

Windows Standard VPN Client 6.86

User Guide

Latest update: 26 June 2021

Table of Contents

1	Overview	4
1.1	Introduction	4
1.2	Important information	4
1.3	What's new in release 6.8	5
2	Installing the software	6
2.1	Introduction	6
2.2	Installation procedure	7
2.3	Canceling installation	13
2.4	Trial period	13
3	Activating the software	15
3.1	Step 1	15
3.2	Step 2	15
3.3	Activation errors	16
3.4	Manual activation	17
3.5	Temporary license	19
3.6	License and activated software	21
4	Updating the software	22
4.1	How to get an update	22
4.2	Update procedure	23
5	Uninstalling the software	24
6	Using the test tunnel	25
7	Configuration Wizard	27
7.1	Step 1	28
7.2	Step 2	28
7.3	Step 3	30
8	User interface	31
8.1	Overview	31
8.2	Start menu	31
8.3	Desktop	31
8.4	Taskbar icon	32
8.5	Contextual menu of the taskbar icon	32
8.6	Fade-out pop-up	32
9	Connection Panel	34
10	Configuration Panel	35
10.1	Menus	35
10.2	Status bar	36
10.3	Shortcuts	36
10.4	VPN tunnel tree	37
11	"About..." window	41
12	Importing and exporting the VPN configuration	42
12.1	Importing a VPN configuration	42
12.2	Exporting a VPN configuration	43
12.3	Merging VPN configurations	44
12.4	Splitting a VPN configuration	44
13	Configuring a VPN tunnel	45
13.1	IPsec IKEv1, IPsec IKEv2 or SSL VPN	45
13.2	Editing and saving a VPN configuration	45
13.3	Configuring an IPsec IKEv1 tunnel	46
13.4	Configuring an IPsec IKEv2 tunnel	58

13.5	Configuring an SSL VPN tunnel	67
14	Redundant gateway	75
15	Automation.....	76
16	Fallback tunnel.....	78
17	IPv4 and IPv6	79
18	Managing certificates	80
18.1	Selecting a certificate ("Certificate" tab)	80
18.2	Importing a certificate	82
18.3	Windows Certificate Store	84
18.4	VPN gateway certificate	84
18.5	Managing certification authorities.....	84
18.6	Using a VPN tunnel with a certificate stored smart card or token	85
19	Remote Desktop Sharing.....	86
20	Configuring the Connection Panel	87
21	USB mode	89
21.1	Overview	89
21.2	Configuring the USB mode.....	89
21.3	Using the USB mode.....	92
22	GINA mode.....	94
22.1	Overview	94
22.2	Configuring the GINA mode	94
22.3	Using the GINA mode	94
23	Options	96
23.1	Displaying/hiding the interface	96
23.2	General	97
23.3	Managing logs.....	98
23.4	PKI options.....	98
23.5	Managing languages.....	100
24	Administrator logs, console, and traces	102
24.1	Administrator logs	102
24.2	Console	103
24.3	Trace mode	104
25	Security recommendations	105
25.1	General recommendations.....	105
25.2	Operating precautions.....	105
25.3	VPN Client administration	105
25.4	VPN configuration	106
26	Contact	108
26.1	Information	108
26.2	Sales	108
26.3	Support.....	108
27	Appendixes.....	109
27.1	Shortcuts	109
27.2	Administrator logs	110
27.3	Technical data of the Windows Standard VPN Client	111
27.4	License and credits	113

1 Overview

1.1 Introduction

Thank you for downloading our Windows Standard VPN Client software.

The Standard edition is made for private individuals and SMBs. It provides a high level of communication security and is also easy to deploy, integrate, and use.

As it does not require the existing infrastructure to be reconsidered (OS, network, PKI), the Windows Standard VPN Client is designed to be transparently integrated into security policies that have been set up.

The Windows Standard VPN Client is marketed on the basis of a perpetual license. You can also subscribe to an annual subscription to benefit from dedicated support and ongoing software maintenance.

1.2 Important information

1.2.1 Encrypted configuration files

VPN configuration files that have been encrypted using versions of the Windows 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 Installation and configuration

- Use of a Microsoft Windows Installer (MSI) to facilitate deployment and software updates
- The following items will be preserved when updating from version 6.64:
 - Software settings
 - VPN configuration
 - License
- The entire software is compiled in 64-bit mode to Windows 10 for optimized performance and security
- Access to the VPN configuration can be restricted to Windows administrators

1.3.2 Cryptography

- Support for RFC 4304 Extended Sequence Numbers (ESNs) and RFC 6023 (Childless IKE Initiation) for enhanced security
- Support for Digital Signature authentication algorithms RFC 4754 “EC-DSA with SHA-2” (Method 9) and RFC 7427 “RSA with SHA-2” (Method 14) for strong certificate authentication using elliptic curves
- End of support for so-called “weak” algorithms (DES, 3DES, SHA, DH 1-2, DH 5) to guarantee strong authentication
- Reinforced encryption of the VPN configuration

1.3.3 Smart cards and tokens

- Support for the Microsoft CNG API (Cryptography API: Next Generation) brings support for the latest generation of tokens smart card readers
- End of support for Microsoft CSP API (Cryptographic Service Providers) in IKEv2 to guarantee strong authentication

1.3.4 Protecting VPN configurations

- Option for restricting the VPN configuration to OS administrators only
- Password has been removed from Configuration Panel
- Increased configuration file protection with SHA-2

1.3.5 SSL/TLS

- Support for Lz4 compression

2 Installing the software

2.1 Introduction

The Windows Standard VPN Client is installed by executing the program that you can download from our website:

https://www.thegreenbow.fr/vpn_client.html.

The default installation procedure, which consists in double-clicking the icon of the program you have downloaded, opens a window that allows you to customize the installation.

👉 Refer to section 2.2 Installation procedure.

2.1.1 Installation conditions

The Windows Standard VPN Client is available for Windows 10 64-bit.

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

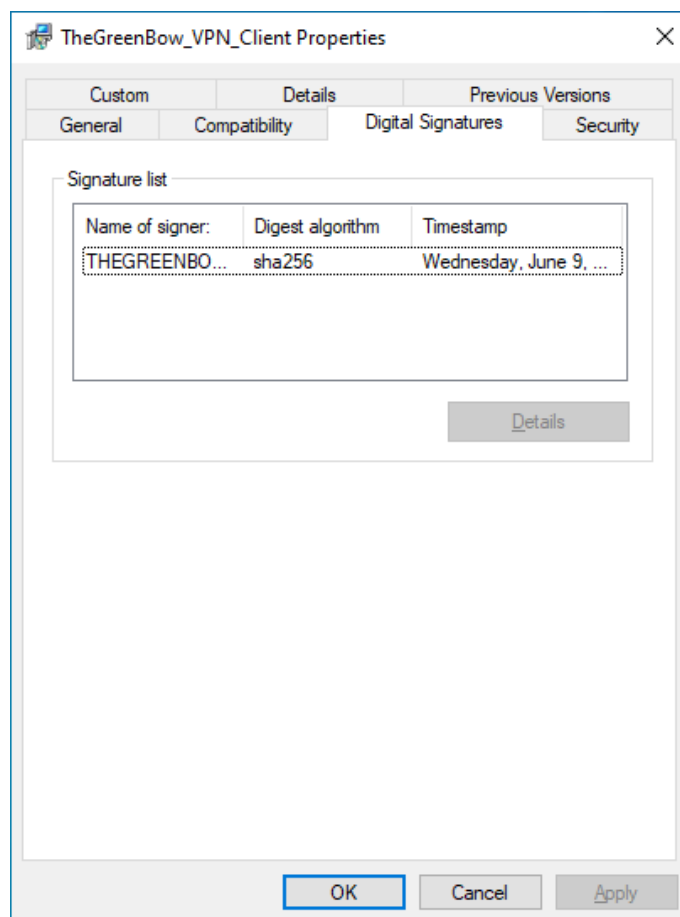
- Processor: 1 gigahertz (GHz) or faster processor or SoC
- RAM: 2 GB
- Hard disk space available: 40 MB

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 installation program for the Windows Standard VPN Client (and all its constituent binaries) is signed by a TheGreenBow certificate. 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 Standard VPN Client in the “About...” window of the software.
➞ Refer to section 11 “About...” window.

2.1.3 Vulnerabilities

Users of the Windows Standard VPN Client who subscribe to the TheGreenBow newsletter (available on our website) 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.).

Such a subscription is made automatically for the software’s clients, i.e. those who provided their email address when purchasing the software.



See also the [security recommendations](#) for the Windows Standard VPN Client.

2.2 Installation procedure

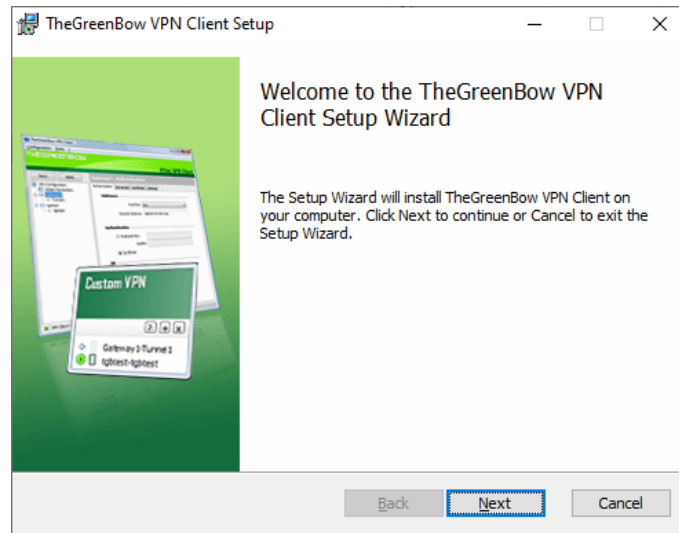
Once you have downloaded the Windows Standard VPN Client installer and verified its integrity (see section 2.1.2 Digital signature and version above), you can proceed with its installation by following the steps described below.

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

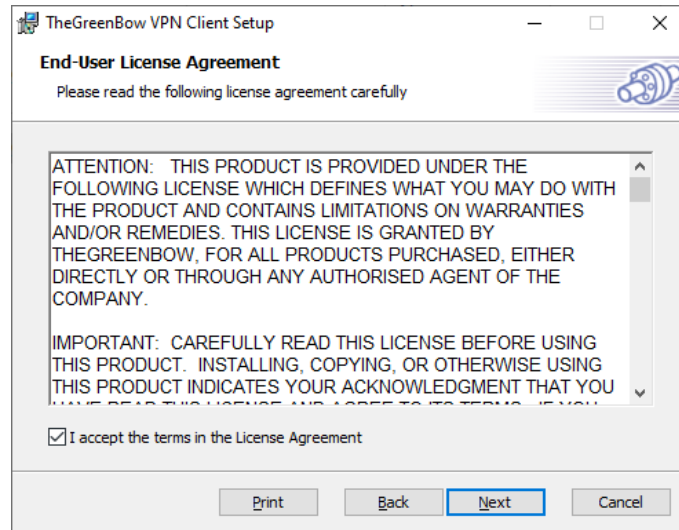


You can only update the software if you install a minor update or if you subscribed to ongoing maintenance (see section 4.1 How to get an update).

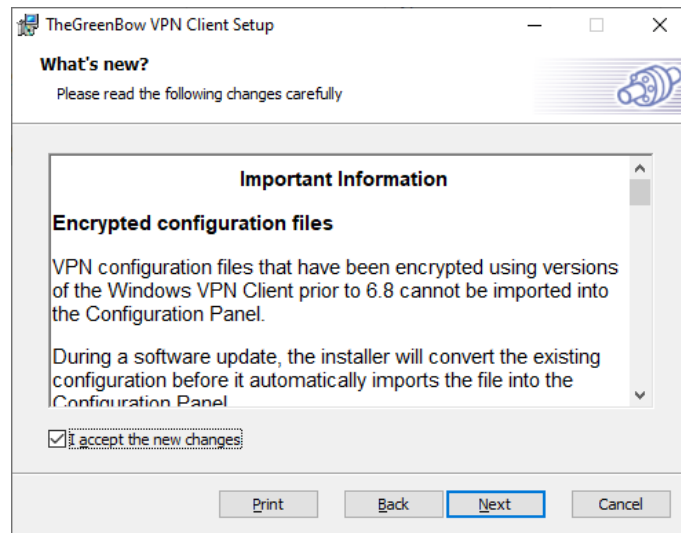
- 1/ Double-click the installation program you downloaded. The following window is displayed:



- 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 Standard VPN Client. The following window is displayed:

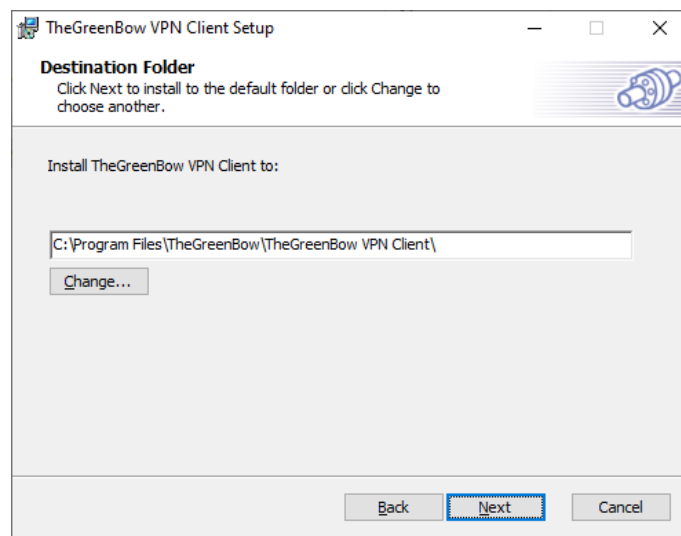


- 4/ Carefully read the information about what's new and the note about how the existing configuration will be converted during an update.

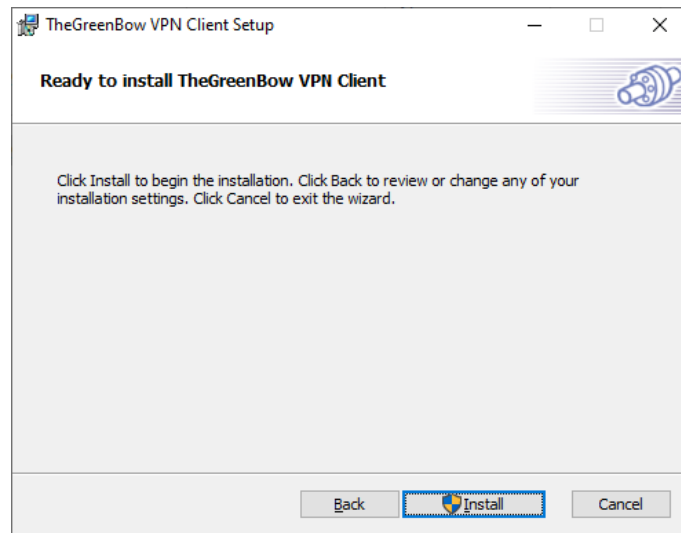


Once the installation is complete, you will not be able to revert to an earlier version of the software. If in doubt, back up your VPN configuration to a separate folder or to a removable storage medium.

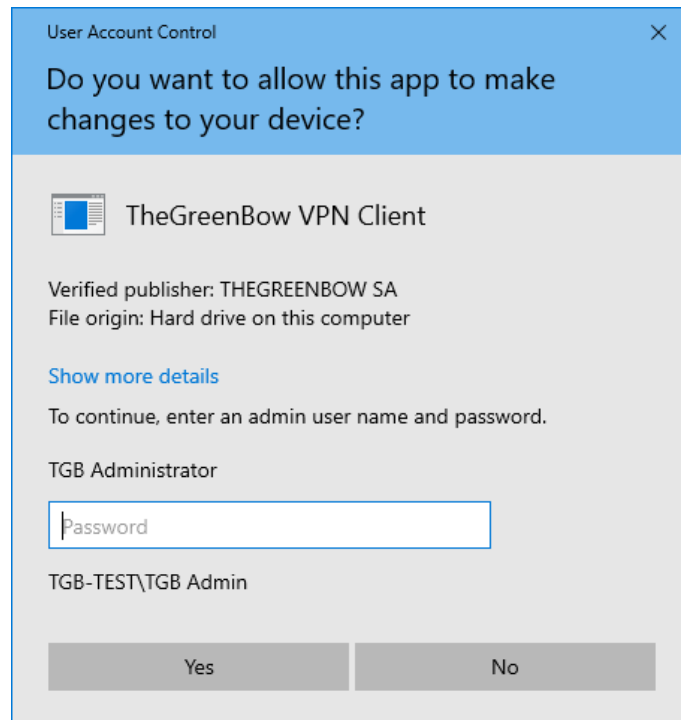
If you accept all the terms of the agreement, select the “I accept the new changes” checkbox, and then click “Next”. The following window is displayed:



- 5/ If you want to install the Windows Standard 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:



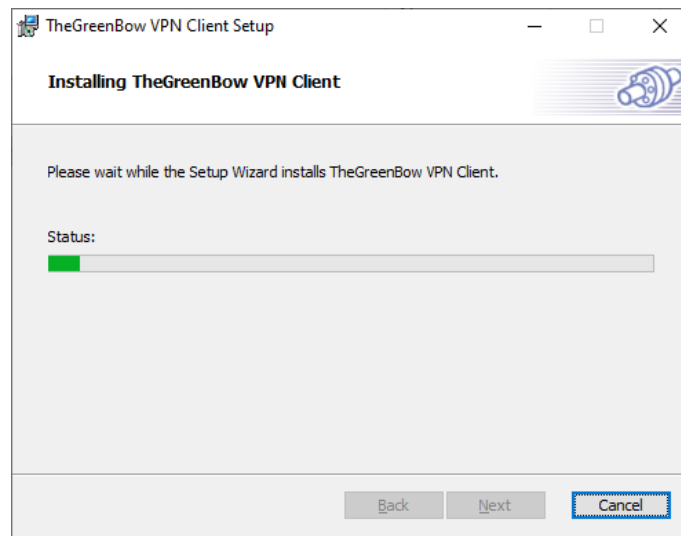
- 6/ The program is ready to install. If you want to go back to check or change your installation settings, click “Back”. Otherwise, click “Install”. If you are installing from an account that does not have administrator rights, the following window is displayed:



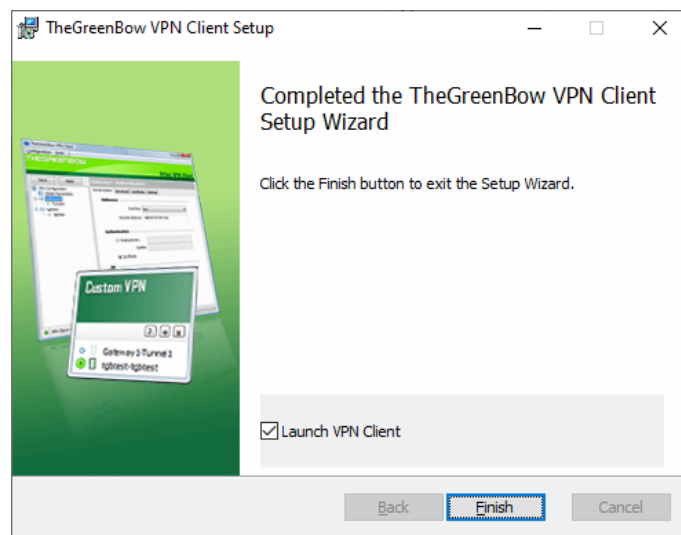
- 7/ To proceed with the installation, you must enter an administrator name and password to allow the installer to make changes to your computer. Otherwise, the software will not be installed.

