "Edit language…" link to display the translation window:



	ID	Original	Translation
0	IDS_ABOUTBOX	&About...	&About...
1	IDS_ANY	Any	Any
2	IDS_SAVE_CONFIG	Save VPN Configuration...	Save VPN Configuration...
3	IDS_WARNING	Warning	Warning
4	IDS_MSG_P2_VIRTIP	Warning: Phase2 "%s":\n\nThe VPN Client addr...	Warning: Phase2 "%s":\n\nThe VPN Client address...
5	IDS_MSG_BADSECTIONGENERAL	Error in section [General] of the configuration file.	Error in section [General] of the configuration file.
6	IDS_MSG_BADSECTIONPHASE1	Error in section [Phase1] of the configuration file.	Error in section [Phase1] of the configuration file.
7	IDS_MSG_WRONGSIGNATURE	Configuration file signature corrupted!	Configuration file signature corrupted!
8	IDS_MSG_ERRORLOADING	Error while loading VPN Configuration file	Error while loading VPN Configuration file
9	IDS_CONFIG_ERROR	Code 100: Unable to load VPN policy.	Code 100: Unable to load VPN policy.
10	IDS_NAMEERROR	Unable to find the name of the computer.\nGet...	Unable to find the name of the computer.\nGetCo...
11	IDS_TREE_ROOT	VPN Configuration	VPN Configuration
12	IDS_TREE_FIREWALL	VPN Firewall	VPN Firewall
13	IDS_TREE_GENERAL	IKE V1 Parameters	IKE V1 Parameters
14	IDS_SOCKETS_INIT_FAILED	Error initializing Winsocket.	Error initializing Winsocket.
15	IDS_ADDRESSES	Addresses	Addresses
16	IDS_AUTHENTICATION	Authentication	Authentication
17	IDS_ENCRYPTION	Encryption	Encryption

The translation window is split into 4 columns, which display the number of the character string, its identifier, its string in the original language and its translation in the selected language respectively.

Using the translation window, you can perform the following actions:

1/ Translate each character string by clicking on the corresponding row.
2/ Search for a specific character string in any column of the table (use the "Find" field then the "F3" key to browse through every occurrence of the character string you have entered).
3/ Save the changes ("Save" button).

   Any language you have edited or created is saved in a ".lng" file.

4/ Immediately apply changes to the software: this function lets you assess the relevance of any character string and ensure that it is properly displayed in real time ("Apply" button).
5/ Send a new translation to TheGreenBow ("Submit" button).

The name of the currently edited language file will appear as a reminder in the header of the translation window.

Any translation sent to TheGreenBow will be checked, published on TheGreenBow's website, and then included in the software, usually in the official release following receipt of the translation.

The characters or character strings below must not be modified during translation:

"%s" the software will replace it by a character string
"%d" the software will replace it by a number
"\n" indicates a carriage return
"&" indicates that the following character must be underlined
"%m-%d-%Y" indicates a date format (in this case US format: month-day-year).
Only edit this field if you are certain of the format used in the target language.

The string "IDS_SC_P11_3" must be left as is.

25 Administrator logs, console, and traces

The Windows Enterprise VPN Client comes equipped with three types of logs:

1/ "Administrator" logs are specifically designed for software activity and usage reports.
2/ The "Console" provides detailed information on the tunnels as well as the related opening and closing steps. It essentially consists of the IKE messages and provides high-level information about the establishment of the VPN tunnel. It is intended for administrators to identify possible VPN connection issues.
3/ The "Trace" mode makes every component of the software write an activity log about its inner workings. This mode is intended for TheGreenBow support to diagnose software issues.

