

Windows Enterprise VPN Client 7.5

Administrator's Guide

TheGreenBow is a registered trademark.

Microsoft, Windows 10, and Windows 11 are either registered trademarks or brand names owned by Microsoft Corp. in the U.S.A. and/or in other countries.

Any other third-party trademarks mentioned in this document are the property of their respective owners.

All reproduction rights are reserved, including for iconographic or photographic representations. No part of this document may be copied and/or published by any means whatsoever without our express written consent.

All the information provided is subject to modifications at any time and without notice.

Despite our utmost care and attention in producing this document and its regular updates, errors may have been introduced in the information provided. If you notice any issues, please feel free to contact us and let us know. We will make the necessary changes.

Table of contents

1	Overview	1
1.1	Introduction	1
1.2	What's new in release 7.5	1
1.2.1	Endpoint compliance monitoring (requires SCA).....	1
1.2.2	Audit trace forwarding to the CMC (requires SCA).....	1
1.2.3	New features in the TrustedConnect Panel	1
1.2.4	Support for IPsec Restricted mode in line with latest changes to the framework.....	1
1.2.5	OpenSSL 3.0 has been adopted.....	2
1.2.6	Certificate authentication and revocation.....	2
1.2.7	New dynamic parameters have been added	2
1.2.8	Improved selection of certificate to use	2
1.3	Other new features introduced in v7	3
1.3.1	Implements Zero Trust Network Access	3
1.3.2	Filtering Mode	3
1.3.3	Cryptography	3
1.3.4	IKEv1 and vulnerable algorithms have been deprecated.....	3
1.3.5	SSL/OpenVPN	3
1.3.6	Certificate authentication and revocation.....	4
1.3.7	New features in the TrustedConnect Panel	4
1.3.8	New dynamic parameters have been added	5
1.3.9	Enhanced security	5
1.3.10	Improved smart card/token identification	5
2	Installing the software.....	6
2.1	Introduction	6
2.1.1	Minimum requirements.....	6
2.1.2	Digital signature and version	6
2.1.3	Vulnerabilities.....	7
2.2	Installation procedure	7
2.3	Canceling installation	14
2.4	Trial period	14
2.5	Configuring Windows.....	16
3	Activating the software.....	19



3.1	Step 1	19
3.2	Step 2	20
3.3	Activation errors	20
3.4	Manual activation	21
3.5	License and activated software.....	24
4	Updating the software.....	25
4.1	How to get an update	26
4.2	Update procedure.....	26
4.3	Updating the VPN configuration	27
4.4	Automation	28
5	Uninstalling the software.....	29
6	Getting started with the software.....	30
6.1	Introduction	30
6.2	Starting the software	30
6.3	Opening a test VPN tunnel from the Connection Panel.....	33
6.4	Configuring a VPN tunnel	35
6.5	Automating the opening of a VPN tunnel	36
6.6	Opening a VPN tunnel from the TrustedConnect Panel	37
7	Configuration Wizard	39
7.1	Step 1	40
7.2	Step 2	40
7.2.1	Configuring an IPsec/IKEv2 tunnel.....	40
7.2.2	For an SSL tunnel (OpenVPN)	41
7.3	Step 3	42
8	Connection Panel	43
9	Configuration Panel	45
9.1	Menus.....	46
9.2	Status bar.....	46
9.3	Shortcuts.....	47
9.4	VPN configuration tree.....	47

9.4.1	Usage	47
9.4.2	Contextual menus.....	48
9.4.3	Shortcuts.....	51
10	TrustedConnect Panel.....	52
10.1	Introduction	52
10.2	Interface.....	52
10.3	Taskbar icon and color codes	53
10.4	Contextual menu.....	54
10.5	Usage.....	55
10.5.1	Workstation connected to corporate network.....	55
10.5.2	Workstation not connected to corporate network	56
10.6	Error cases.....	57
10.7	Generating logs and Console.....	58
10.8	Selecting the language	59
10.9	Choosing the connection	59
10.10	Current limitations.....	60
11	“About...” window	62
12	Importing and exporting the VPN configuration	63
12.1	Importing a VPN configuration	63
12.2	Exporting a VPN configuration	65
12.3	Merging VPN configurations.....	66
12.4	Splitting a VPN configuration.....	66
13	Configuring a VPN tunnel.....	67
13.1	SSL or IPsec IKEv2 VPN	67
13.2	Editing and saving a VPN configuration.....	67
13.3	Configuring an IPsec IKEv2 tunnel.....	68
13.3.1	IKE Auth: Authentication	68
13.3.2	IKE Auth: Protocol.....	71
13.3.3	IKE Auth: Gateway.....	74
13.3.4	IKE Auth: Certificate.....	75
13.3.5	Child SA: Overview	76
13.3.6	Child SA: Child SA.....	76

13.3.7	Child SA: Advanced.....	80
13.3.8	Child SA: Automation.....	81
13.3.9	Child SA: Remote sharing.....	81
13.4	Configuring an SSL/OpenVPN tunnel	82
13.4.1	Introduction	82
13.4.2	SSL: Authentication	82
13.4.3	SSL: Security	83
13.4.4	SSL: Gateway.....	85
13.4.5	SSL: Establishment.....	88
13.4.6	SSL: Automation.....	90
13.4.7	SSL: Certificate.....	90
13.4.8	SSL: Remote sharing.....	90
14	Redundant gateway	91
15	Automation.....	92
15.1	Tunnel fallback	92
15.2	Automatic Open mode	93
15.3	GINA mode.....	93
15.4	Scripts.....	93
16	Fallback tunnel.....	95
17	IPv4 and IPv6	96
18	Managing certificates	97
18.1	Introduction	97
18.2	User certificate	98
18.2.1	Overview.....	98
18.2.2	Dynamic parameters.....	98
18.2.3	Automatic selection	99
18.3	Selecting a certificate (Certificate tab)	101
18.4	Importing a certificate to the VPN configuration.....	104
18.4.1	Importing a PEM/PFX certificate.....	104
18.4.2	Importing a PKCS #12 certificate.....	105
18.5	Using a certificate stored on a smart card or token.....	106
18.6	Using a certificate stored in the Windows Certificate Store	107
18.6.1	Required characteristics.....	107

18.6.2	Importing a certificate depending on the store used	108
18.7	PKI options: specifying the certificate and its storage device	108
18.8	VPN gateway certificate.....	108
18.8.1	Preventing or limiting CRL download.....	109
18.8.2	Constraints on the Key Usage extension.....	110
18.8.3	Constraints on the Extended Key Usage extension	111
18.9	Managing certificate authorities	112
18.9.1	Overview.....	112
18.9.2	Importing a certificate authority.....	113
18.9.3	IPsec DR mode.....	113
19	Remote Desktop Sharing.....	115
20	Configuring the Connection Panel	117
21	Configuring the TrustedConnect Panel	120
21.1	Always-On.....	120
21.1.1	Operating principle	120
21.1.2	Configuring Always-On.....	121
21.2	Trusted Network Detection (TND)	122
21.2.1	Operating principle	122
21.2.2	Configuring TND.....	124
21.2.3	Disabling TND	130
21.3	Scripts.....	131
21.4	Minimizing the panel.....	131
21.5	Disabling the disconnect button.....	132
21.6	Removing menu items.....	132
21.7	Automatically restarting the TrustedConnect Panel	132
21.8	Purging logs.....	133
21.9	Behavior when smart card or token is removed.....	133
22	GINA mode.....	134
22.1	Overview	134
22.2	Configuring the GINA mode.....	135
22.3	Using the GINA mode.....	136
23	Filtering Mode.....	137

24	Secure Connection Agent	138
24.1	Overview	138
24.2	Endpoint compliance monitoring	138
24.2.1	Introduction	138
24.2.2	Configuring the VPN Client	139
24.2.3	Selecting the tunnel to open according to the compliance level	140
24.3	Forwarding audit traces from the VPN Client to the CMC	143
24.3.1	Introduction	143
24.3.2	Configuring the VPN Client	143
25	Options	145
25.1	View	145
25.1.1	Showing options in systray menu	145
25.1.2	Showing the systray fade-out pop-up	146
25.1.3	Restricting access to the Configuration Panel	146
25.2	General	147
25.2.1	VPN Client startup mode	147
25.2.2	Disabling detection of network interface disconnection	147
25.2.3	Show connection popup	148
25.2.4	Displaying more parameters	148
25.3	Managing logs	150
25.4	PKI Options	150
25.4.1	Certificate Check	152
25.4.2	Certificate Access	153
25.4.3	Token/Smart Card Reader choice	153
25.5	Managing languages	153
25.5.1	Choosing a language	153
25.5.2	Editing or creating a language	154
26	Administrator logs, Console, and traces	156
26.1	Administrator logs	156
26.2	Console	158
26.3	Trace mode	159
27	Security recommendations	160
27.1	Assumptions	160
27.1.1	Profile and responsibilities of administrators	160

27.1.2	Profile and responsibilities of users	160
27.1.3	Compliance with management rules for cryptographic elements.....	160
27.2	User workstation.....	160
27.3	VPN Client administration	161
27.4	VPN configuration	162
27.4.1	Sensitive information in the VPN configuration.....	162
27.4.2	User authentication	162
27.4.3	VPN gateway authentication	163
27.4.4	Protocol.....	163
27.4.5	“All through the tunnel” and “split tunneling” modes	163
27.4.6	GINA mode.....	163
27.4.7	ANSSI recommendations	164
28	Contact	165
28.1	Information.....	165
28.2	Sales.....	165
28.3	Support	165
29	Appendixes.....	166
29.1	Shortcuts.....	166
29.1.1	Connection Panel.....	166
29.1.2	VPN configuration tree.....	166
29.1.3	Configuration Panel.....	167
29.2	Administrator logs.....	167
29.3	TrustedConnect Panel diagnostics.....	168
29.4	Basic cryptography concepts	172
29.4.1	SHA, RSA, ECDSA, and ECSDSA algorithms	172
29.4.2	Accessing certificates.....	173
29.4.3	Determining a certificate’s container type.....	175
29.4.4	Certificate format	176
29.4.5	Certificate authentication methods	181
29.5	Windows Enterprise VPN Client technical data.....	182
29.5.1	General.....	182
29.5.2	Operating mode.....	182
29.5.3	Connection/Tunnel.....	183
29.5.4	Cryptography and authentication.....	183
29.5.5	Miscellaneous.....	184

29.5.6	Administration.....	185
29.6	Third-party licenses.....	186
29.6.1	OpenSSL.....	186
29.6.2	LZ4.....	188

Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2024-01-22	All	Initial release	FB, BB
1.1	2024-02-15	18.6.1 et 25.2.4	Corrected written form of dynamic parameter <code>MachineStore</code> .	FB, BB
1.2	2024-05-24	13.3.3.1 18.4.2 21.1.2 21.8 All	Added a warning Added a warning Corrected description for how to add several network interfaces Specified MSI property concerned Rephrased passages for greater clarity and corrected minor errors	BB

1 Overview

1.1 Introduction

This guide is intended for administrators of the Windows Enterprise VPN Client.

It contains all the information required to implement and configure the software so that secure VPN tunnels can be opened.

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

1.2 What's new in release 7.5

1.2.1 Endpoint compliance monitoring (requires SCA)

The VPN Client changes the behavior of the **Connection Panel** and of the **TrustedConnect Panel** according to the compliance level reported by the Secure Connection Agent (SCA), which determines whether an endpoint should be authorized to access the corporate network.

1.2.2 Audit trace forwarding to the CMC (requires SCA)

The VPN Client is now able to forward audit traces to the Connection Management Center (CMC) when working in combination with the SCA add-on.

1.2.3 New features in the TrustedConnect Panel

The following features have been added to the **TrustedConnect Panel**:

- The VPN Client can now use Active Directory (AD) for Trusted Network Detection (TND)
- You can now specify the web browser to be used for Captive Portal Detection (CPD) and add a command line, e.g. to disable the proxy in order to secure the connection

1.2.4 Support for IPsec Restricted mode in line with latest changes to the framework

Complies with ANSSI recommendations to ensure compatibility with gateways operating in "IPsec DR strict" (Restricted) mode, including use of SHA-2 hashing algorithm in the certificate request payload and support for OCSP stapling.



1.2.5 OpenSSL 3.0 has been adopted

All components in the VPN Client that rely on OpenSSL have been migrated to version 3.0.

1.2.6 Certificate authentication and revocation

In accordance with security requirements, the `keyEncipherment` value has been deprecated and replaced with the `nonRepudiation` value, which is now accepted by default.

1.2.7 New dynamic parameters have been added

The following dynamic parameters have been added:

- `user_smartcard_tip` used to display a customized message in the PIN code request pop-up window to clearly identify the smart card reader to be used for a given tunnel
- `local_virtual_network_size` used to define the size of the local virtual network

Moreover, in order to ensure compatibility with gateways that operate in IPsec Restricted mode, the following dynamic parameters have been added:

- `use_method_214` used to define the default authentication method to be used with Brainpool user certificates (14 or 214)
- `sha2_in_cert_req` used to define the format to be used (SHA-1 or SHA-2) for the certificate request payload [CERTREQ]
- `enable_OCSP` used to enable the Online Certificate Status Protocol Stapling (OCSP Stapling)

1.2.8 Improved selection of certificate to use

The following improvements have been made to the selection of the certificate to use:

- Finer granularity in how certificate selection is configured: you can now specify the certificate's location (user store or machine store) at the tunnel level
- Certificate selection has been automated regardless of medium, including when there are several tokens and smart cards

1.3 Other new features introduced in v7

1.3.1 Implements Zero Trust Network Access

The following Zero Trust Network Access (ZTNA) principles have been implemented for better workstation protection:

- Inbound and outbound connections are permanently filtered when using the Filtering Mode
- VPN remains permanently active when the disconnect button of the **TrustedConnect Panel** is disabled
- VPN cannot be disabled when all or part of the options in the **TrustedConnect Panel**'s contextual menu are removed

1.3.2 Filtering Mode

The following improvements have been made to the Filtering Mode:

- Added a feature to filter data flows in combination with the CPD state
- Time given users to connect to the captive portal can now be configured
- The Filtering Mode now supports up to 30 rules

1.3.3 Cryptography

Support has been added for the following elements that use the BrainpoolP256r1 curve:

- Diffie-Hellman key group DH 28 (BrainpoolP256r1) [RFC 5639]
- ECDSA "BrainpoolP256r1" asymmetric signing using SHA-2

1.3.4 IKEv1 and vulnerable algorithms have been deprecated

The security of our software has been enhanced with the following:

- End of support for the vulnerable IPsec/IKEv1 protocol, which has been deprecated by the IETF in September 2019
- End of support for vulnerable algorithms DES, 3DES, SHA-1, DH 1, DH 2, DH 5 in IPsec/IKEv2 (even in "auto" mode)

1.3.5 SSL/OpenVPN

The following changes have been introduced:

- End of support for vulnerable algorithms in SSL/OpenVPN: MD5, SHA-1, BF-CBC, TLS 1.1, LOW security suite for TLS V1.2

- Compression is no longer enabled by default

1.3.6 Certificate authentication and revocation

Due to increased security requirements, deprecation of certain algorithms, and stricter rules for using certificates, version 7 of the Windows Enterprise VPN Client comes with certain restrictions on certificates.



Refer to chapter 18 Managing certificates for further details.

- Support for the following certificate authentication methods:
 - Method 1: RSA Digital Signature with SHA-2 [RFC 7296]
 - Method 9: ECDSA “secp256r1” with SHA-2 (256 bits) on the P-256 curve [RFC 4754]
 - Method 10: ECDSA “secp384r1” with SHA-2 (384 bits) on the P-384 curve [RFC 4754]
 - Method 11: ECDSA “secp521r1” with SHA-2 (512 bits) on the P-521 curve [RFC 4754]
 - Method 14: Digital Signature RSASSA-PSS, RSASSA-PKCS1-v1_5, and Brainpool with SHA-2 (256/384/512 bits) [RFC 7427]
 - Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) on the BrainpoolP256r1 curve (only available with gateways that support this method)
- End of support for Method 1: RSA Digital Signature with SHA-1 [RFC 7296]
- RSA certificates with less than 2048-bit key length are rejected
- Key Usage and Extended Key Usage of certificates is verified
- Verification of the user certificate CRL has become optional

1.3.7 New features in the TrustedConnect Panel

The following features have been added to the **TrustedConnect Panel**:

- A new entry in the **TrustedConnect Panel**'s contextual menu gives access to the same **Console** as the one available in the **Configuration Panel**
- A new MSI property called `DIALERBEHAVIOR` can be used to add the following three options to the **TrustedConnect Panel**:
 - Select the desired behavior when the compliance level changes
 - A button to disable trusted network detection (TND) so that users may open a tunnel in the **TrustedConnect Panel** even if a trusted network has been detected
 - Enable multiconnection mode so that users can choose the active connection by clicking the connection name in the **TrustedConnect Panel**'s title banner

- A new MSI property named `RESTARTGUITC` allows you to automatically restart the **TrustedConnect Panel** after it has been shut down (crash or quit)

1.3.8 New dynamic parameters have been added

The following dynamic parameters have been added:

- `local_subnet` allows you to choose the source IP address of the network interface if it has several addresses
- `crl_cache_duration` allows you to implement a cache memory to store the CRL and define its expiration time

1.3.9 Enhanced security

Security has been enhanced in the software with more robust password protection for the configuration file in line with ANSSI's recommendations

1.3.10 Improved smart card/token identification

When several smart cards and/or tokens are connected to the workstation and a tunnel uses one of them, the dialog box for password entry now clearly specifies the smart card or token for which the password is requested



2 Installing the software

2.1 Introduction

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

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

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



Refer to section 2.2 Installation procedure.

2.1.1 Minimum requirements

The Windows Enterprise VPN Client is available for Windows 10 and 11 64-bit.

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

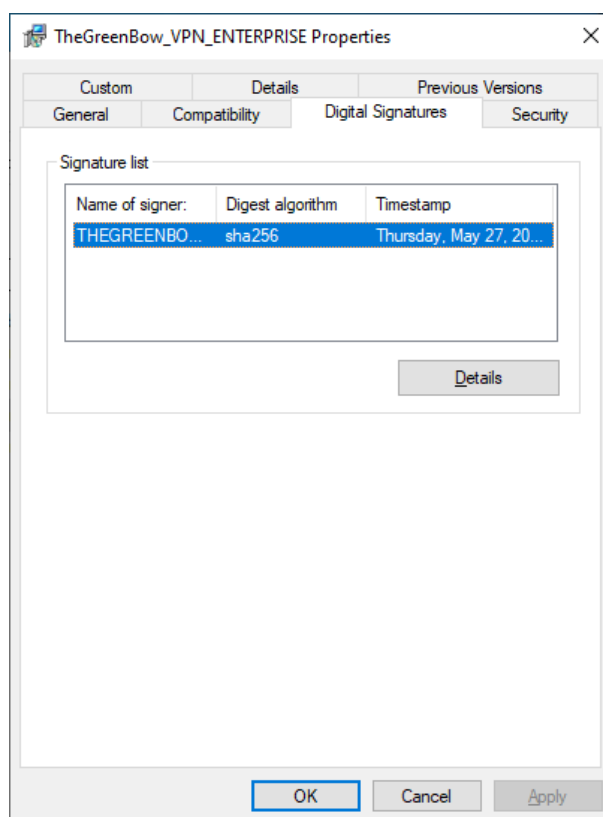
- Processor: 1 GHz or faster processor
- RAM: 2 GB
- Hard disk space available: 40 MB

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

2.1.2 Digital signature and version

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

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



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

2.1.3 Vulnerabilities

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



See also our [security recommendations](#).

2.2 Installation procedure

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

The installation procedure is the same whether it is an initial installation or an update (see chapter 4 Updating the software). When performing an update,

the software settings, the existing VPN configuration¹, and the license are preserved.

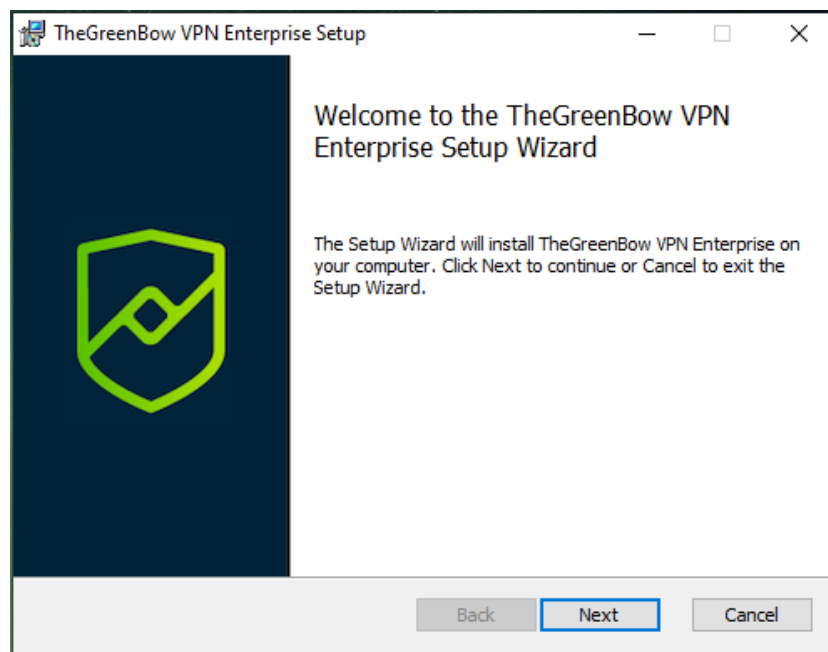


You can only update the software if your subscription is still valid (see section 4.1 How to get an update).



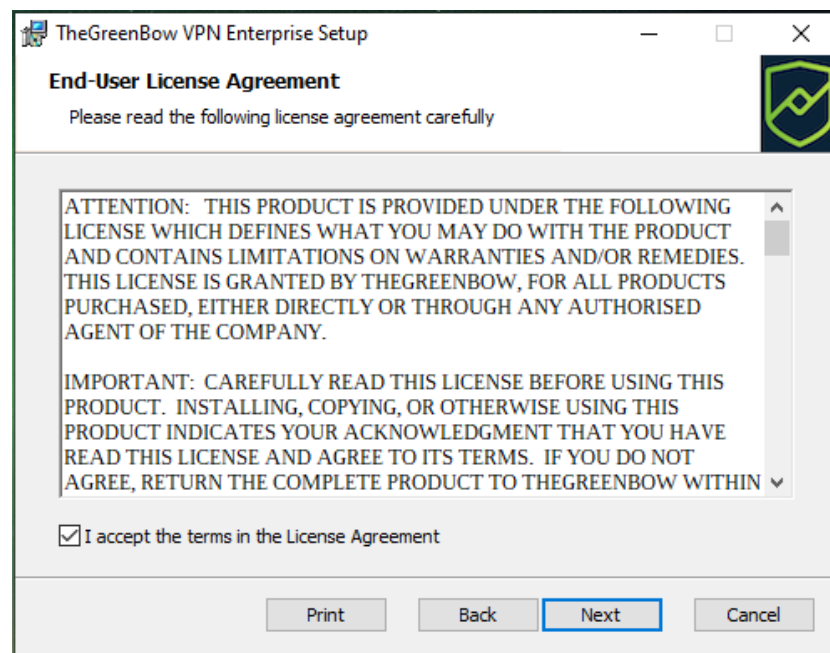
If you want to perform a silent installation, pass specific parameters during installation or perform a large-scale deployment, refer to the "Deployment Guide".

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

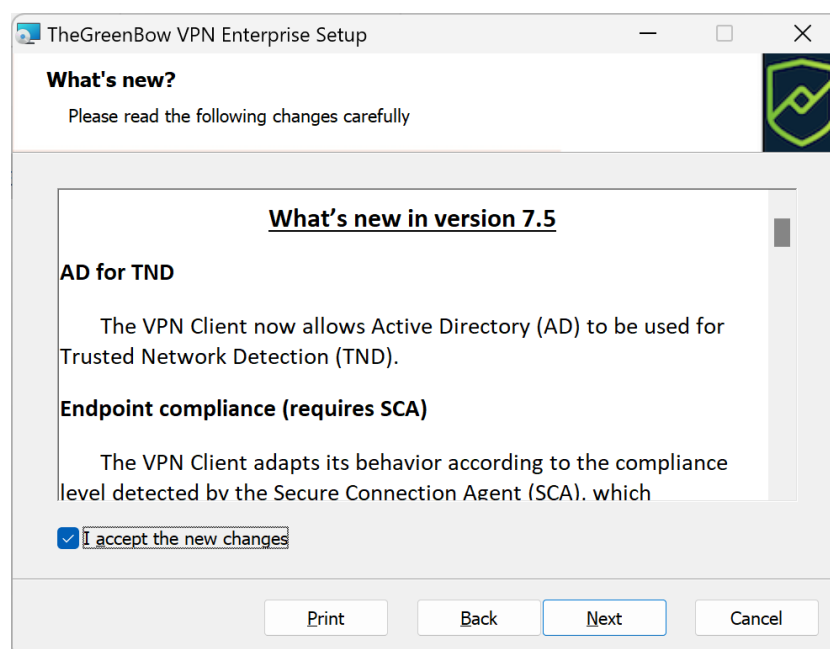


¹ In some cases, see section 4.3 Updating the VPN configuration.