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:



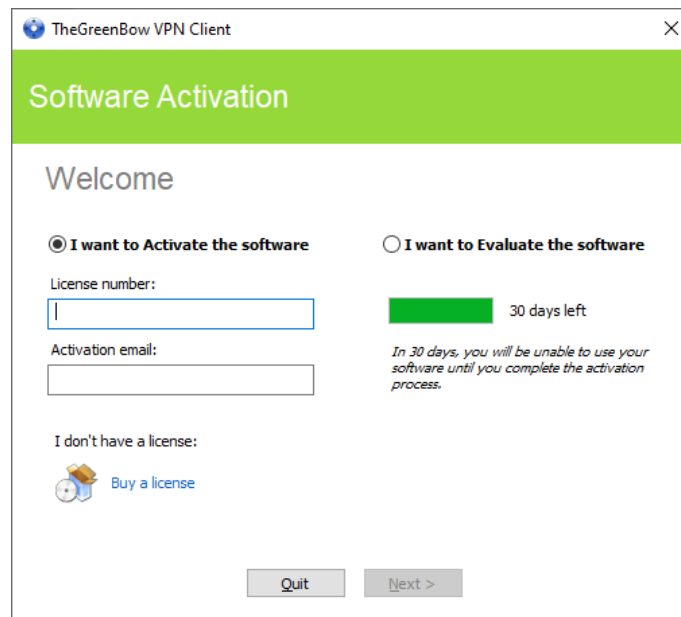
9/ Wait for the installation of the Windows Standard VPN Client including all its components to complete. If installation has succeeded, the following window is displayed:



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 Using the test tunnel).

Otherwise, the activation screen is displayed:



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

If you already own a license for the Windows Standard 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 section 3 Activating the software.

If you want to try the Windows Standard 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.

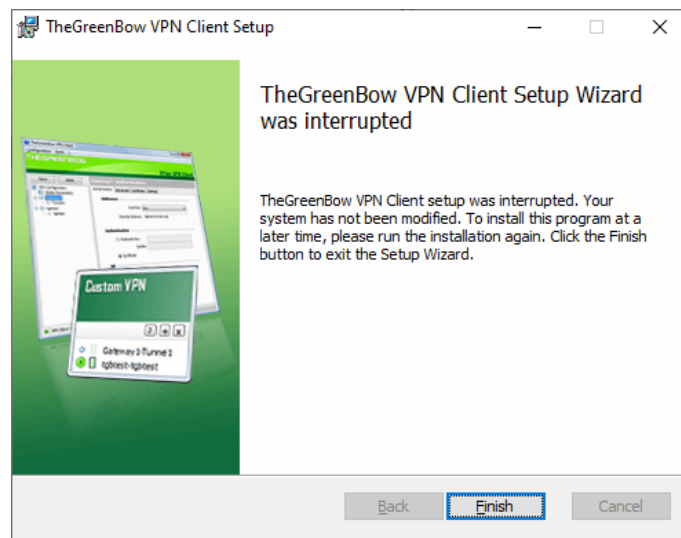
If you do not have a license and want to buy one, click "Buy a license". TheGreenBow online store is displayed in a browser window. Here, you can buy one or several licenses. For further details on the activation procedure, refer to section 3 Activating the software.

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

- To start using the Windows Standard VPN Client immediately, refer to section 6 Using the test tunnel.
- For a detailed presentation of the various user interface elements, refer to section 8 User interface.
- For a comprehensive explanation of all tunnel configuration options, refer to section 13 Configuring a VPN tunnel.
- To uninstall the Windows Standard VPN Client, refer to section 5 Uninstalling the software.

2.3 Canceling installation

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

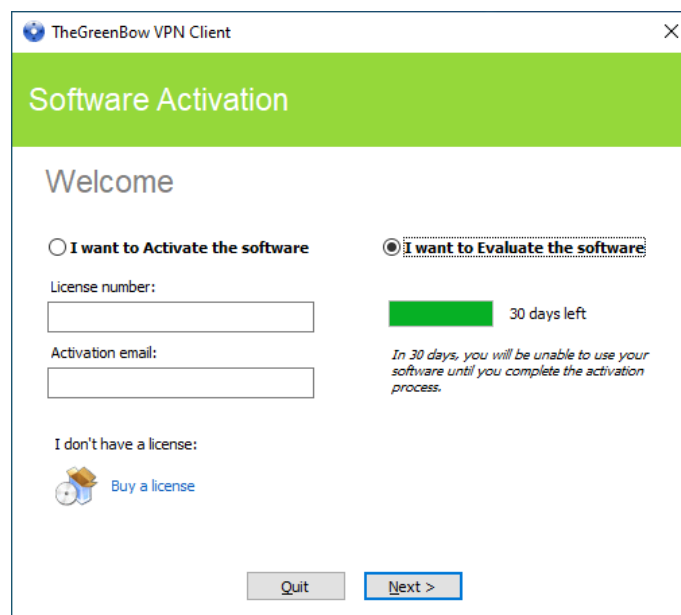


Your system has not been modified and you can resume installation at a later time.

2.4 Trial period

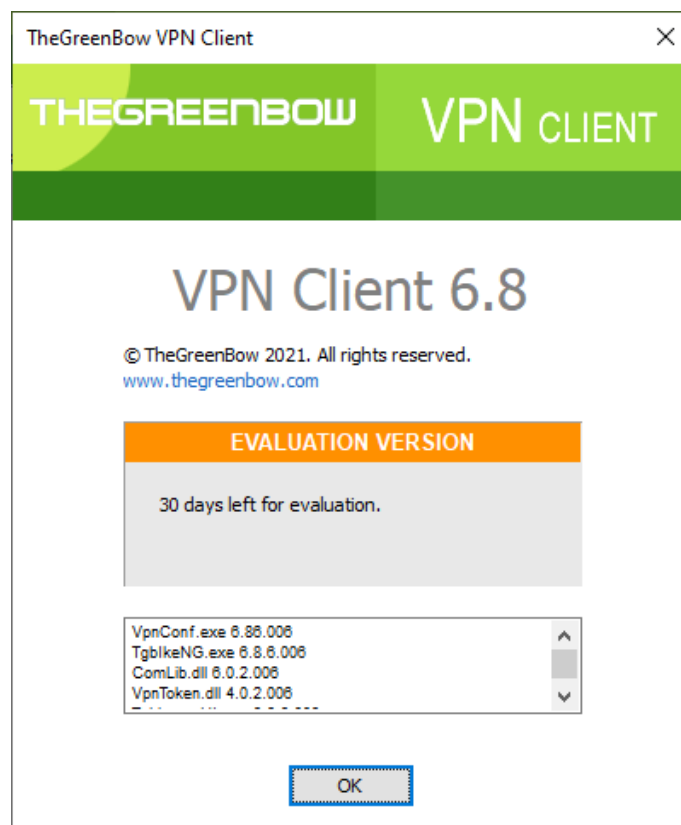
The first time the software is installed on a workstation, if no license key is provided to the installer, the VPN Client will enter a 30-day trial period. During this trial period, the VPN Client is fully operational, and all functions are unlocked.

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.

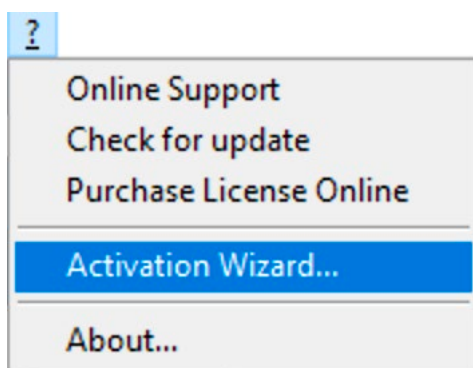


Select “I want to Evaluate the software”, then click “Next >” to run the software.

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 through the "? > Activation Wizard..." menu of the main interface (Configuration Panel).



3 Activating the software

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 from the “? > Activation Wizard...” menu in the main interface.

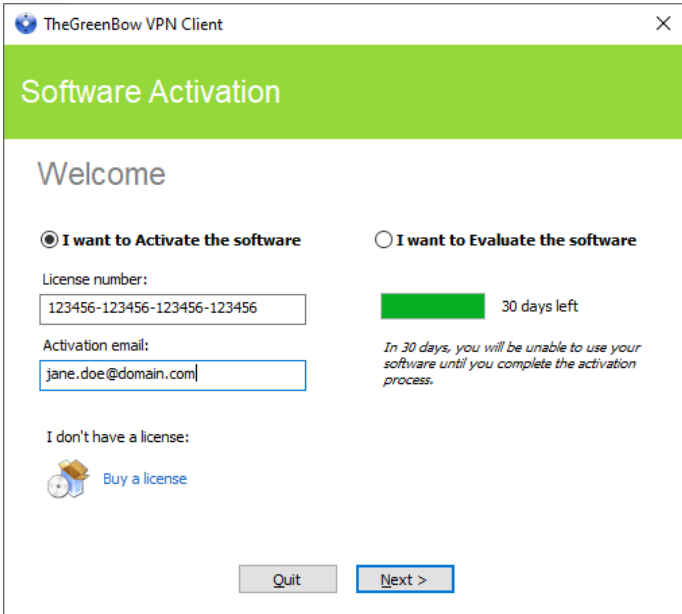
3.1 Step 1

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 screenshot shows the 'Software Activation' window of TheGreenBow VPN Client. It has a green header bar with the title 'Software Activation'. Below the header, the word 'Welcome' is displayed. There are two radio buttons: 'I want to Activate the software' (selected) and 'I want to Evaluate the software'. Under the 'Activate' option, there is a 'License number:' label and a text box containing '123456-123456-123456-123456'. Below that is an 'Activation email:' label and a text box containing 'jane.doe@domain.com'. Under the 'Evaluate' option, there is a green bar indicating '30 days left' and a note: 'In 30 days, you will be unable to use your software until you complete the activation process.' At the bottom left, there is a link 'I don't have a license:' with a 'Buy a license' button. At the bottom right, there are 'Quit' and 'Next >' buttons.

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.

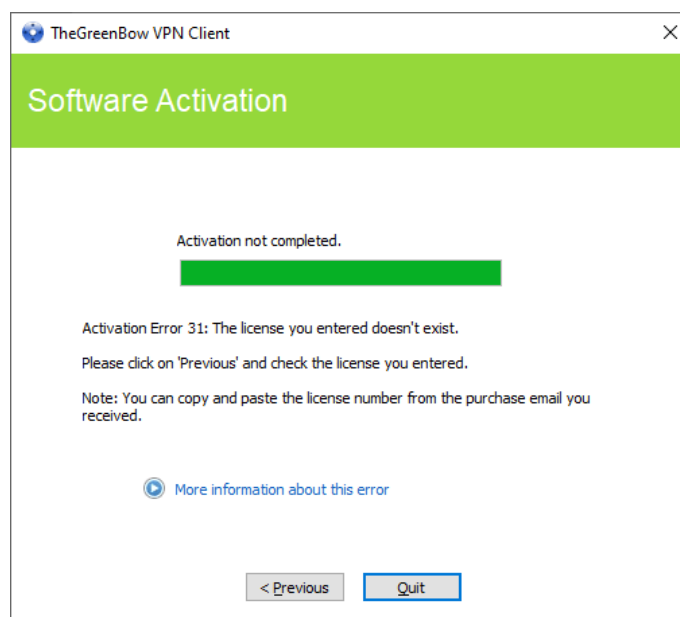


The software activation is linked to the workstation on which the software has been installed. Consequently, a license number allowing a single activation cannot be reused on another workstation once it is activated.

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.



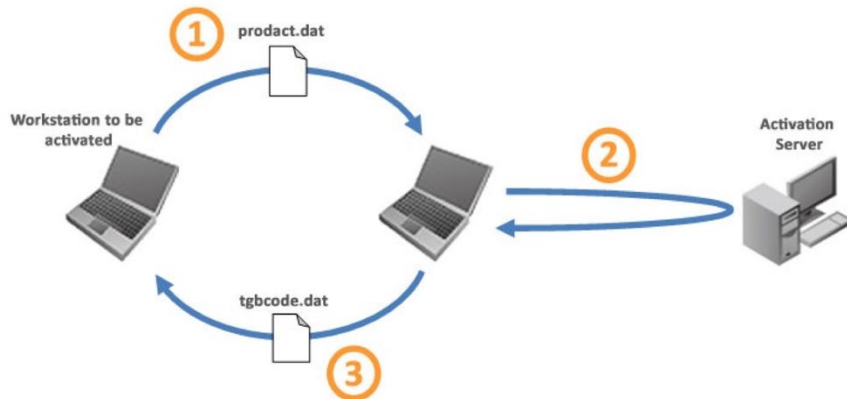
The TheGreenBow website lists all activation errors and [procedures for solving activation issues](#).

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

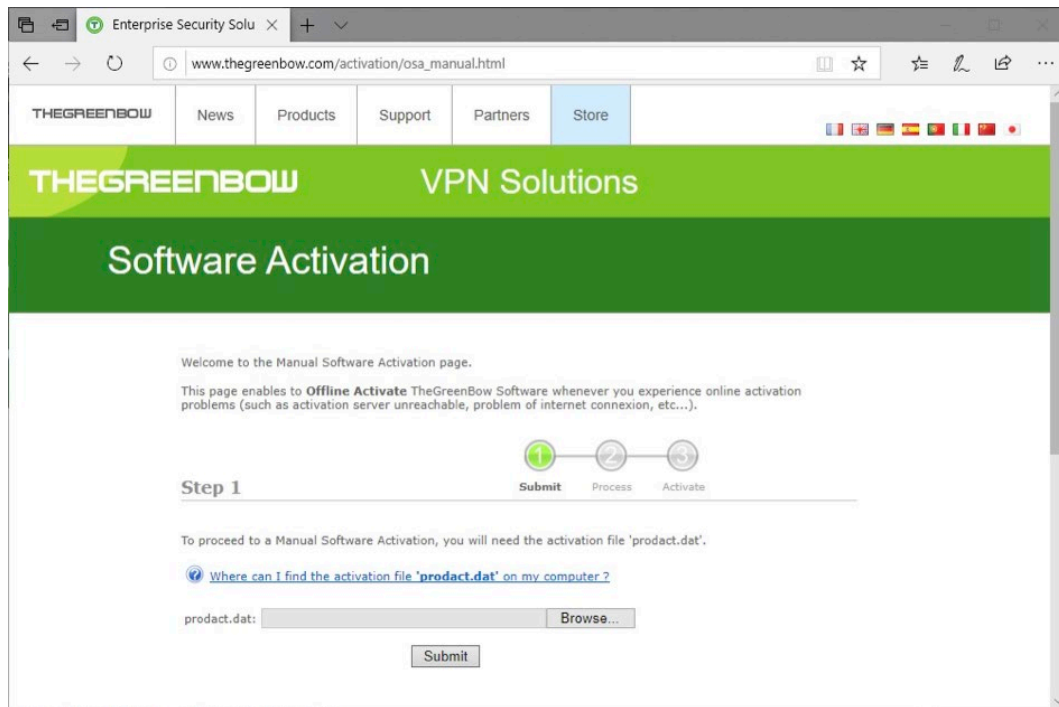
When activation fails because of a communication issue with the activation server, the software can be activated manually on the TheGreenBow website. The procedure is as follows:



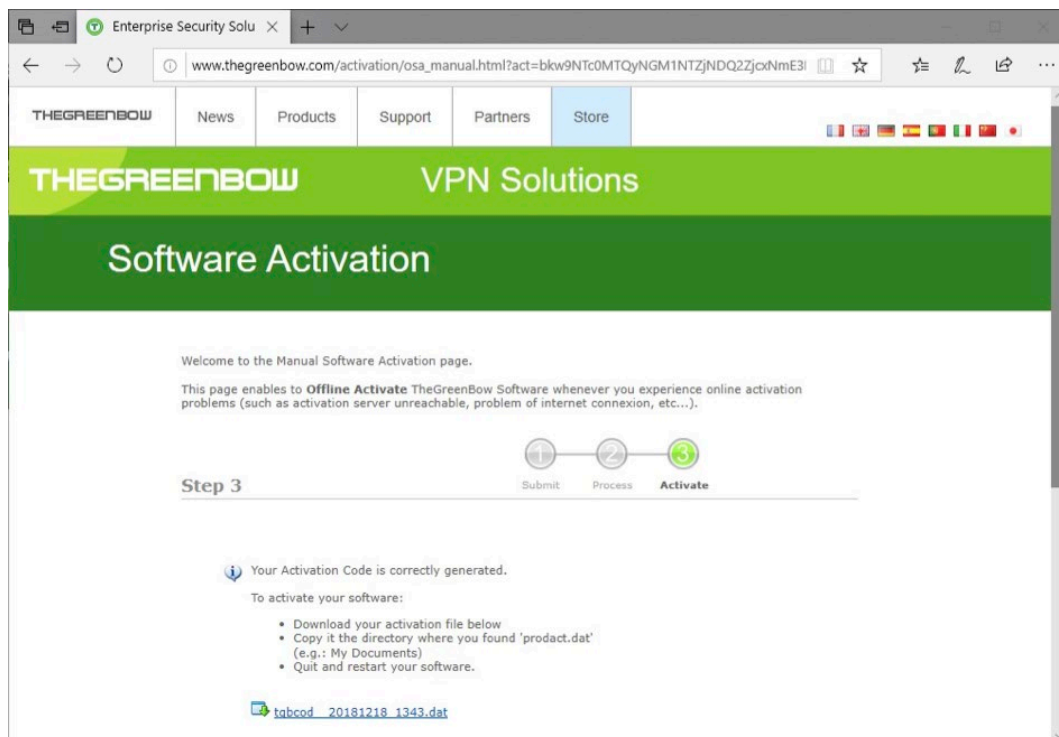
- 1** "product.dat" file
Retrieve the "product.dat" file from the "My Documents" Windows directory on the workstation that should be activated. (1)
 - 2** Activate
On a workstation that is connected to the activation server (2), open the manual activation page (3), and post the "product.dat" file. Let the server automatically create the tgbcode file.
 - 3** "tgbcode" file
Copy the "tgbcode" file to the "My Documents" Windows directory on the workstation that you want to activate. Start the software; it will be activated.
- (1) The "product.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 the manual activation, follow the steps below:

- 1/ On a workstation connected to the www.thegreenbow.com website, open the following webpage:
http://www.thegreenbow.com/activation/osa_manual.html?lang=en



- 2/ Click "Choose File" (or equivalent depending on the browser) and open the "product.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 "product.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 name of this file has the following format: tgbcod_[date]_[code].dat (e.g. tgbcod__20210615_1029.dat).