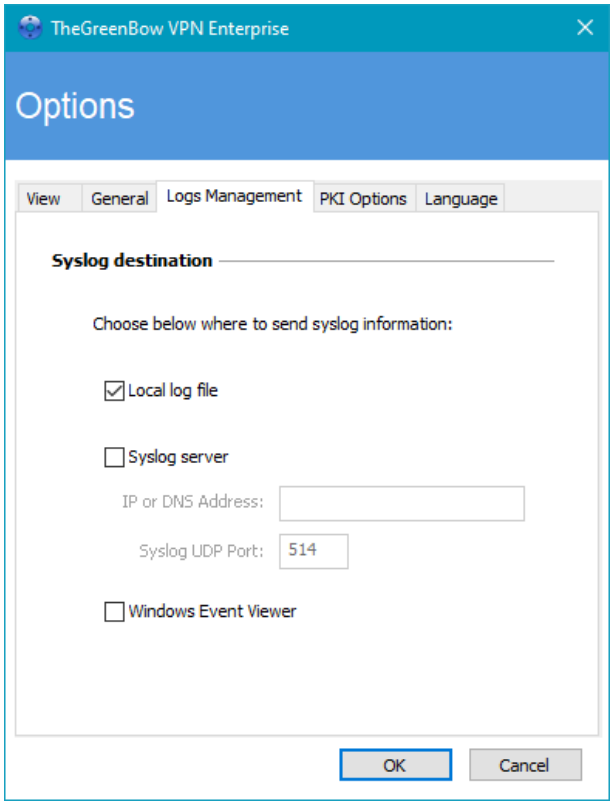
25.1 Administrator logs

The Windows Enterprise VPN Client can collect "administrator" logs: tunnel opening, expired certificate, connection duration, wrong login/password, changes to the VPN configuration, import or export of this configuration, etc. "Administrator" logs provide a first level of analysis for any issues that may be encountered.

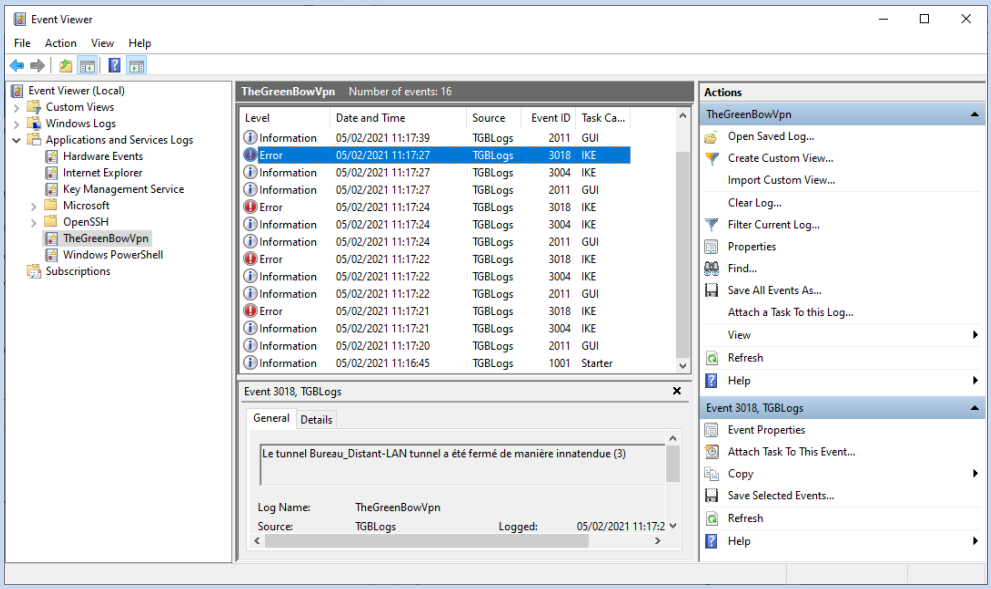
The following actions can be performed on collected logs either exclusively or simultaneously:

- Store in a local file
- Record in the Windows Event Log
- Send to a Syslog server in syslog format

Administrator logs are configured in the "Tools > Options..." window on the "Logs management" tab.



The path for Windows Enterprise VPN Client logs in the Windows Event Viewer is the following:



Administrator logs are listed in section 27.2 Administrator logs in the appendixes.