2. Click **Next**. The following window is displayed:



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

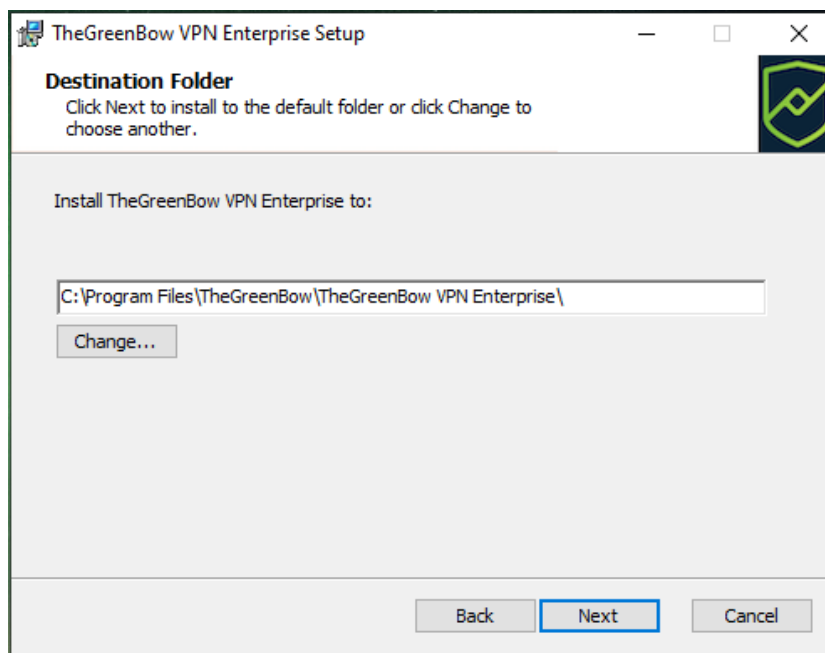


4. Carefully read the information about what's new and the note about how the existing VPN configuration will be converted during an update.



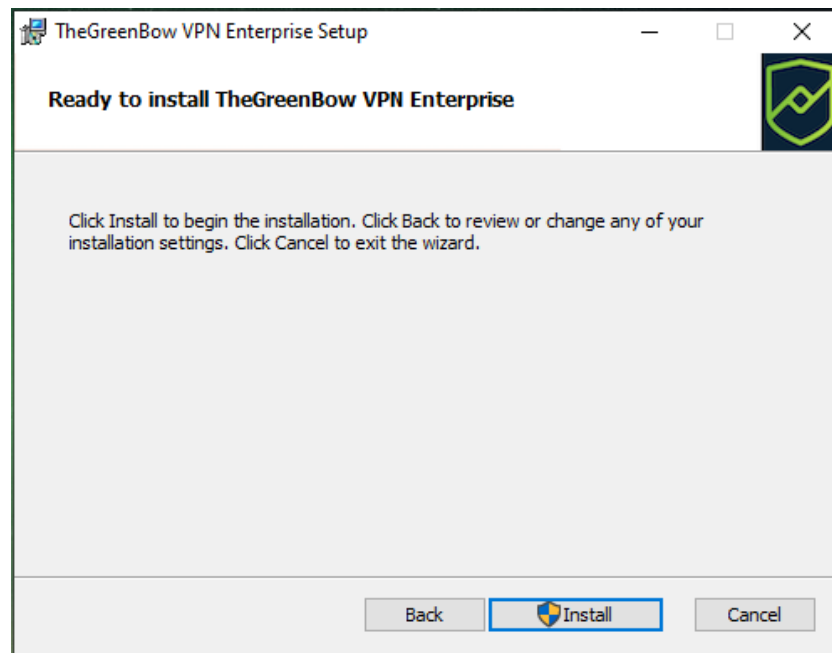
Once the installation is complete, you will not be able to revert to an earlier version of the software without manual intervention. If in doubt, back up your VPN configuration to a separate folder or to a removable storage medium.

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

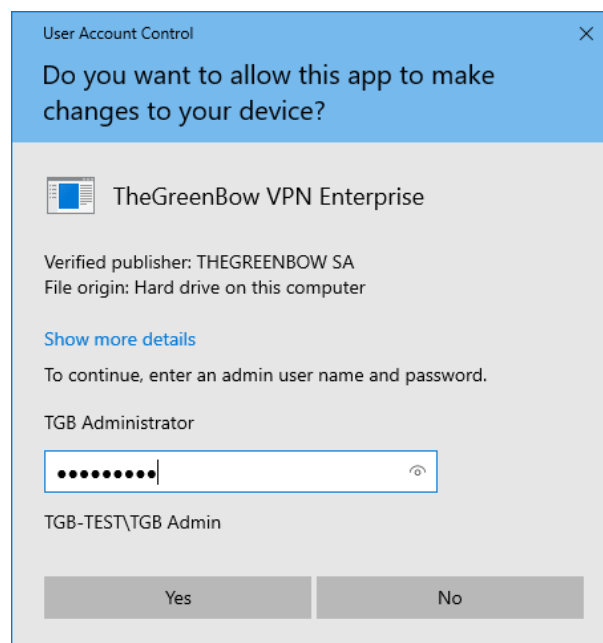


5. If you want to install the Windows Enterprise VPN Client in a specific directory, click **Change...** and select the desired directory. Otherwise, you can keep the default directory. Then, click **Next**.

The following window is displayed:



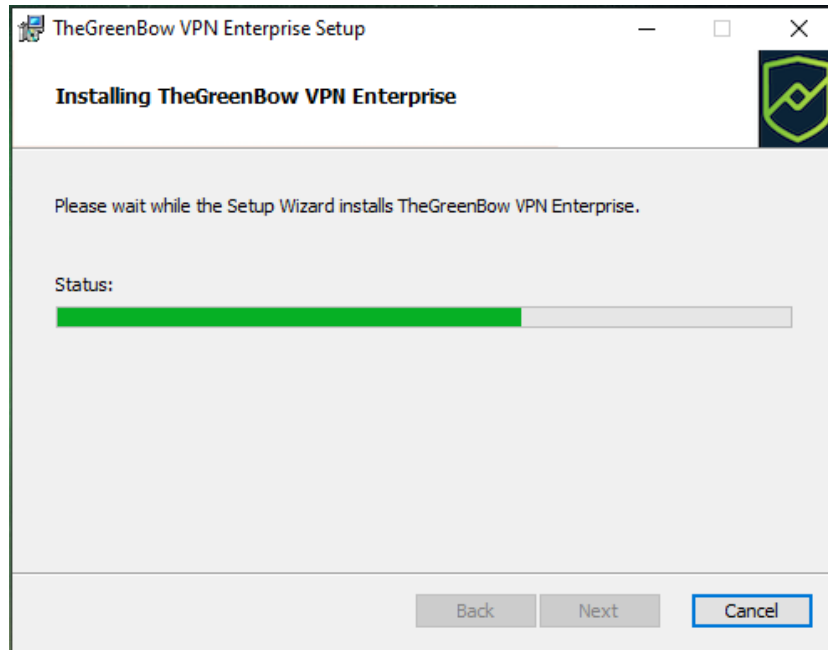
6. The program is ready to install. If you want to go back to check or change your installation settings, click **Back**. Otherwise, click **Install**. If you are installing from an account that does not have administrator rights, the following window is displayed:



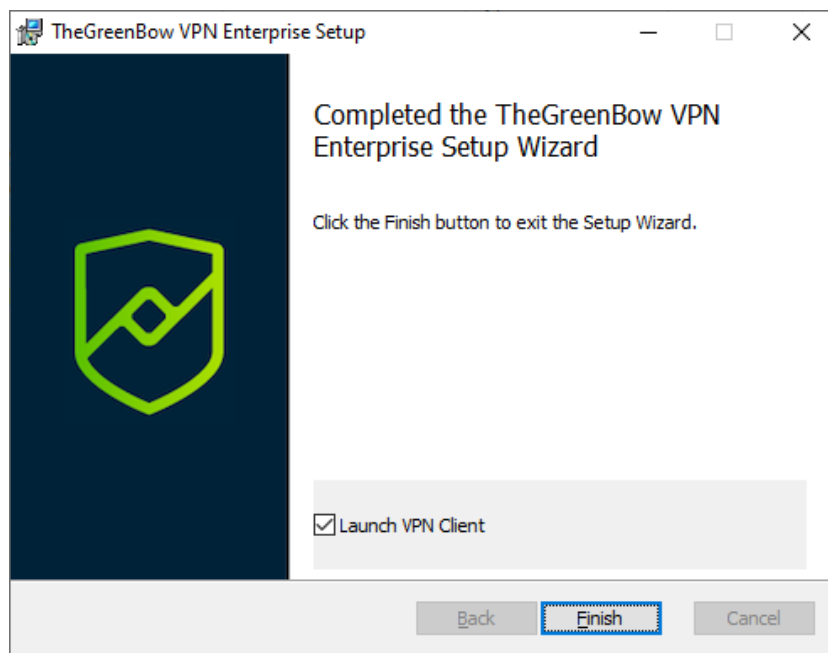
7. To proceed with the installation, you must enter an administrator name and password to allow the installation program to make changes to your computer. Otherwise, the software will not be installed.

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

8. Installation begins and the following window is displayed:



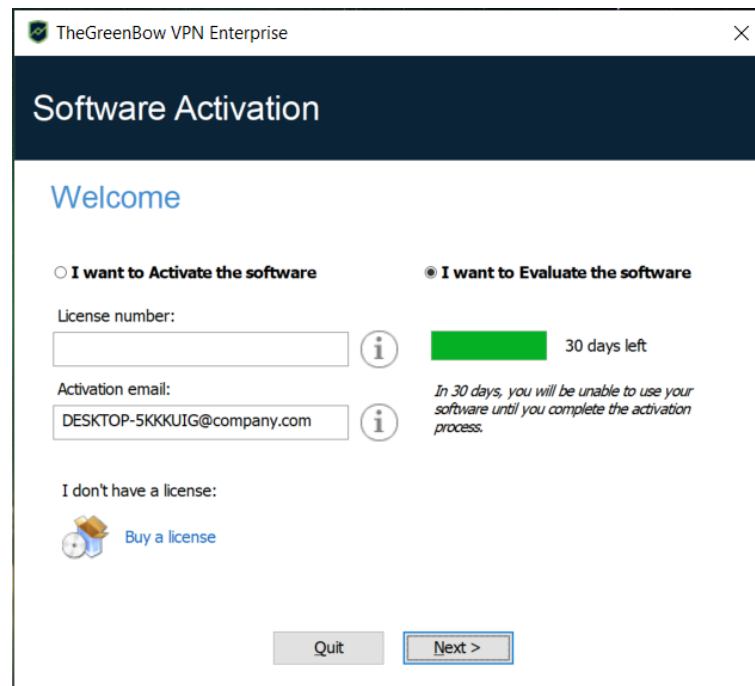
9. Wait for the installation of the Windows Enterprise VPN Client including all its components to complete. If installation has succeeded, the following window is displayed:



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

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

Otherwise, the activation screen is displayed:



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

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

- Select **I want to Activate the software**,
- Enter the license number and activation e-mail
- Then, click **Next >**

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

If you want to try the Windows Enterprise VPN Client:

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

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

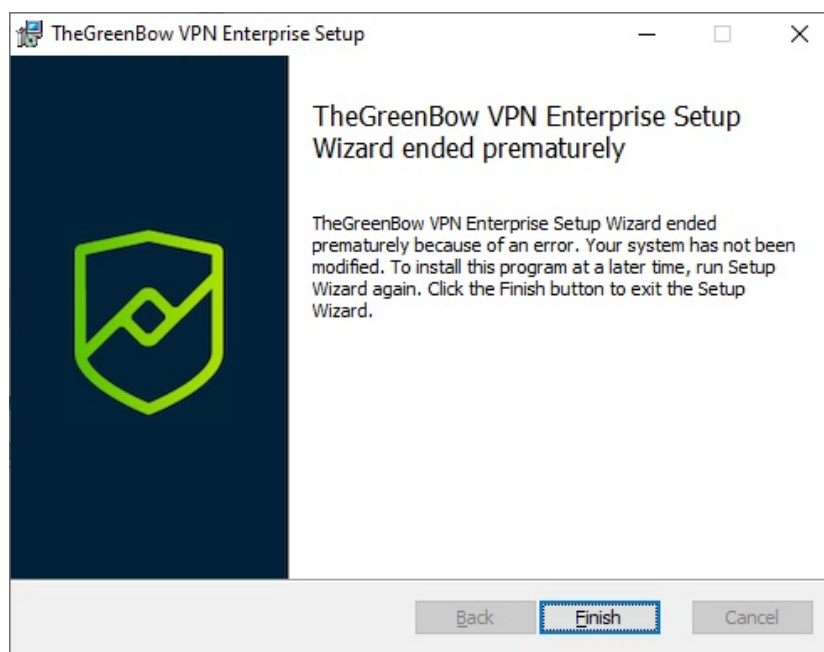
If you do not have a license and want to buy one, click **Buy a license**. TheGreenBow online store is displayed in a browser window. Here, you can buy one or several licenses. For further details on the activation procedure, refer to chapter 3 Activating the software.

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

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

2.3 Canceling installation

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



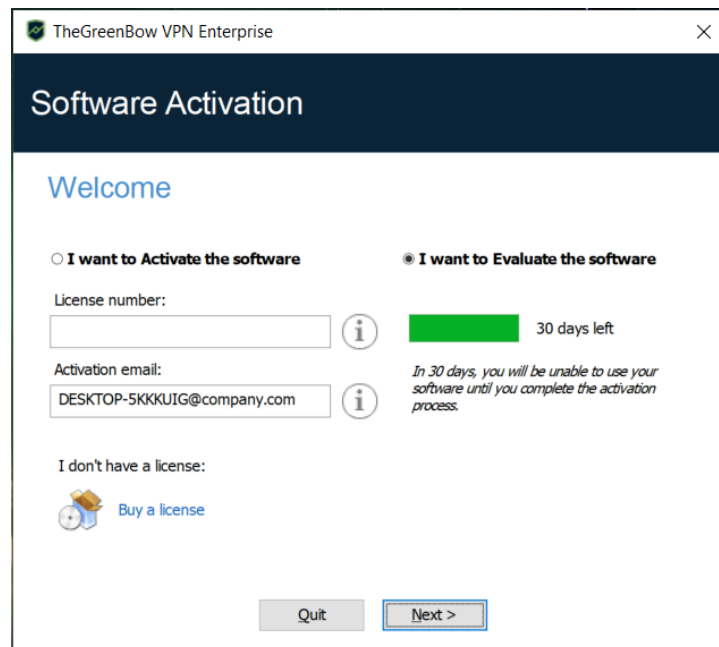
Your system has not been modified and you can resume installation at a later time.

2.4 Trial period

The first time the software is installed on a workstation, if no license key is provided to the installer, the VPN Client will enter a 30-day trial period.

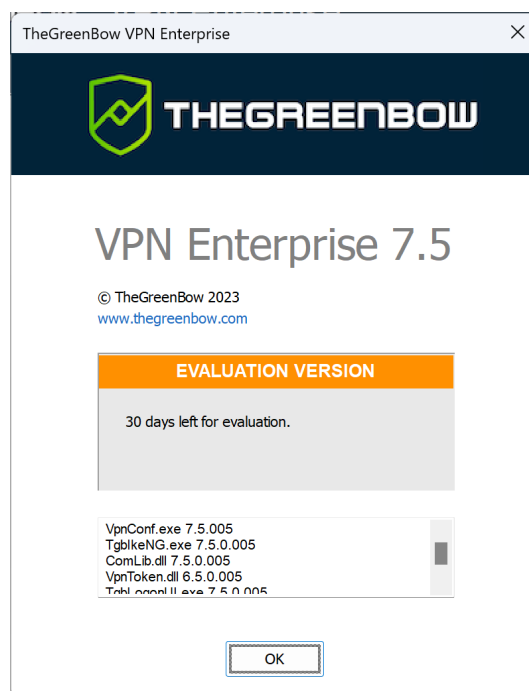
During this trial period, the VPN Client is fully operational, and all functions are unlocked.

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

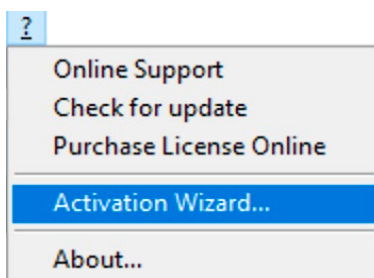


Select **I want to Evaluate the software**, then click **Next >** to run the software.

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



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



2.5 Configuring Windows

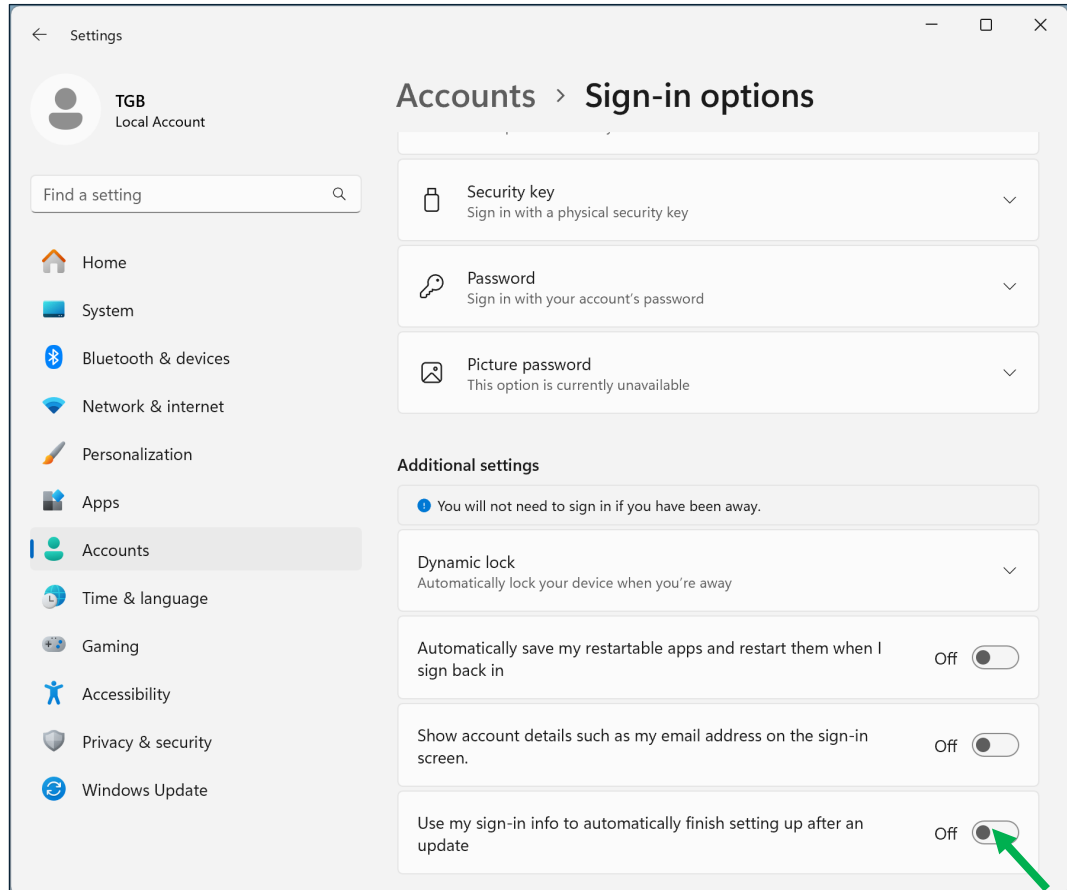
Once you have completed installation, you need to make sure that a Windows sign-in option is disabled.



This option is not available (Windows 10) or grayed out (Windows 11) if your workstation is joined to a domain, or if your organization has applied work or e-mail policies to your workstation.

Windows 11

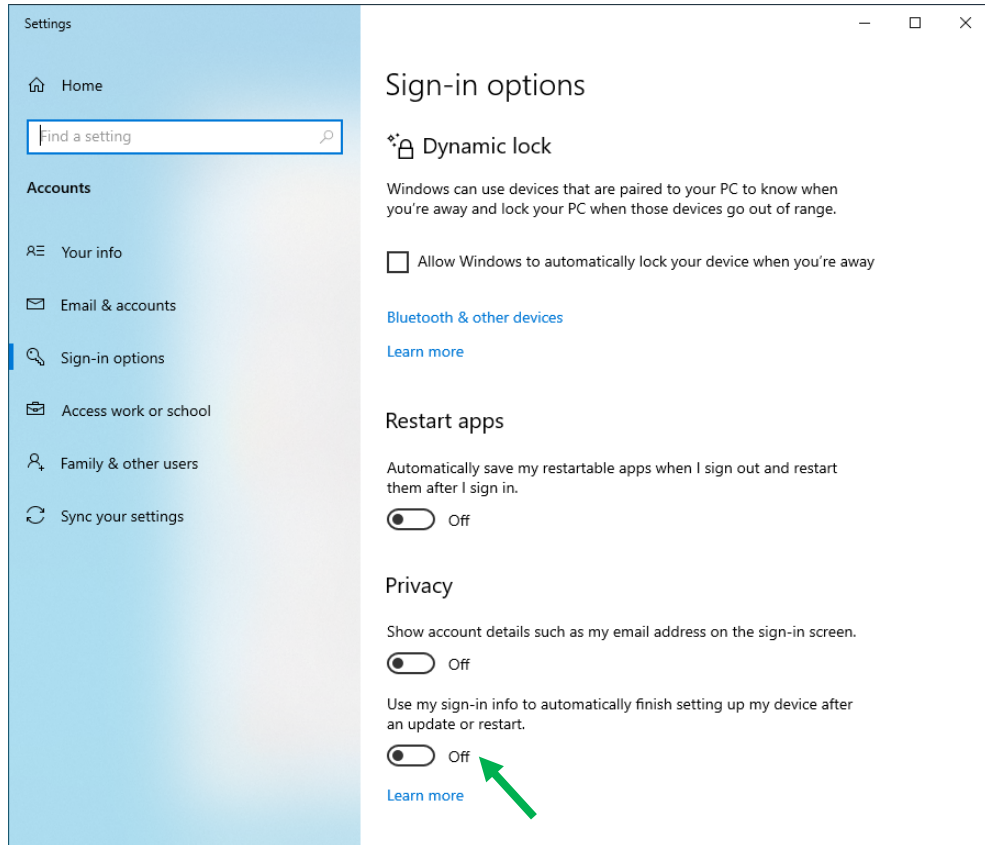
In Windows 11, select **Start**, and then **Settings > Accounts > Sign-in options** and under **Additional settings** disable **Use my sign-in info to automatically finish setting up after an update**, as shown in the screenshot below:





Windows 10

In Windows 10, select **Start**, then **Settings > Accounts > Sign-in options** and under **Privacy** disable **Use my sign-in info to automatically finish setting up my device after an update or restart**, as shown in the screenshot below:



3 Activating the software

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

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

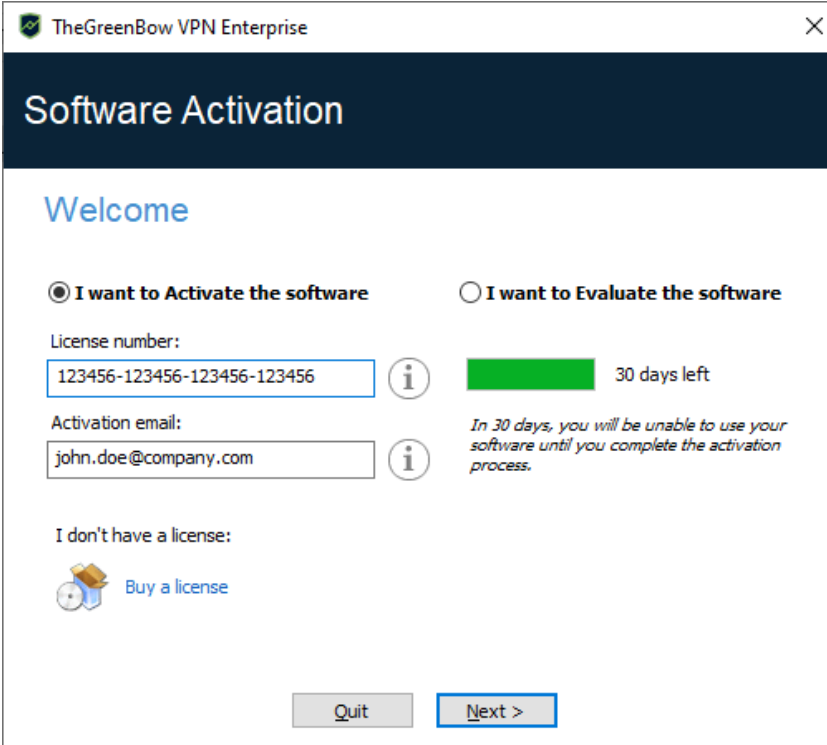
3.1 Step 1

If you do not yet have a license, click **Buy a license**. 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 e-mail. The license number can be copy-pasted directly from the purchase confirmation e-mail 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 e-mail 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 for TheGreenBow VPN Enterprise. The window has a dark blue header with the title 'Software Activation'. Below the header, there is a 'Welcome' section. Two radio buttons are present: 'I want to Activate the software' (selected) and 'I want to Evaluate the software'. Under the 'Activate' option, there are two input fields: 'License number' (containing '123456-123456-123456-123456') and 'Activation email' (containing 'john.doe@company.com'). To the right of the 'License number' field, there is a green progress bar and the text '30 days left'. Below the 'Activation email' field, there is 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 section 'I don't have a license:' with a 'Buy a license' button. At the bottom right, there are two buttons: 'Quit' and 'Next >'.