3.5 Temporary license

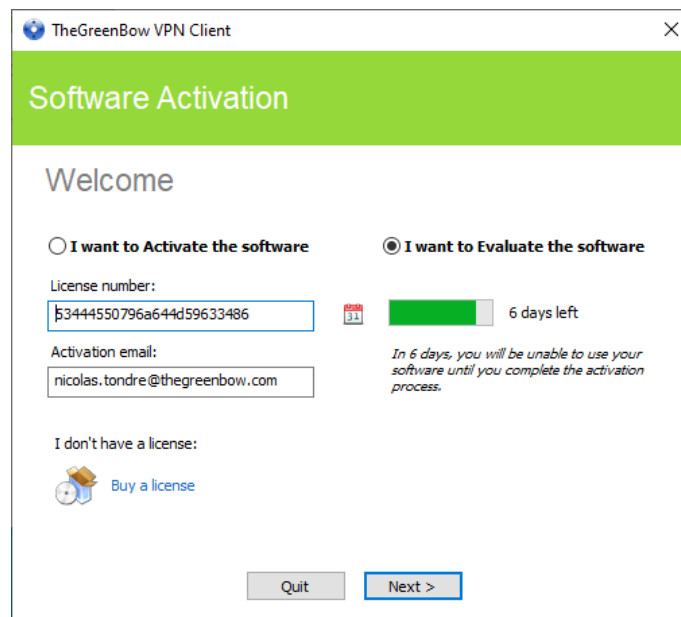
You can request TheGreenBow trial licenses, called temporary licenses, for example to continue using the software beyond the end of the standard trial period.

If you would like to get a temporary license, please contact the Sales department by email at sales@thegreenbow.com

To activate the temporary license, enter the license number and activation email in the corresponding fields:

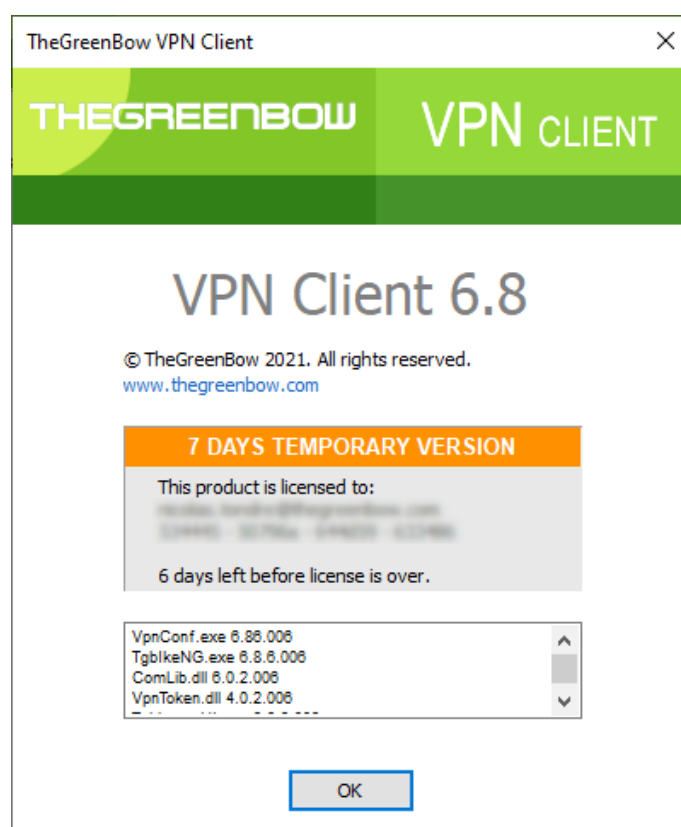
Then, click « Next ». A confirmation window is displayed:

The activation window will continue to appear when the software starts for as long as a temporary license is used. A calendar icon indicates that this license is temporary, and the number of days remaining is shown.



Click “Next >” to run the software.

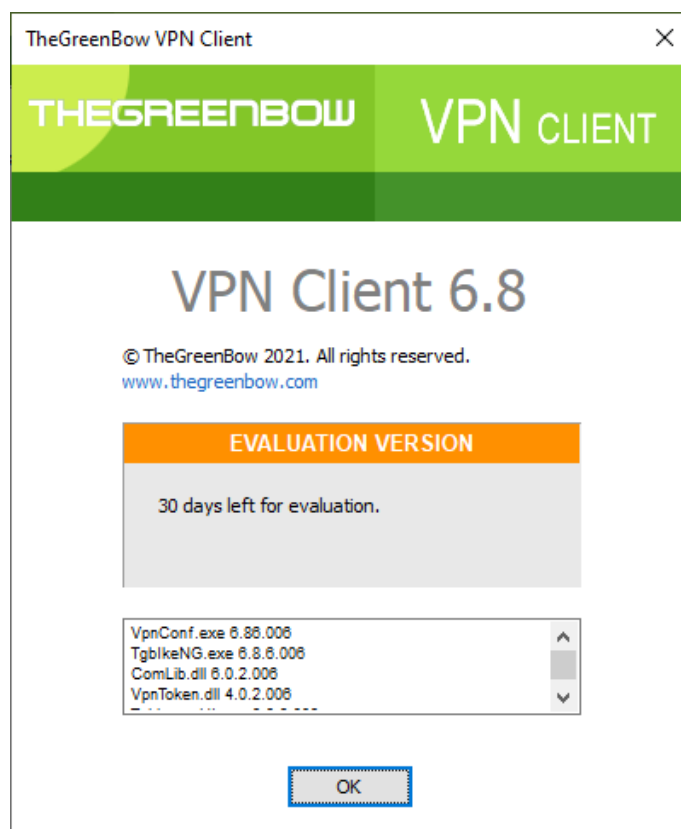
You will find all the information about the license and email used for activation in the “About...” window (see section 11 “About...” window):



Once the validity period of the temporary license expires, you must activate the software with a definitive license to keep using it.

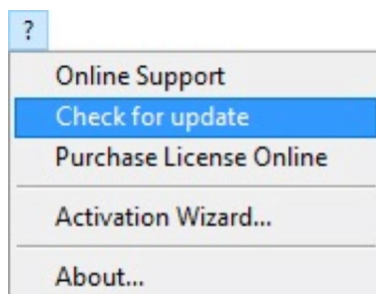
3.6 License and activated software

Once the software is activated, the license and email used for activation can be viewed in the “About...” window of the software (see 11 “About...” window).



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.

Example:

THEGREENBOW
VPN Solutions

Software license information

This page provides information on the latest Software Release you are allowed to install, based on the options of your purchase.

	Latest release	6.86.009	Download
	Release date	Jun 21st, 2021	
	Download size	19.8 Mb	Release Note

4.1 How to get an update

Software updates are provided according to the following rules:

During the maintenance period (1)	All updates can be installed
Outside the maintenance period or without a maintenance agreement	All minor updates can be installed (2)

- (1) The maintenance period starts on the date of purchase of the software.
 (2) Minor updates (or maintenance updates) are identified by the last digit of the version number, e.g. the last “6” in “6.86”.



Performing an update from an Enterprise, Premium, or Certified edition to a Standard edition and vice versa is not allowed.

Example:

You activated version 6.86 of the software. Your maintenance period has expired.

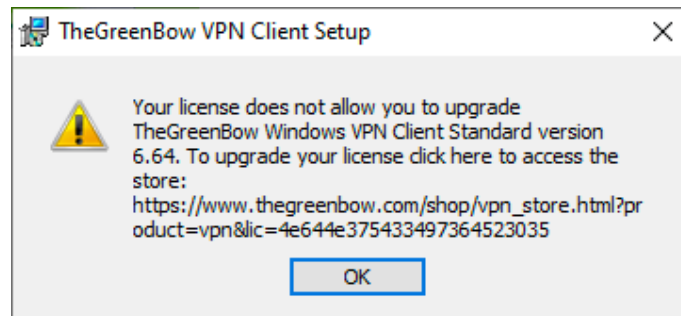
All updates from versions 6.87 to 6.89 are authorized.

All updates from version 6.90 and higher will be denied.

4.2 Update procedure

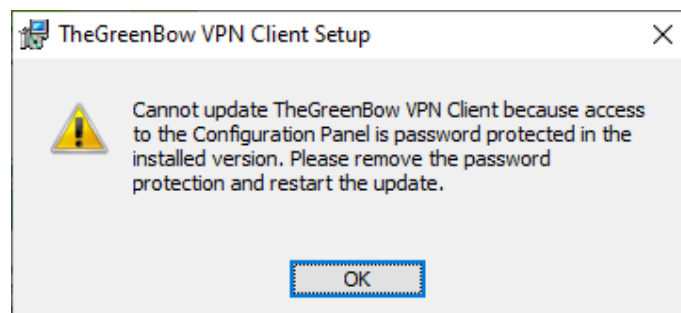
Updating the Windows Standard VPN Client allows you to upgrade to a newer version of the software while preserving the settings, the VPN configuration, and the license. It is performed in the same way as a normal installation (see section 2.2 Installation procedure) except in the following two cases:

- 1/ If the license of the installed product is not compatible with the Windows Standard 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:



We recommend removing the password protection for access to the Configuration Panel in the installed version. The update can then be performed normally.

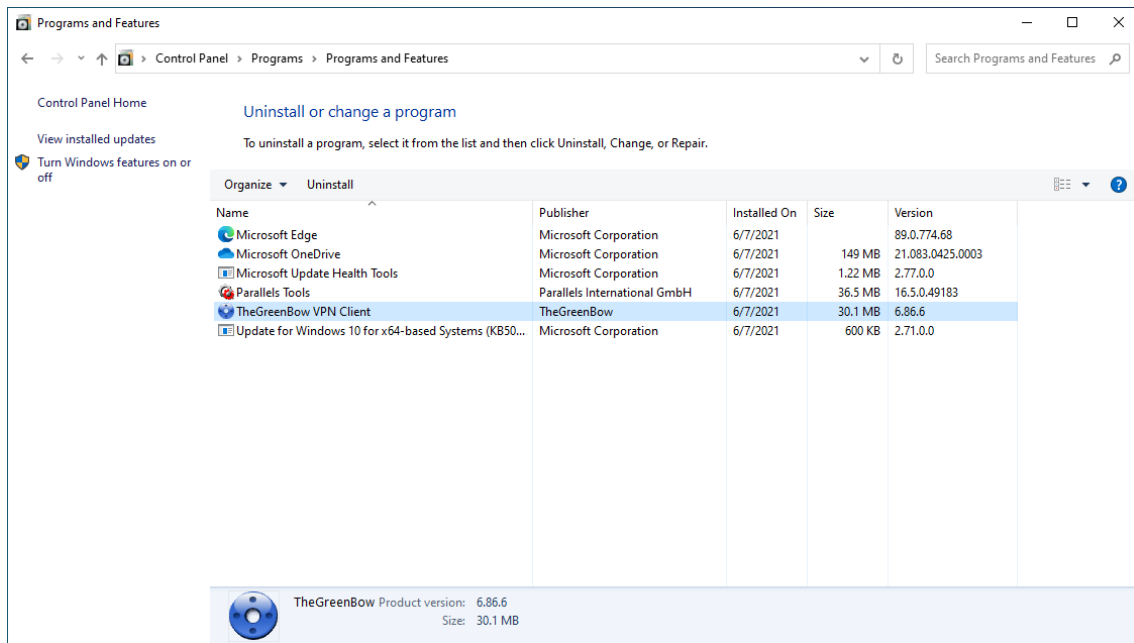


Password protection for access to the Configuration Panel has been replaced in version 6.8 of the Windows Standard VPN Client by a more secure mechanism. It consists in limiting access to the Configuration Panel to Windows administrators only. This option is not enabled by default but can be enabled as described in section 23.1 Displaying/hiding the interface, check the "Restrict access to Configuration Panel to administrator" option.

5 Uninstalling the software

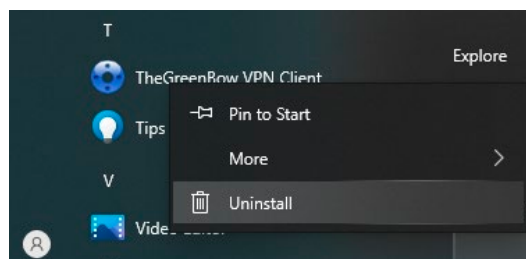
To uninstall the VPN Client, proceed as follows:

- 1/ Open the Windows Control Panel.
- 2/ Select « Uninstall a program ».
- 3/ Select “TheGreenBow VPN Client” 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 Client” program, then select “Uninstall”.



- 3/ The Windows Control Panel is displayed. Select “TheGreenBow VPN Client” 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 Using the test tunnel

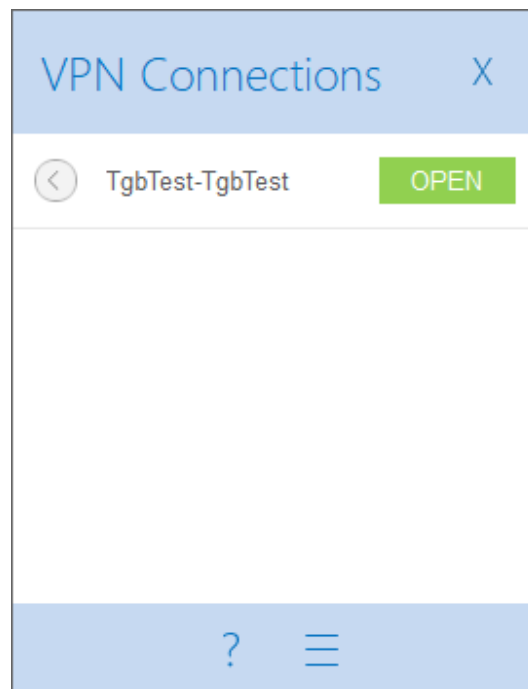
The Windows Standard VPN Client comes equipped with a VPN configuration containing a VPN test tunnel named “TgbTest-TgbTest”.

Once the installation or update is complete, if you have not unchecked the “Launch VPN Client” checkbox, the Windows Standard VPN Client will start minimized and the TheGreenBow VPN Client icon will appear in the taskbar. The taskbar icon is described in detail in section 8.4 Taskbar icon.

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 Standard 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.

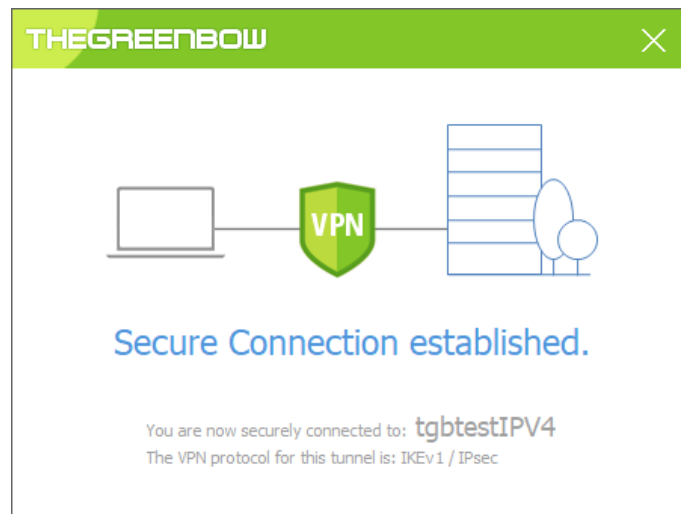
To open the Connection Panel, right-click the taskbar icon (see section 8.4 Taskbar icon) and then select the “Connection Panel” option. The Connection Panel is described in section 9 Connection Panel.

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

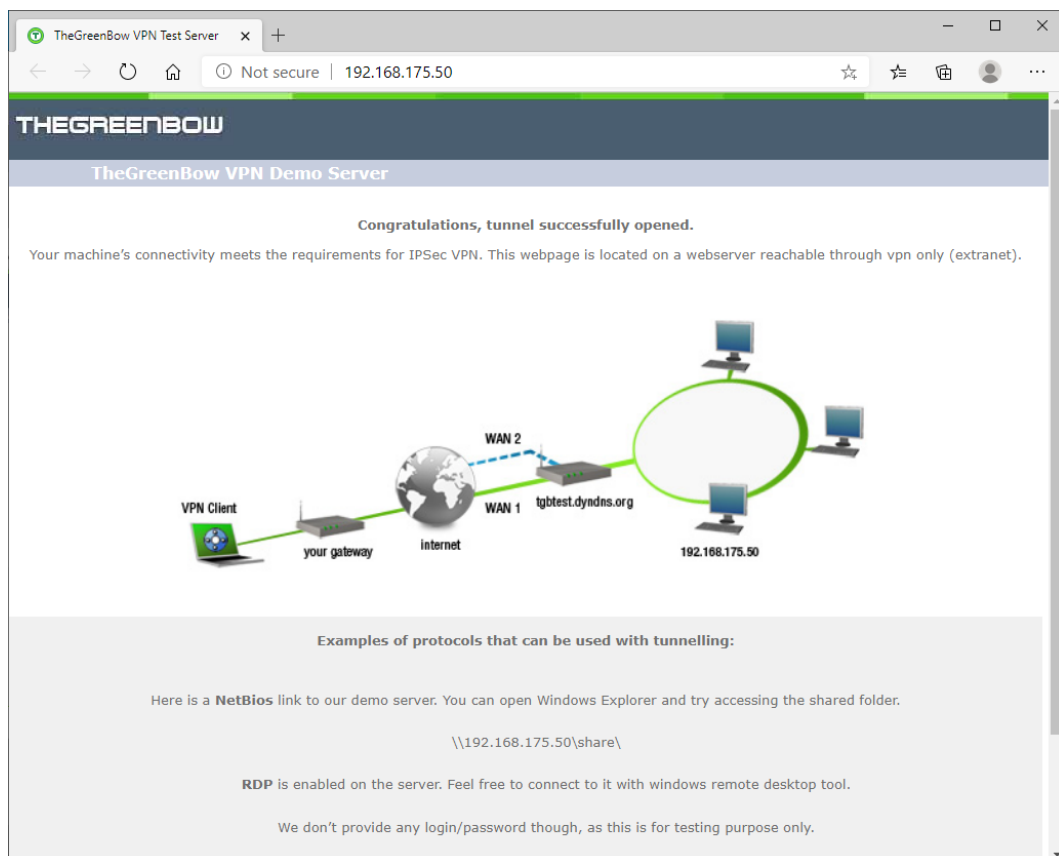


You can also open a test tunnel from the Configuration Panel (see section 10 Configuration Panel). To do this, double-click the “TgbTest-TgbTest” tunnel in the tree structure.