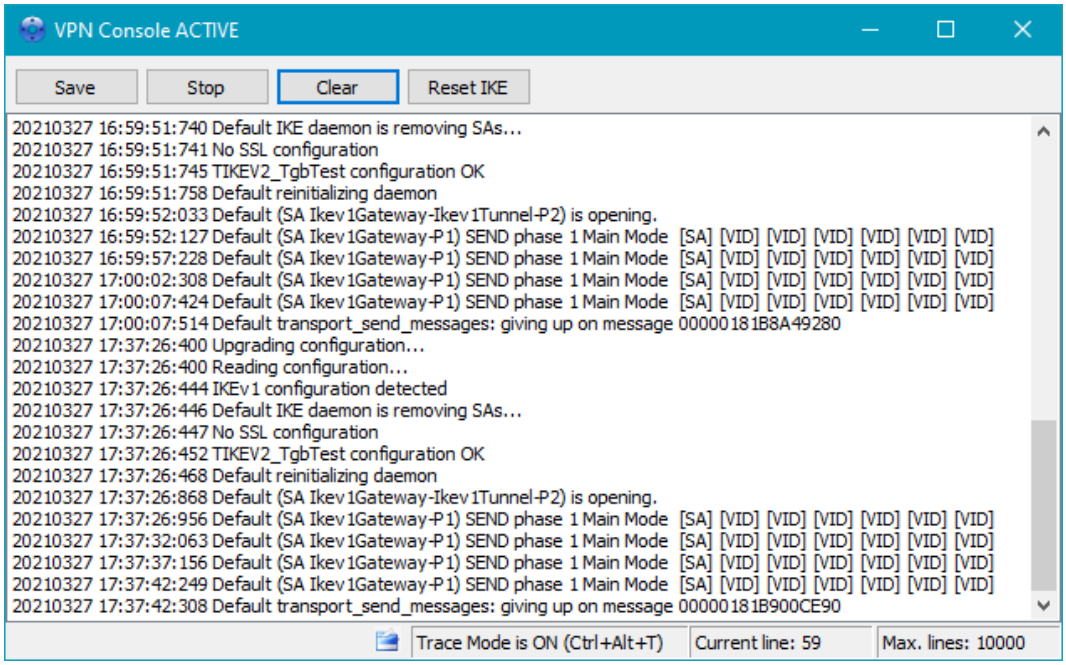
When administrator logs are stored in a local file, the path to these logs is the "System" sub-directory in the logging directory: "C:\ProgramData\TheGreenBow\TheGreenBow VPN\LogFiles\System".

Read access to this directory is available in all modes, but write access is only available in Administrator mode.

25.2 Console

Access the Console using either of the following methods:

- "Tools > Console" menu in the Configuration Panel (main interface)
- CTRL+D shortcut when the Configuration Panel is open
- From the software's taskbar menu, choose "Console"



The Console has the following functions:

- Save: Saves all the traces displayed in the window into a file
- Start/Stop: Starts/stops a console log
- Clear: Clears the contents of the window
- Reset IKE: Restarts the IKE service

25.3 Trace mode

Trace mode is enabled using the following shortcut: CTRL+ALT+T

You do not need to restart the software when you enable the trace mode.

When the trace mode is enabled, every component of the Windows Enterprise VPN Client generates activity logs. The logs produced are stored in a folder that you can access by clicking the blue "folder" icon located in the status bar of the Configuration Panel (main interface).

Logs can only be enabled on the Configuration Panel and access to the Configuration Panel can be restricted to administrators.

Even though logs do not contain any sensitive information, we recommend that, if enabled by the administrator, said administrator ensures that they are disabled and, if possible, deleted when quitting the software.

Trace logs are kept for 10 days. The software automatically deletes any older files.

When stored in a local file, "administrator" logs are not deleted.

26 Security recommendations

26.1 Assumptions

To maintain a proper security level, the operating conditions and usages listed below must be observed:

1/ The system and network administrator as well as the security administrator, respectively tasked with installing the software and defining the VPN security policies, are nonhostile. They are trained to carry out the tasks for which they are responsible and follow administrative manuals and procedures.
2/ The security administrator regularly ensures that the product's configuration is in line with the one that he or she has set up and performs the necessary updates when necessary.
3/ Users of the software are nonhostile and have been properly trained on how to use it. More specifically, users execute the tasks for which they are responsible to ensure proper operation of the product and do not reveal the information used for their authentication with the VPN gateway.
4/ The user workstation is safe and properly administered. It is equipped with an up-to-date antivirus software and is protected by a firewall.
5/ Bi-keys and certificates used to open the VPN tunnel are generated by a trustworthy certification authority that guarantees compliance with management rules for these cryptographic elements and, more specifically, with the specifications laid out by your local cybersecurity agency, e.g. [RGS_B1] and [RGS_B2] in France (only available in French).
6/ The product's logging function is enabled and properly configured. Administrators are responsible for regularly reviewing the logs.