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

3.2 Step 2

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

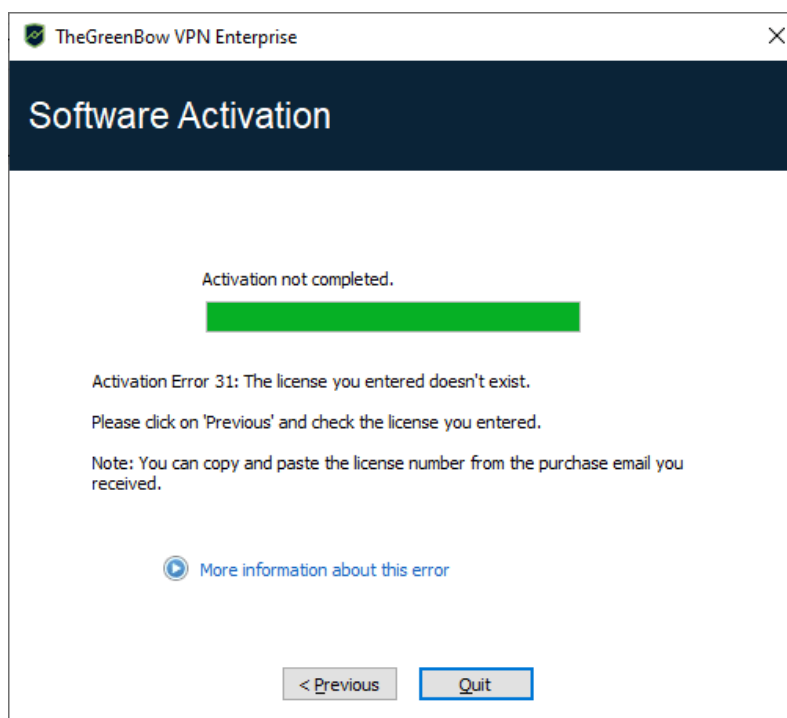
Once the activation has been carried out successfully, click **Run** to run the software.



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

3.3 Activation errors

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



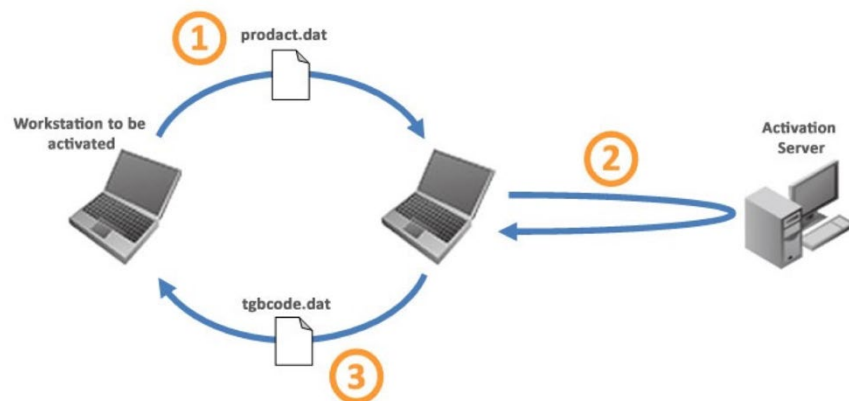
TheGreenBow lists all activation errors and [procedures for solving activation issues](#) on its website.

The following are the most common activation errors:

No.	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

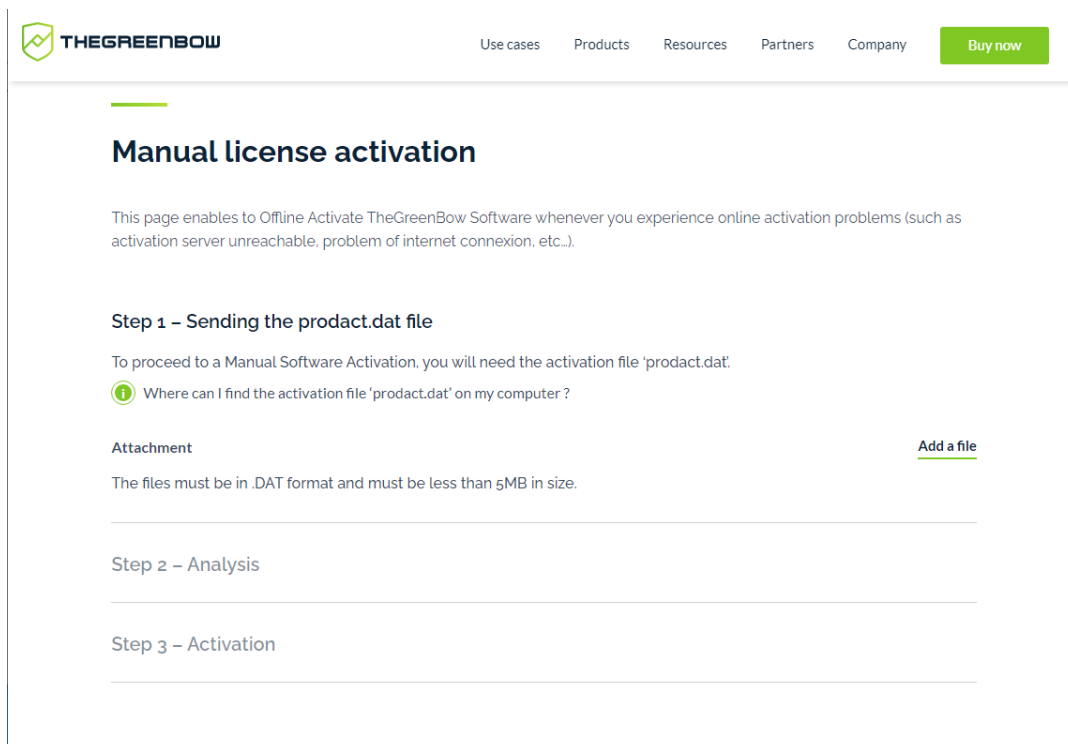
When activation fails due to a communication issue with the activation server, the software can be activated manually on [TheGreenBow's website](#). The procedure is as follows:



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

To proceed with manual activation, follow the steps below:

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



The screenshot shows the 'Manual license activation' page on the TheGreenBow website. The page has a header with the logo and navigation links: 'Use cases', 'Products', 'Resources', 'Partners', 'Company', and a green 'Buy now' button. The main content area is titled 'Manual license activation' and includes a sub-header 'Step 1 – Sending the product.dat file'. Below this, it states: 'To proceed to a Manual Software Activation, you will need the activation file 'product.dat''. There is a green information icon followed by the text 'Where can I find the activation file 'product.dat' on my computer?'. Below this is an 'Attachment' section with a note: 'The files must be in .DAT format and must be less than 5MB in size.' and a green 'Add a file' button. The page also shows 'Step 2 – Analysis' and 'Step 3 – Activation' as sections below.

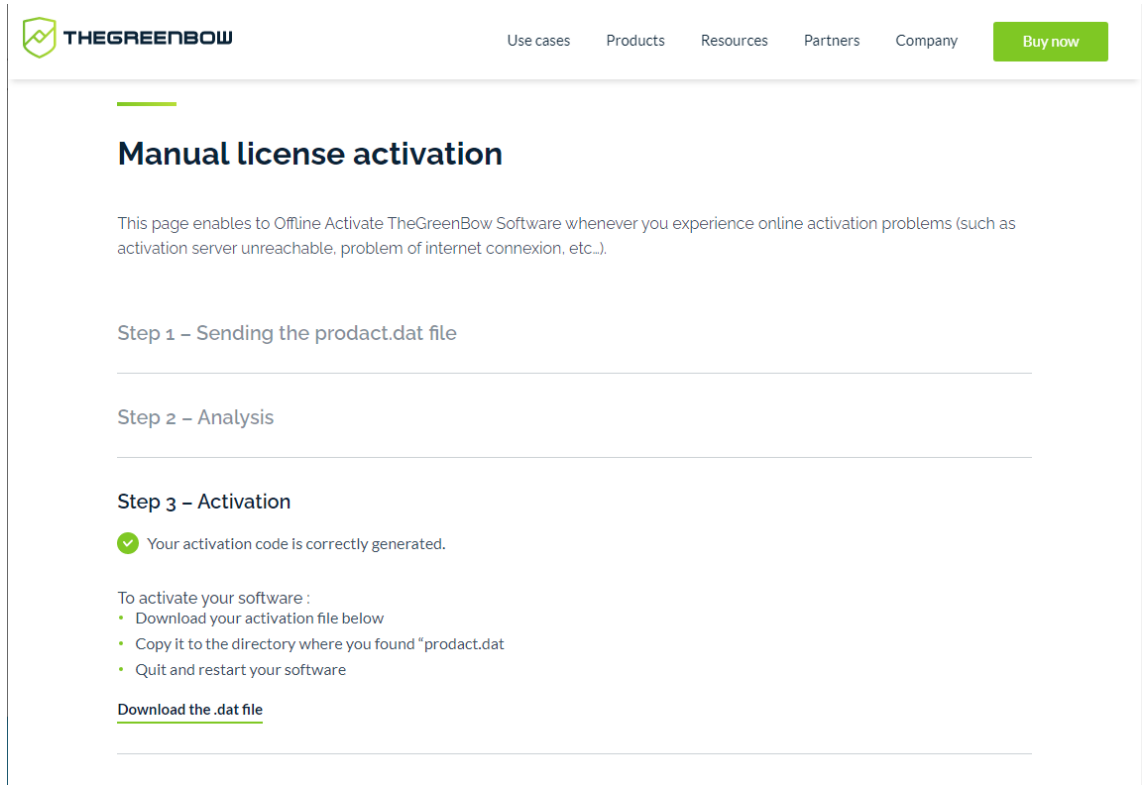
2. Click **Add a file** and open the `product.dat` file created on the workstation that you want to activate.

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 **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.

3. Click **Send**. The activation server will check the validity of the information contained in the `product.dat` file.
4. Click **Submit**. The activation server will provide a link to download a file containing the activation code for the workstation to be activated.



The screenshot shows the 'Manual license activation' page on the TheGreenBow website. The page has a navigation bar with links for 'Use cases', 'Products', 'Resources', 'Partners', 'Company', and a 'Buy now' button. The main content area is titled 'Manual license activation' and includes a sub-header 'Manual license activation'. Below this, a paragraph explains that the page enables offline activation when online activation fails. The page is divided into three steps: 'Step 1 - Sending the product.dat file', 'Step 2 - Analysis', and 'Step 3 - Activation'. Step 3 includes a green checkmark icon and the text 'Your activation code is correctly generated.' It also lists instructions for activating the software: download the activation file, copy it to the directory containing 'product.dat', and quit and restart the software. A link 'Download the .dat file' is provided at the bottom of the step.

Manual license activation

This page enables to Offline Activate TheGreenBow Software whenever you experience online activation problems (such as activation server unreachable, problem of internet connexion, etc.).

Step 1 – Sending the product.dat file

Step 2 – Analysis

Step 3 – Activation

✓ Your activation code is correctly generated.

To activate your software :

- Download your activation file below
- Copy it to the directory where you found "product.dat"
- Quit and restart your software

[Download the .dat file](#)

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

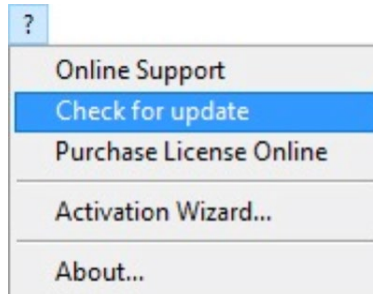
3.5 License and activated software

Once the software is activated, the license number and e-mail address used for activation is shown in the **About...** window of the software.



4 Updating the software

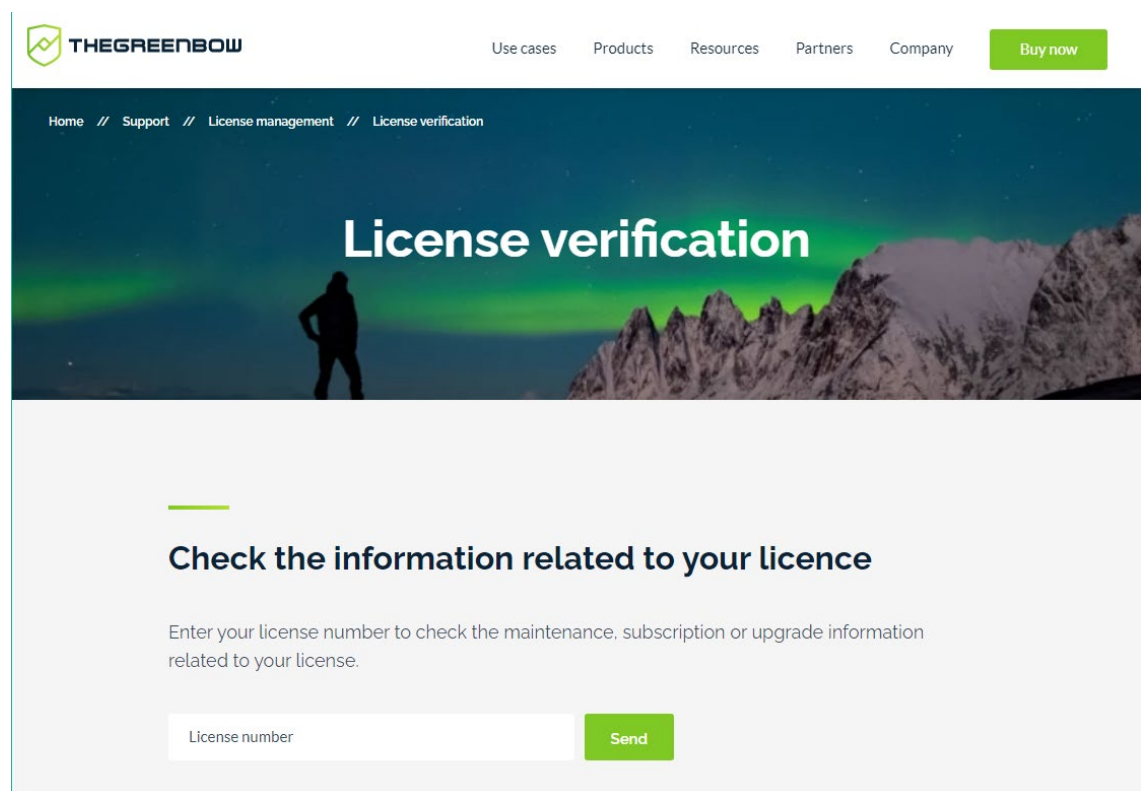
You can also check whether an update is available for the software at any time using the main interface menu ? > **Check for update**.



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

<https://www.thegreenbow.com/en/support/license-management/checking-license/>

Example



4.1 How to get an update

Software updates are provided according to the following rules:

During the subscription period ¹	All updates can be installed
No subscription	The software cannot be used or updated

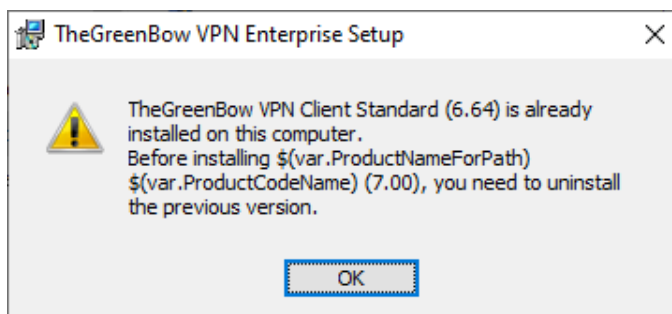


Performing an update from a Standard edition to an Enterprise edition and vice versa is not allowed. However, you can update from any previous version of the Enterprise VPN Client (including Premium and Certified).

4.2 Update procedure

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

1. If the license of the installed product is not compatible with the Windows Enterprise VPN Client 7.5, updating will not be possible and the following screen is displayed:

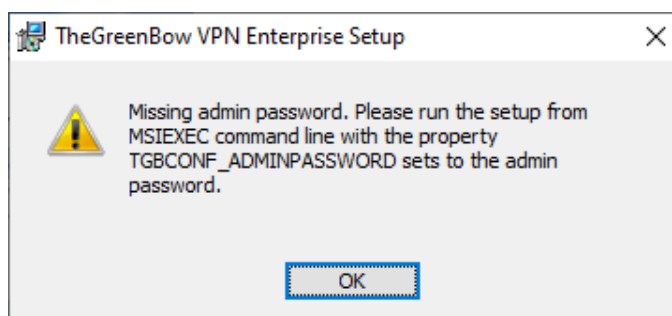


In this case, you will need to uninstall the previous version of the software before you install the new one.

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

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

the graphical interface of the installation program. In this case, the following screen is displayed:



Password protection for access to the **Configuration Panel** has been replaced in version 6.8 of the Windows Enterprise VPN Client by a more secure mechanism. It consists in limiting access to the **Configuration Panel** to Windows administrators only. This option is not enabled by default but can be enabled as described in section 25.1.3 Restricting access to the Configuration Panel, check the **Restrict access to Configuration Panel to administrator** option.

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

4.3 Updating the VPN configuration

During an update, the VPN configuration is backed up and restored, except in the cases mentioned below.



When updating from version 6.6x or higher of the Premium product you cannot keep the previous configuration. The new version is installed correctly, but it does not restore the configuration from version 6.6x.



When updating from version 6.5 of the Premium product or 6.8 of the Enterprise product, the configuration from the previous version is restored, but obsolete protocols and algorithms, e.g. IKEv1, are not kept.



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



4.4 Automation

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

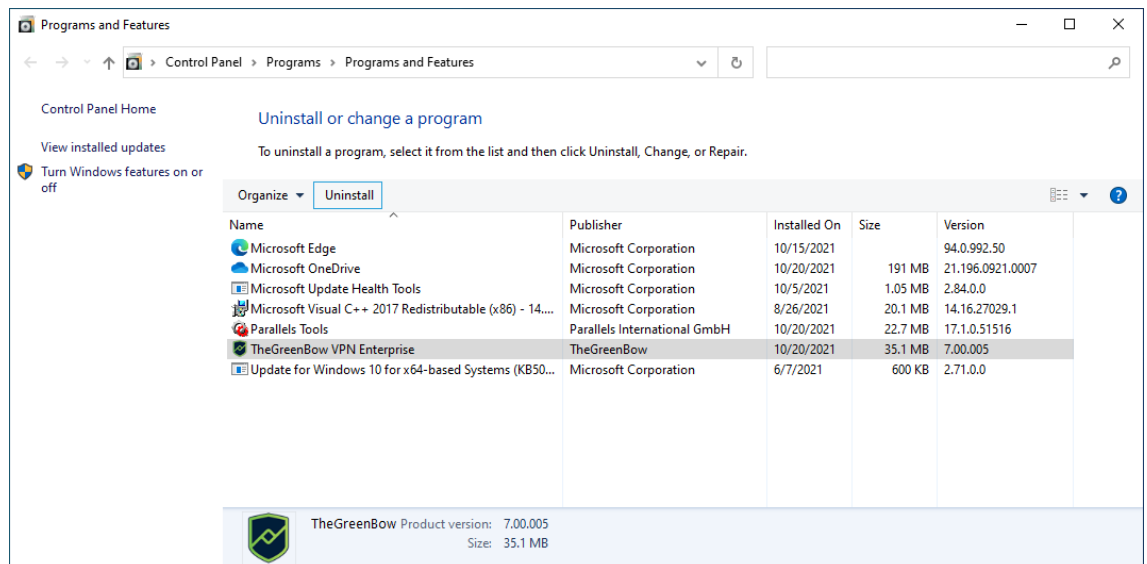


These options are described in the “Deployment Guide”.

5 Uninstalling the software

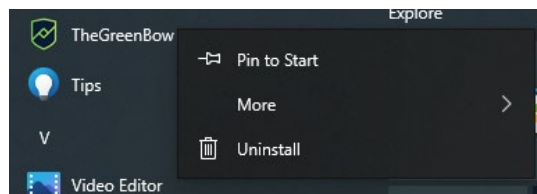
To uninstall the VPN Client, proceed as follows:

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



OR

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



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



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



6 Getting started with the software

6.1 Introduction

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

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

The graphical interface includes the following elements:

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

6.2 Starting the software

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

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

Verifying the VPN Client's integrity

All the binaries that make up the Windows Enterprise VPN Client (except drivers) are signed with a certificate issued for THEGREENBOW

(SISTECH S.A.), whereas drivers are signed with a certificate issued for THEGREENBOW SA. This allows users to verify the integrity of the software and its modules.

You can verify the authenticity of the software by displaying the properties of any of its modules by right-clicking the module and then selecting the **Digital signatures** tab.

If one of the VPN Client's modules is corrupted, the software will not be operational. Depending on the case, a Windows pop-up will be shown or a message will be displayed in the **Console**.

Starting the VPN Client using the shortcut on the desktop

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

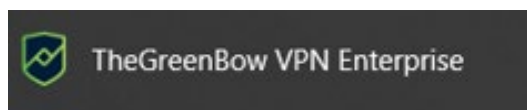
The Windows Enterprise VPN Client can be started directly by double-clicking on this icon.



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

Starting the VPN Client using the Windows Start menu

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

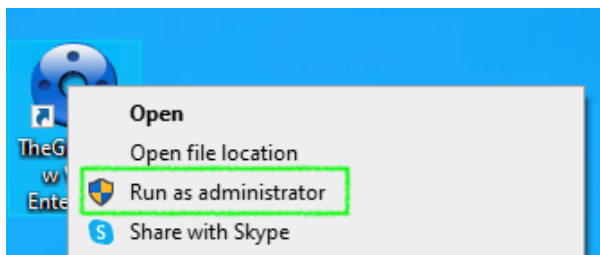


The VPN Client will start minimized and the TheGreenBow VPN Enterprise icon will appear in the taskbar (see paragraph entitled [Taskbar icon](#) below).

Running the VPN Client as administrator

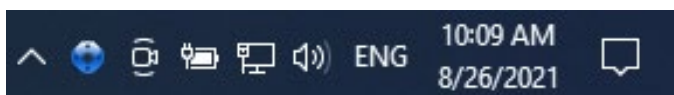
By default, access to the VPN Client's **Configuration Panel** is restricted to Windows administrators only.

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



Taskbar icon

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



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



Blue icon: no VPN tunnel open



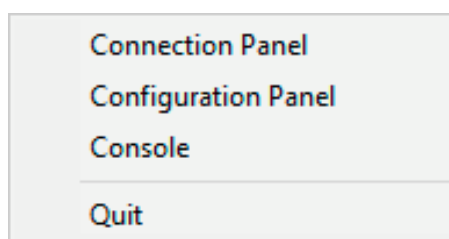
Green icon: at least one VPN tunnel is open

The tooltip for the icon always shows the software status:

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

Left-clicking the icon opens the **Connection Panel**.