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



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



You have installed the Windows Standard VPN Client and you know how to activate the license and start a test tunnel. You can now create your own VPN configuration using your gateway settings in one of the following two ways:

- Using the Configuration Wizard, see section 7 Configuration Wizard)
- By directly entering the settings in the Configuration Panel, see section 10 Configuration Panel)



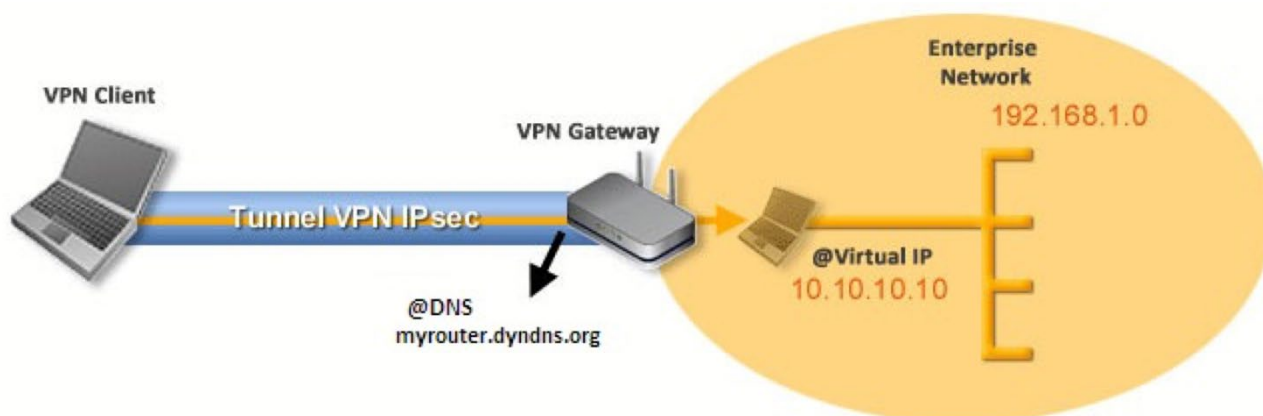
On our website, you will find many configuration guides for most VPN gateways:
http://www.thegreenbow.fr/vpn_gateway.html.

7 Configuration Wizard

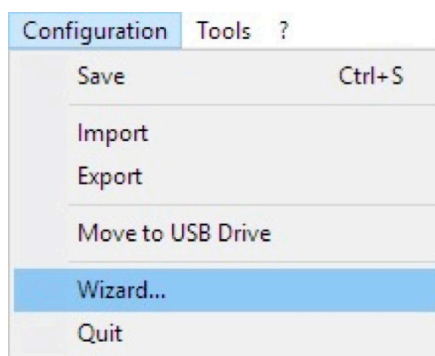
The Configuration Wizard in the Windows Standard VPN Client allows you to configure a VPN tunnel in three easy steps.

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



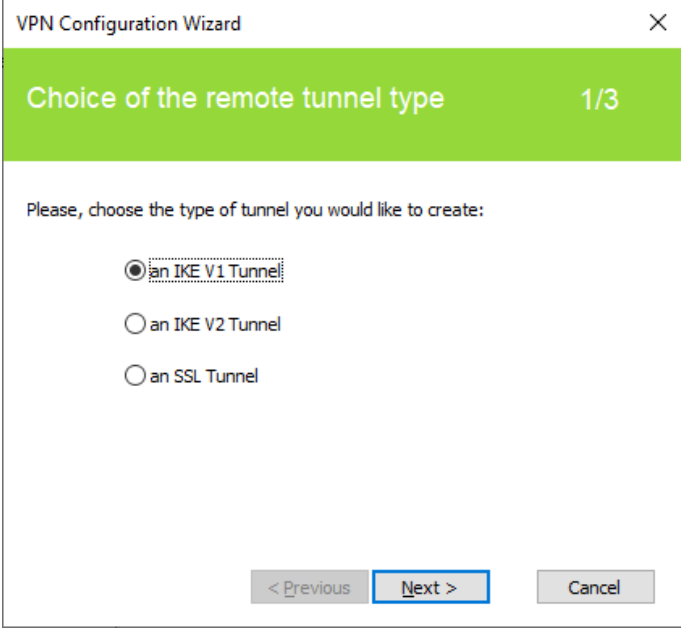
In the main interface, open the VPN Configuration Wizard: "Configuration > Wizard...".



Security recommendation: We recommend configuring IKEv2 tunnels with a certificate. Refer to section 25 Security recommendations.

7.1 Step 1

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



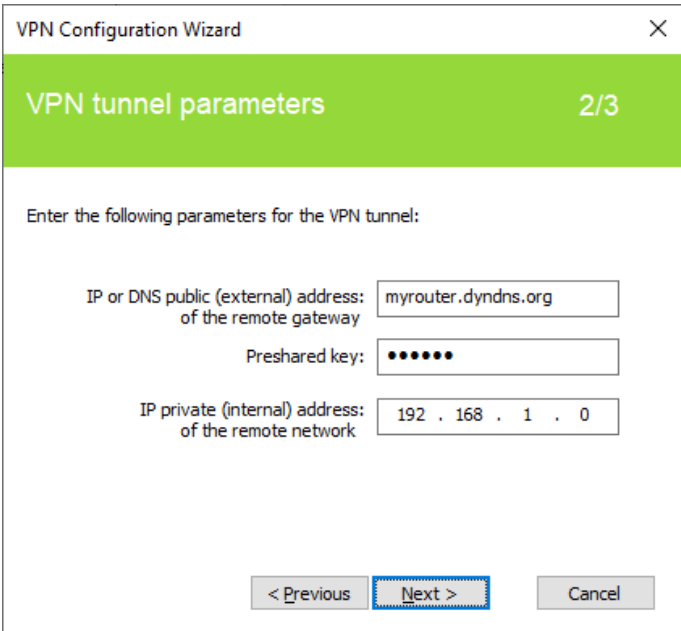
The screenshot shows the 'VPN Configuration Wizard' window at step 1/3, titled 'Choice of the remote tunnel type'. It prompts the user to 'Please, choose the type of tunnel you would like to create:'. There are three radio button options: 'an IKE V1 Tunnel' (which is selected), 'an IKE V2 Tunnel', and 'an SSL Tunnel'. At the bottom, there are three buttons: '< Previous' (disabled), 'Next >' (active/highlighted), and 'Cancel'.

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 company network (e.g. 192.168.1.0). (1)



The screenshot shows the 'VPN Configuration Wizard' window at step 2/3, titled 'VPN tunnel parameters'. It prompts the user to 'Enter the following parameters for the VPN tunnel:'. There are three input fields: 'IP or DNS public (external) address: of the remote gateway' with the value 'myrouter.dyndns.org', 'Preshared key:' with a masked value of seven dots, and 'IP private (internal) address: of the remote network' with the value '192 . 168 . 1 . 0'. At the bottom, there are three buttons: '< Previous' (disabled), 'Next >' (active/highlighted), and 'Cancel'.

(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 18.2 Importing a certificate)

The screenshot shows the 'VPN Configuration Wizard' window, step 2/3 titled 'VPN tunnel parameters'. It prompts the user to enter parameters for the VPN tunnel. The fields are: 'IP or DNS public (external) address: of the remote gateway' with the value 'myrouter.dyndns.org', and 'Preshared key' with a masked input (dots). There is an 'Import Certificate...' button. Below these, there are two radio buttons: 'Preshared Key' (selected) and 'Certificate'. At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

7.2.3 For an SSL tunnel (OpenVPN)

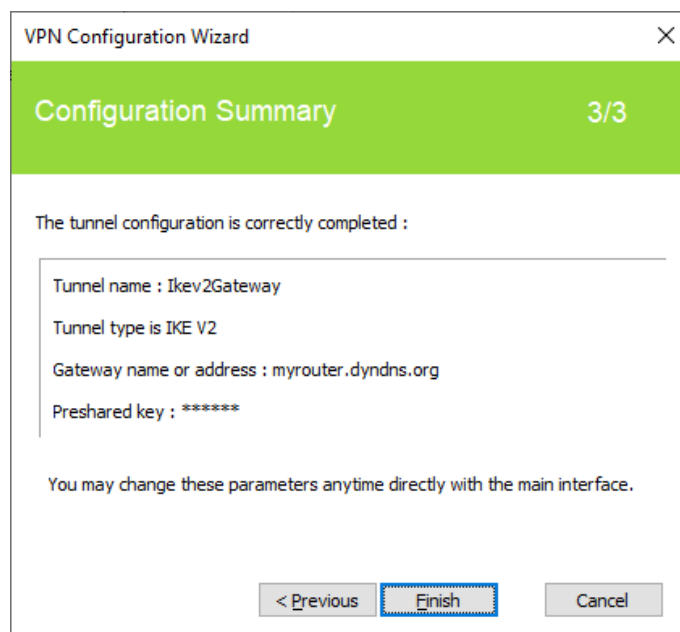
Enter the following values:

- 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 18.2 Importing a certificate)

The screenshot shows the 'VPN Configuration Wizard' window, step 2/3 titled 'VPN tunnel parameters'. It prompts the user to enter parameters for the VPN tunnel. The fields are: 'IP or DNS public (external) address: of the remote gateway' with the value 'myrouter.dyndns.org', and 'Certificate Common Name' with the placeholder '<Click the import button>'. There is an 'Import Certificate...' button. Below these, there is a 'Login required' checkbox which is unchecked. At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

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 User interface

8.1 Overview

The Windows Standard VPN Client user interface allows you to perform the following actions:

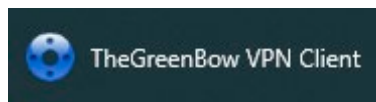
- 1/ Configure the software (startup mode, language, access control, etc.)
- 2/ Manage VPN configurations (VPN tunnel configuration, certificate management, import, export, etc.)
- 3/ Use VPN tunnels (open, close, identify incidents, etc.)

The user 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:
 - o A [set of menus](#) for VPN configuration and software management
 - o [The VPN tunnel tree](#)
 - o VPN tunnel configuration tabs
 - o A [status bar](#)
- An [icon on the taskbar](#) and the associated menu

8.2 Start menu

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

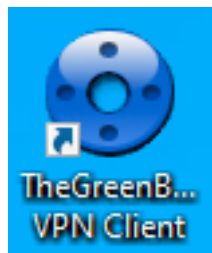


The VPN Client will start minimized and the TheGreenBow VPN Client icon will appear in the taskbar (see section 8.4 Taskbar icon).

8.3 Desktop

During the installation of the software, an icon is created for the application on the Windows desktop.

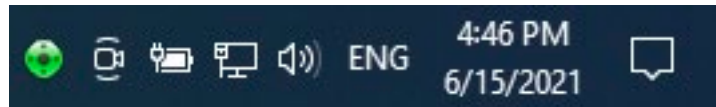
The Windows Standard VPN Client can be started directly by double-clicking this icon.



The VPN Client will start minimized and the TheGreenBow VPN Client icon will appear in the taskbar (see section 8.4 Taskbar icon).

8.4 Taskbar icon

Under normal operating conditions, the taskbar icon shows the status of the Windows Standard 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 VPN Client icon always shows the software status:

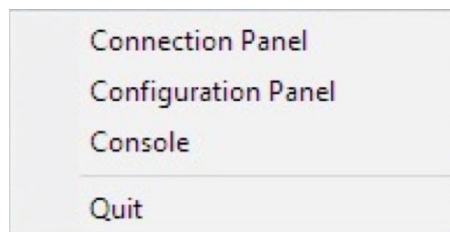
- "VPN Tunnel opened" if one or several tunnels are open
- "TheGreenBow VPN Client" when the VPN Client is running, but no tunnels are open

Left-clicking the icon opens the Connection Panel.

Right clicking the icon opens the contextual menu associated with the icon.

8.5 Contextual menu of the taskbar icon

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



The contextual menu contains the following options:

- 1/ Connection Panel: opens the Connection Panel
- 2/ Configuration Panel: opens the Configuration Panel (if the VPN Client has been run with administrator privileges)
- 3/ Console: opens the VPN traces window
- 4/ Quit: closes all open VPN tunnels and quits the software

8.6 Fade-out pop-up

When opening or closing a VPN tunnel, a 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



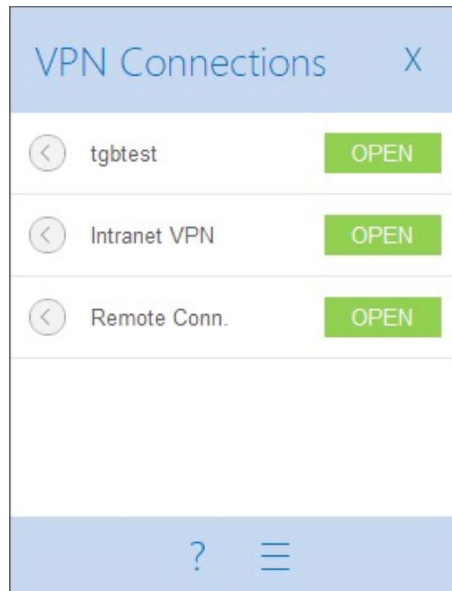
Failed to open the tunnel: the window will briefly explain what happened and provide a hyperlink for more information about the incident.



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.

9 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.

🔗 See section 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 configuration of this connection in the Configuration Panel.



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

Close the Connection Panel



Access to the Configuration Panel may be restricted. See section 23.1 Displaying/hiding the interface.

The following keyboard shortcuts are available for the Connection Panel:

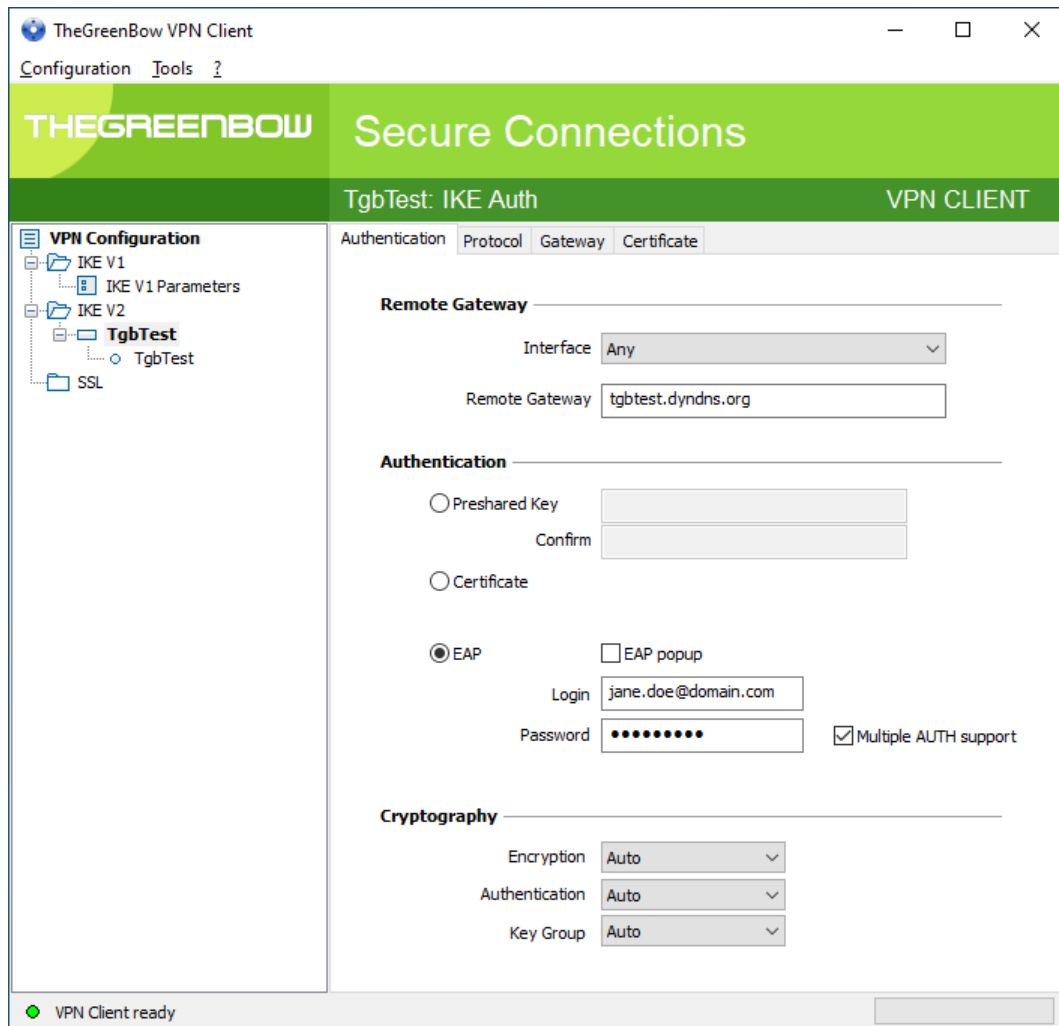
- ESC (or ALT+F4) closes the window
- CTRL+ENTER opens the Configuration Panel (main interface)
- CTRL+O opens the selected VPN connection
- CTRL+W closes the selected VPN connection
- The Up and Down arrow keys can be used to navigate up or down the VPN connection list

10 Configuration Panel

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

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



10.1 Menus

The following menus are available in the Configuration Panel:

–Configuration

- Save
- Import: Importing a VPN configuration
- Export: Exporting a VPN configuration
- Move to a USB drive: USB mode
- [Configuration Wizard](#)
- Quit: Close all open VPN tunnels and quit the software

- Tools

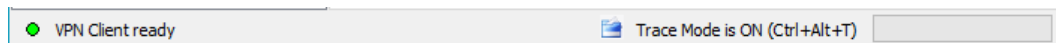
- [Connection Panel](#)
- [Configuring the Connection Panel](#)
- Console: IKE connection traces window
- Reset IKE: Restart the IKE service
- Options: Protection, display, startup, language management, PKI management options


- ?