26.2 User workstation

The machine on which the Windows Enterprise VPN Client is installed and run must be clean and properly administered. More specifically:

1/ Antivirus software must be installed, and its signature database must be updated on a regular basis.
2/ It must be protected by a firewall that controls (partitions or filters) the workstation's inbound and outbound communications that do not go 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 on the ANSSI website (in French), 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)
- Password (Mot de passe, document only available in French)

26.3 VPN Client administration

The Windows Enterprise VPN Client is designed to be installed and configured with "administrator" privileges and then to be used with "user" privileges only.

We recommend that you protect access to the VPN configuration with a password and restrict the software's visibility to end users (default behavior of the Windows Enterprise VPN Client) as detailed in section 24.1 Displaying/hiding the interface .

The software must therefore be run as administrator to be able to access the Configuration Panel.
We recommend keeping the "Start VPN Client after Windows Logon" mode enabled, which is the default mode upon installation.

Lastly, please note that the Windows Enterprise VPN Client will apply the same VPN configuration to all users of a multiple-user workstation. We therefore recommend running the software on a dedicated workstation (for instance by keeping an administrator account and a user account, as mentioned above).

26.4 VPN configuration

26.4.1 Sensitive information in the VPN configuration

We recommend that you do not store any sensitive data in the VPN configuration file.

In this regard, we recommend that you do not use the following features of the software:

1/ Do not use the EAP (password/login) mode alone, but only in combination with a certificate.
2/ If EAP is used, do not store the EAP login name/password in the VPN configuration (function described in section 13.4.1 IKE Auth: IKE SA, paragraph entitled Authentication).
3/ Do not import any certificates to the VPN configuration (function described in section 18.3 Importing a certificate) and preferably use certificates stored on removable devices (tokens) or in the Windows Certificate Store.
4/ Do not use the "Preshared key" mode (function described in section 13.4.1 IKE Auth: IKE SA") and preferably use the "Certificate" mode with certificates stored on removable media (tokens) or in the Windows Certificate Store.
5/ Do not export the VPN configuration without encrypting it, i.e. not password-protected (function described in section 12.2 Exporting a VPN configuration).

26.4.2 Authenticating users

The user authentication functions available in the Windows Enterprise VPN Client are described below, from the weakest to the strongest.

It should be noted that preshared key authentication, despite being easy to implement, enables any user of the workstation to establish a VPN tunnel without cross-checking their authentication.

Type of user authentication	Strength
Preshared key	Weak
EAP	
EAP popup	
Certificate stored in the VPN configuration	
Certificate in the Windows Certificate Store	
Certificate on a smart card or token	Strong

26.4.3 Authenticating the VPN gateway

We recommend that you implement a check on the VPN gateway certificate as described in section 24.4 PKI options.

26.4.4 Protocol

We recommend that you only configure IKEv2 tunnels.

26.4.5 "All through the tunnel" and "split tunneling" modes

We recommend that you configure the VPN tunnel using the "All traffic through the tunnel" mode and enable the "Disable Split Tunneling" mode.

☞ Refer to the paragraph entitled Configuring the Address type in section 13.4.6 Child SA: Child SA and to the paragraph entitled Miscellaneous in section 13.4.7 Child SA: Advanced).

26.4.6 GINA mode

We recommended that you choose a strong authentication method for all tunnels configured in GINA mode.

26.4.7 ANSSI recommendations

The recommendations described above can be complemented by French National Cybersecurity Agency's (ANSSI) IPsec configuration document: Recommendations for securing IPsec networks.