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



The administrator can limit the options displayed in the menu (see section 25.1.1 Showing options in systray menu). The contextual menu contains the following items:

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

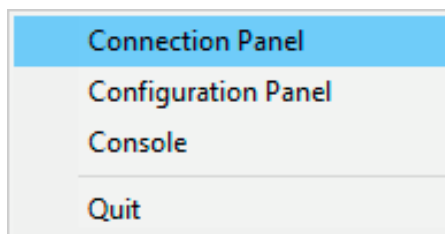


If the software has not been run as administrator and the **Restrict access to Configuration Panel to administrator** option has not been disabled, when the user selects the **Configuration Panel** option, a message is displayed indicating that the software must be run as administrator to access the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

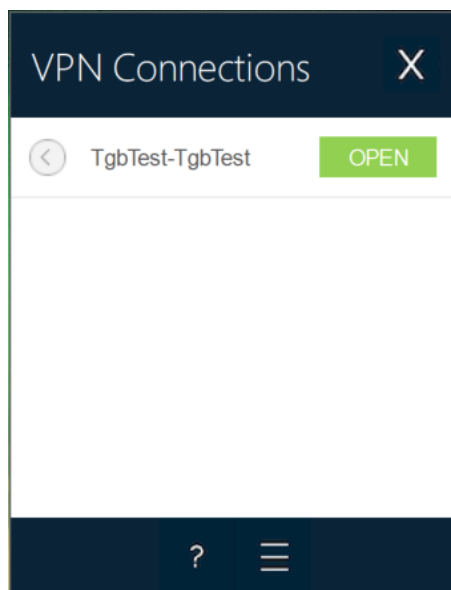
6.3 Opening a test VPN tunnel from the Connection Panel

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

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

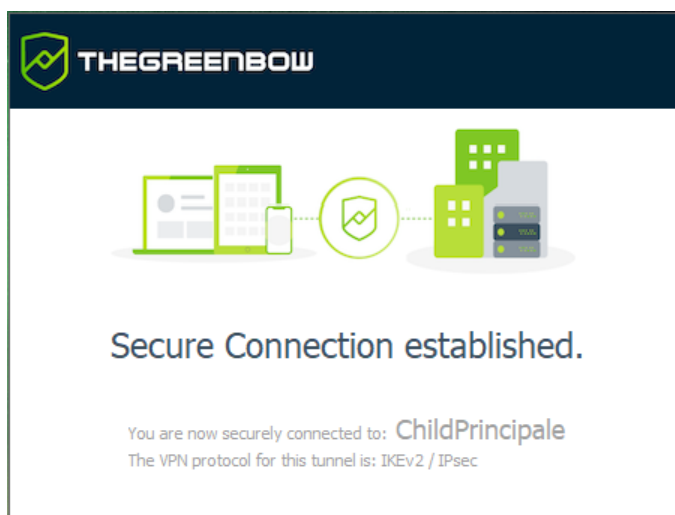


In the **Connection Panel**, click the **OPEN** button next to the **TgbTest-TgbTest** VPN tunnel.




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

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

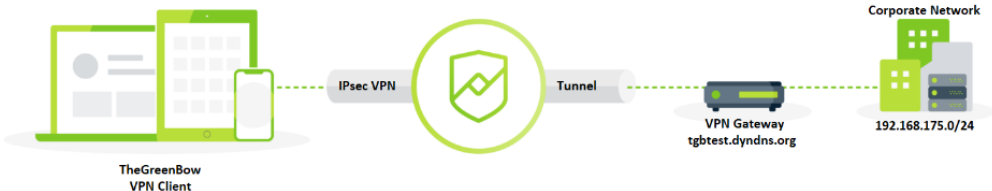


The TheGreenBow test website is then displayed in a browser window:


THEGREENBOW
VPN TEST SERVER

Congratulations! You've successfully opened a VPN tunnel.

Your machine's connectivity meets the requirements for IPsec VPN. This webpage is located on a webserver reachable through vpn only (extranet).



TheGreenBow
VPN Client

IPsec VPN

Tunnel

VPN Gateway
tgbttest.dyndns.org

Corporate Network
192.168.175.0/24

Examples of protocols that can be used with tunneling:

The following is a **NETBIOS** link to our demo server. You can open Windows Explorer and try accessing the shared folder :
`\\192.168.175.50\share\`

You can try to **RDP** using the Windows Remote Desktop tool. However, we do not provide any login/password though, as this is for testing purpose only.



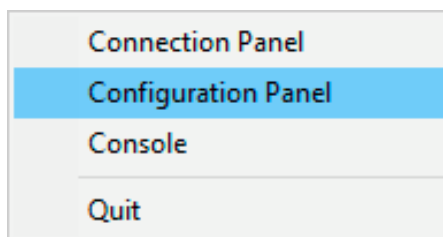
You can also open a test tunnel from the **Configuration Panel** (see chapter 9 Configuration Panel).

You have installed the Windows Enterprise 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 chapter 9 Configuration Panel)

6.4 Configuring a VPN tunnel

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



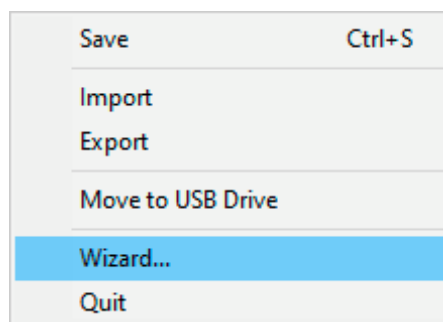
When the **Restrict access to Configuration Panel to administrator** option is disabled (see section 25.1.3 Restricting access to the Configuration Panel), you do not need to run the VPN Client as administrator to be able to access the **Configuration Panel**.

Then, open the **Configuration Wizard** by selecting the **Configuration > Configuration Wizard** menu item.



On our website, you will find many configuration guides for most VPN firewalls/routers/gateways:

<https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-routers/>.



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

6.5 Automating the opening of a VPN tunnel

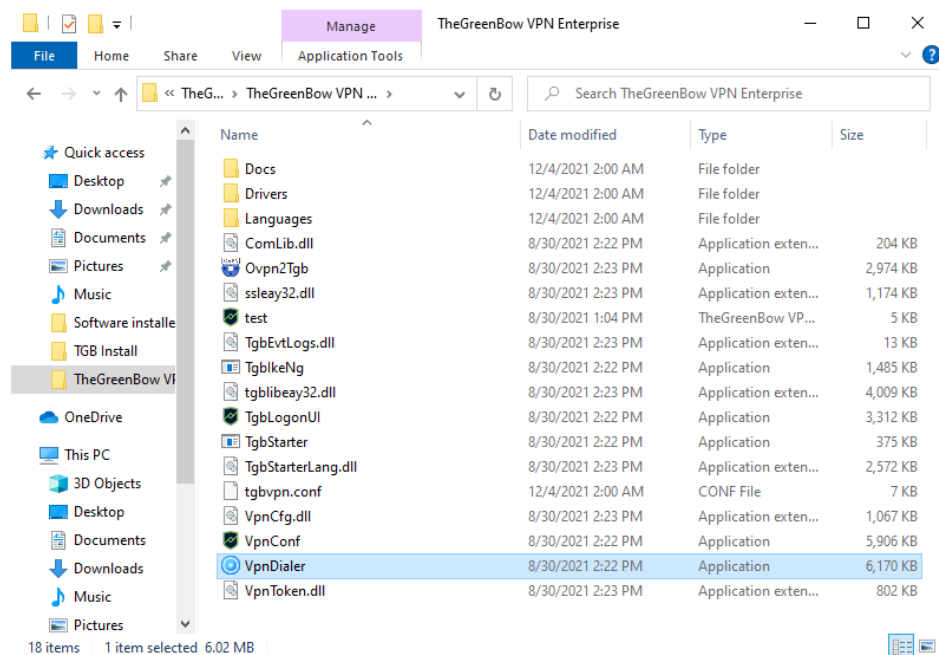
The Windows Enterprise VPN Client allows you to automate the opening of a VPN tunnel. It can be opened automatically in the following ways:

1. When Windows is started, before or after logging on
2. When traffic to the remote network is detected (see chapter 15 Automation)
3. When inserting the smart card or token containing the certificate used for this tunnel (see section 18.5 Using a certificate stored on a smart card or token)
4. When the **TrustedConnect Panel** is used, if the VPN Client detects that the workstation is not located in the trusted network (see chapter 21 Configuring the TrustedConnect Panel).

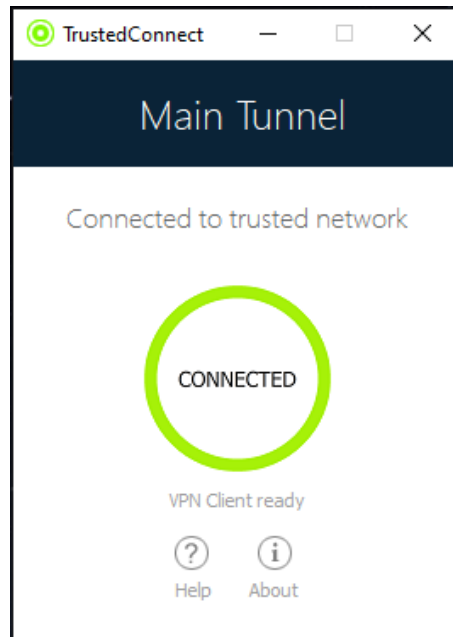
6.6 Opening a VPN tunnel from the TrustedConnect Panel

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

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



The tunnel **TgbTest-TgbTest** should open automatically.



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



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

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

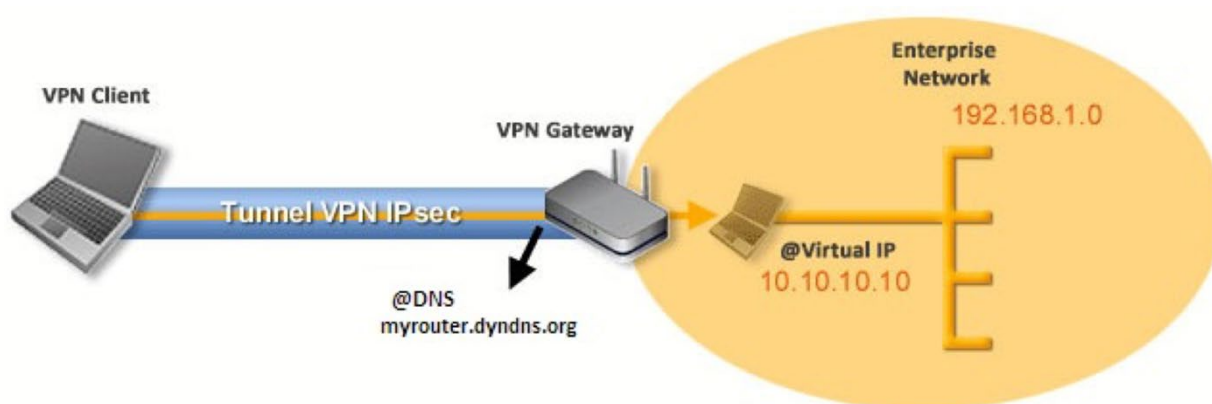
However, when `VpnDialer.exe` (TrustedConnect) is running, you cannot run `VpnConf.exe` immediately. You must first quit `VpnDialer.exe` before you can run `VpnConf.exe`.

7 Configuration Wizard

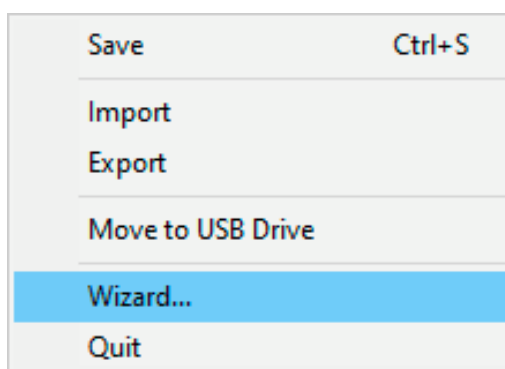
The **Configuration Wizard** is used to configure a VPN tunnel in three easy steps.

The way the **Configuration Wizard** works is illustrated in the example below:

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



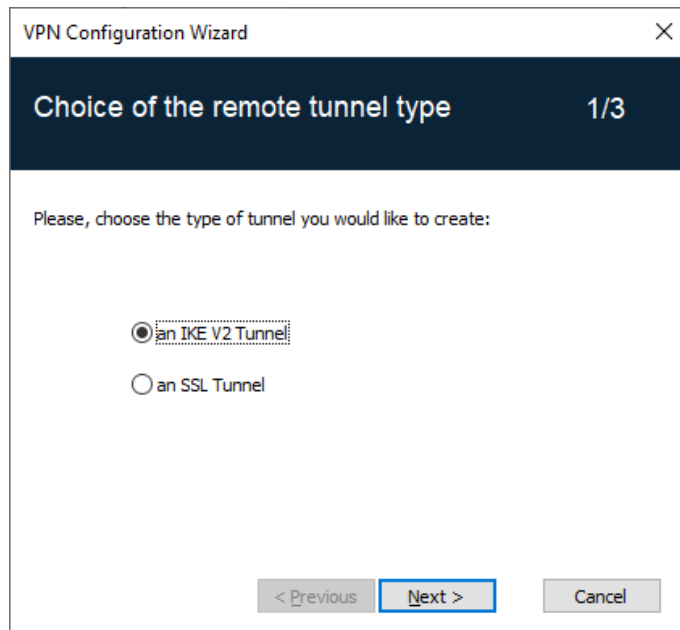
In the main interface, open the **VPN Configuration Wizard: Configuration > Wizard....**



We recommend configuring IKEv2 tunnels with a certificate. Refer to chapter 27 Security recommendations.

7.1 Step 1

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



7.2 Step 2

7.2.1 Configuring an IPsec/IKEv2 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 18.4 Importing a certificate to the VPN configuration)

VPN Configuration Wizard

VPN tunnel parameters 2/3

Enter the following parameters for the VPN tunnel:

IP or DNS public (external) address: of the remote gateway myrouter.dyndns.org

Preshared key: •••••

Import Certificate...

Preshared Key ☒

Certificate ☐

< Previous Next > Cancel

7.2.2 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 18.4 Importing a certificate to the VPN configuration)

VPN Configuration Wizard

VPN tunnel parameters 2/3

Enter the following parameters for the VPN tunnel:

IP or DNS public (external) address: of the remote gateway myrouter.dyndns.org

Certificate Common Name <Click the import button>

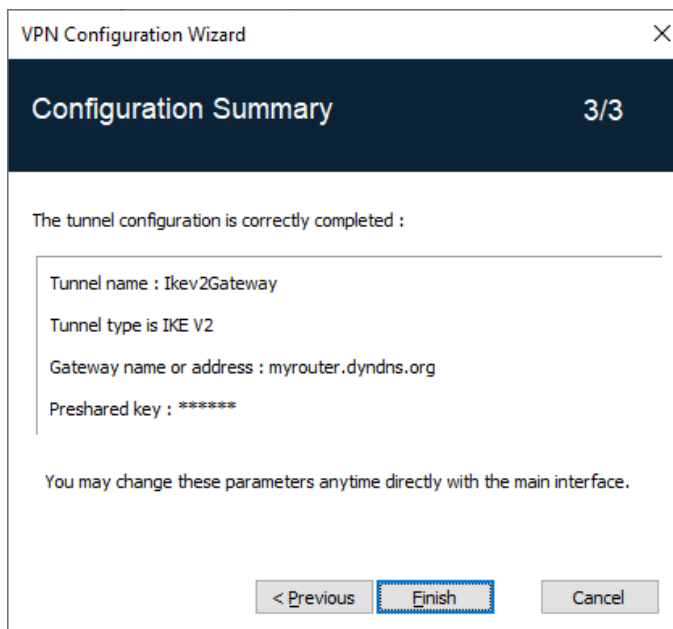
Import Certificate...

Login required ☐

< Previous Next > Cancel

7.3 Step 3

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

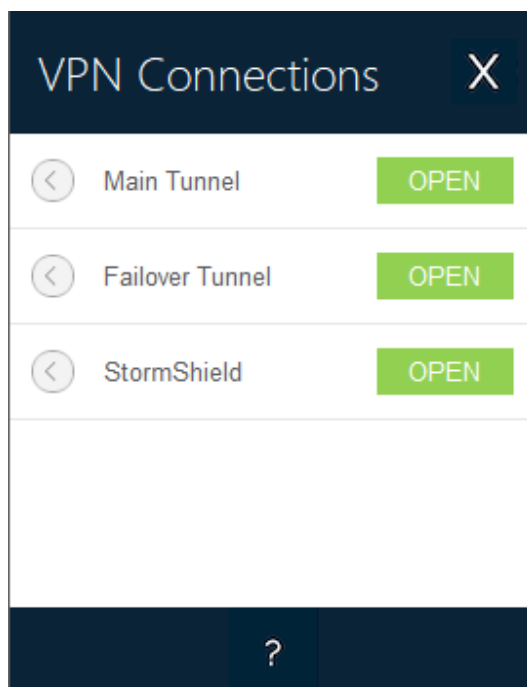


The tunnel that has just been configured now appears in the VPN configuration tree of the main interface.

Double-click the tunnel to open it or use the tabs of the main interface for further configuration.

8 Connection Panel

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



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



Refer to chapter 20 Configuring the Connection Panel.

To open a VPN connection, simply click the relevant **OPEN** button.

To increase the height of the **Connection Panel** window to display a greater number of tunnels at once, press the Ctrl key and the + key on the numeric keypad.

To decrease the height of the **Connection Panel** window, press the Ctrl key and the - key on the numeric keypad.

The icon to the left of the connection name indicates the status of the connection:



Connection closed.

Click this icon to open the VPN configuration for this connection in the **Configuration Panel**.

Caution: Access to the **Configuration Panel** may be restricted (see section 25.1.3 Restricting access to 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 buttons on the **Connection Panel** have the following function:



Opens the **About...** window.



Opens the **Configuration Panel**.

Caution: Access to the **Configuration Panel** may be restricted (see section 25.1.3 Restricting access to the Configuration Panel).



Closes the **Connection Panel**.

The following keyboard shortcuts are available for the **Connection Panel**:

Esc (or Alt+F4)	Closes the Connection Panel .
Ctrl+Enter	Opens the Configuration Panel (if enabled).
Ctrl+O	Opens the selected VPN connection.
Ctrl+W	Closes the selected VPN connection.
Up/down arrows	Moves the cursor from one VPN connection to another.

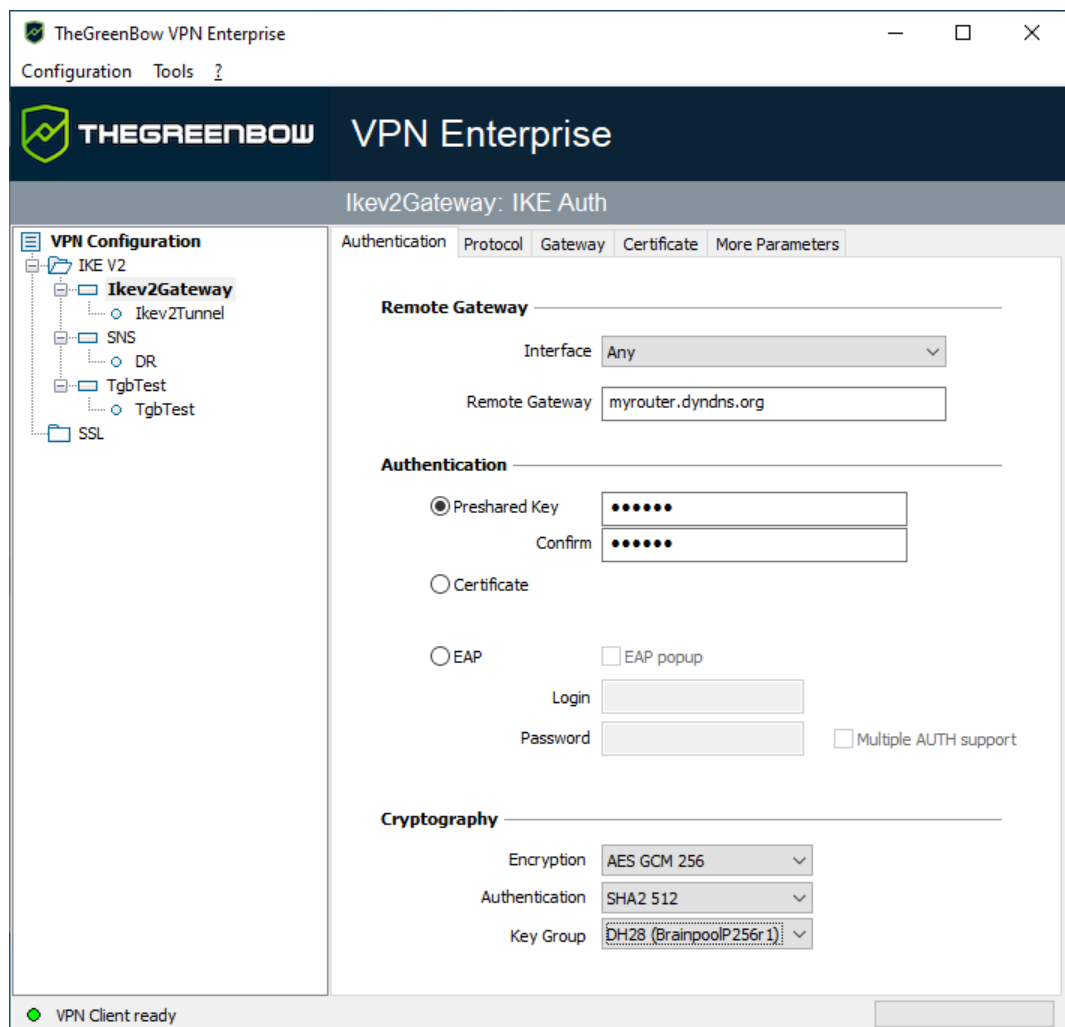
9 Configuration Panel

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

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

It includes the following items:

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



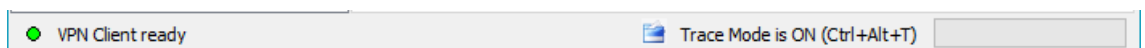
9.1 Menus


The following menus are available in the **Configuration Panel**:

- Configuration
 - Save
 - Import: [Import a VPN configuration](#)
 - Export: [Export a VPN configuration](#)
 - [Configuration Wizard](#)
 - Quit: Close all open VPN tunnels and quit the software
- Tools
 - [Connection Panel](#)
 - [Connections Configuration](#)
 - **Console**: IKE connection traces window
 - Reset IKE: Restart the IKE service
 - Options: Protection, display, startup, language management, PKI management options
- ?
 - Online support: Access to online support
 - [Check for update](#): Check for available updates
 - Purchase license online: Access the online store
 - [Activation Wizard...](#)
 - [About...](#)

9.2 Status bar

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



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

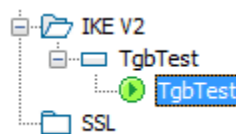
9.3 Shortcuts

Ctrl+S	Save the VPN configuration
Ctrl+Enter	Switch to the Connection Panel
Ctrl+D	Opens the VPN Console window
Ctrl+Alt+R	Restart the IKE service
Ctrl+Alt+T	Enable the trace mode (log generation)

9.4 VPN configuration tree

9.4.1 Usage

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



Under the root called “VPN Configuration”, there are two levels that allow you to create the following respectively:





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

1. IPsec IKEv2 tunnel
 - [IKEv2 \(IKE Auth\): Authentication](#)
 - [IKEv2 \(Child SA\): IPsec](#)
2. SSL tunnel (OpenVPN)
 - [SSL: TLS](#)



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

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

You can edit and change the name of any item in the tree by clicking twice in a row on it, without double-clicking.

If there are any unsaved changes in the VPN configuration, the modified item is shown in bold. As soon as the tree is saved, all text formatting is removed.



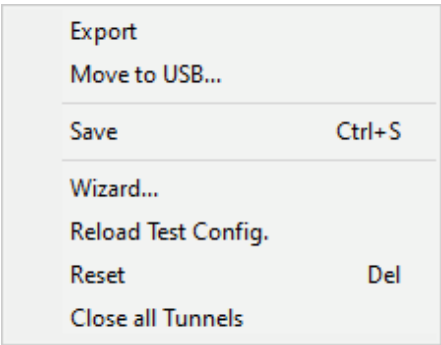
Two items in the tree cannot have the same name. The software displays a message to the user if the name entered is already in use.

9.4.2 Contextual menus

9.4.2.1 VPN configuration

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

Export	Exports the entire VPN configuration.
Save	Saves the VPN configuration.
Configuration Wizard	Opens the VPN Configuration Wizard .
Reload default configuration	The Windows Enterprise VPN Client comes with a default VPN configuration that can be used to test opening a VPN tunnel. This menu is used to reload the default configuration at any time.
Reset	Resets the VPN configuration after confirmation by the user.
Close all tunnels	Closes all open tunnels.