- Online support: Access to online support
- [Updating](#) the software: Check for available updates
- Purchase license online: Access the online store
- [Activation Wizard](#)
- About...

10.2 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.

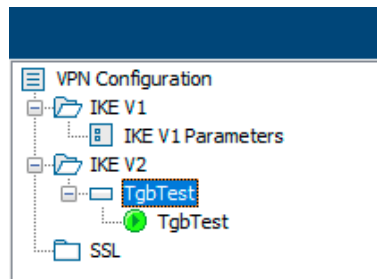
10.3 Shortcuts

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)

10.4 VPN tunnel tree

10.4.1 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 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.

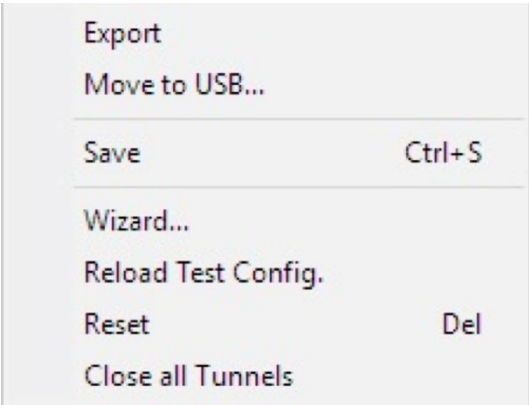


Two items in the tree cannot have the same name. The software displays a message to the user if the name entered is already in use.

10.4.2 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 Standard VPN Client comes with a default 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

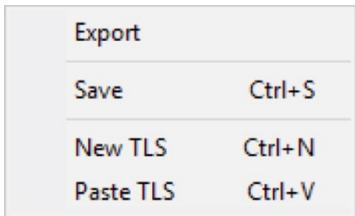
Right clicking the IKEv1, IKEv2 or SSL items will display the following contextual menu, which allows you to export, save, create, or paste a Phase 1/IKE Auth/SSL:



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	Ctrl+C	Copy	Ctrl+C
Rename	F2	Rename	F2
Delete	Del	Delete	Del
New Child SA	Ctrl+N	New Phase 2	Ctrl+N
Paste Child SA	Ctrl+V	Paste Phase 2	Ctrl+V

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).

3. Phase 2, Child SA, or TLS

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

Open tunnel	Ctrl+O	Close tunnel	Ctrl+W
Export		Export	
Copy	Ctrl+C	Copy	Ctrl+C
Rename	F2	Rename	F2
Delete	Del	Delete	Del

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.

10.4.3 Shortcuts

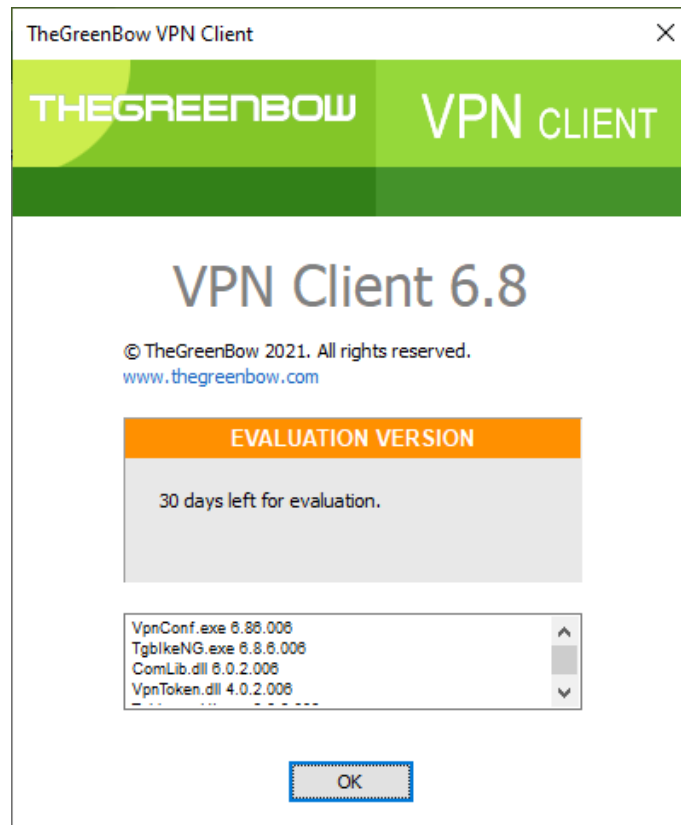
The following shortcuts are available for tree management:

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 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.

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.



The “About...” window displays the following information:

- The name and version number of the software.
- A web link to the TheGreenBow 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.

12 Importing and exporting the VPN configuration

12.1 Importing a VPN configuration

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

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



As of version 6.8 of the Windows Standard 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.

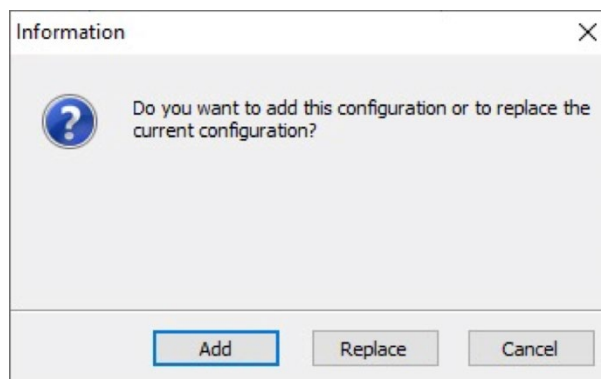


The Windows Standard VPN Client does not monitor VPN configuration file integrity. No signature is generated during an export and no check is performed for a possible signature during an import.

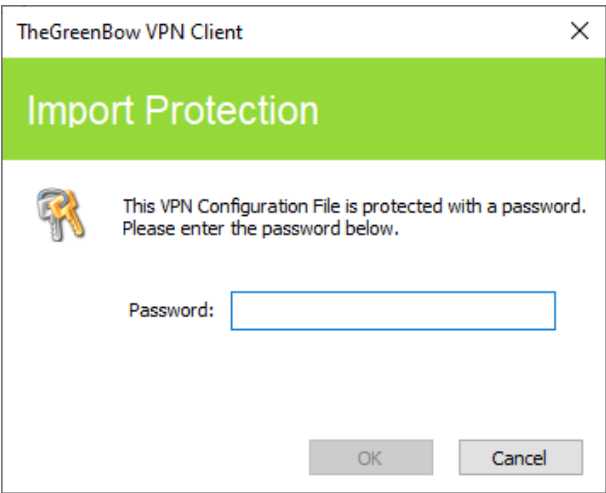


As of version 6.8 of the Windows Standard VPN Client, the function that allows you to double-click on a configuration file to import it is no longer available.

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 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 Configuration is empty	Current 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

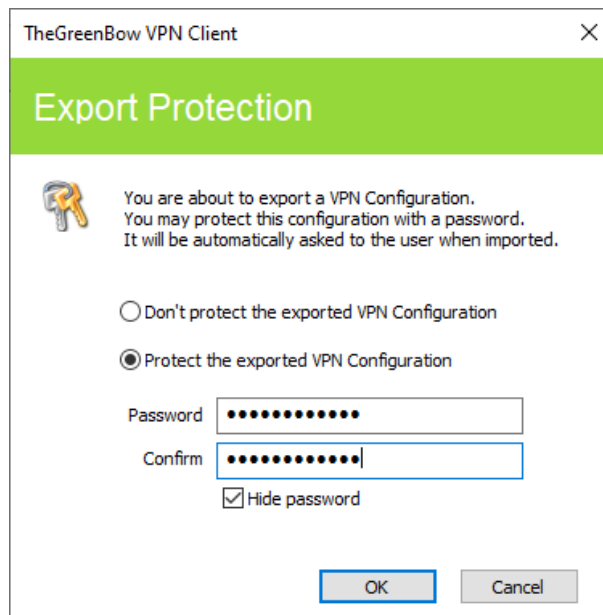
The Windows Standard VPN Client allows you to export a VPN configuration in various ways:

- 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).



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 or without password protection (encryption). If a password has been set, users will be required to enter it when importing.



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

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 below).

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 below).

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

The Windows Standard 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 10.4 VPN tunnel tree > 10.4.2 Contextual menus.



Security recommendation: We recommend configuring IKEv2 tunnels with a certificate. Refer to section 25 Security recommendations.

13.2 Editing and saving a VPN configuration

The Windows Standard VPN Client allows you to edit the VPN tunnels and to test your changes “on-the-fly” without needing to save the configuration.

All unsaved changes in the VPN configuration are clearly shown in the tree, as the name of modified items appears in bold.

The 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 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

Authentication

Protocol

Gateway

Certificate

Remote Gateway

Interface

Any

Remote Gateway

tgbtest.dyndns.org

Authentication

Preshared Key

.....

Confirm

.....

Certificate

X-Auth

Enabled

X-Auth Popup

Login

Password

Once

Hybrid Mode

Cryptography

Encryption

AES 128

Authentication

SHA-1

Key Group

DH2 (1024)

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".
<div><div>Interface</div><div><div>Any</div><div>192.168.205.52</div><div>Any</div></div></div>	
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 section 25 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 section 25 Security recommendations.

Refer to the dedicated section: 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.

X-Auth

☒ Enabled

☒ X-Auth Popup

Login

☐ Once

Password



☐ Hybrid Mode

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).

Gateway Authentication

Enter Authentication login and password to open the tunnel.

Login:

Password:

OK Cancel

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.


X-Auth

☒ Enabled ☐ X-Auth Popup

Login

Password

☐ Once ☐ Hybrid Mode



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.

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 section 18 Managing certificates) and the X-Auth function must be configured.


X-Auth

☒ Enabled ☒ X-Auth Popup

Login

Password

☐ Once ☒ Hybrid Mode





We recommend that you refer to section 25 Security recommendations to assess whether this option should be used.

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 section 25 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

The screenshot shows the 'Protocol' tab of the VPN Client configuration window. At the top, there are four tabs: 'Authentication', 'Protocol' (selected), 'Gateway', and 'Certificate'. Below the tabs, the 'Identity' section contains two rows: 'Local ID' with a dropdown menu set to 'DER ASN1 DN' and a text box containing 'C = FR, ST = IDF, L = Paris, O = TheGreenBow', and 'Remote ID' with an empty dropdown and text box. Below this is the 'Advanced features' section, which includes a 'Fragmentation' checkbox (unchecked), a 'Fragment size' text box, 'IKE Port' set to '500', 'NAT Port' set to '4500', an 'Enable NATT offset' checkbox (unchecked), and a 'Childless' checkbox (unchecked).




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 section 18 Managing certificates)

If this parameter is not set, the VPN Client's IP address is used by default.

Remote ID	<p>“Remote ID” is the identifier that the VPN Client expects to receive from the VPN gateway.</p> <p>According to the type selected, this identifier can be any of the following:</p> <ul style="list-style-type: none"> - 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) <p>If this parameter is not set, the VPN Client will accept any identifier sent by the gateway without checking it.</p> <div>  <div> <p>Security advisory: See section 25 Security recommendations for Remote ID management when the VPN Client is configured to check the gateway certificate.</p> </div> </div>
<h2>Advanced functions</h2>	
Fragmentation/ Fragment size	<p>This function enables IKE fragmentation, which prevents packets from becoming fragmented (and potentially blocked) by the IP network they're passing through. 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.</p>
IKE port	<p>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.</p> <div>  <p>The remote VPN gateway must also be able to perform the IKE Phase 1 exchanges on a port other than 500.</p> </div>
NAT port	<p>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.</p> <div>  <p>The remote VPN gateway must also be able to perform the IKE Phase 2 exchanges on a port other than 4500.</p> </div>
Enable NATT offset	<p>When the IKE port is different from 500, it may be necessary to check this option for the gateway to accept the connection.</p>
Mode Config	<p>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.</p>
Aggressive mode	<p>The VPN Client uses the Aggressive mode to connect to the VPN gateway.</p>

NAT-T	<p>“NAT-Traversal” mode.</p> <p>The VPN Client can handle three types of NAT-T modes:</p>	
	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)

Important: 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 0 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

Authentication Protocol **Gateway** Certificate

Dead Peer Detection (DPD)

Check interval sec.

Max. number of retries

Delay between retries sec.

Lifetime

Lifetime sec.

Gateway related parameters

Redundant Gateway

Retransmissions

Dead Peer Detection (DPD)

Dead Peer Detection	<p>The Dead Peer Detection (DPD) function enables the VPN Client to detect whether the VPN gateway has become unreachable or inactive. (1)</p> <ul style="list-style-type: none">- 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	<p>Lifetimes are negotiated when the tunnel is established. (1)</p> <p>When the lifetime is reached, the Phase 1 will be renegotiated.</p> <p>The default value for the lifetime of the Phase 1 is 2700 s (45 min).</p>
----------	---

(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	<p>Defines the address of a spare VPN gateway that the VPN Client will switch to when the initial gateway is unavailable or unreachable.</p> <p>The address of the redundant VPN gateway can be either an IP or a DNS address.</p> <p>👉 See section 14 Redundant gateway.</p>
Retransmissions	<p>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.</p>

13.3.4 Phase 1: Certificate

👉 Refer to section 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 configuration for it to be taken into account. The tunnel can be tested with the modified configuration immediately.

13.3.6 Phase 2: IPsec

IPsec

AdvancedAutomationRemote SharingMore Parameters

IPV4IPV6

Addresses

VPN Client address0 . 0 . 0 . 0

Address typeSubnet address

Remote LAN address192 . 168 . 1 . 0

Subnet mask255 . 255 . 255 . 0

ESP

EncryptionAES256

AuthenticationSHA-512

ModeTunnel

PFS

☒ PFS

GroupDH18 (8192)


Lifetime

IPsec Lifetime1800 sec.

Trace Mode is ON (Ctrl+Alt+T)

Addresses

VPN Client address	<p>“Virtual” IP address of the workstation, the way it will be “seen” on the remote network.</p> <p>From a technical standpoint, it is the source IP address of the IP packets going through the IPsec tunnel.</p> <p>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.</p> <div><div><div>i</div><div>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.</div></div></div>
--------------------	--

Address type	<p>The endpoint of the tunnel can be a network or a remote workstation.</p> <p> To find out how to configure the address type, refer to the paragraph entitled <u>Configuring the address type</u> below.</p>
--------------	---

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 section 25 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 section 25 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



See section 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:

Address type	Subnet address ▼
Remote LAN address	192 . 168 . 175 . 0
Subnet mask	255 . 255 . 255 . 0

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

Address type	Range address ▼
Start address	192 . 168 . 175 . 1
End address	192 . 168 . 175 . 10

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

Address type	Single address ▼
Remote host address	192 . 168 . 175 . 1



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: http://www.thegreenbow.com/vpn_gateway.html.

13.3.1 Phase 2: Advanced

Child SA Advanced Automation Remote Sharing IPv4 IPv6

Alternate servers

DNS Suffix: dev.corporate

Alternate servers

Type	IP Address
WINS	192.168.175.2

Tunnel traffic check

Period and IP Address of the remote host to ping:

IPv4 Address: 0 . 0 . 0 . 0

Check interval: 0 sec.

Miscellaneous

☐ Disable Split Tunneling

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



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.

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.

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.

13.3.2 Phase 2: Automation

📖 Refer to section 15 Automation.

13.3.3 Phase 2: Remote sharing

📖 Refer to section 19 Remote Desktop Sharing.

13.3.4 IKEv1 parameters

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

IKE V1 Parameters

Miscellaneous

Retransmissions2

IKE Port

X-Auth timeout60

NAT Port

☒ Disable Split Tunneling

☐ Cisco Mode Config

Other

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. <div><div><div>i</div><div>The IKE ports that can be configured in every tunnel have the priority over this parameter.</div></div></div>
NAT port	This field is used to configure the NAT port for all IKEv1 tunnels. <div><div><div>i</div><div>NAT ports that can be configured in every tunnel have the priority over this parameter.</div></div></div>
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 13.3.6 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

Authentication

Protocol

Gateway

Certificate

Remote Gateway

Interface

Any

Remote Gateway

tgbtest.dyndns.org

Authentication

Preshared Key

.....

Confirm

.....

Certificate

EAP

EAP popup

Login

Password

Multiple AUTH support

Cryptography

Encryption

Auto

Authentication

Auto

Key Group

Auto

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”.
	<div>Interface<div>Any</div><div>Any</div><div>Ethernet0</div></div>
	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

Preshared key	Password or key shared by the remote gateway.
	<div><div>i</div><div>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 section 25 Security recommendations.</div></div>

Windows Standard VPN Client

Property of TheGreenBow © 2021

58/115

Certificate	Use of certificates for VPN connection authentication. <div><div>Using Certificate strengthens the security in terms of VPN connection management (mutual authentication, verification of validity periods, revocation, etc.) Refer to section 25 Security recommendations.</div></div> <div> Refer to the dedicated section: 18 Managing certificates.</div>
EAP	<p>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.</p> <p>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.</p> <p>We recommend not to use the latter mode, see section 25 Security recommendations).</p>
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 section 25 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 section 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)

If this parameter is not set, the VPN Client will accept any identifier sent by the gateway without checking it.

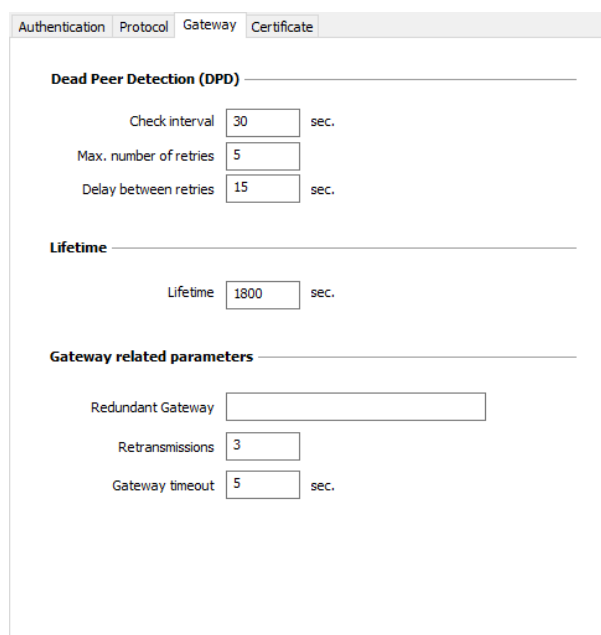


Security advisory: See section 25 Security recommendations for Remote ID management when the VPN Client is configured to check the gateway certificate.