27 Appendixes

27.1 Shortcuts

Connection Panel

- ESC — Closes the window
- CTRL+ENTER — Opens the Configuration Panel (main interface)
- Arrow keys — The Up and Down arrow keys are used to select a VPN connection
- CTRL+O — Opens the selected VPN connection
- CTRL+W — Closes the selected VPN connection

Configuration Panel tree

- F2 — Used to edit the name of the selected Phase
- DEL — Deletes a selected phase, if any, after confirmation by the user
  If the actual configuration is selected (root of the tree), the software asks whether a full reset of the configuration should be performed.
- CTRL+O — Opens the corresponding VPN tunnel if a Phase 2 is selected
- CTRL+W — Closes the corresponding VPN tunnel if a Phase 2 is selected
- CTRL+C — Copies the selected phase to the clipboard
- CTRL+V — Pastes (adds) the Phase copied to the clipboard
- CTRL+N — If the VPN Configuration is selected, creates a new phase 1, or creates a new phase 2 for the selected phase 1
- CTRL+S — Saves the VPN configuration

Configuration Panel

- CTRL+ENTER — Switches to the Connection Panel
- CTRL+D — Opens the "Console" window with VPN traces
- CTRL+ALT+R — Restarts the IKE service
- CTRL+ALT+T — Enables the trace mode (log generation)
- CTRL+S — Saves the VPN configuration

27.2 Administrator logs

ID Log define	ID Log value	Severity	Log string
LOGID_STARTERINIT	1001	Notice	Starter service is started.
LOGID_VPNCONFSTARTING	2001	Notice	GUI is starting.
LOGID_VPNCONFSTOPPED	2002	Notice	GUI has closed.
LOGID_PWDSET	2004	Info	Admin password has been changed.
LOGID_PWDCHECK	2005	Error/Info	Admin password has been verified (status %d).
LOGID_PWDRESET	2006	Warning	Admin password has been reset.
LOGID_TGBIKESTARTED	3001	Notice	IKE has started (status %d).
LOGID_TGBIKESTOPPED	3002	Notice	IKE has stopped.
LOGID_TUNNELOPEN	3004	Info	Tunnel %s is asked to open.
LOGID_VPNCONFCRASHED	2003	Notice	GUI crashed (state %d).
LOGID_TGBIKECRASHED	3003	Notice	IKE crashed (state %d).
LOGID_STARTERSTOP	1002	Notice	Starter service is stopped.
LOGID_RESETIKE	2007	Warning	IKE is asked to reset.
LOGID_VPNCONFSTARTED	2008	Notice	GUI has started from user %s.
LOGID_VPNCONFSTOPPING	2009	Notice	GUI is stopping from user %s.
LOGID_VPNCONFLOADERROR	2010	Error	Configuration couldn't load (reason: %s).
LOGID_VPNCONFOPENTUNNEL	2011	Info	GUI opens tunnel (source: %s).
LOGID_VPNCONFCLOSETUNNEL	2012	Info	GUI closes tunnel (source: %s).
LOGID_VPNCONFSAVE	2013	Notice	New configuration is saved.
LOGID_VPNCONFIMPORT	2014	Info	%s has been imported.
LOGID_VPNCONFIMPORTERR	2015	Error	%s could not be imported (status %d).
LOGID_VPNCONFEXPORT	2016	Info	%s has been exported.
LOGID_TOKENINSERT	2017	Info	Token %s has been inserted.
LOGID_TOKENEXTRACT	2018	Info	Token %s has been extracted.
LOGID_USBINSERT	2019	Info	USB Key has been inserted
LOGID_USBEXTRACT	2020	Info	USB Key has been extracted
LOGID_INSTALLATION	2021	Info	VPN running for the 1st time.
LOGID_UPDATE	2022	Info	VPN software has been updated to version %s.
LOGID_VERSION	2023	Info	VPN Version is %s.
LOGID_GINASTARTED	4001	Notice	GINA has started.
LOGID_GINASTOPPING	4002	Notice	GINA is stopping.
LOGID_GINAOPENTUNNEL	4003	Info	GINA opens tunnel (source: %s).
LOGID_GINACLOSETUNNEL	4004	Info	GINA closes tunnel (source: %s).
LOGID_TUNNELAUTH_OK	3005	Info	Tunnel authentication Ok (%s).
LOGID_TUNNELTRAFIC_OK	3006	Info	Tunnel %s Ok
LOGID_TUNNELAUTH_NOK	3007	Error	Tunnel authentication failed (reason %d).
LOGID_TUNNELTRAFIC_NOK	3008	Error	Tunnel %s failed (reason %d).
LOGID_AUTHREKEYING	3009	Info	Tunnel %s initiated rekey (source %d).
LOGID_AUTHREKEYED	3010	Info	Tunnel %s rekeyed.
LOGID_TUNNELREKEYING	3011	Info	Tunnel %s initiated rekey (source %d).
LOGID_TUNNELREKEYED	3012	Info	Tunnel %s rekeyed.
LOGID_PINCODE	3013	Notice/Error	Pin code is entered (status %d).
LOGID_DRIVERNOK	3014	Critical	Driver could not be loaded (status %d).
LOGID_IKEEXT_STOP	1003	Warning	IKEEXT service is stopped.
LOGID_IKEEXT_RESTART	1004	Notice	IKEEXT service is restarted.
LOGID_IKEEXT_ERROR	1005	Critical	IKEEXT could not be stopped (status %d).
SYSTEMLOGID_VIRTIFOK	3015	Info	Virtual interface created successfully (instance %d).
SYSTEMLOGID_VIRTIFNOK	3016	Error	Virtual interface could not be created (error %d).
LOGID_TUNNELCLOSED	3017	Notice	%s tunnel successfully closed (%d min).
LOGID_TUNNELCLOSED_ERR	3018	Error	%s tunnel closed unexpectedly (%d).
LOGID_CERTERROR	3019	Error	Error %d when handling certificate %s.
LOGID_TUNNELDATA_UL	3020	Info	%d bytes sent inside the tunnel.
LOGID_TUNNELDATA_DL	3021	Info	%d bytes received inside the tunnel.