9.4.2.2 IKEv2, SSL

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



Export	Exports all IKEv2 tunnels.
Save	Saves all IKEv2 tunnels.
New IKE Auth	Creates a new IKE Auth/TLS.
New TLS	The parameters of this new IKE Auth/TLS will be filled in with default values.
Paste IKE Auth	Adds an IKE Auth/TLS that has been previously copied to the clipboard.
Paste TLS	

9.4.2.3 IKE Auth

Right-clicking an IKE Auth displays the following contextual menu:

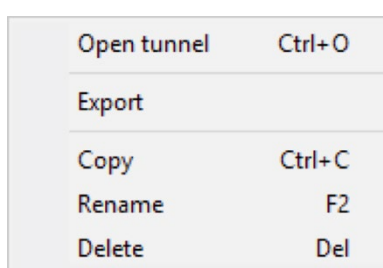




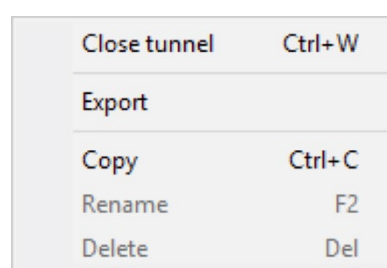
Copy	Copies the selected IKE Auth to the clipboard.
Rename¹	Renames the IKE Auth.
Delete²	Deletes the IKE Auth, including any associated Child SAs, after confirmation by the user.
New Child SA	Adds a new Child SA to the selected IKE Auth.
Paste Child SA	Adds the Child SA that has been copied to the clipboard to the IKE Auth.

9.4.2.4 Child SA or TLS

Right-clicking a Child SA or TLS displays the following contextual menu:



Menu with tunnel closed



Menu with tunnel open

Open tunnel	Displayed if the VPN tunnel is closed. Opens the selected (Child SA or TLS) tunnel.
Close tunnel	Displayed if the VPN tunnel is open. Closes the selected (Child SA or TLS) tunnel.
Export³	Exports the selected Child SA/TLS.
Copy	Copies the selected Child SA/TLS.
Rename⁴	Renames the selected Child SA/TLS.
Delete⁵	Deletes the selected Child SA/TLS after confirmation by the user.

¹ This menu is disabled as long as one of the tunnels of the relevant IKE Auth is open.

² *ibid*

³ This function allows users to export the entire tunnel, i.e. both the 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).

⁴ This menu is disabled while the tunnel is open.

⁵ *ibid*

9.4.3 Shortcuts

The following shortcuts are available for tree management:

F2	Used to edit the name of the selected phase
Del	Deletes a selected phase, following confirmation by the user. If the actual VPN configuration is selected (root of the tree), the software asks whether a full reset of the configuration should be performed.
Ctrl+O	Opens the corresponding VPN tunnel if a Child SA/TLS is selected.
Ctrl+W	Closes the corresponding VPN tunnel if a 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 IKE Auth. If an IKE Auth is selected, creates a Child SA/TLS.
Ctrl+S	Saves the VPN configuration.



10 TrustedConnect Panel

10.1 Introduction

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

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



As of version 7.5 of the Windows Enterprise VPN Client, the **TrustedConnect Panel's** behavior changes according to the compliance level reported by the Secure Connection Agent (SCA), which determines whether a workstation should be allowed to access the corporate network (see section 24.2.3 Selecting the tunnel to open according to the compliance level).

10.2 Interface

When it is used for the first time, the **TrustedConnect Panel** is displayed in the center of the screen.

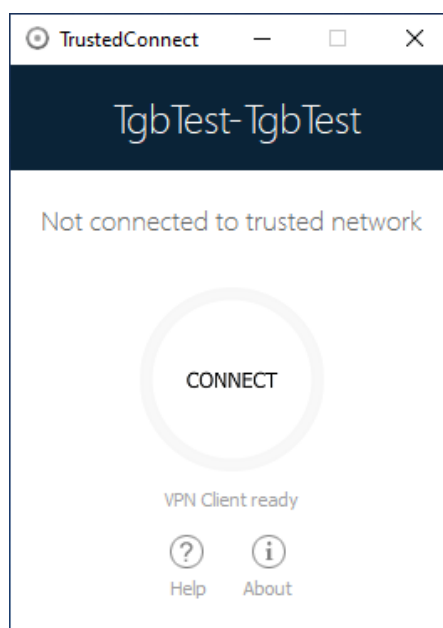
For subsequent uses, the **TrustedConnect Panel** memorizes the place to which the user has moved it.

The interface of the **TrustedConnect Panel** includes the following items:

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



As of version 7.4 of the Windows Enterprise VPN Client, you can enable an option that allows users to select the desired connection by clicking the title banner (see section 10.9 Choosing the connection).



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

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

To quit the software right-click the **TrustedConnect** icon in the notification area and then select **Quit**.



Administrators can disable the disconnect button. In this case, a tunnel can no longer be closed once it is open. Refer to section 21.5 Disabling the disconnect button for more details.

10.3 Taskbar icon and color codes

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

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



This state means that the **TrustedConnect Panel** is not managing any connection on the workstation. Generally, this state is encountered when the user explicitly requests the VPN connection to be closed.



This state means that the workstation is directly connected to the corporate network, which is considered as a trusted network.



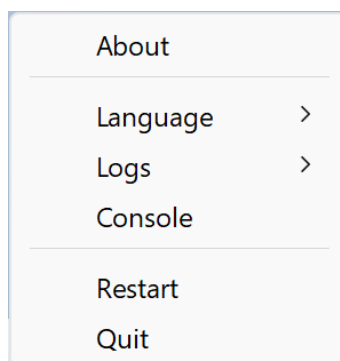
This state means that the workstation is connected to the corporate network through a VPN connection. The workstation thus is physically located on a network that is not considered as trusted.



This state means that the VPN connection could not be established.

10.4 Contextual menu

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



The contextual menu contains the following items:

About...	Opens the About... window.
Language	Used to switch between French and English.
Logs	Used to start logging. Once logging is started, two additional options are shown to display the logs and stop logging.
Console	Opens the Console window with VPN traces.
Restart	Restarts the tunnel.
Quit	Closes the VPN tunnel and quits the software.



Administrators can disable the menu or some of its options. Refer to section 21.6 Removing menu items for more details.

10.5 Usage

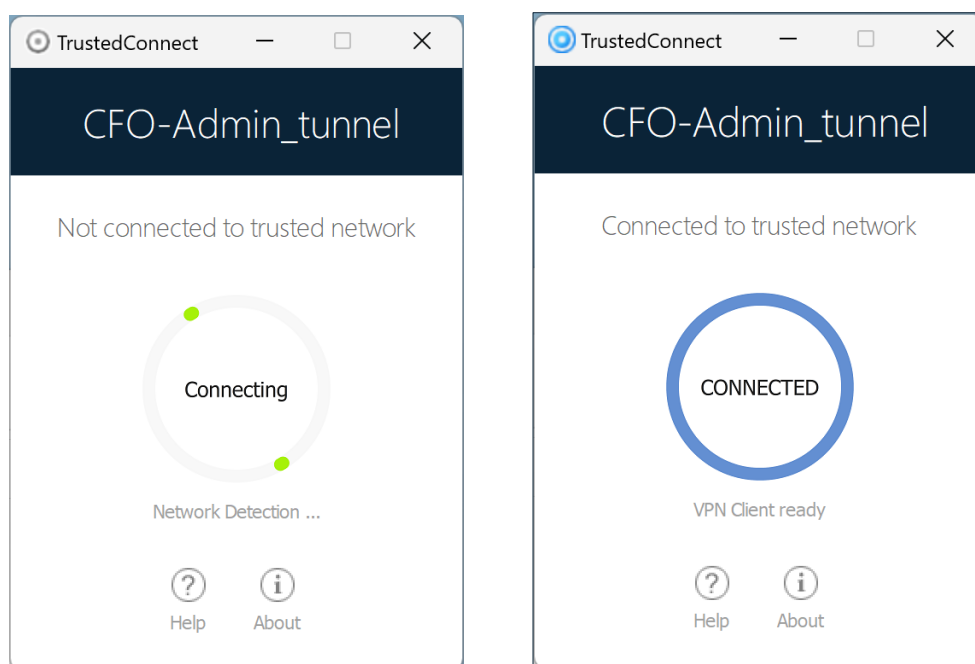
There are two types of use depending on whether the workstation is already connected to the corporate network or not.



As of version 7.3 of the Windows Enterprise VPN Client, you can disable the TND function to open a tunnel even when the workstation is located on the trusted network. Refer to section 21.2.3 Disabling TND for more details.

10.5.1 Workstation connected to corporate network

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



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



Refer to the “Deployment Guide”.

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

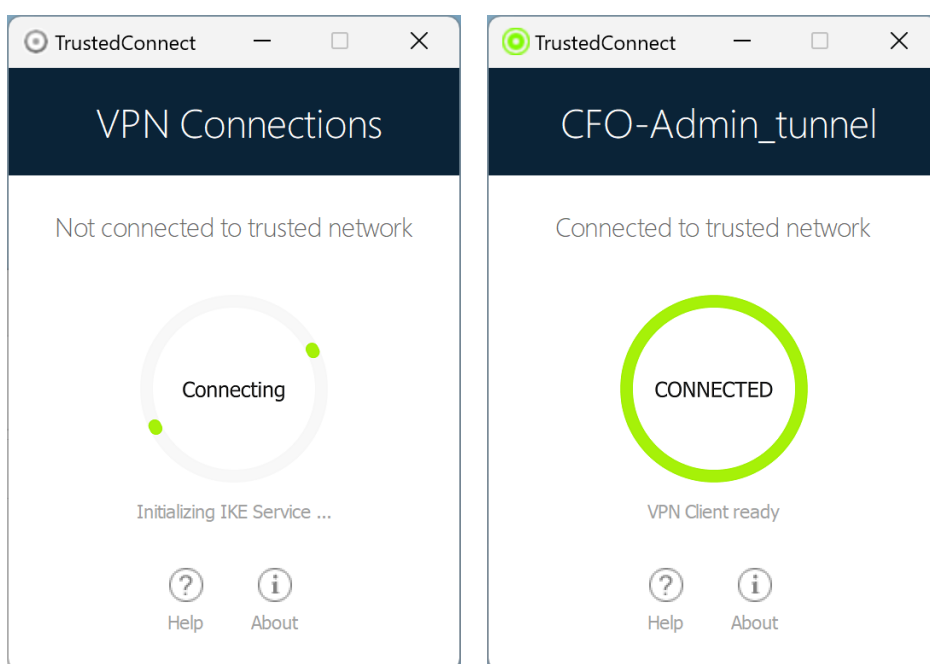


As of version 7.3 of the Windows Enterprise VPN Client, you can disable the THN function to open a tunnel even when the workstation is located on the trusted network. Refer to section 21.2.3 Disabling TND for more details.

10.5.2 Workstation not connected to corporate network

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

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

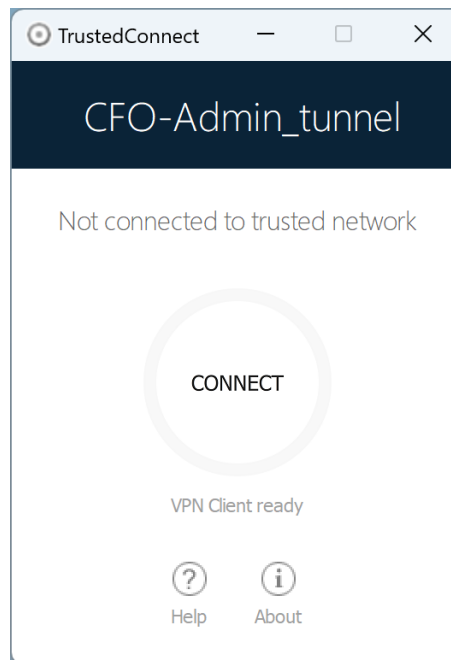


Once the connection is established, the window of the **TrustedConnect Panel** automatically minimizes either to the taskbar or to the notification area, depending on the behavior that the administrator has configured.

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

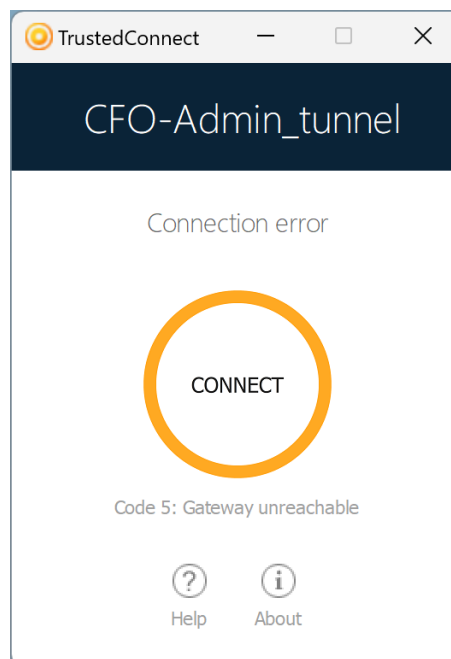
When the tunnel is mounted and the workstation is shown as being on the corporate network, you can click inside the connection status indicator ring to stop the tunnel.

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



10.6 Error cases

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



Contact the network administrator to resolve the issue. The error code shown may provide some indication or explanation as to the issue encountered. If

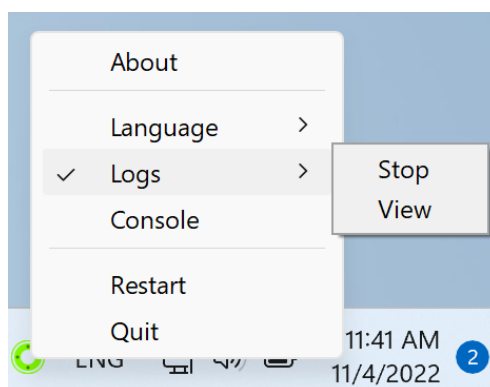
the administrator requests the logs, refer to the procedure described in the next section.

The list of error codes is provided in the appendix of this document (see section 29.3 TrustedConnect Panel diagnostics).

10.7 Generating logs and Console

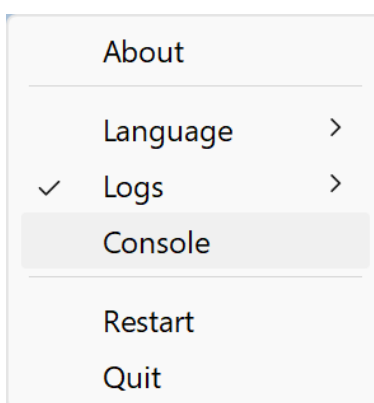
The **TrustedConnect Panel** allows you to create and view logs.

To initiate the creation of log files, right click the **TrustedConnect** icon in the notification area, select **Logs**. A check mark next to the menu item indicates that logging is enabled:



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

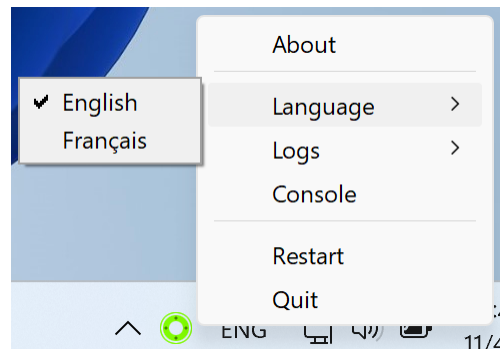
You can now also display the **Console** window with VPN traces directly from the **TrustedConnect Panel's** contextual menu.



To find out how to use the **Console** window, refer to section 26.2 Console.

10.8 Selecting the language

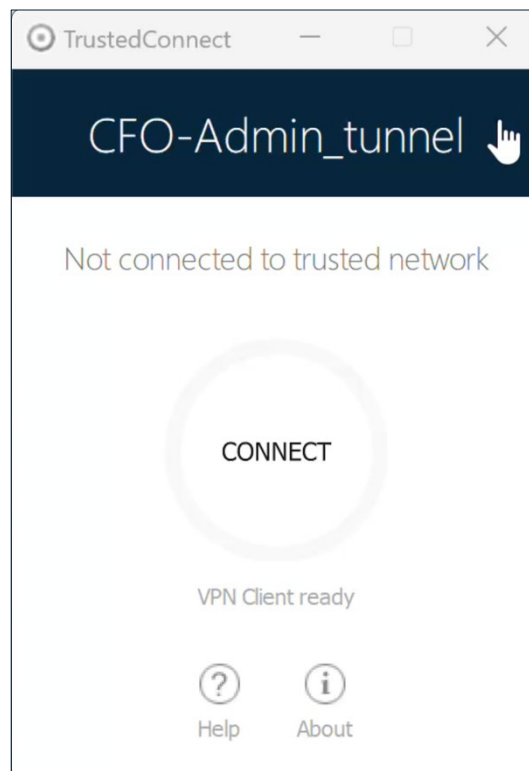
The **TrustedConnect Panel** allows you to select the software's display language: French or English. To select the language, access the menu and select the **Languages** item. In the submenu, select **English** or **Français**:



10.9 Choosing the connection

If you enabled this option using the MSI property `DIALERBEHAVIOR` when you installed the VPN Client (refer to the “Deployment Guide”), as of version 7.4 of the Windows Enterprise VPN Client, users can choose between the connections available in the VPN configuration, if it contains two or more.

When this option is enabled, users will see the mouse pointer change into a hand when it hovers over the connection name in the **TrustedConnect Panel**'s title banner after having closed any open tunnel.





The pointer does not change into a hand and users cannot change active connections while a connection is open or being initialized or closed.

To change connection, follow these steps:

3. If the **TrustedConnect Panel** is not displayed on the screen, click its icon in the taskbar to display it.
4. If a connection is open, click the **CONNECTED** button to close the tunnel. The connection status indicator ring becomes gray, and the button label changes to **CONNECT**.
5. Click the connection name in the blue title banner. The name of the next connection available in the configuration is displayed. Keep clicking to scroll through the names of all the connections available in the configuration until you reach the one you want to enable.
6. Click the **CONNECT** button. The VPN Client will attempt to establish the connection. If it succeeds, the connection status indicator ring becomes green and the button label changes to **CONNECTED**. The **TrustedConnect Panel** is then minimized to the taskbar.



The **TrustedConnect Panel** stores the last connection that has been enabled. If you quit the **TrustedConnect Panel**, this connection will open automatically the next time you start.



When the **TrustedConnect Panel** is configured with several connections of which at least one is in GINA mode, make sure to account for the information provided in the paragraph entitled [Special use case](#) in section 22.1 Overview.



For error cases, refer to section 10.6 Error cases.

10.10 Current limitations

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

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

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

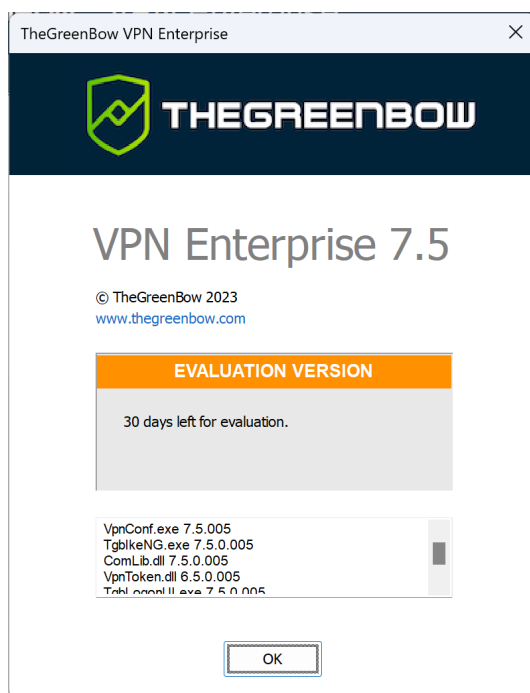
The **TrustedConnect Panel** (`VpnDialer.exe`) is currently only available in French and English.



11 “About...” window

The **About...** window can be accessed as follows:

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



The **About...** window displays the following information:

- The name and version number of the software
- A web link to TheGreenBow's website
- When the software is activated, the license number and e-mail address used for activation
- During the software trial period, the number of days remaining before the trial period expires
- The version numbers of all software components¹

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

12 Importing and exporting the VPN configuration

12.1 Importing a VPN configuration

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

- From the **Configuration** menu in the **Configuration Panel** (main interface), choose **Import**
- From the command line, use the `/import` option¹



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

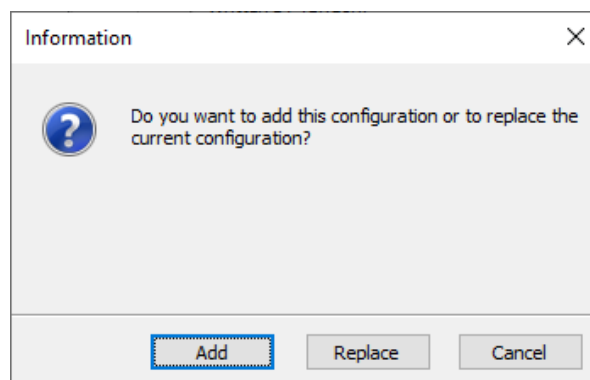


As of version 6.8 of the Windows Enterprise VPN Client, the function that allows you to double-click on a VPN configuration file to import it is no longer available.



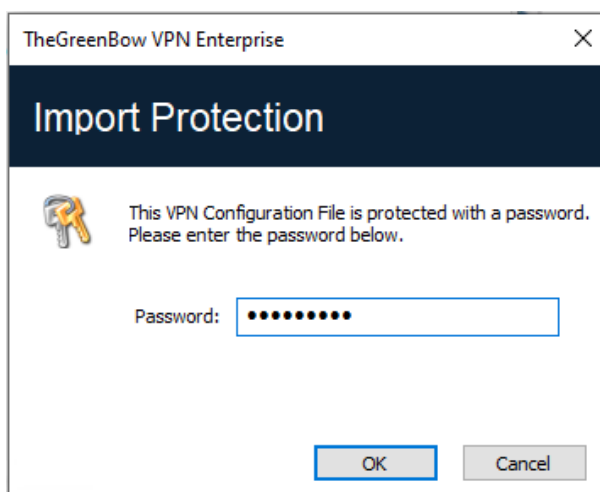
The Windows Enterprise VPN Client can check the integrity of the VPN configuration file (see MSI property `SIGNFILE` in the “Deployment Guide”). In this case, a signature is generated during export and the integrity of the file is checked during import.

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

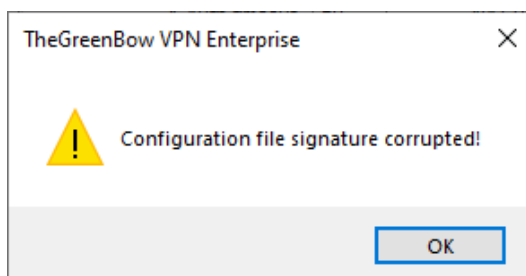


¹ The use of command-line options within the software is covered in the “Deployment Guide”. In particular, it details all the options available for importing a VPN configuration: `/import`, `/add`, `/replace` or `/importonce`.

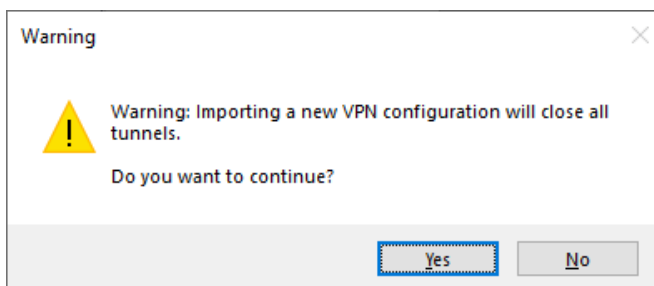
If the imported VPN configuration has been exported with a password protection (see section 12.2 Exporting a VPN configuration below), users will have to provide the password.



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



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



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



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

12.2 Exporting a VPN configuration

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

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



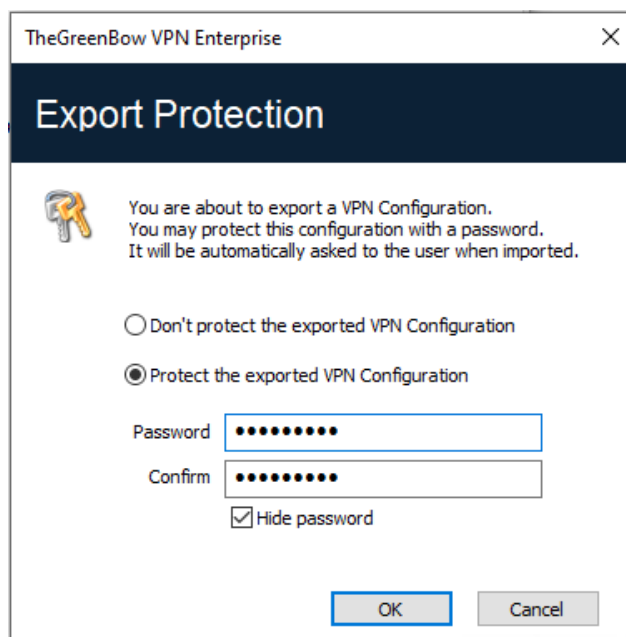
By default, the extension of exported VPN configuration files is `.tgb`.



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

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

¹ The use of command-line options within the software is covered in the "Deployment Guide". In particular, it details all the options available for exporting a VPN configuration: `/export` or `/exportonce`. Regardless of the method used, the export starts with the choice of protection for the exported VPN configuration: it can be exported with (encryption) or without (clear text) password protection. If a password has been set, users will be required to enter it when importing.