Advanced functions

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	<p>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.</p> <div> The remote VPN gateway must also be able to perform the IKE Auth exchanges on a port other than 500.</div>
NAT port	<p>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.</p> <div> The remote VPN gateway must also be able to perform the IKE Child SA exchanges on a port other than 4500.</div>
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.

13.4.3 IKE Auth: Gateway



Authentication Protocol **Gateway** Certificate

Dead Peer Detection (DPD)

Check interval sec.

Max. number of retries

Delay between retries sec.

Lifetime

Lifetime sec.

Gateway related parameters

Redundant Gateway

Retransmissions

Gateway timeout sec.

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.  See section 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 section: 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 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

Child SA Advanced Automation Remote Sharing **IPV4** IPV6

Traffic selectors

VPN Client address 10 . 60 . 60 . 20

Address type Subnet address

Remote LAN address 192 . 168 . 175 . 0

Subnet mask 255 . 255 . 255 . 0

☒ Request configuration from the gateway

Cryptography

Encryption Auto

Integrity Auto

Diffie-Hellman Auto

Extended Sequence Number No

Lifetime

Child SA Lifetime 1800 sec.

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.
--------------------------	--


- (1) Refer to section 25 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	 See section 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:	Address type	Subnet address ▾
	Remote LAN address	192 . 168 . 175 . 0
	Subnet mask	255 . 255 . 255 . 0

As an alternative, you can also select “Range address” and enter the Start and End addresses:	Address type	Range address ▾
	Start address	192 . 168 . 175 . 1
	End address	192 . 168 . 175 . 10

If the endpoint of the tunnel is a workstation, choose the “Single address” type and then enter the Remote host address:	Address type	Single address ▾
	Remote host address	192 . 168 . 175 . 1



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: http://www.thegreenbow.com/vpn_gateway.html.

13.4.7 Child SA: Advanced

The screenshot shows the 'Child SA: Advanced' configuration window. It has four tabs: 'Child SA', 'Advanced', 'Automation', and 'Remote Sharing'. The 'Advanced' tab is active. The window is divided into three main sections: 'Alternate servers', 'Tunnel traffic check', and 'Miscellaneous'. In the 'Alternate servers' section, there is a 'DNS Suffix' text box and a table for 'Alternate servers' with columns 'Type' and 'IP Address'. Below the table are 'Add DNS' and 'Add WINS' buttons. The 'Tunnel traffic check' section has a label 'Period and IP Address of the remote host to ping:' followed by an 'IPv4 Address' field (showing 0.0.0.0) and a 'Check interval' field (showing 0 sec.). The 'Miscellaneous' section contains a checkbox labeled 'Disable Split Tunneling'.

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



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.

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.

Tunnel traffic check

Traffic check when tunnel is opened



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.

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.

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.

Other

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 13.3.6 Phase 2: IPsec), this option guarantees the complete leakproofness of the workstation provided the VPN tunnel is open.

We recommend using this mode.

13.4.8 Child SA: Automation

Refer to section 15 Automation.

13.4.9 Child SA: Remote sharing

Refer to section 19 Remote Desktop Sharing.

13.5 Configuring an SSL VPN tunnel

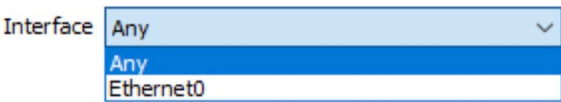
13.5.1 Introduction

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


13.5.2 Main

The screenshot shows the 'Authentication' tab of the Windows Standard VPN Client configuration window. The window has tabs for Authentication, Security, Gateway, Establishment, Automation, Certificate, and Remote Sharing. The Authentication tab is active. It contains sections for Remote Gateway, Authentication, and Extra Authentication. The Remote Gateway section has a dropdown for Interface (set to Any) and a text field for Remote Gateway (set to remotehost). The Authentication section has a Select Certificate button. The Extra Authentication section has checkboxes for Enabled and Popup when tunnel opens (both checked), and text fields for Login and Password.

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 section: 18 Managing certificates.
--------------------	--

Extra Authentication

Extra authentication	<p>This option increases the security level by asking the user to enter a login name and password whenever a tunnel is opened.</p> <p>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.</p>
----------------------	---

13.5.3 Security

Initial Authentication (TLS)

Security Suite	<p>This parameter is used to configure the security level of the authentication phase during the SSL exchange.</p> <ul style="list-style-type: none"> - 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. <p>For further information: https://www.openssl.org/docs/apps/ciphers.html</p>
----------------	---

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

Authentication Security Gateway Establishment Automation Certificate Remote Sharing

Dead Peer Detection (DPD)

Ping Gateway (s)0

Detect Gateway (s)0

On Dead Peer Detection

Close tunnel

Re-open tunnel

Gateway related parameters

☐ Explicit Exit

Check Gateway CertificateYes

Check Gateway OptionsApply

Validate the subject of the gateway certificate

Redundant Gateway

Miscellaneous

☐ Disable Split Tunneling

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	<p>This parameter configures the VPN Client to send a specific VPN tunnel closing frame to the gateway when closing the tunnel.</p> <p>If this option is not selected, the gateway will use DPD to close the tunnel at its end, which is less effective.</p>
Check Gateway Certificate	<p>Specifies the control level of the gateway’s certificate.</p> <p>In the current version, two levels are available:</p> <ul style="list-style-type: none">- Yes (the validity of the certificate is verified)- No (the validity of the certificate is not verified) <p>The “Lite” option is reserved for future use, and, in the current version, it is equivalent to “Yes”.</p>

Check Gateway Options	<p>Used to determine the coherence level between the VPN tunnel and gateway parameters (encryption algorithms, compression, etc.).</p> <ul style="list-style-type: none"> - 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	<p>Defines the address of a spare VPN gateway that the VPN Client will switch to when the initial gateway is unavailable or unreachable.</p> <p>The address of the redundant VPN gateway can be either an IP or a DNS address.</p> <p>👉 See section 14 Redundant gateway.</p>

Other

Disable Split Tunneling	<p>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.</p>
-------------------------	---

13.5.5 Establishment

The screenshot shows the 'Establishment' tab of the Windows Standard VPN Client configuration window. The window has a title bar with tabs: Authentication, Security, Gateway, Establishment (selected), Automation, Certificate, and Remote Sharing.

Key Renegotiation

- Bytes (KB): 0
- Packets: 0
- Lifetime (sec): 3600

Tunnel Options

- Physic.If MTU: 0
- Tunnel MTU: 0
- Tunnel IPV4: Auto (dropdown)
- Tunnel IPV6: Auto (dropdown)

Tunnel Establishment Options

- Port: 1194
- ☐ TCP
- Authentication timeout: 15
- Retransmissions: 2
- Traffic setup timeout: 10

Traffic

Traffic detection to open tunnel

IPV4: [] / []

IPV6: [] / []

Tunnel traffic check

IPV4: []

IPV6: []

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 section 15 Automation.

13.5.7 Certificate

👉 Refer to section 18 Managing certificates.

13.5.8 Remote sharing

👉 Refer to section 19 Remote Desktop Sharing.

14 Redundant gateway

The Windows Standard 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.

15 Automation

The Windows Standard 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).

AuthenticationSecurityGatewayEstablishmentAutomationCertificateRemote Sharing

Tunnel fallback

Tunnel to switch toNone

Message to display

Fallback retries0

Allow the user to refuse the fallback.

Automatic Open mode

Automatically open this tunnel when VPN Client starts after logon.

Automatically open this tunnel when USB stick is inserted.

Automatically open this tunnel on traffic detection.

Gina mode

Enable before Windows logon.

Automatically open this tunnel when Gina starts at logon

Scripts

Run this script :

Before tunnel opens

Browse...

When tunnel is opened

Browse...

Before tunnel closes

Browse...

After tunnel is closed

Browse...

Tunnel fallback

👉 Refer to section 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 section 21 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.

Windows Standard VPN Client

Property of TheGreenBow © 2021

76/115

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 (see section 22 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. "http://192.168.175.50"
- etc.

There are many possible applications, such as the following:

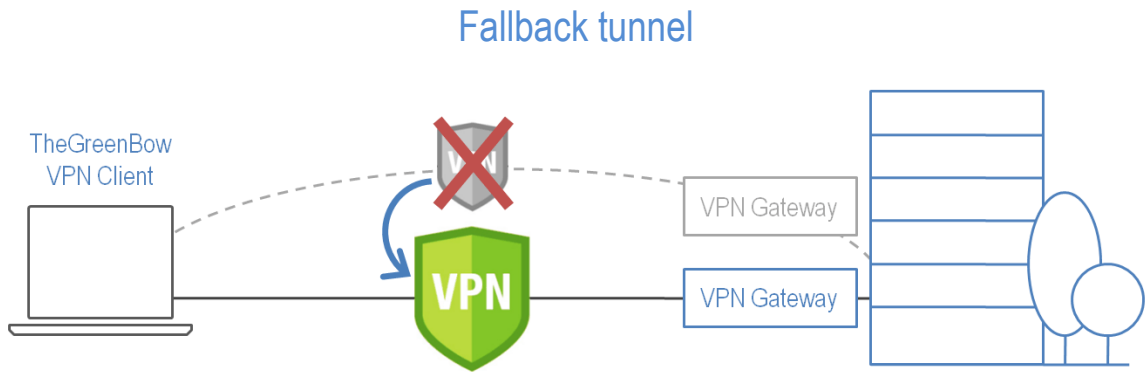
- Creating a semaphore file when the tunnel is open, so that a third-party application can detect the instant when the tunnel is open
- Opening one of the company's intranet servers automatically once the tunnel is open
- Cleaning or checking a configuration before opening the tunnel
- Checking the workstation (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 Standard 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 fallback

Tunnel to switch to (IKEv2) TgbTest-TgbTest

Message to display Attention : Tunnel fallback.

Fallback retries 1

☒ Allow the user to refuse the fallback.

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 Standard 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.

The image shows two side-by-side screenshots of the Windows Standard VPN Client configuration window, specifically the 'Child SA' tab. Both screenshots show the 'Traffic selectors' section. The left screenshot is for IPv4 configuration, and the right screenshot is for IPv6 configuration. The 'IPv4' button is highlighted in blue in the left screenshot, and the 'IPv6' button is highlighted in blue in the right screenshot.

IPv4 Configuration (Left Screenshot):

- Traffic selectors
- VPN Client address: 0 . 0 . 0 . 0
- Address type: Subnet address (dropdown)
- Remote LAN address: 0 . 0 . 0 . 0
- Subnet mask: 0 . 0 . 0 . 0

IPv6 Configuration (Right Screenshot):

- Traffic selectors
- VPN Client address: ::
- Address type: Subnet address (dropdown)
- Remote LAN address: ::
- Prefix length: 0



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 Standard 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 token, smart card, certificate store, etc.

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

- Use of any type of certificate storage medium: token, smart card, certificate store, file, VPN configuration, USB drive
- PKCS#11 and CNG access to tokens and smart cards
- Support for X.509 certificate formats: PKCS#12, PEM, PFX
- Management of certificates at the user end (VPN Client end) such as VPN gateway certificates, including validity date, certificate chain, root certificate 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)
- Use of private keys in PKCS#1 and PKCS#8 format

The list of smart card readers and tokens compatible with the Windows Standard VPN Client is available on our website at: http://www.thegreenbow.com/vpn_token.html.

The certificates to be used are configured and specified in three steps as follows:

- 1/ The “Certificate” tab of the relevant tunnel: Phase 1 (IKEv1), IKE Auth (IKEv2) or TLS (SSL).
- 2/ The “PKI Options” tab of the “Tools > Options” window in the Configuration Panel

18.1 Selecting a certificate (“Certificate” tab)

The Windows Standard 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 Windows Standard VPN Client allows you to choose a stored certificate:

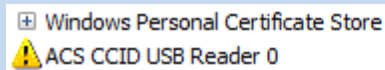
- In the VPN configuration file (see below “Importing a certificate”)
- In the Windows Certificate Store (see below “Windows Certificate Store”)
- On a smart card or token (see below “Configuring a smart card or token”)

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

- The token or smart card is compatible with CNG or PKCS#11
- The token or smart card 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).

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



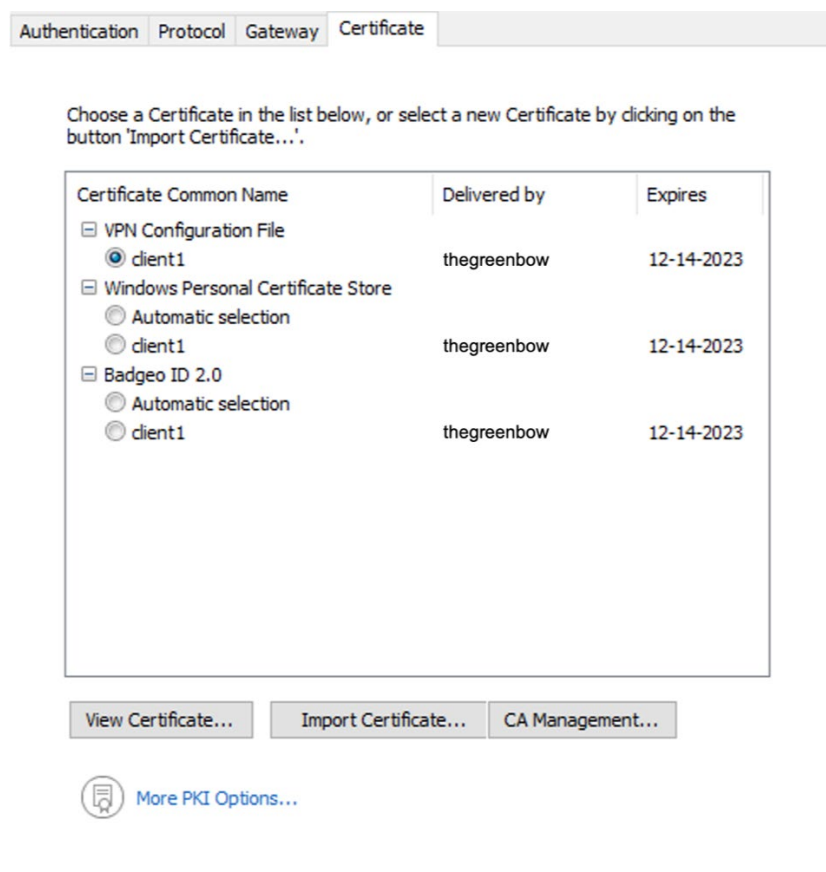
Clicking the desired medium displays the list of certificates it contains.



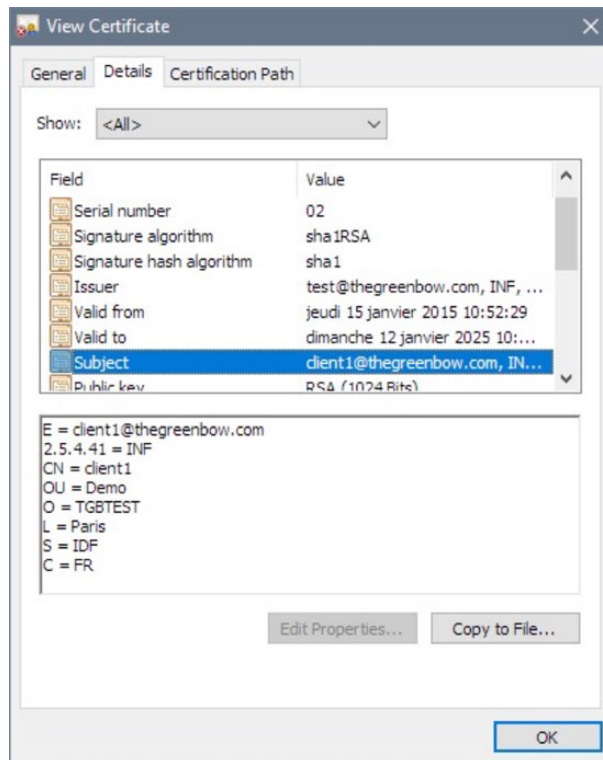
Only available certificates that have not expired are displayed.

Click the desired certificate to assign it to the VPN tunnel.

You can also click “Automatic selection”. In this case, the VPN Client will automatically select a certificate in the Windows Certificate Store or on the token/smart card reader when it needs it.



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".

Identity

Local ID	Subject from X509	C = FR, ST = IDF, L = Paris, O = TGI
Remote ID		

18.2 Importing a certificate

The Windows Standard 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 or a smart card, but it makes it easier to transport certificates.

Importing a PEM certificate



The file containing the private key may not be encrypted.

- 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.

TheGreenBow VPN Client

Import a new Certificate

Choose below the new certificate format:

☒ PEM Format

☐ P12 Format

Next > Cancel

TheGreenBow VPN Client

Import a new Certificate

Import a PEM Certificate in the VPN Configuration file.

Root Certificate Browse...

User Certificate Browse...

User Private Key Browse...

< Previous OK Cancel

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.

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.

TheGreenBow VPN Client

Import a new Certificate

Choose below the new certificate format:

☐ PEM Format

☒ P12 Format

Next > Cancel

TheGreenBow VPN Client

Import a new Certificate

Import a P12 Certificate in the VPN Configuration file.

P12 Certificate Browse...

< Previous OK Cancel

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.

18.3 Windows Certificate Store

For the Windows Standard VPN Client to identify a certificate available in the Windows Certificate Store, it 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)



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.

18.4 VPN gateway certificate

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

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 or to the Windows Certificate Store.

Checking each item in the chain implies that the following are checked:

- Gateway certificate expiration date
- Certificate validity start date
- Signatures of all certificates in the certificate chain (including root certificate, intermediate certificates, and server certificate)



The Windows Standard VPN Client does not check the Certification Revocation List (CRL).

18.5 Managing certification authorities

If the Windows Standard VPN Client is configured to check the client and gateway certificates, you may need to import the Certification Authorities (CAs) in addition to the certificates used.

This is 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 (typically, it is not found in the Windows Certificate Store).
- 2/ The gateway certificate’s CA is the same as the client’s, but the client’s CA is stored on a token or smart card. 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.

18.6 Using a VPN tunnel with a certificate stored 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 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 an incorrect PIN code is entered, the Windows Standard VPN Client will show a warning, informing users that they only have 3 consecutive attempts to unlock the smart card.

The Windows Standard VPN Client implements a mechanism to automatically detect smart card insertion.