27.3 TrustedConnect Panel diagnostics

The TrustedConnect Panel informs the user of any issues that may have occurred while establishing the VPN connection by displaying an error code.

These error codes, their diagnosis and possible solutions are detailed below. This list allows administrators to find possible answers to any issues that users may encounter and report.

Code	Diagnostics	Solution
0	**VPN configuration issue** VPN connection not found in configuration	• Make sure that the `tgbvpn.conf` file is available in the VPN Client installation directory.
1	**Issue with a certificate** The VPN configuration uses a certificate whose private key cannot be found.	• Check the VPN Client's configuration and any possible associated authentication devices (smart card reader, token, or Windows Certificate Store). • Reimport the VPN configuration and then reimport the certificate concerned. • Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
3	**Configuration issue** The message "No proposal chosen" has been received during an IKE exchange: the cryptographic algorithm suite configured for the IKE_SA_INIT sequence does not match the one configured on the gateway.	• Verify that the cryptographic algorithm suite for THE IKE_SA_INIT sequence of the VPN connection matches that of the gateway (refer to IKE Auth in the Configuration Panel).
4	**Configuration issue** The message "No proposal chosen" has been received during an IKE exchange: the cryptographic algorithm suite of the ESP protocol does not match the one configured on the gateway.	• Verify that the cryptographic algorithm suite of the ESP protocol (refer to Child SA in the Configuration Panel) matches that of the gateway.
5	**Cannot access gateway** The gateway address ("Remote Router Address") specified in the VPN configuration is not reachable. If it is an IP address, it cannot be found or cannot be reached. If it is a DNS address it may be inaccessible, indefinite, or cannot be resolved.	• Check the address of the gateway/remote workstation. For example, try "pinging" this address.
6	**Configuration issue** The message "Remote ID other than expected" has been received. This means that the value of the "Remote ID" does not match the value expected by the remote VPN gateway.	• Make sure that the "Local ID" parameter on the VPN client's Protocol tab matches the Remote ID of the remote gateway (or workstation). **Caution**: The Remote ID on the router is the Local ID on the VPN Client and vice versa.