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



As of version 7.3, the password must follow ANSSI recommendations, i.e. be at least 16 characters in length and use a 90-character alphabet, including at least one uppercase character, one lowercase character, and one special character.

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

12.3 Merging VPN configurations

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

12.4 Splitting a VPN configuration

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

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

13 Configuring a VPN tunnel

13.1 SSL or IPsec IKEv2 VPN

The Windows Enterprise VPN Client allows you to create and configure several types of VPN tunnels.

It also allows you to open them simultaneously.

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

- IPsec IKEv2
- SSL

The procedure used to create a new VPN tunnel is described in the previous sections: 7 Configuration Wizard and 9.4 VPN configuration tree > 9.4.2 Contextual menus.



We recommend configuring IKEv2 tunnels with a certificate. Refer to chapter 27 Security recommendations.

13.2 Editing and saving a VPN configuration

The Windows Enterprise VPN Client allows you to modify the VPN tunnels and test these modifications “on-the-fly” without saving the VPN configuration.

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

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

- Ctrl+S shortcut
- **Configuration** > **Save** menu item

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

13.3 Configuring an IPsec IKEv2 tunnel

13.3.1 IKE Auth: Authentication

Authentication
Protocol
Gateway
Certificate

Remote Gateway

Interface
Any

Remote Gateway
tgbtest.dyndns.org

Integrity

☒ Preshared Key

.....

Confirm.....

☐ Certificate

☐ EAP

☐ EAP popup

Login

Password

☐ Multiple AUTH support

Cryptography


Encryption
AES GCM 256

Integrity
SHA2 512

Key Group
DH21 (ECP 521)

13.3.1.1 Addresses

Interface Name of the network interface on which the VPN connection is open. The software can decide automatically which interface to use by selecting **Any**.

A screenshot of a configuration window showing a dropdown menu for the 'Interface' field. The dropdown is open, displaying three options: 'Any' (highlighted in blue), '192.168.205.52', and 'Any'.

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



When the network interface has several IP addresses, you can specify the address using the dynamic parameter `local_subnet` (see section 25.2.4 Displaying more parameters). Only IPv4 addresses are supported. The address format to be entered as a dynamic parameter value is as follows: `aaa.bbb.ccc.ddd/xx`. If the subnet mask is omitted by entering only `aaa.bbb.ccc.ddd`, the address will correspond to `aaa.bbb.ccc.ddd/32`.

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

13.3.1.2 Authentication

Preshared Key Password or key shared by the remote gateway.



The preshared key is an easy way to configure a VPN tunnel. However, it is less flexible in terms of security management than the use of certificates. Refer to chapter 27 Security recommendations.

Certificate Use a certificate to authenticate the VPN connection.



Using the **Certificate** option strengthens the security in terms of VPN connection management (mutual authentication, verification of validity periods, revocation, etc.). Refer to chapter 27 Security recommendations.



Refer to the dedicated chapter 18 Managing certificates.



EAP The Extensible Authentication Protocol (EAP) mode is used to authenticate the user based on a login name and password. When the EAP mode is selected, a pop-up window will prompt the user to enter a login name and password every time the tunnel is opened.

When the EAP mode is selected, you can choose to display a prompt for the EAP login name and password every time the tunnel is opened (using the **EAP popup** checkbox) or to store them in the VPN configuration by entering them in the **Login** and **Password** fields.

We recommend not to use the latter mode (see chapter 27 Security recommendations).

Multiple AUTH support Enables the combination of certificate and EAP authentications.¹

13.3.1.3 Cryptography

Encryption	Encryption algorithm negotiated during the authentication phase ² : Auto ³ , AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
-------------------	--

Integrity	Integrity algorithm negotiated during the authentication phase ⁴ : Auto ⁵ , SHA2 256, SHA2 384, SHA2 512.
------------------	--

Key Group	Length of Diffie-Hellman key ⁶ : Auto ⁷ , DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521) DH28 (BrainpoolP256r1).
------------------	---

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

² Refer to chapter 27 Security recommendations on the choice of algorithm.

³ **Auto** means that the VPN Client automatically adapts to the gateway parameters.

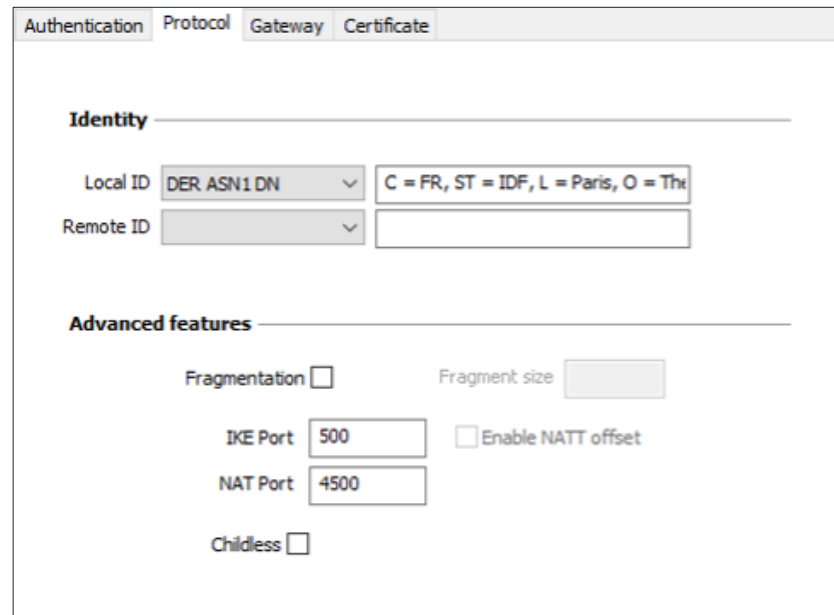
⁴ See note 1.

⁵ See note 2.

⁶ See note 1.

⁷ See note 2.

13.3.2 IKE Auth: Protocol



The screenshot shows the 'IKE Auth: Protocol' configuration window. It has four tabs: 'Authentication', 'Protocol' (selected), 'Gateway', and 'Certificate'. The 'Protocol' tab contains two main sections: 'Identity' and 'Advanced features'. In the 'Identity' section, there is a 'Local ID' dropdown menu set to 'DER ASN1 DN' and a text field containing 'C = FR, ST = IDF, L = Paris, O = The'. Below it is a 'Remote ID' dropdown menu and an empty text field. The 'Advanced features' section includes a 'Fragmentation' checkbox, a 'Fragment size' input field, an 'IKE Port' input field set to '500', a 'NAT Port' input field set to '4500', an 'Enable NATT offset' checkbox, and a 'Childless' checkbox.



If you use an IPsec DR gateway, you must add the dynamic parameter `nonce_size` (see section 25.2.4 Displaying more parameters) and set its value to 16. These gateways will not accept any other nonce size.

13.3.2.1 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:

- **IPV4 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 e-mail address (type = USER FQDN), e.g. support@thegreenbow.com
- **IPV6 Address:** an IPv6 address (type = IPV6 ADDR), e.g. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3
- **DER ASN1 DN:** the X.509 subject of a certificate (type = DER ASN1 DN); this field is automatically filled in with the subject of an X.509 certificate when the tunnel is associated with a user certificate (see chapter 18 Managing certificates)

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



Remote ID Remote ID is the identifier of the authentication phase that the VPN Client expects to receive from the VPN gateway.

According to the type selected, this identifier can be any of the following:

- **IPV4 Address:** an IPv4 address (type = IPV4 ADDR), e.g. 80.2.3.4
- **DNS:** a domain name (type = FQDN), e.g. router.mydomain.com
- **Email:** an e-mail address (type = USER FQDN), e.g. admin@mydomain.com
- **IPV6 Address:** an IPv6 address (type = IPV6 ADDR), e.g. 2345:0:9d38:6ab8:1c47:3a1c:a96a:b1c3
- **DER ASN1 DN:** the X.509 subject of a certificate (type = DER ASN1 DN)
- **KEY ID:** a character string (type = KEY ID), e.g. 123456

This setting is required since version 6.8 for security reasons.

13.3.2.2 Advanced features

IKEv2 fragmentation	<p>Enables IKEv2 packet fragmentation in accordance with RFC 7383.</p> <p>This function prevents IKEv2 packets from being fragmented by the IP network they're passing through.</p> <p>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 Init exchanges (during the IKE Authentication phase) use the UDP protocol and port 500 by default. IKE port configuration can bypass the networking hardware (firewalls, 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 Auth exchanges, IKE Child SA exchanges, and IPsec traffic use the UDP protocol and port 4500 by default. NAT port configuration can bypass the networking hardware (firewalls, 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	<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>
Childless	<p>When this mode is enabled, the VPN Client will attempt to initiate IKE exchanges without creating any Child SA in accordance with RFC 6023. We recommend using this mode.</p>



13.3.3 IKE Auth: Gateway

Authentication	Protocol	Gateway	Certificate	More Parameters
Dead Peer Detection (DPD)				
Check interval <input type="text" value="30"/> sec.				
Max. number of retries <input type="text" value="5"/>				
Delay between retries <input type="text" value="15"/> sec.				
Lifetime				
Lifetime <input type="text" value="1800"/> sec.				
Gateway related parameters				
Redundant Gateway <input type="text"/>				
Retransmissions <input type="text" value="3"/>				
Gateway timeout <input type="text" value="5"/> sec.				

13.3.3.1 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.



A possible cause for the DPD function not working after a tunnel has been mounted could be that the gateway's IP address belongs to the remote network, either due to a local configuration or because that's the address the gateway sent. If this is the case, all IKE packets intended for the gateway are routed through the tunnel, instead of being sent outside of it. This is what's causing the issue.

You therefore need to check whether this is the case and make the required changes where necessary to correct the issue.

13.3.3.2 Lifetime

Lifetime Lifetime of the IKE Authentication phase.

The lifetime is expressed in seconds.

The default value is 14,400 seconds (4 h).

13.3.3.3 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.



The **Redundant Gateway** function cannot be configured together with the **Fallback Tunnel** function. You must choose one or the other, failing which the VPN Client could invoke undefined behavior.

Refer to chapter 14 Redundant gateway.

Retransmissions Number of IKE protocol message resends before failure.

Gateway timeout Delay between two retransmissions

13.3.4 IKE Auth: Certificate

Refer to chapter 18 Managing certificates.

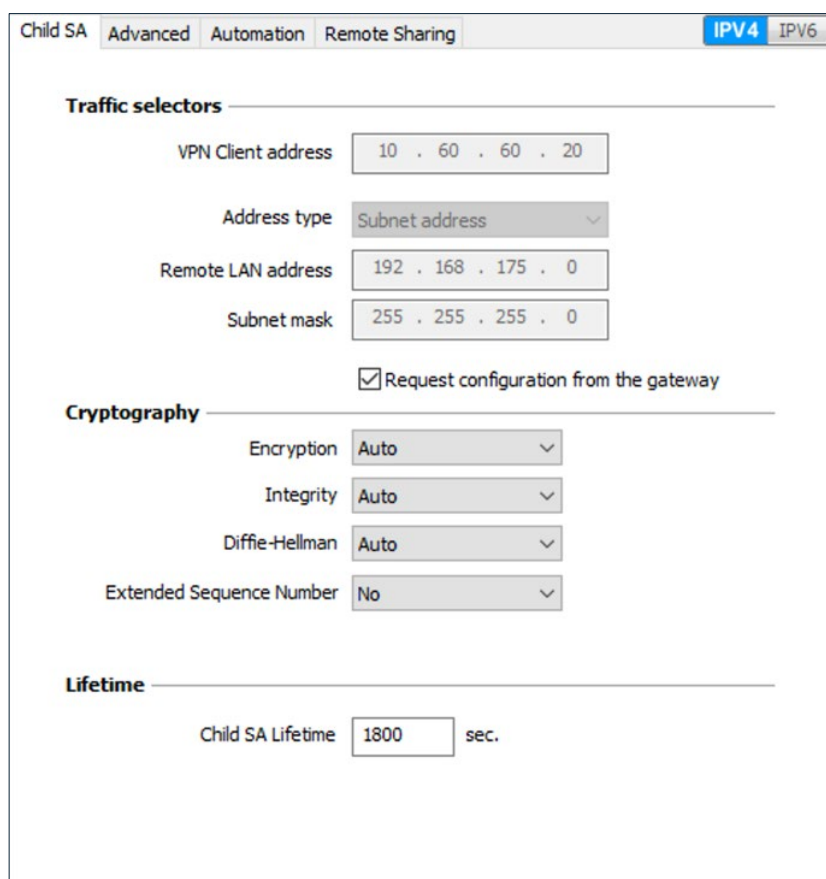
13.3.5 Child SA: Overview

The purpose of the Child SA (Security Association IPsec) of a VPN tunnel 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 VPN configuration 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 configuration tree. You do not need to save a VPN configuration for it to be taken into account. The tunnel can be tested with the modified configuration immediately.

13.3.6 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.

13.3.6.1 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.



The default size of the local virtual network is 24. To use another network size (e.g. 32), you must add the dynamic parameter `local_virtual_network_size` set to the desired value (possible values: 1 to 32; see section 25.2.4 Displaying more parameters).

Address type	<p>The endpoint of the tunnel can be a network or a remote workstation.</p> <p> Refer to section 13.3.6.5 Configuring the address type below.</p>
Request configuration from the gateway	<p>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 address, remote LAN address, subnet mask, and DNS addresses.</p> <p>When this option is checked, all corresponding fields are disabled (uneditable).</p> <p>They are filled in dynamically as the tunnel is opened with the values sent by the VPN gateway during the Mode CP exchange.</p> <div> Mode CP allows the gateway to configure up to 16 subnetworks. In this case, only the first subnetwork must be entered in the Traffic Selectors section. All the subnetworks configured by the gateway must be entered in the Console. </div> <div> If more than 16 subnetworks are configured by the gateway, only the first 16 will be taken into account. </div>

13.3.6.2 Cryptography

Encryption	<p>Encryption algorithm negotiated during the IPsec phase¹:</p> <p>Auto², AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).</p>
Integrity	<p>Integrity algorithm negotiated during the IPsec phase³:</p> <p>Auto⁴, SHA2 256, SHA2 384, SHA2 512.</p>
Diffie-Hellman	<p>Length of Diffie-Hellman key⁵:</p>

¹ Refer to chapter 27 Security recommendations on the choice of algorithm.

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

³ See note 1.

⁴ See note 2.

⁵ See note 1.



Auto¹, DH14 (MODP 2048), DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521), DH28 (BrainpoolP256r1).

Extended Sequence Number

Allows you to use 64-bit extended sequence numbers (see RFC 4304):

Auto², No, Yes. We recommend using the ESN mode.



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.

13.3.6.3 Lifetime

Child SA Lifetime

Time interval, expressed in seconds, between two renegotiations.
The default value for the Child SA lifetime is 1,800 s (30 min).

13.3.6.4 IPv4/IPv6

IPv4/IPv6

 Refer to chapter 17 IPv4 and IPv6.

¹ See note 2.

² See note 2.

13.3.6.5 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 address** and **End address**:

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).



“All traffic through the VPN tunnel” configuration

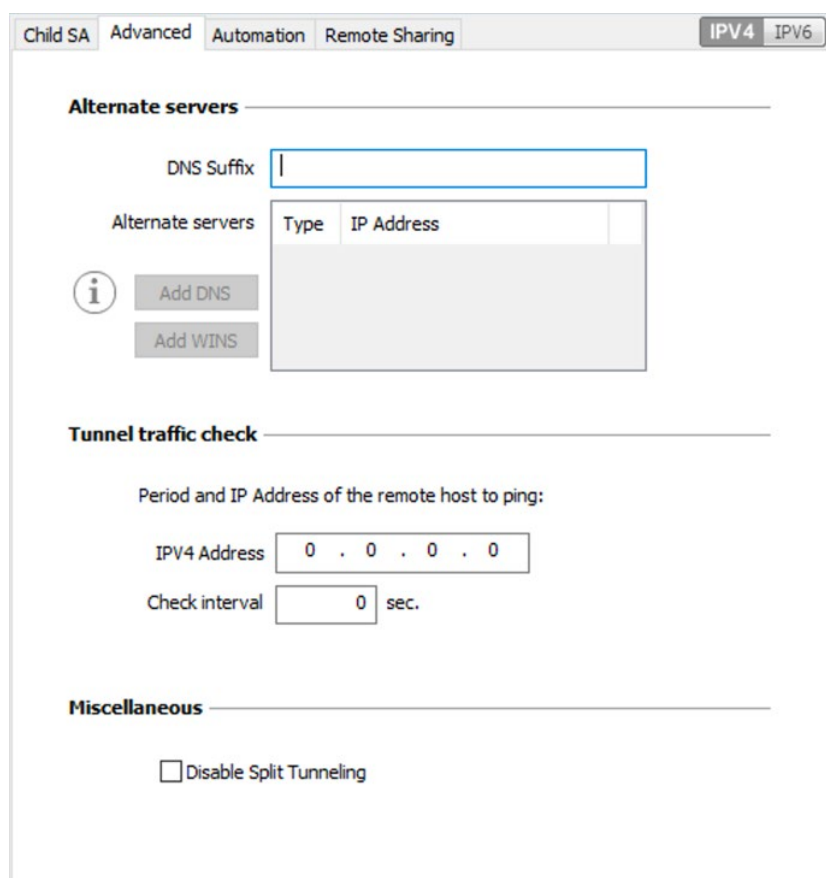
The VPN Client can be configured so that all the workstation's outbound traffic goes through the VPN tunnel. To implement this function, select **Subnet address** as the address type and specify 0 . 0 . 0 . 0 as the **Remote LAN address** and **Subnet mask**.



Several VPN Client configuration guides for various VPN gateways are available on our website at:

<https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-routers/>.

13.3.7 Child SA: Advanced



Child SA **Advanced** Automation Remote Sharing **IPv4** **IPv6**

Alternate servers

DNS Suffix

Alternate servers

Type	IP Address

i Add DNS Add WINS

Tunnel traffic check

Period and IP Address of the remote host to ping:

IPv4 Address

Check interval sec.

Miscellaneous

☐ Disable Split Tunneling

13.3.7.1 Alternate servers

DNS Suffix

Domain suffix to be added to all machine names, e.g. `mozart.dev.thegreenbow`.

This is an optional parameter. When it is specified, the VPN Client will try to translate the machine address without adding the DNS suffix. However, if translation fails, the DNS suffix will be added, and the Client will try to translate the address again.

Alternate servers

Table containing the IP addresses of the DNS (maximum 2) and WINS (maximum 2) servers available on the remote network. The IP addresses will be IPv4 or IPv6 addresses depending on the network type configured in the **Child SA** tab.



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

13.3.7.2 Tunnel traffic check

Traffic check after opening

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.

13.3.7.3 Miscellaneous

Disable Split Tunneling

When this option is selected, only the traffic going through the tunnel is authorized.¹

13.3.8 Child SA: Automation



Refer to chapter 15 Automation.

13.3.9 Child SA: Remote sharing



Refer to chapter 19 Remote Desktop Sharing.

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. When combined with the **All traffic through the VPN tunnel** configuration (see section 13.3.6.5 Configuring the address type), this option guarantees the complete leakproofness of the workstation, provided that the VPN tunnel is open. We recommend using this mode.



13.4 Configuring an SSL/OpenVPN tunnel

13.4.1 Introduction

Versions 6 and later of the Windows Enterprise VPN Client can be used to open SSL VPN tunnels.

SSL VPN tunnels established by the Windows Enterprise VPN Client are compatible with OpenVPN and can establish secure connections with all gateways implementing this protocol.

13.4.2 SSL: Authentication

Authentication Security Gateway Establishment Automation Certificate Remote Sharing

Remote Gateway

Interface Any

Remote Gateway remotehost

Authentication

Select Certificate

Extra Authentication

☒ Enabled ☒ Popup when tunnel opens

Login

Password

13.4.2.1 Remote Gateway

Interface Name of the network interface on which the VPN connection is open. The software can decide automatically which interface to use by selecting **Any**.

Interface

Any

Any

Ethernet0

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.

13.4.2.2 Authentication

Select Certificate

Choose a certificate for VPN connection authentication.

 Refer to the dedicated chapter 18 Managing certificates.

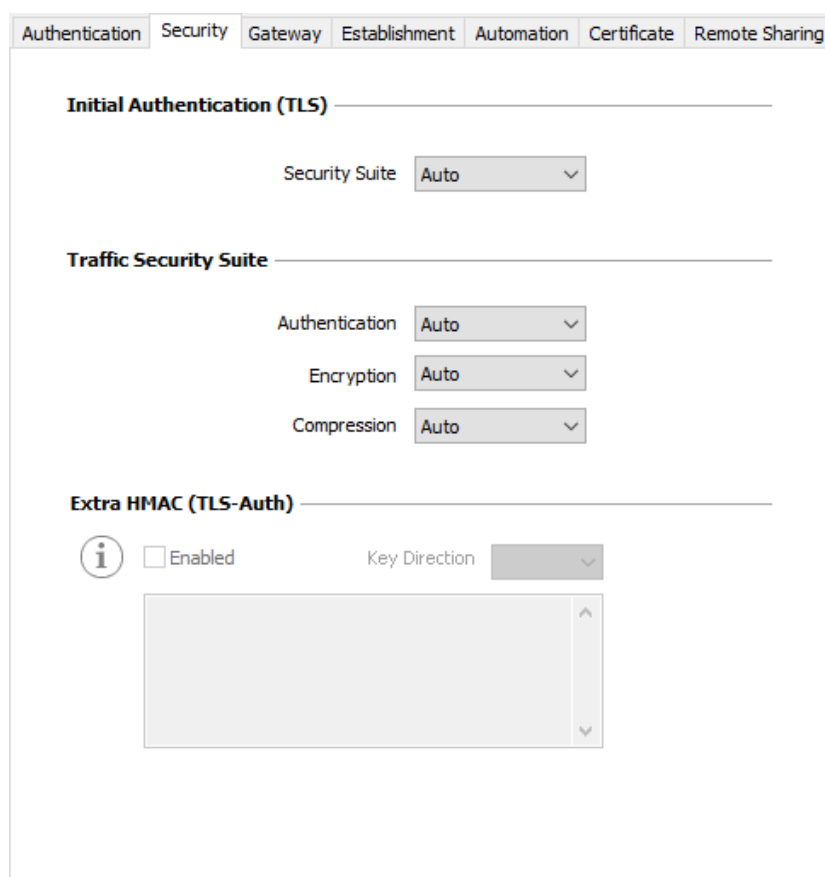
13.4.2.3 Extra Authentication

Extra Authentication

This option increases the security level by asking the user to enter a login name and password whenever a tunnel is opened.

When the box **Popup when tunnel opens** is checked, users will be prompted for their login name and password whenever they open the tunnel. When it is unchecked, the login name and password must be entered here permanently. Users therefore will not need to enter them every time they open the tunnel.

13.4.3 SSL: Security



Authentication Security Gateway Establishment Automation Certificate Remote Sharing

Initial Authentication (TLS)

Security Suite Auto


Traffic Security Suite

Authentication Auto

Encryption Auto

Compression Auto

Extra HMAC (TLS-Auth)

 ☐ Enabled Key Direction



13.4.3.1 Initial Authentication (TLS)

Security Suite This parameter is used to configure the security level of the authentication phase during the SSL exchange.

- **Auto:** All cryptography suites (except null) are sent to the gateway, which will use the best fit.
- **TLS v1.2 – Medium:** Only “medium” cryptography suites are sent to the gateway. In the current version, these are suites that use 128-bit encryption algorithms.
- **TLS v1.2 – 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.
- **TLS v1.3:** TLS 1.3 suite negotiated with the gateway, including:
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_CCM_SHA256
 - TLS_AES_128_CCM_8_SHA256

For further information:

<https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>

13.4.3.2 Traffic Security Suite

Authentication Authentication algorithm negotiated for traffic:
Auto¹, SHA-224, SHA-256, SHA-384, SHA-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:
Auto², AES-128-CBC, AES-192-CBC, AES-256-CBC.

Compression Traffic compression: Auto³, LZ0, No, LZ4.

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

² *ibid*

³ *ibid*

13.4.3.3 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** in the gateway.
- **Server**: The key direction must be defined as **Client** in the gateway.

13.4.4 SSL: Gateway

The screenshot shows the 'Gateway' tab of the VPN Client configuration window. It contains the following sections and controls:

- Dead Peer Detection (DPD)**:
 - Ping Gateway (s):
 - Detect Gateway (s):
 - On Dead Peer Detection: ☐ Close tunnel, ☐ Re-open tunnel
- Gateway related parameters**:
 - ☐ Explicit Exit
 - Check Gateway Certificate:
 - Check Gateway Options:
 - Validate the subject of the gateway certificate:
 - Redundant Gateway:
- Miscellaneous**:
 - ☐ Disable Split Tunneling



13.4.4.1 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 (s)	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 (s)	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.