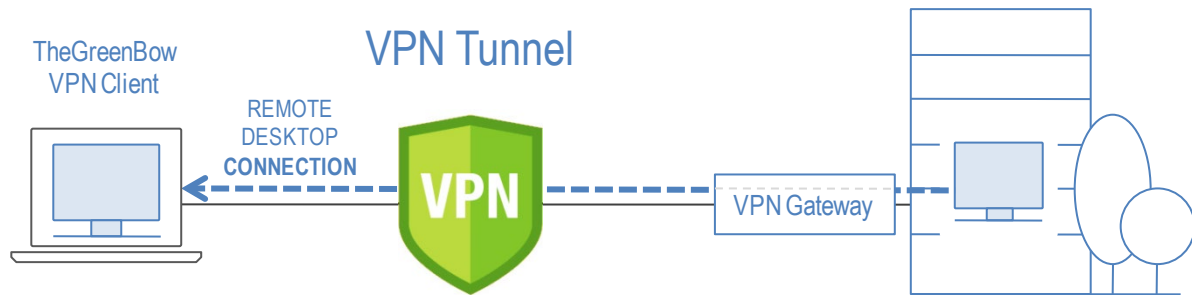
Tunnels that are associated with a certificate stored on a smart card will therefore be established automatically when the smart card is inserted. Likewise, removing the smart card will close all the corresponding tunnels.

To activate 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 Standard 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.

Child SA Advanced Automation Remote Sharing IPV4 IPV6

Enter below the IP address of the remote computer you want to connect to, and choose an alias.

Alias

Computer name or IP address

Alias	Name or IP address
-------	--------------------

Child SA Advanced Automation Remote Sharing IPV4 IPV6

Enter below the IP address of the remote computer you want to connect to, and choose an alias.

Alias

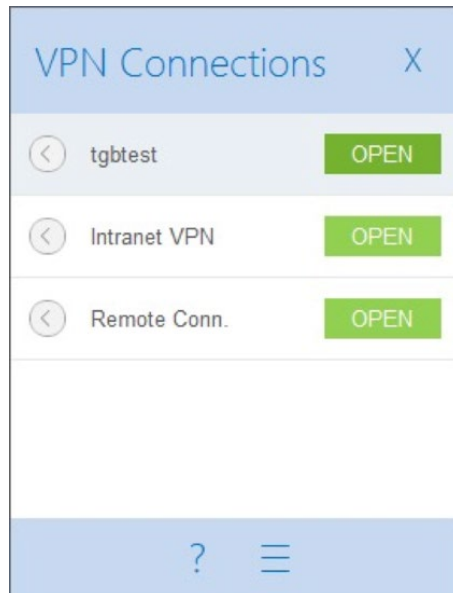
Computer name or IP address

Alias	Name or IP address
Corporate_desktop	192.168.175.50

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.

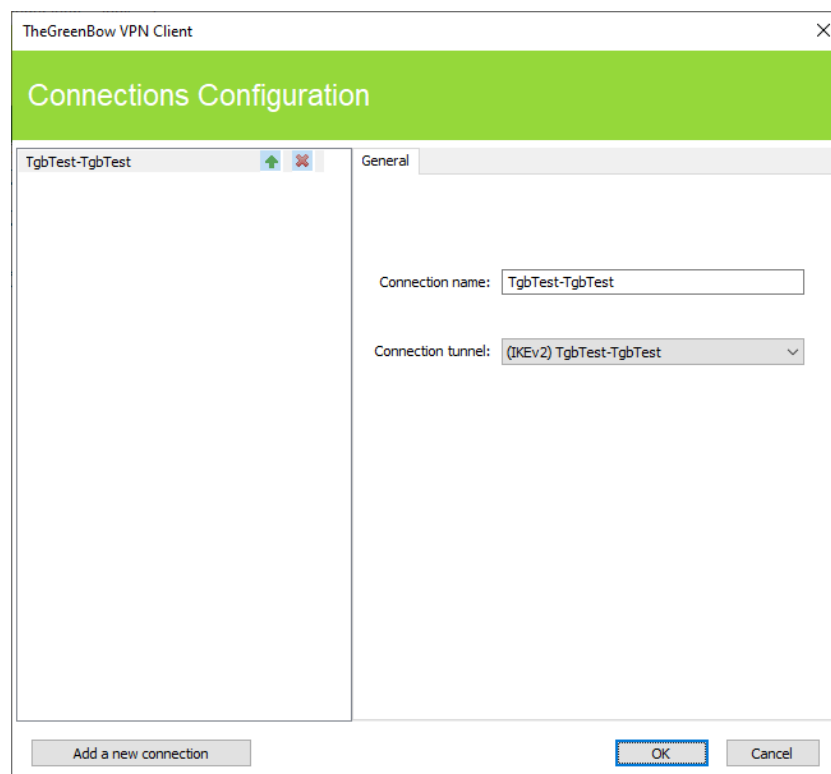
20 Configuring the Connection Panel

The Connection Panel of the Windows Standard 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

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

The right side contains the General tab, which shows the parameters of each connection: its name and the associated VPN tunnel.

To create a new VPN connection, click “Add a new connection”, choose a name and select the corresponding VPN tunnel. Once they have been confirmed, changes made in the Connection Panel configuration window instantly appear in the Connection Panel.



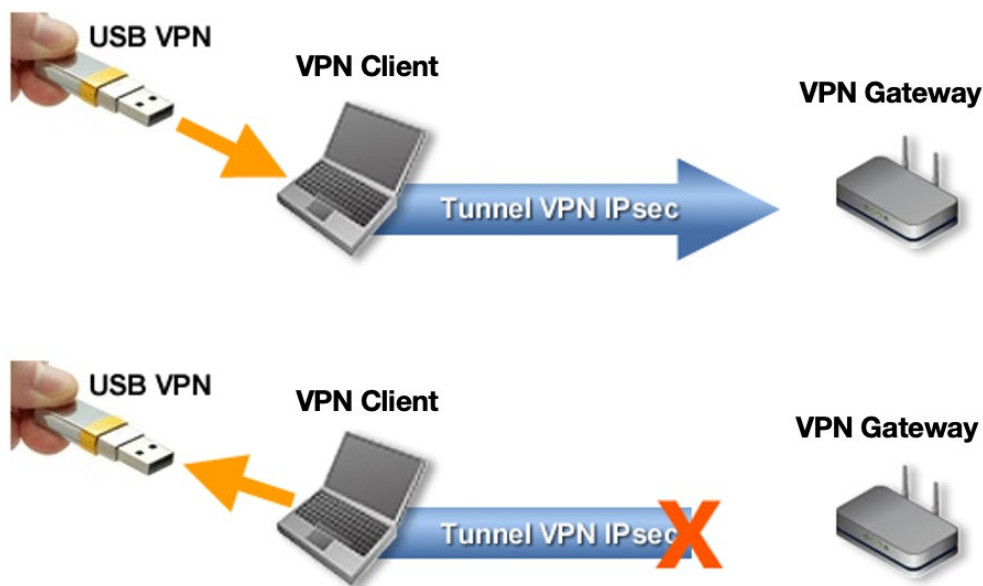
The Connection Panel configuration is stored in the VPN configuration file. It can therefore be exported into .tgb files, which are useful for deploying an identical Connection Panel across all workstations.

21 USB mode

21.1 Overview

The Windows Standard 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.



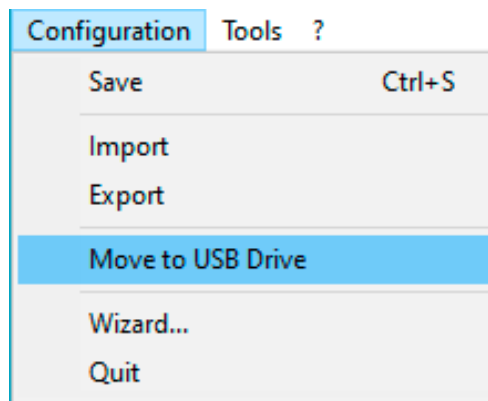
The following apply to the USB mode:

- No security elements are stored on the workstation from which the VPN connection is opened, as there is no VPN configuration on the workstation.
- The security elements are transported securely on the removable storage device (USB drive).
- The removable storage device can be a standard USB drive.
- The security elements are stored on the USB drive and protected with a password.
- The VPN connection automatically opens when the USB drive is inserted.
- The VPN connection automatically closes when the USB drive is removed.

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

21.2 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.

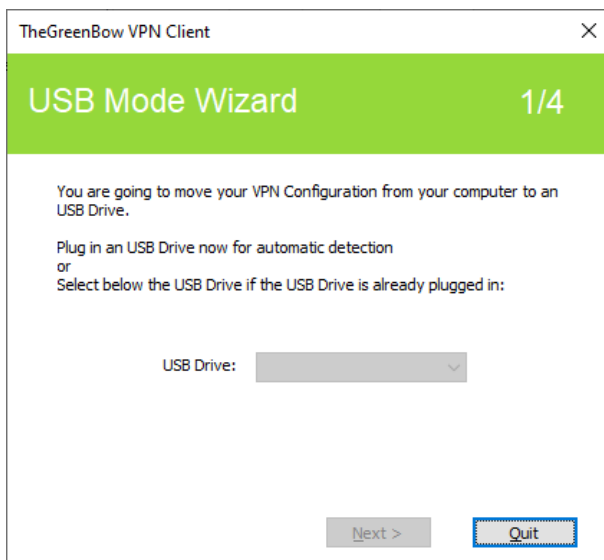


Step 1: Choosing a USB drive

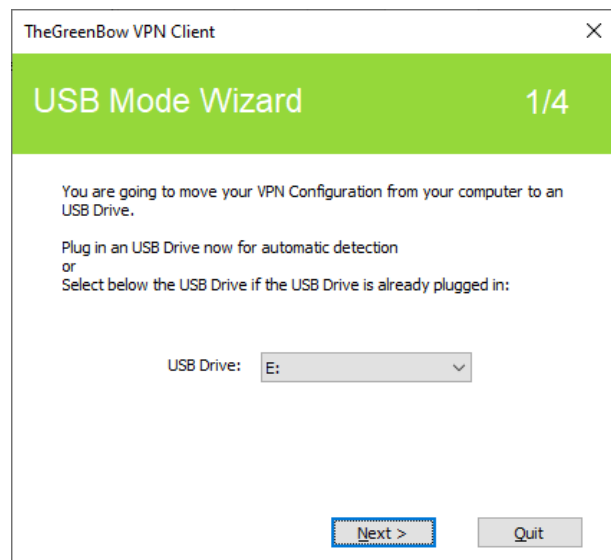
Screen 1 allows you to choose the removable storage device (USB drive) to use to protect the VPN configuration. If a drive is already inserted, it is automatically displayed in the list of available USB drives.

Otherwise, simply insert the selected USB drive at this stage. It will be detected automatically as soon as it is inserted.

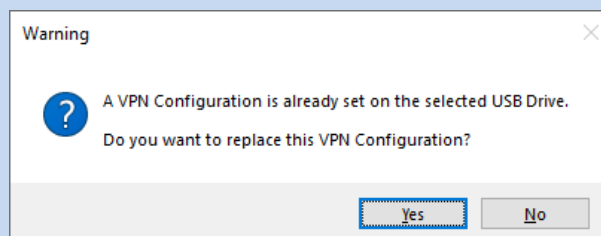
No USB drive inserted



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:

In USB mode, the 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 Windows Standard VPN Client.

2/ Password protection:

In USB mode, the VPN configuration can be password-protected.

In this case, the password will be required every time the VPN USB drive is inserted.

The screenshot shows the 'USB Mode Wizard' window, step 2/4. The title bar reads 'TheGreenBow VPN Client'. The window has a green header with 'USB Mode Wizard' and '2/4'. The main content area contains the following text: 'Your VPN Configuration is going to be moved on the USB Drive: E:'. Below this is the question 'Do you allow this USB Drive to be used:' with two radio button options: 'With this computer only' (unselected) and 'On any computer' (selected). Further down is the text 'Protect the VPN Configuration on the USB Drive with a password:' followed by a 'Password:' label and a text input field. Below the input field is a checkbox labeled 'Hide password' which is currently unchecked. At the bottom of the window are three buttons: '< Previous' (disabled), 'Next >' (active/highlighted), and 'Quit' (disabled).

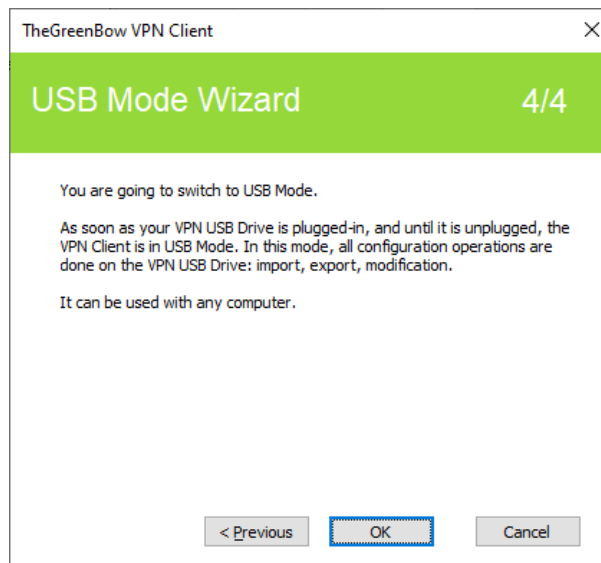
Step 3: Automatically opening the tunnel

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

The screenshot shows the 'USB Mode Wizard' window, step 3/4. The title bar reads 'TheGreenBow VPN Client'. The window has a green header with 'USB Mode Wizard' and '3/4'. The main content area contains the text: 'Select the tunnel below if you want it to be automatically opened when the VPN USB Drive is plugged-in:'. Below this is the text 'Automatically open when VPN USB Drive is plugged-in:' followed by a list box containing one item: 'TgbTest - TgbTest' with an unchecked checkbox to its left. At the bottom of the list box is a note: 'Note: The tunnel will also automatically close when the VPN USB Drive is unplugged.' At the bottom of the window are three buttons: '< Previous' (disabled), 'Next >' (active/highlighted), and 'Quit' (disabled).

Step 4: Summary

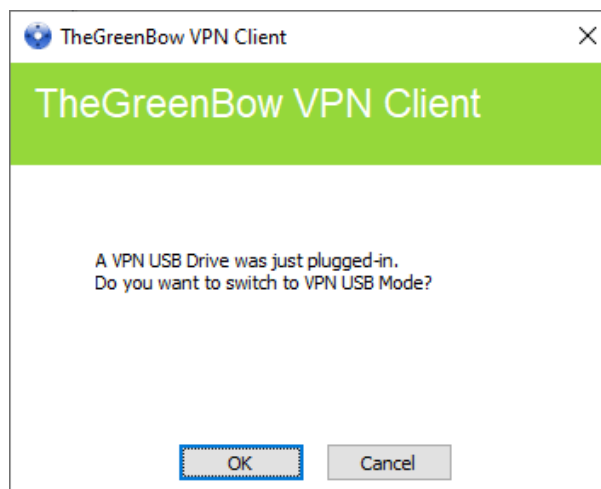
The summary gives you the opportunity to check whether the VPN USB drive has been properly configured.



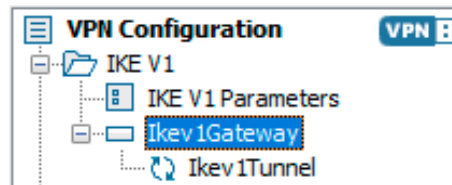
Once this final step is confirmed, the workstation's VPN configuration is transferred onto the USB drive. It remains enabled for as long as the USB drive is inserted. When the VPN USB drive is removed, the Windows Standard VPN Client will revert to an empty VPN configuration.

21.3 Using the USB mode

After starting the Windows Standard 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 mode VPN configuration is automatically loaded 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 USB mode VPN connections 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 Standard 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.

22 GINA mode

22.1 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.

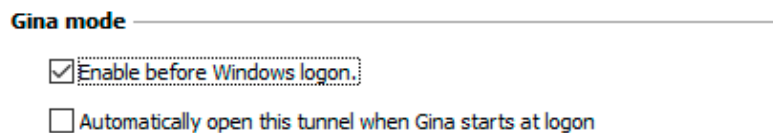
When a tunnel is configured in GINA mode, a window allowing you to open a tunnel that is similar to the Connection Panel will be displayed on the Windows logon screen. It allows you to open a VPN tunnel manually or automatically.



22.2 Configuring the GINA mode

Configuring the GINA mode for a VPN connection is done on the “Automation” tab of the relevant tunnel.

➞ Refer to section 15 Automation.



22.3 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 VPN tunnel configured in GINA mode can effectively implement an X-Auth or EAP authentication (users must enter their login name and password) or a certificate-based authentication on a token or smart card (users must enter the PIN code to access the token or smart card).



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 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 an authentication method, a strong one where possible, for tunnels configured in GINA mode, e.g. an X-Auth or EAP authentication or preferably a certificate-based authentication, on a removable device if possible.

👉 See section 13.3.1 Phase 1: Authentication.

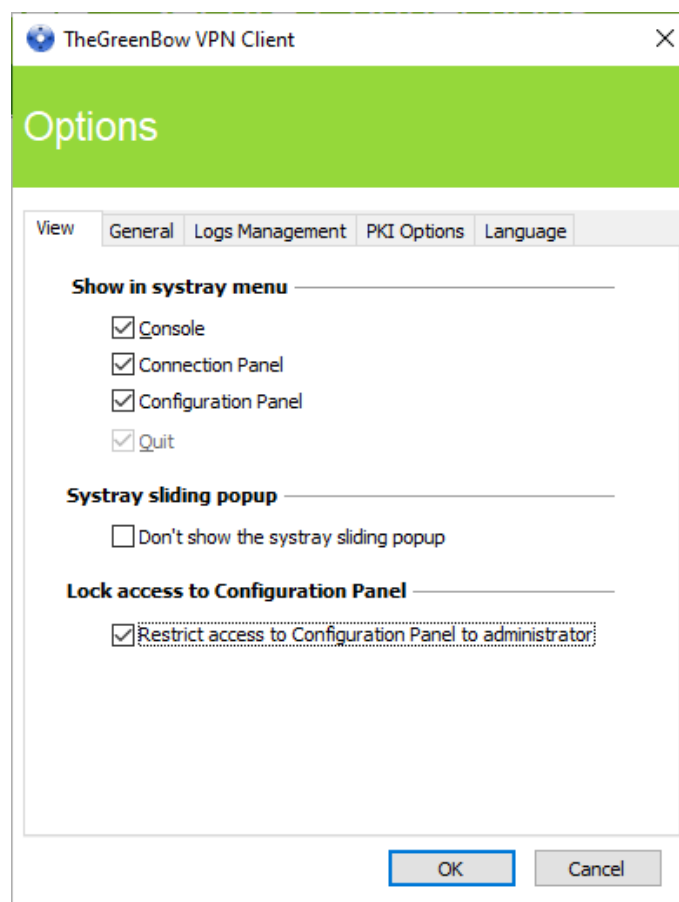
23 Options

23.1 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”.