7	**Gateway certificate** Checking the certificate chain of the certificate received from the VPN gateway is enabled. The gateway certificate chain could not be validated.	• Check the gateway certificate expiration date. • Check the validity start date of the gateway certificate. • Check the signatures of all certificates in the certificate chain (including root certificate, intermediate certificates, and gateway certificate). • Check whether the CRLs of all certificate issuers in the certificate chain are up to date. • Make sure that none of the certificates concerned have been revoked in the corresponding CRL lists. • Make sure that the root certificate and all certificates in the certificate chain (root certification authority and intermediate certification authorities) are available in the Windows Certificate Store on the workstation. • Make sure that the CRLs of the various certification authorities are available in the Windows Certificate Store, or that these CRLs can be downloaded when the VPN connection is opened.
9	**No response from gateway** The VPN Client has abandoned the connection, most often after several connection attempts.	• Check whether the gateway is still accessible from the workstation.
10	**Authentication issue** The gateway has declined the user's authentication credentials.	• Check the user certificate. • Check that the Local ID on the Protocol tab of the Configuration Panel matches the value and type defined on the gateway. **Caution**: The Local ID on the VPN Client is the Remote ID on the router and vice versa. • Check the logs on the remote gateway to get more information about this issue.
13	**Configuration issue** An error occurred while establishing the VPN connection. Establishing the VPN connection has been abandoned.	• Retrieve the user log files. They must be analyzed. • Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
14	**Network configuration** An error occurred while creating the virtual interface used for the VPN connection.	• Retrieve the user log files. They must be analyzed. • Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
15	**Network configuration** The virtual IP address assigned during the VPN connection already exists on one of the workstation's interfaces.	• Change the virtual IP address ("VPN Client address" parameter) specified in the VPN Client's configuration. • Change the IP address provided by the gateway to the VPN Client.
16	**Network configuration** An error occurred while creating the virtual interface used for the VPN connection.	• Retrieve the user log files. They must be analyzed. • Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.

24	**Configuration issue** The gateway did not accept the cryptographic algorithm suite provided by the VPN Client.	• Make sure that the VPN Client's cryptographic algorithm suites match those of the gateway. • Check the Local ID and Remote ID. **Caution**: The Local ID on the router is the Remote ID on the VPN Client and vice versa.
25	**Configuration issue** The gateway did not accept the remote network configured in the VPN Client or the virtual IP address provided by the VPN Client.	• Make sure that the virtual IP address ("VPN Client address" parameter) specified in the VPN Client's configuration is acceptable at the gateway end. • Make sure that the remote network ("Remote network address" parameter) specified in the VPN Client's configuration is acceptable on the gateway end.
26	**Configuration issue** The VPN client provides its own traffic selectors, while the gateway is configured to provide them.	• Check the "Request configuration from the gateway" parameter in the "Child SA" tab.
27	**Gateway error** The gateway reported an error not supported by the VPN Client.	• Analyze the logs on the gateway end. • Retrieve the user log files. They must be analyzed. • Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
28	**Login/password error** The gateway has rejected the EAP authentication while establishing the VPN connection.	• Check the EAP authentication parameters in the VPN Client's configuration. • Make sure that the user knows his or her credentials, should he or she need them while establishing the connection.
30	**Smart card or token error** Cannot access the certificate stored the on the smart card or token.	• Check that the smart card reader or token is correctly configured on the workstation, and that the VPN Client can access it.
31	**Captive portal authentication timeout expired** No session has been opened on the captive portal. The workstation therefore has no internet connectivity.	• Click the Connect button in order to authenticate on the captive portal.
100	**Cannot load the VPN configuration** No VPN connection has been found in the configuration file.	• Make sure that at least one tunnel is configured in the Connection Panel. Go to Tools -> Connections Configuration, then add a tunnel and save the configuration.
101	**GINA configuration error** A tunnel is active before logon, but has not been configured to be used by the TrustedConnect Panel.	• Make sure that the tunnel which is active before logon is also configured in the Connection Panel. Go to Tools -> Connections Configuration, then add a tunnel and save the configuration.
102	**IKE initialization error** An error occurred while initializing the IKE daemon.	• Retrieve the user log files. • Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.

103	**DNS error** A DNS name could not be resolved in the set of rules for the filtering mode.	• Make sure that the workstation can access the internet. • Make sure that the filtering mode does not itself block access to DNS queries. • Replace DNS names with IP addresses.
200	**Software activation** The software is not activated and the trial period has expired.	• Retrieve the user log files. • Check software activation.