13.4.4.2 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 applied to the gateway certificate.</p> <p>In the current version, two levels are available:</p> <ul style="list-style-type: none">• Yes (the certificate's validity is checked)• No (the certificate's validity is not checked) <p>The Lite option is reserved for future use. In this version, it is equivalent to the Yes option.</p> <p>If the Check gateway certificate signature option is enabled in the PKI Options (see section 25.4 PKI Options), the present option on the Gateway tab is grayed out and the option is set to Yes.</p>
Check Gateway Options	<p>Used to determine the level of consistency between the VPN tunnel and gateway parameters (encryption algorithms, compression, etc.).</p> <ul style="list-style-type: none">• Yes: Consistency is checked for all VPN parameters. The VPN tunnel will not open if any parameter is different.• No: Consistency is not checked 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 checked for essential parameters.• Apply: Gateway parameters will be applied.

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.

Validate the subject of the gateway certificate

If this field is filled in, the VPN Client will check that the subject of the certificate received from the gateway is, indeed, the one specified.

Redundant Gateway

Defines the address of a spare VPN gateway that the VPN Client will switch to when the initial gateway is unavailable or unreachable.

The address of the redundant VPN gateway can be either an IP or a DNS address.



The **Redundant Gateway** function cannot be configured together with the **Fallback Tunnel** function. You must choose one or the other, failing which the VPN Client could invoke undefined behavior.



Refer to chapter 14 Redundant gateway.

13.4.4.3 Miscellaneous

Disable Split Tunneling

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

13.4.5 SSL: Establishment

Authentication	Security	Gateway	Establishment	Automation	Certificate	Remote Sharing
Key Renegotiation						
Bytes (KB)		0		Lifetime (sec)		3600
Packets		0				
Tunnel Options						
Physic.If MTU		0		Tunnel IPV4		Auto
Tunnel MTU		0		Tunnel IPV6		Auto
Tunnel Establishment Options						
Port		1194	<input type="checkbox"/> TCP	Authentication timeout		15
Retransmissions		2		Traffic setup timeout		10
Traffic						
Traffic detection to open tunnel				Tunnel traffic check		
IPV4				IPV4		
IPV6				IPV6		

13.4.5.1 Key Renegotiation

**Bytes (KB),
Packets,
Lifetime (sec)**

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.

13.4.5.2 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	<p>Virtual interface MTU.</p> <p>When values have been entered, we recommend setting a lower value for the tunnel MTU than that of the physical interface MTU.</p> <p>The default value for MTU is 0, meaning that the software will use the MTU value of the physical interface.</p>
-------------------	---

Tunnel IPv4	<p>Defines the VPN Client's behavior when it receives an IPv4 configuration from the gateway:</p> <ul style="list-style-type: none">• 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 in the Console and the tunnel is not established.• No: Ignores
--------------------	--



Please check that **Tunnel IPv4** and **Tunnel IPv6** aren't both set to **No**.

Tunnel IPv6	<p>Defines the VPN Client's behavior when it receives an IPv6 configuration from the gateway:</p> <ul style="list-style-type: none">• 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 in the Console and the tunnel is not established.• No: Ignores
--------------------	--



Please check that **Tunnel IPv4** and **Tunnel IPv6** aren't both set to **No**.

13.4.5.3 Tunnel Establishment Options

Port/TCP	<p>Port number used to establish the tunnel. The default port value is set to 1194.</p> <p>The tunnel will use UDP by default. The TCP option is used to transport the tunnel over TCP.</p>
-----------------	--

Authentication timeout	<p>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.</p>
-------------------------------	--

Retransmissions	<p>Number of retries for sending a protocol message.</p> <p>If there is no response by the time the defined number of retries is reached, the tunnel is closed.</p>
------------------------	---



Traffic setup timeout	Tunnel establishment phase: time after which the tunnel is closed, if not all the steps have been completed.
------------------------------	--

13.4.5.4 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.

13.4.6 SSL: Automation



Refer to chapter 15 Automation.

13.4.7 SSL: Certificate



Refer to chapter 18 Managing certificates.

13.4.8 SSL: Remote sharing



Refer to chapter 19 Remote Desktop Sharing.

14 Redundant gateway

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

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

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

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

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

The same algorithm applies to the redundant gateway:

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



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



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



The **Redundant Gateway** function cannot be configured together with the **Fallback Tunnel** function. You must choose one or the other, failing which the VPN Client could invoke undefined behavior.



15 Automation

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

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

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

The screenshot shows the 'Automation' tab in the Windows Enterprise VPN Client configuration window. The tab is selected among others: Authentication, Security, Gateway, Establishment, Automation, Certificate, and Remote Sharing. The 'Automation' tab contains several sections:

- Tunnel fallback**: Includes a dropdown for 'Tunnel to switch to' (set to 'None'), a text box for 'Message to display', a numeric input for 'Fallback retries' (set to 0), and a checkbox for 'Allow the user to refuse the fallback'.
- Automatic Open mode**: Includes three checkboxes: 'Automatically open this tunnel when VPN Client starts after logon.', 'Automatically open this tunnel when USB stick is inserted.', and 'Automatically open this tunnel on traffic detection.'.
- Gina mode**: Includes two checkboxes: 'Enable before Windows logon.' and 'Automatically open this tunnel when Gina starts at logon'.
- Scripts**: Includes a section 'Run this script :' with four rows, each with a text box and a 'Browse...' button: 'Before tunnel opens', 'When tunnel is opened', 'Before tunnel closes', and 'After tunnel is closed'.

15.1 Tunnel fallback



The **Fallback Tunnel** function cannot be configured together with the **Redundant Gateway** function. You must choose one or the other, failing which the VPN Client could invoke undefined behavior.

 Refer to chapter 16 Fallback tunnel.

15.2 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 configured with a certificate stored on a smart card or token, it will automatically be opened when the smart card or token is inserted.
Automatically open this tunnel on traffic detection	The tunnel will automatically open when traffic is detected that is heading towards an IP address on the remote network.

15.3 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 chapter 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.

15.4 Scripts

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

The command lines can be as follows:

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

There are many possible applications, such as the following:

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



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

16 Fallback tunnel

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

This function can be configured on the **Automation** tab of each tunnel (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.



The **Fallback Tunnel** function cannot be configured together with the **Redundant Gateway** function. You must choose one or the other, failing which the VPN Client could invoke undefined behavior.

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



17 IPv4 and IPv6

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

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

For IKEv2 VPN tunnels, the IPv4 or IPv6 protocol configuration can be accessed in the top-right corner of the **Child SA** tab.

The screenshot shows the 'Child SA' configuration window with the 'Advanced' tab selected. In the top right corner, there are two buttons: 'IPv4' (highlighted in blue) and 'IPv6'. The 'Traffic selectors' section contains the following fields:

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

At the bottom, there is a checkbox labeled 'Request configuration from the gateway' which is checked.

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

The screenshot shows the 'Child SA' configuration window with the 'Advanced' tab selected. In the top right corner, there are two buttons: 'IPv4' and 'IPv6' (highlighted in blue). The 'Traffic selectors' section contains the following fields:

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

At the bottom, there is a checkbox labeled 'Request configuration from the gateway' which is checked.



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.

18 Managing certificates

18.1 Introduction

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

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

- Automatic selection of the medium to use from among several
- PKCS #11 and CNG access to tokens and smart cards
- Selection of certificates to use according to multiple criteria: subject, key usage, etc.
- Management of certificates on user's side (the VPN Client's side), such as VPN gateway certificates, including validity date, certificate chain, root certificate, intermediate certificate, and CRL management
- Certificate authority (CA) management
- Option to pre-configure all PKI parameters for automatic integration during installation

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

The list of smart cards and tokens compatible with the Windows Enterprise VPN Client is available on TheGreenBow's website at:

<https://www.thegreenbow.com/en/support/integration-guides/compatible-vpn-tokens/>.

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

1. The **Certificate** tab of the relevant tunnel: IKE Auth (IKEv2) or TLS (SSL).
2. The **PKI Options** tab of the **Tools > Options** window in the **Configuration Panel**.
3. A configuration file for smart card readers and tokens called `vpnconf.ini` (refer to the "Deployment Guide").

The following certificate types are supported:

- RSASSA-PKCS1-v1.5 with SHA-2 (only if the corresponding dynamic parameter has been configured, see section 29.4.5 Certificate authentication methods)
- RSASSA-PSS with SHA-2 (only if the corresponding dynamic parameter has been configured, see section 29.4.5 Certificate authentication methods)
- ECDSA “secp256r1” with SHA-2 (256 bits)
- ECDSA “BrainpoolP256r1” with SHA-2 (256 bits)



To find out more about the authentication methods and cryptography used in the Windows Enterprise VPN Client, refer to section 29.4 Basic cryptography concepts in the appendix.

18.2 User certificate

18.2.1 Overview

The VPN Client sends the user certificate to the gateway so that it can authenticate the user.

It must comply with the following constraints (ANSSI security recommendations):

- The Key Usage extension must be present, marked as critical, and only contain the value `digitalSignature`.
- The Extended Key Usage extension must be present, marked as critical, and only contain the value `id-kp-clientAuth`.

If these constraints are not observed, the VPN Client will display a warning in the **Console** but will not prevent communication with the gateway. However, the gateway should refuse the authentication of the VPN Client.

18.2.2 Dynamic parameters

As of version 7.4 of the Windows Enterprise VPN Client, two dynamic parameters now replace the corresponding MSI properties. They are defined within the IKE_AUTH authentication payload and apply to a given tunnel, whereas the MSI properties apply to all tunnels.

18.2.2.1 user_cert_dnpattern

The dynamic parameter `user_cert_dnpattern` is used to specify the certificate to be used. When it is defined, the Windows Enterprise VPN Client

searches for the certificate whose subject contains the [text] pattern on the token, smart card or in the Windows certificate store.

If this dynamic parameter is not specified, the VPN Client searches for the first certificate that meets the other characteristics configured.

18.2.2.2 user_cert_keyusage

The dynamic parameter `user_cert_keyusage` is used to select a certificate based on its "key usage" field:

- 0
or undefined
- Certificate is not selected based on "key usage" field.
- 1 Certificate is selected based on "key usage" field whose attribute `digitalSignature=1`.
 - 2 Certificate is selected based on "key usage" field whose attributes `digitalSignature=1` and `keyEncipherment=1`.



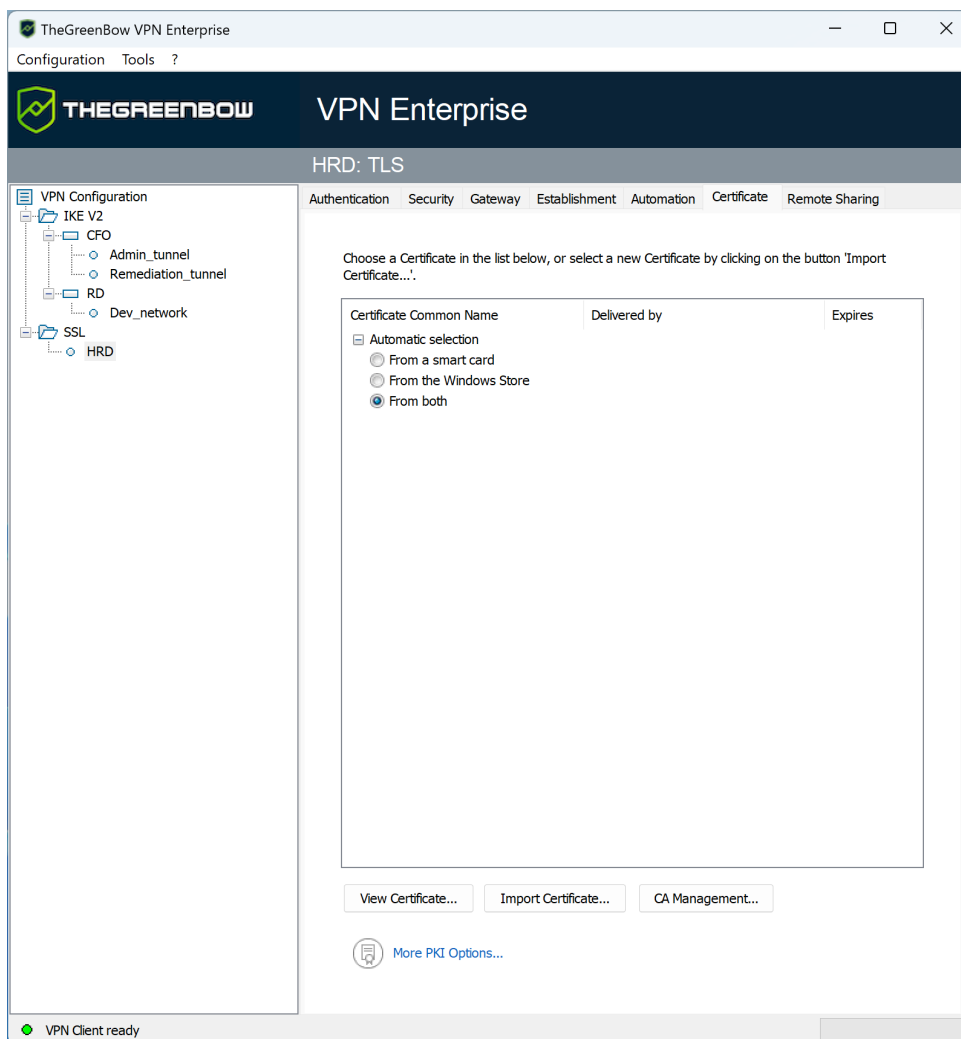
When the value of the dynamic parameter `user_cert_keyusage` is set to 2, the **Only use authentication certificate** check box on the **PKI Options** tab is grayed out (see section 25.4 PKI Options).

18.2.3 Automatic selection

As of version 7.4 of the Windows Enterprise VPN Client, an option can be used to automatically select the user certificate from a token/smart card, the Windows certificate store, or both.

The **Certificate** tab of an IKE or SSL connection includes an **Automatic selection** entry with the following options:

- From a smart card
- From the Windows Store
- From both



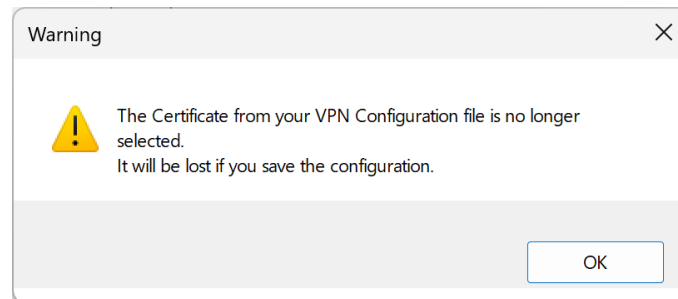
If you choose the latter option, the software will first look for the user certificate on a token/smart card. If it cannot find any, it will continue to search for a certificate in the Windows Certificate Store.

If you choose **From a smart card** or **From both** and you use several token/smart card readers, you must configure the dynamic parameter `reader_pattern` to specify the reader from which the certificate should be selected (see section 25.2.4 Displaying more parameters). As value for this parameter, specify the name of the drive (e.g. `NEOWAVE`) or `Virtual` if it is a Trusted Platform Module (TPM).



As of version 7.5 of the Windows Enterprise VPN Client, when several smart cards from the same manufacturer are used with identical smart card readers, the dynamic parameter `user_smartcard_tip` can be set to a desired value at the IKE Auth level, which will be displayed when the password is requested to help clearly identify the smart card (see section 25.2.4 Displaying more parameters).

If you have previously imported a certificate into the configuration and you decide to choose automatic selection, a warning will be displayed to inform you that the certificate will be removed from the configuration when you save it.



18.3 Selecting a certificate (Certificate tab)

The VPN Client can assign a user certificate to a VPN tunnel.

There can only be one certificate per tunnel, but each tunnel can have its own certificate.

The VPN Client allows you to choose a stored certificate:

- In the VPN configuration file (see 18.4 Importing a certificate to the VPN configuration)
- On a smart card or token (see 18.5 Using a certificate stored on a smart card or token)
- In the Windows Certificate Store (see 18.6 Using a certificate stored in the Windows Certificate Store)

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

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

If a medium does not contain any certificates, it simply will not appear in the list (e.g. if the VPN configuration file does not contain any certificates, it will not appear in the list).

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

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



Certificate Common Name	Delivered by	Expires
<input type="checkbox"/> Windows Personal Certificat...		
<input type="radio"/> Automatic selection		
 <input type="radio"/> CXP-Demo	CXP_CA	03-15-2031

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




Only available certificates that have not expired are displayed.

Authentication
Protocol
Gateway
Certificate
More Parameters

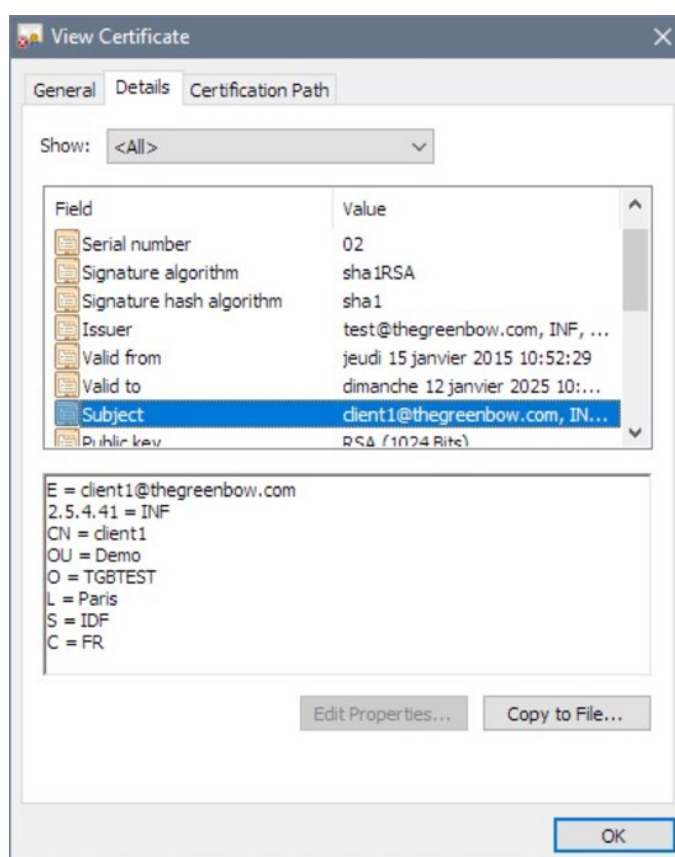
Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...'.

Certificate Common Name	Delivered by	Expires
<input type="checkbox"/> Automatic selection <ul style="list-style-type: none"> <input type="radio"/> From a smart card <input type="radio"/> From the Windows Store <input type="radio"/> From both 		
<input type="checkbox"/> VPN Configuration File <ul style="list-style-type: none"> <input checked="" type="radio"/> CLIENT1_RSA_OCT2022 		
<input type="checkbox"/> Windows Personal Certifica... <ul style="list-style-type: none"> <input type="radio"/> CLIENT1_RSA_OCT2022 		
<input type="checkbox"/> Badgeo ID 2.0 <ul style="list-style-type: none"> <input type="radio"/> CLIENT1AUGUST2022_1 		
CLIENT1_RSA_OCT2022	FGCAINTER2MAY2022	04-06-2032
CLIENT1_RSA_OCT2022	FGCAINTER2MAY2022	04-06-2032
CLIENT1AUGUST2022_1	FGCAINTER2MAY2022	04-06-2032

View Certificate...
Import Certificate...
CA Management...

 More PKI Options...

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 **DER ASN1 DN** and the certificate's subject will be used as the default value of this **Local ID**. See below to find out how to automatically assign a DNS or e-mail value retrieved from the certificate.

Authentication	Protocol	Gateway	Certificate
<p>Identity _____</p> <p>Local ID DER ASN1 DN ▼ <input type="text"/></p> <p>Remote ID ▼ <input type="text"/></p>			

As of version 7.3 of the Windows Enterprise VPN Client, you can select **DNS** or **Email** from the **Local ID** drop-down list to automatically assign to the Local ID a DNS or e-mail value retrieved from the certificate.

If you choose **DNS**, the Local ID will automatically take the value of the `dNSName` field of the certificate subject alternative name (`SubjAltName`). If this field has not been filled in (no `SubjAltName` in the certificate or no `dNSName` in the `SubjAltName`), the `CN` value of the certificate subject will be

used instead. If the latter value is also missing, no certificate is available to configure the tunnel and any attempt to establish the tunnel will fail.

If you choose **Email**, the Local ID will automatically take the value of the `rfc822Name` field of the certificate subject alternative name (`SubjAltName`). If this field has not been filled in (no `SubjAltName` in the certificate or no `rfc822Name` in the `SubjAltName`), the `Email` value of the certificate subject will be used instead. If the latter value is also missing, no certificate is available to configure the tunnel and any attempt to establish the tunnel will fail.



As of version 7.4 of the Windows Enterprise VPN Client, an option can be used to automatically select the user certificate from a token/smart card, the Windows certificate store, or both (see section 18.2.3 Automatic selection).

18.4 Importing a certificate to the VPN configuration

The Windows Enterprise VPN Client can import certificates in PEM/PFX or PKCS #12 format to the VPN configuration. This solution is less secure than using the Windows Certificate Store, a smart card, or a token, but it makes it easier to transport certificates.

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

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



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

18.4.1 Importing a PEM/PFX certificate

1. On the **Certificate** tab of an IKE Auth, click **Import Certificate....**
2. Choose **PEM Format**.
3. Click **Browse** to select the **Root Certificate** and the **User Certificate** as well as the **User Private Key** to import.
4. Click **OK** to confirm.

The certificate is shown and is selected in the certificate list displayed on the **Certificate** tab.

Save the VPN configuration. The certificate will be saved in the VPN configuration.



The file containing the private key may not be encrypted.

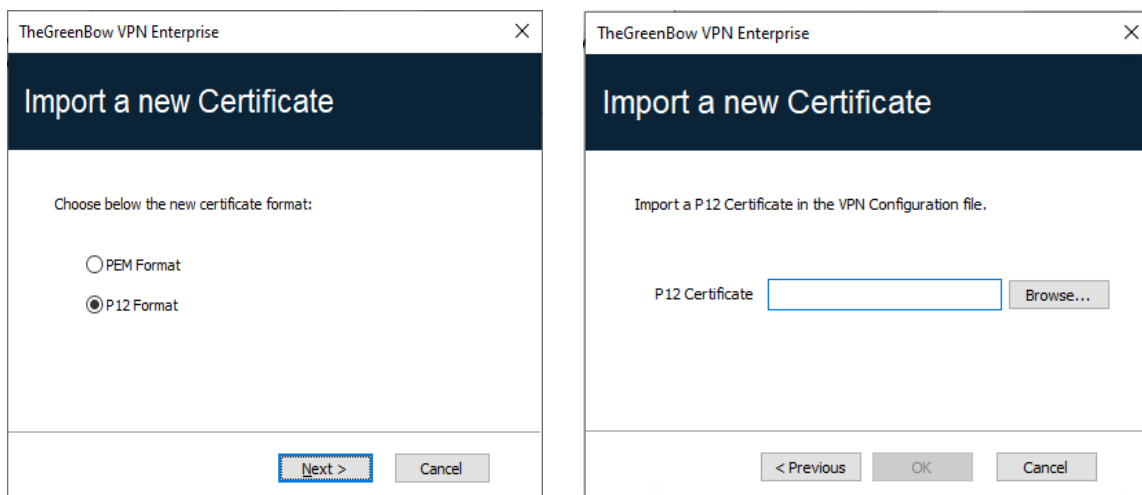
18.4.2 Importing a PKCS #12 certificate

1. On the **Certificate** tab of a Child SA, click **Import Certificate....**
2. Choose **P12 Format**.
3. Click **Browse** to select the PKCS #12 certificate to import.



For security reasons, as of version 7.5 of the Windows Enterprise VPN Client, PKCS #12 certificates encrypted with the RC2 algorithm are no longer supported and cannot be imported.

4. If it is password-protected, enter the password and then click **OK** to confirm.



The certificate is added to the certificate list displayed on the **Certificate** tab and is selected.

Save the VPN configuration. The certificate will be saved in the VPN configuration.



All CAs in the file that are in PKCS #12 format will also be imported to the VPN configuration.

18.5 Using a certificate stored on a smart card or token

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

If the smart card is not inserted or the token cannot be accessed, the tunnel will not open.

If the certificate found does not meet the configured criteria (see section 18.6.2 Importing a certificate depending on the store used below), the tunnel will not open.

If an incorrect PIN code is entered, the Windows Enterprise VPN Client will show a warning, informing users that they only have three (in most cases) consecutive attempts to unlock the smart card or token.

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

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

To implement this function, check **Automatically open this tunnel when a USB stick is inserted** (see chapter 15 Automation).