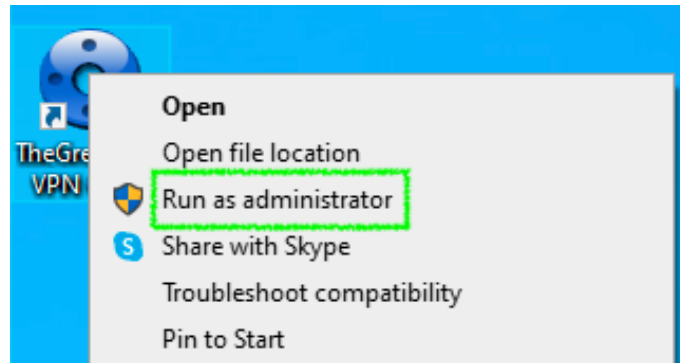
The taskbar menu’s “Quit” item cannot be removed using the software. However, it can be removed using the installation options (see Deployment Guide).

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).

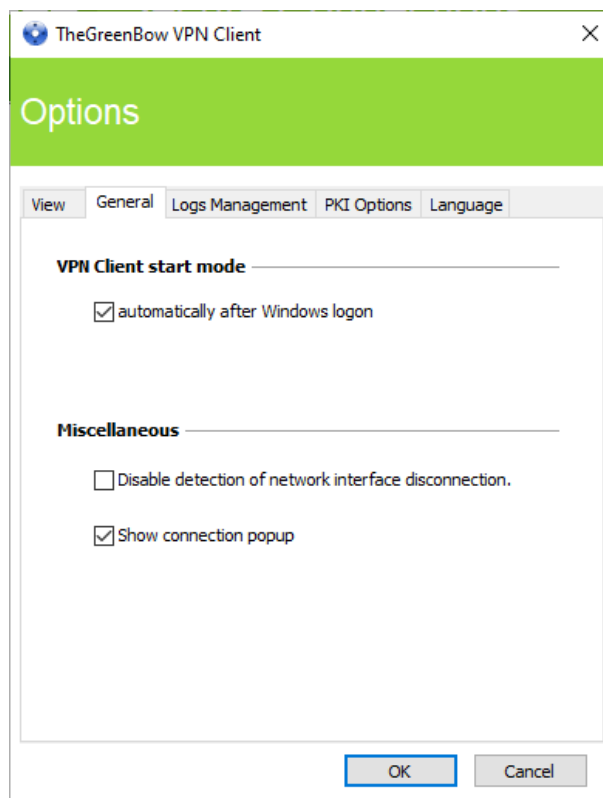


In the Windows Standard VPN Client, the interface of the Configuration Panel is accessible to all users, by default. To restrict access to the Configuration Panel to administrators, check the “Restrict access to Configuration Panel to administrator” option.

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



23.2 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 8.3 Desktop.

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).

By checking the “Disable detection of network interface disconnection” box, the VPN Client won’t close tunnels as soon as a disconnection is observed. This guarantees a very stable VPN tunnel, even on unreliable physical networks, typically wireless networks such as Wi-Fi, 4G, 5G or satellite.

Show connection popup

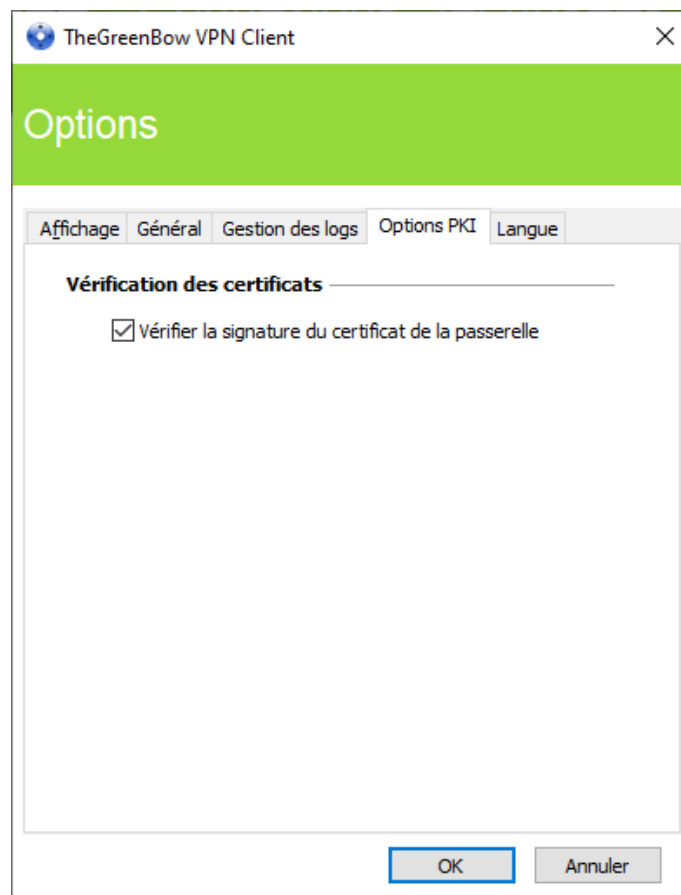
A connection window will be displayed automatically every time a VPN connection is established. This feature can be disabled by unchecking the “Show connection popup” box.

23.3 Managing logs

👉 Refer to section 24.1 Administrator logs.

23.4 PKI options

The “PKI Options” tab provides access to the “Check gateway certificate signature” option.



Checking certificates

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.



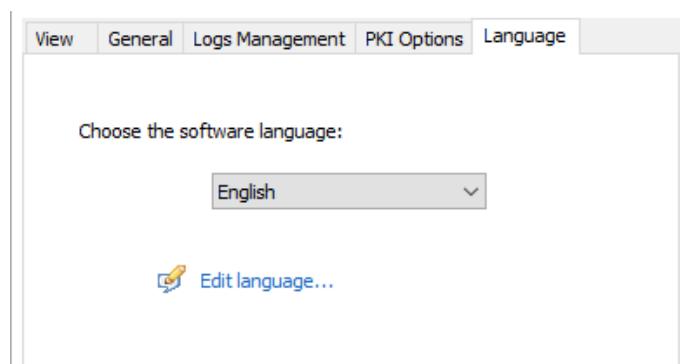
Security advisory: When this option is selected, we recommend entering the subject of the gateway certificate in the Remote ID of the tunnel concerned, to prevent vulnerability [2018_7293](#).

23.5 Managing languages

23.5.1 Choosing a language

The Windows Standard 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:

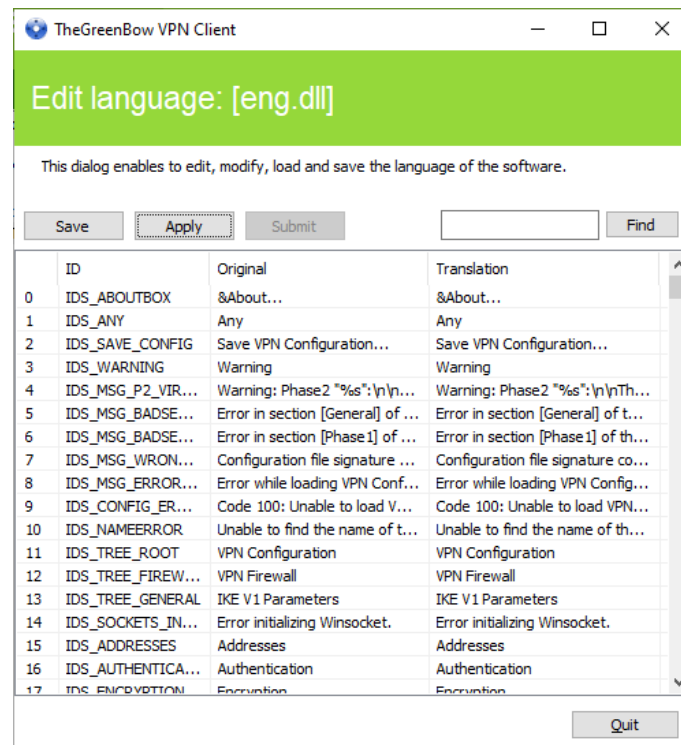


The list of languages available in the standard version of the software is provided in an appendix in section 27.3 Technical data of the Windows Standard VPN Client.

23.5.2 Editing or creating a language

The Windows Standard VPN Client lets you create new translations or edit the language used, then test these changes dynamically using the integrated translation tool.

In the “Language” tab, click the “Edit language...” link to display the translation window:



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 the TheGreenBow 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.

24 Administrator logs, console, and traces

The Windows Standard VPN Client provides three types of logs:

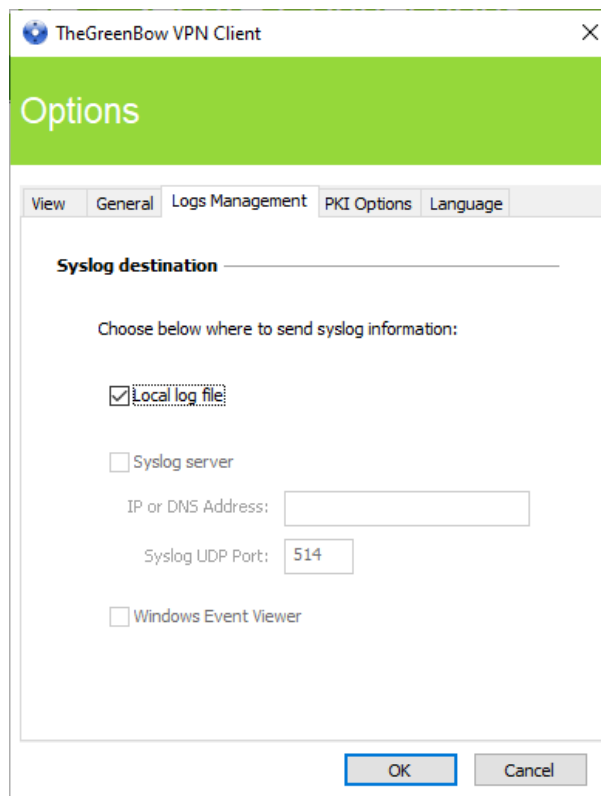
- 1/ “Administrator” logs are specifically designed for software activity and usage reports.
- 2/ The “Console” provides detailed information on the tunnels as well as the related opening and closing steps. It essentially consists of the IKE messages and provides high-level information about the establishment 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.

24.1 Administrator logs

The Windows Standard VPN Client can collect “administrator” logs: tunnel opening, expired certificate, connection duration, wrong login name/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.

Collected logs can be stored in a local file.

Administrator logs are configured in the “Tools > Options...” window on the “Logs Management” tab.



Administrator logs are listed in the appendix [27.2 Administrator logs](#).

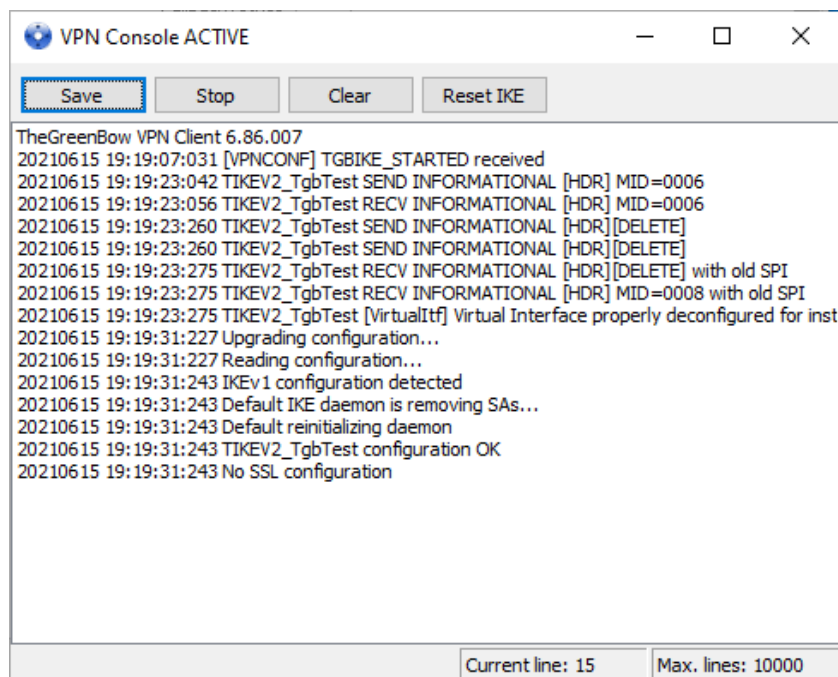


When administrator logs are stored in a local file, the path to these logs is the “System” sub-directory in the logging directory: “C:\ProgramData\TheGreenBow\TheGreenBow VPN\LogFiles\System”. Read access to this directory is available in all modes, but write access is only available in Administrator mode.

24.2 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

24.3 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 Standard 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, when administrators enable them, said administrators ensure that they are disabled and, if possible, deleted when they quit 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.

25 Security recommendations

The following recommendations are intended for software administrators.

25.1 General recommendations

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

- The system administrator and the security administrator, tasked respectively with installing the software and defining the VPN configurations, are considered trustworthy.
- Users of the software have been properly trained on how to use it. They must not reveal the information used to authenticate them within the encryption system.
- The VPN gateway that the VPN Client connects to can trace the VPN activity and, if necessary, lead back to the causes of malfunctions or security policy violations.
- The user workstation is safe and properly administered. It is equipped with an up-to-date antivirus software and is protected by a firewall.
- Bi-keys and certificates used to open the VPN tunnel are generated by a trustworthy certification authority.

25.2 Operating precautions

The machine on which the Windows Standard VPN Client is installed and run must be safe 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)

[Security updates](#) (Mises à jour de sécurité, document only available in French)

[- Password](#) (Mot de passe, document only available in French)

25.3 VPN Client administration

We strongly recommend that you protect access to the VPN security policy with a password and restrict the software's visibility to end users as detailed in section 23.1 Displaying/hiding the interface.

We recommend that you monitor the users of the Windows Standard VPN Client in a "user" environment and restrict use of the operating system with administrator privileges as far as possible.

We recommend keeping the "General > VPN Client start mode > automatically after Windows Logon" option enabled, which is the default behavior upon installation.

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

25.4 VPN configuration

25.4.1 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 store the EAP login name/password in the configuration (function described in section 13.4.1 IKE Auth: IKE SA, paragraph entitled Authentication).
- 2/ Do not import any certificates to the configuration (function described in section 18.2 Importing a certificate) and preferably use certificates stored on removable devices (tokens) or in the Windows Certificate Store.
- 3/ 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.
- 4/ Do not export the VPN configuration without encrypting it, i.e. not password-protected (function described in section 12.2 Exporting a VPN configuration).

25.4.2 Authenticating users

The user authentication functions available in the 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
Static X-Auth	
Dynamic X-Auth	
Certificate stored in the VPN configuration	
Certificate in the Windows Certificate Store	
Certificate on a smart card or token	Strong

25.4.3 Authenticating the VPN gateway

We recommend that you implement a check on the VPN gateway certificate as described in section 23.4 PKI options.



In this configuration, to prevent vulnerability [2018 7293](#) from being exploited, you must enter the subject of the VPN gateway certificate in the Remote ID of the relevant VPN tunnel.

25.4.4 IKE protocol

We recommend that you only configure IKEv2 tunnels.

25.4.5 “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 sections 13.4.6 Child SA: Child SA and 13.4.7 Child SA: Advanced.

25.4.6 GINA mode

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

25.4.7 Cypher algorithms and key lengths

As of version 6.64 of the Windows Standard VPN Client, all available cypher algorithms and key lengths comply with Appendix B-1 of RGS 2.0.

25.4.8 ANSSI IPsec configuration recommendations

The recommendations described above can be complemented by French National Cybersecurity Agency's (ANSSI) IPsec configuration document: [Security recommendations regarding IPsec for network flows protection](#).

26 Contact

26.1 Information

All the information on TheGreenBow products is available on the following websites:

English: www.thegreenbow.com

French: www.thegreenbow.fr

26.2 Sales

Phone contact: +33.1.43.12.39.30

Mail contact: sales@thegreenbow.com

26.3 Support

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

Support

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

French: <http://www.thegreenbow.fr/support.html>

Online help

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

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

FAQ

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

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

Contact

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

support@thegreenbow.com

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_VPNCONFLOADERERROR	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_TUNNELTRAFFIC_OK	3006	Info	Tunnel??? Ok
LOGID_TUNNELAUTH_NOK	3007	Error	Tunnel authentication failed (reason %d).
LOGID_TUNNELTRAFFIC_NOK	3008	Error	Tunnel??? 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 Technical data of the Windows Standard VPN Client

General

Windows version	Windows 10 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
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

Connection/Tunnel

Connection mode	Peer-to-Gateway (see the list of certified gateways and corresponding configuration guides)
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: <ul style="list-style-type: none">- Static or dynamic X-Auth (prompt every time a tunnel is opened)- Hybrid Authentication- Preshared key- EAP (MSCHAP-V2)- Multiple Auth
PKI	<ul style="list-style-type: none">- Support for certificates in X.509 format: PKCS#12, PEM- Multiple media: Windows Certificate Store, smart card, token, configuration file- Access tokens/smart cards 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)

Administrative

Security installation and updates	Installation and updates using Microsoft Installer (MSI)
VPN configuration management	Import and export options for VPN configurations Securing import/export using passwords, encryption
Logs and traces	IKE/IPsec and SSL log console and trace mode can be enabled Administrator logs: local file
Live update	Check for available updates from within the software
License and activation	Software license activation performed online

27.4 License and credits

Credits and references to third-party licenses:

```

/*
 * Copyright (c) 1998, 1999 Niels Provos. All rights reserved.
 * Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>. All rights reserved.
 * Copyright (c) 1998, 1999, 2000, 2001 Niklas Hallqvist. All rights reserved.
 * Copyright (c) 1999, 2000, 2001, 2002, 2004 Håkan Olsson. All rights reserved.
 * Copyright (c) 1999, 2000, 2001 Angelos D. Keromytis. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 */

/* =====
 * Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 * software must display the following acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 * endorse or promote products derived from this software without
 * prior written permission. For written permission, please contact
 * openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 * nor may "OpenSSL" appear in their names without prior written
 * permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 * acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

```

```
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
-----

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are adhered to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * "This product includes cryptographic software written by
 * Eric Young (eay@cryptsoft.com)"
 * The word 'cryptographic' can be left out if the routines from the library
 * being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 * the apps directory (application code) you must include an acknowledgement:
 * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The license and distribution terms for any publicly available version or
 * derivative of this code cannot be changed. i.e. this code cannot simply be
 * copied and put under another distribution license
 * [including the GNU Public License.]
*/
```

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software