27.4 Windows Enterprise VPN Client technical data

General

Windows version	Windows 10 & 11, 64-bit
Languages	Arabic, Chinese (simplified), Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, Turkish

Operating mode

Invisible mode	Automatically open tunnel when traffic is detected Control access to VPN configurations Hide part or all the interfaces
USB mode	No more VPN configurations stored on the workstation Open tunnel when a USB drive configured for VPN is inserted Automatically close tunnel when a USB drive configured for VPN is removed
Gina	Open a tunnel before Windows logon using: GINA/Credential providers on Windows 10 & 11
Scripts	Run configurable scripts when opening or closing a VPN tunnel
Remote Desktop Sharing	Open a remote computer with a single click via RDP and VPN tunnel
TrustedConnect Panel	Automatically open tunnel with Always-On and trusted network detection (TND)

Connection/Tunnel

Connection mode	Peer-to-gateway
Media	Ethernet, DSL, cable, Wi-Fi, 4G, 5G, satellite
Protocols	IPsec IKEv1 or IKEv2 (IKE based on OpenBSD 3.1 (ISAKMPD)) SSL Diffie-Hellman DH group 14 to 21
Tunneling modes	Main mode and Aggressive mode
Mode Config/Mode CP	Automatically retrieve network parameters from VPN gateway

Cryptography

Encryption	Symmetric: AES CBC/CTR/GCM 128/192/256 bits Asymmetric: RSA Diffie-Hellman: DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521) Hash: SHA2-256, SHA2-384, SHA2-512
Authentication	Administrator: Protect access to the VPN configurations User: - Static or dynamic X-Auth (prompt every time a tunnel is opened) - Hybrid Authentication - Preshared key - EAP (MSCHAP-V2) - Multiple Auth
PKI	- Support for certificates in X.509 format: PKCS#12, PEM - Multiple media: Windows Certificate Store, smart card, token, configuration file - Support for Certificate Revocation List (CRL) - Automatically detect a smart card reader or token according to criteria - Access smart cards and tokens in PKCS#11 or CNG format - Check "Client" and "Gateway" certificates

Miscellaneous

NAT/NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 and RFC 3947, IP address emulation, includes support for: NAT_OA, NAT keepalive, NAT-T aggressive mode, NAT-T in forced, automatic or disabled mode
DPD	RFC3706. Detection of inactive IKE endpoints.
Redundant gateway	Redundant gateway management, automatically selected when DPD is triggered (inactive gateway)

Administration

Deployment	Silent installation using Microsoft Installer (MSI)
VPN configuration management	Import and export options for VPN configurations Secure import/export using passwords, encryption, and integrity control
Automation	Ability to open, close, and monitor a tunnel using command lines (batch and scripts) Ability to start and quit the software using batches
Logs and traces	IKE/IPsec and SSL/OpenVPN log console and trace mode can be enabled Administrator logs: local file, Windows Event Log, syslog server
Updates	Check for available updates from within the software
License and activation	Licenses available on a subscription basis, manual/automatic/silent activation

27.5 Third-party licenses

Credits and references to third-party licenses.

27.5.1 OpenSSL

OpenSSL is licensed under the Apache License 2.0 reproduced below.

the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents

of the NOTICE file are for informational purposes only and
do not modify the License. You may add Your own attribution
notices within Derivative Works that You distribute, alongside
or as an addendum to the NOTICE text from the Work, provided
that such additional attribution notices cannot be construed
as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions
for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

27.5.2 LZ4

Lz4 is licensed under the Simplified BSD License reproduced below.

28 Contact

28.1 Information

All the information on TheGreenBow products is available on our website:
https://thegreenbow.com/

28.2 Sales

Phone: +33.1.43.12.39.30
E-mail: sales@thegreenbow.com

28.3 Support

There are several pages related to the software's technical support on TheGreenBow's website:

Online help

https://www.thegreenbow.com/en/support/online-support/

FAQ

https://www.thegreenbow.com/en/frequently-asked-questions/

Contact form

Technical support can be reached using the form on our website at the following address:
https://www.thegreenbow.com/en/support/online-support/technical-support/

THEGREENBOW

Protect your connections
in any situation

14, rue Auber
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com