As of version 7.4 of the Windows Enterprise VPN Client, an option can be used to automatically select the certificate from a token/smart card, the Windows certificate store, or both (see section 18.2.3 Automatic selection).



As of version 7.5 of the Windows Enterprise VPN Client, when several smart cards from the same manufacturer are used with identical smart card readers, the dynamic parameter `user_smartcard_tip` can be set to a desired value at the IKE Auth level, which will be displayed when the password is requested to help clearly identify the smart card (see section 25.2.4 Displaying more parameters).

18.6 Using a certificate stored in the Windows Certificate Store

18.6.1 Required characteristics



To offer finer granularity in how the choice of certificate store to use is configured, as of version 7.5 of the Windows Enterprise VPN Client, this choice is no longer made at the workstation level, but at the tunnel level.

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

- The certificate must be certified by a certificate authority (which excludes self-signed certificates)
- By default, the certificate must be located in the “Personal” Certificate Store (it represents the personal identity of the user who wants to open a VPN tunnel to the corporate network) To use the Windows Machine Certificate Store, add dynamic parameter `MachineStore` set to the value `true` (see section 25.2.4 Displaying more parameters).



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.



18.6.2 Importing a certificate depending on the store used

When importing certificates using the CNG middleware, the store used (user or machine store) must be specified in the command line. Below you will find examples of command lines with the options you need to specify.

- User store:

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

- Machine store:

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



In command lines, the `-user` option of the `certutil` command is used to specify the user store. When it is omitted, the machine store will be used by default.



As of version 7.4 of the Windows Enterprise VPN Client, an option can be used to automatically select the user certificate from a token/smart card, the Windows certificate store, or both (see section 18.2.3 Automatic selection).

18.7 PKI options: specifying the certificate and its storage device

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

This feature is available under the [More PKI options](#) link at the bottom of the **Certificate** tab and on the **PKI options** tab of the **Options** configuration window.

18.8 VPN gateway certificate

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



See section 25.4.1 Certificate Check.

To do this, you need to import the root certificate and all certificates in the certificate chain (root certificate authority and intermediate certificate authorities) to the configuration file.

If the option is checked, the VPN Client will also use the Certificate Revocation List (CRL) of the various certificate authorities.

If these CRLs are not in the certificate store, or if these CRLs cannot be downloaded when the VPN tunnel is opened, the VPN Client will not be able to validate the gateway certificate.

Checking each item in the chain implies the following:

- Checking gateway certificate expiration date
- Checking certificate validity start date
- Checking signatures of all certificates in the certificate chain (including root certificate, intermediate certificates, and server certificate)
- Checking whether the CRLs of all certificate issuers within the chain of trust



As of version 7.5 of the Windows Enterprise VPN Client, you can check the revocation of the gateway certificate using Online Certificate Status Protocol Stapling (OCSP Stapling). To do this, you must add the dynamic parameter `enable_OCSP` set to the value `true` (see section 25.2.4 Displaying more parameters).

18.8.1 Preventing or limiting CRL download

18.8.1.1 Introduction

A Certificate Revocation List (CRL) contains all the certificates that are no longer valid (validity date has expired, private key associated with the certificate has been lost or compromised, a field concerning the owner has been changed, etc.) and therefore cannot be trusted.

CRLs are defined in the [RFC 5280](#) and [RFC 6818](#) standards.

CRLs are published by certificate authorities (CAs) and Public Key Infrastructures (PKIs).

In some cases, these lists can be relatively large (several MB). Downloading them can therefore take time and slow down the time it takes to open a tunnel when a great number of users contacts the HTTP server at the same time.

The Windows Enterprise VPN Client provides two dynamic parameters described below to speed up the time it takes to open a tunnel. These parameters work independently from one another and can be combined.

The first dynamic parameter, named `check_user_crl`, prevents the download of the CRL used to validate the user certificate. The second, named



`crl_cache_duration`, limits the download of the CRL used to validate the gateway CRL.

18.8.1.2 Preventing download of CRL used to validate the user certificate

By default, when the VPN Client verifies the user certificate (e.g. because it is issued by a known CA), it also verifies the CRL to determine whether the certificate is still valid. If the certificate is no longer valid, a simple warning is entered in the **Console**. Ultimately, it is up to the gateway to decide whether the user certificate can be accepted or not.

In order to prevent downloading the CRL and thus speed up the time it takes to open a tunnel, you can add the dynamic parameter `check_user_crl` set to the value `false` (see section 25.2.4 Displaying more parameters). In this case, the user certificate CRL is not verified. The gateway will handle this verification.

18.8.1.3 Limiting download of CRL used to validate the gateway certificate

If you want to limit the number of times a CRL is downloaded to validate the gateway certificate without preventing its download altogether—again with the aim to speed up the time it takes to open a tunnel—you can add the dynamic parameter `crl_cache_duration` set to a value corresponding to the number of hours during which the CRL is stored in the cache memory (see section 25.2.4 Displaying more parameters).

When the value of the parameter is set to zero, the caching of the CRL is disabled. Caching is limited to a maximum of seven days, i.e. 168 hours. Any value greater than 168 will be considered equal to the maximum of seven days.

When this dynamic parameter is configured with a value different from zero, the CRL will be stored in a cache memory and an expiration time in hours will be set for this CRL. As long as the expiration time has not passed, the CRL in the cache memory will be used and no download is performed. When the time has expired, the CRL is downloaded and updated in the cache memory.

18.8.2 Constraints on the Key Usage extension

The gateway certificate must comply with the following constraints on the Key Usage extension. The extension must:

- Be present
- Be marked as critical, and
- Only contain the values `digitalSignature` and/or `nonRepudiation`

In the event that the VPN gateway does not comply with the constraints on the Key Usage extension mentioned above, you can configure the VPN Client so that it validates the certificate despite this, by adding the dynamic parameter `allow_server_extra_keyusage` set to the value `true` (see section 25.2.4 Displaying more parameters).

In this configuration, the certificate will also be validated if the Key Usage extension contains one of the following combinations of values:

- `digitalSignature + keyEncipherment + keyAgreement`
- `digitalSignature + keyAgreement`
- `nonRepudiation + keyEncipherment`
- `nonRepudiation + keyEncipherment + keyAgreement`
- `nonRepudiation + keyAgreement`
- `keyEncipherment`
- `keyEncipherment + keyAgreement`

Moreover, in this configuration the Key Usage extension can be marked as non-critical.



In accordance with security requirements, the `keyEncipherment` value of the Key Usage extension has been deprecated and replaced with the `nonRepudiation` value, which is now accepted by default. However, version 7.5 of the Windows Enterprise VPN Client continues to accept the `keyEncipherment` value without needing to use dynamic parameter `allow_extra_keyusage`.



We recommend that you give preference to the `nonRepudiation` value over the `keyEncipherment` value of the Key Usage extension.

18.8.3 Constraints on the Extended Key Usage extension

The gateway certificate must comply with the following constraints on the Extended Key Usage extension. The extension may be present or not. If it is present, it must:

- Be marked as non-critical, and
- Only contain the following values:
 - `id-kp-serverAuth` or
 - `id-kp-serverAuth + id-kp-ipsecIKE`

In the event that the VPN gateway does not comply with the constraints on the Extended Key Usage extension mentioned above, you can configure the VPN Client so that it validates the certificate despite this, by adding the



dynamic parameter `allow_server_and_client_auth` set to the value `true` (see section 25.2.4 Displaying more parameters).

In this configuration, the certificate will also be validated if the Extended Key Usage extension contains one of the following combinations of values:

- `id-kp-ServerAuth + id-kp-ClientAuth` or
- `id-kp-serverAuth + id-kp-ClientAuth + id-kp-ipsecIKE`

18.9 Managing certificate authorities

18.9.1 Overview

If the Windows Enterprise VPN Client is configured to check gateway certificates, the Certificate Authorities (CAs) must also be accessible.

You must import the gateway's root CA into the configuration.

If the gateway is not configured to send CAs, you must also import the intermediate CAs into the configuration.



As of version 7.3 of the Windows Enterprise VPN Client, you can create configurations with more than three certificate authorities (CAs).

The following intermediate CA types are supported:

- RSASSA-PKCS1-v1.5 with SHA-2
- RSASSA-PSS with SHA-2
- ECDSA "secp256r1" with SHA-2
- ECDSA "BrainpoolP256r1" with SHA-2

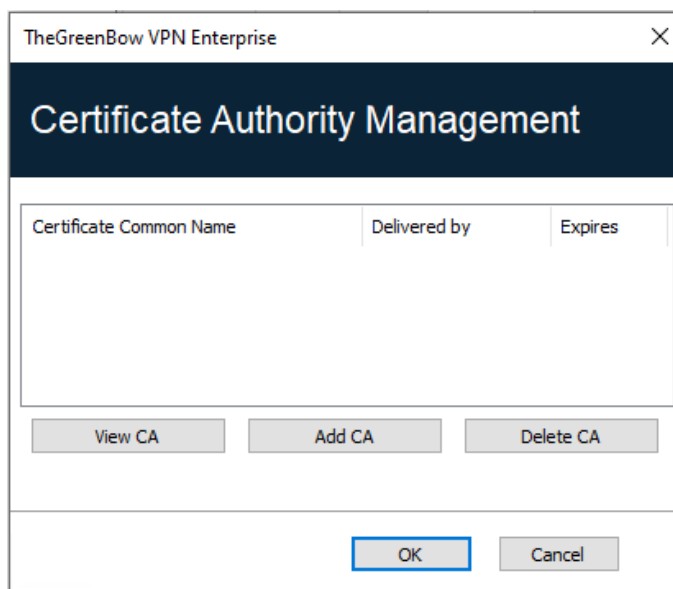
The following root CA types are supported:

- RSASSA-PKCS1-v1.5 with SHA-2
- RSASSA-PSS with SHA-2
- ECDSA "secp256r1" with SHA-2
- ECDSA "BrainpoolP256r1" with SHA-2



For security reasons, the Windows Certificate Store may not be used to access CAs.

18.9.2 Importing a certificate authority



1. In the **Certificate Authority Management** window, click **Add CA**.
2. Choose the desired CA certificate type (PEM or DER).
3. Click **Browse** and then select the CA to import.

18.9.3 IPsec DR mode

To be able to use the Windows Enterprise VPN Client in IPsec DR (Restricted) mode, compliance with ANSSI's IPsec DR framework requires the `Certification Authority` value in the certificate request payload (CERTREQ) to be a concatenated list of SHA-2 hashes derived from the public keys of the trusted certification authorities.

As of version 7.5 of the Windows Enterprise VPN Client, the VPN Client automatically detects the format (SHA-1 or SHA-2) based on the length of the certificate request payload [CERTREQ] it receives from the gateway. This automatic selection is only performed if the dynamic parameter `sha2_in_cert_req` is not present.

If you want to select the format manually, you can add the dynamic parameter `sha2_in_cert_req` set to the value `true` for SHA-2 or `false` for SHA-1 (see section 25.2.4 Displaying more parameters).



If the length of the certificate request payload cannot be used to determine the format, SHA-1 is used. When connecting to a gateway configured in IPsec Restricted mode, you must therefore use the dynamic parameter `sha2_in_cert_req` to make sure the correct format is selected.



To find out how to configure the Windows Enterprise VPN Client for use with a gateway configured for IPsec DR (Restricted) mode, refer to the “VPN Client and IPsec Restricted” configuration guide currently only available in French on [TheGreenBow](#)'s website.

19 Remote Desktop Sharing

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

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

To set up Remote Desktop Sharing, proceed as follows:

1. Select the VPN tunnel (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.

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 Corporate_desktop

Computer name or IP address 192.168.175.50

Add

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

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

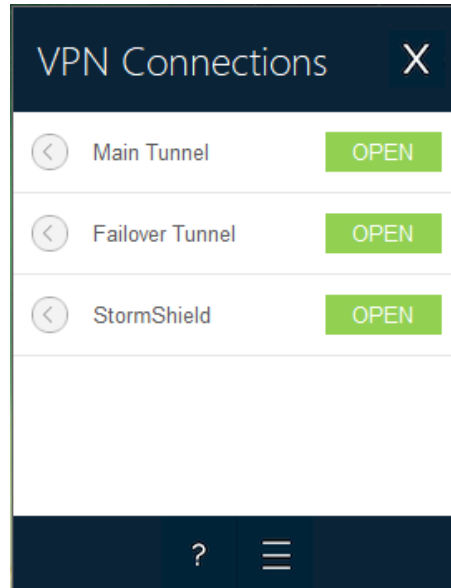
Add

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 [Connections Configuration](#) function described in detail in the next chapter.

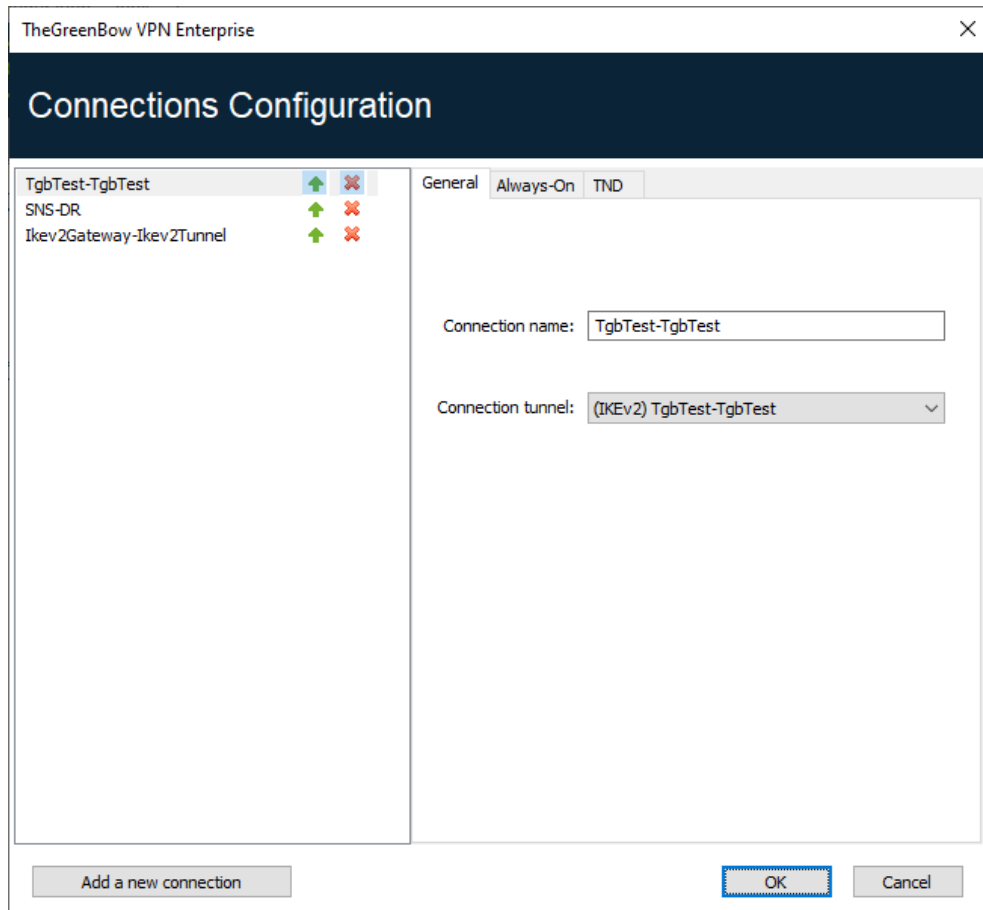
20 Configuring the Connection Panel

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



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

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



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

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

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

The right side contains the following three tabs:

- **General**
- **Always-On**
- **TND**

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

To create a new VPN connection, click **Add a new connection**, choose a name and select the corresponding VPN tunnel. If a Remote Desktop Sharing

connection is configured, an option used to select it automatically appears below the selected tunnel. Once they have been confirmed, changes made in the **Connection Panel** configuration window instantly appear in the **Connection Panel**.

The **Always-On** and **TND** tabs are described in chapter 20 Configuring the Connection Panel below.



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



21 Configuring the TrustedConnect Panel

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

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

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

The following functions of the **TrustedConnect Panel** can be configured:

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

21.1 Always-On

21.1.1 Operating principle

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

The following network interfaces are supported:

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

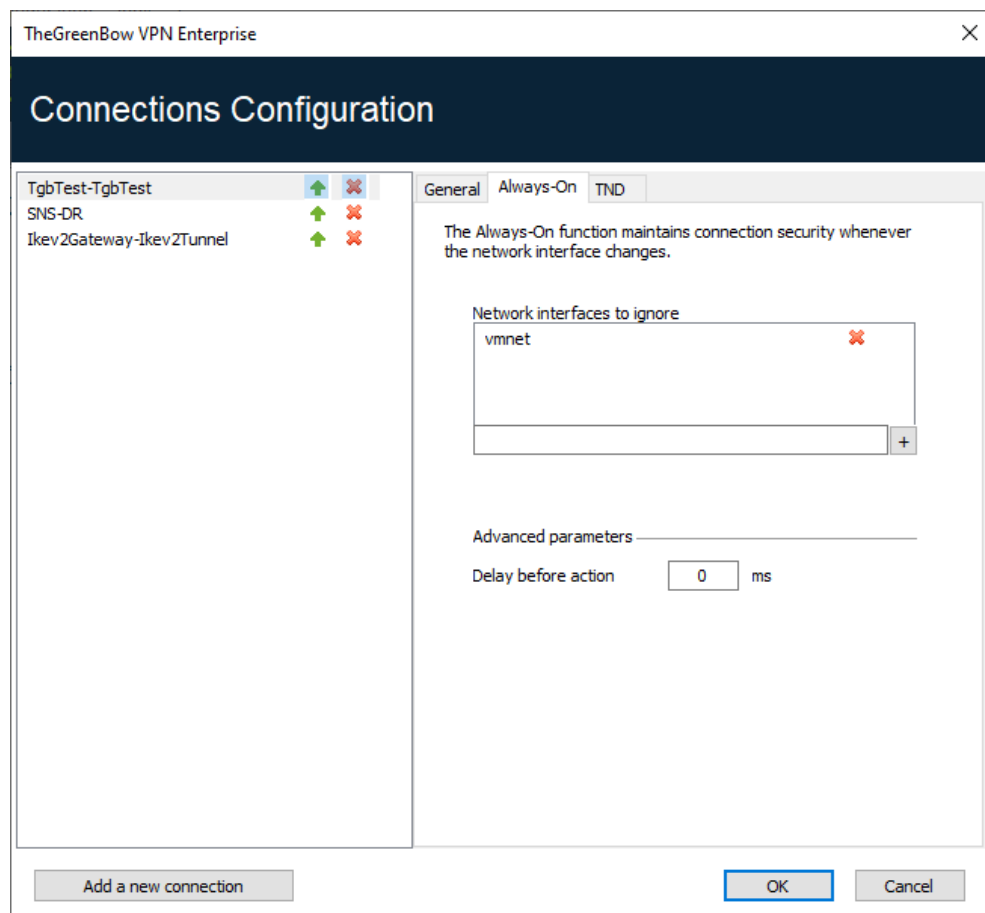
The following network events trigger automatic tunnel reconnection (and, where appropriate, detection of the trusted network), unless they have been explicitly excluded (see section 21.1.2 Configuring Always-On):

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

21.1.2 Configuring Always-On

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

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





Network interfaces to ignore

Network interfaces can be excluded from Always-On monitoring. An interface is excluded using the **description** property (visible with `ipconfig /all`).

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

The values of this parameter are not case sensitive (all character strings are converted to lowercase before comparison).

You can specify several network interfaces to exclude. To do this, enter the name of the network interface you want to exclude, and then click the + button to the right of the input field. The network interface name is added to the exclusion list. Repeat these steps as many times as necessary.

Delay before action

The time required to take into account a new network interface varies from one system to the next. If it is too long, it may interfere with the TND mechanism, which may lead the VPN Client to attempt establishing a VPN connection even though the workstation is connected to the trusted network.

To avoid this issue, this parameter is used to delay the triggering of the TND mechanism (see next section).

It is expressed in milliseconds. If the default value needs to be changed, we recommend specifying a value greater than or equal to 3000 ms.

By default, the value is equal to 0 and the TND mechanism is started immediately, which is suitable in most cases.

21.2 Trusted Network Detection (TND)

21.2.1 Operating principle

21.2.1.1 General information

This feature consists in detecting whether the workstation is connected to the corporate network (trusted network) or not.

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

The **TrustedConnect Panel** uses one of the following two methods to detect whether the workstation is on a trusted network:

1. If it detects a trusted DNS suffix, it verifies whether it can access a trusted web server and whether the server's certificate is valid (see section 21.2.1.2 HTTPS method)
2. If it detects an Active Directory (AD) server, it searches for a domain name that matches a list of trusted domains (see section 21.2.1.3 AD method).



If the Filtering Mode is enabled, you must configure TND as described in the "Filtering Mode User's Guide" available on [TheGreenBow](#)'s website.

21.2.1.2 HTTPS method

The existing HTTPS method remains available. It is carried out in two steps:

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

Both methods are required and must be combined to detect whether the workstation is on a trusted network. To achieve this, the VPN Client starts by testing whether a trusted DNS suffix is available:

- if none are found, the VPN Client does not continue the test and concludes that the workstation is not connected to the trusted network;
- if it does find one, it continues the test sequence by verifying the access to the trusted server and the validity of its certificate.

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

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

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

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

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



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

21.2.1.3 AD method

This Trusted Network Detection (TND) method, introduced with version 7.5 of the Windows Enterprise VPN Client, allows you to use connection to an Active Directory (AD) server to determine whether the workstation is on a trusted network. This method comes in three variants:

- **AD only:** checks whether the workstation is joined to a domain and, if this is the case, the domain name is checked against a list of trusted domain names¹
- **LDAP:** same as **AD only**, plus additional validation by connecting to an LDAP directory service
- **LDAPS:** same as **AD only**, plus additional secure validation by connecting to an LDAPS directory service



In GINA mode, the workstation must be declared as not being part of a trusted network as long as no user has logged on to Windows.

21.2.2 Configuring TND

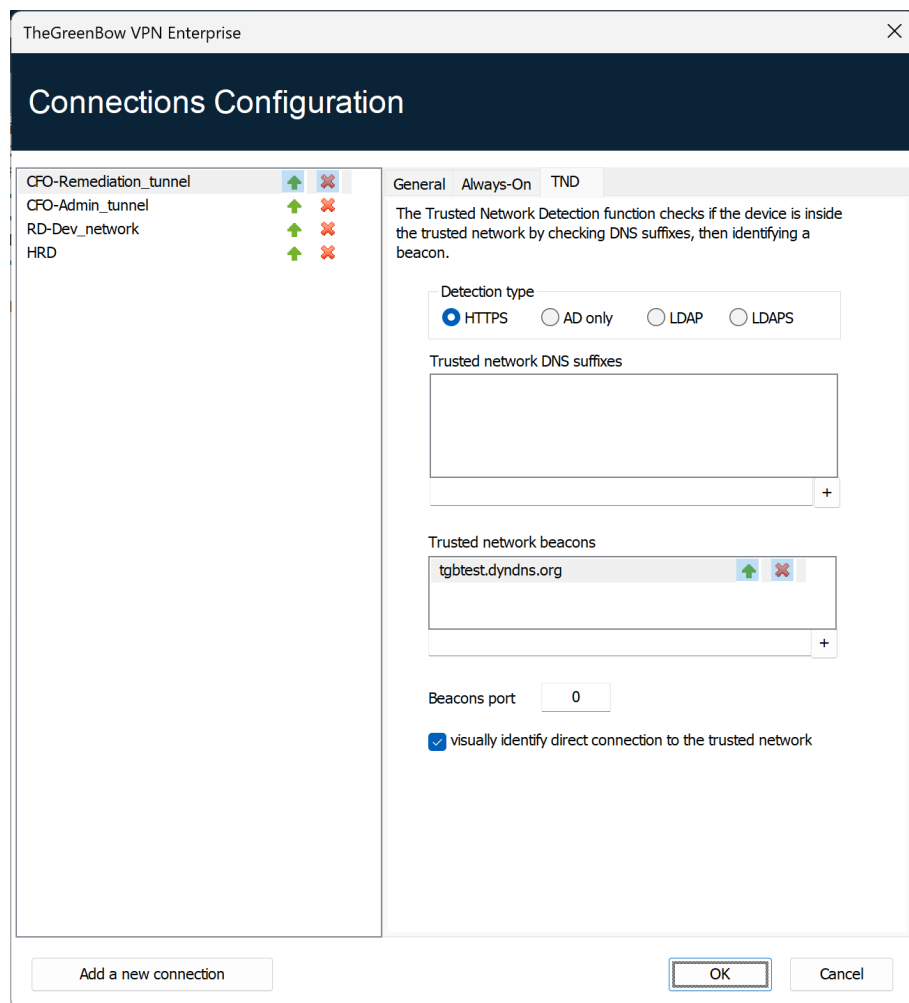
The **TND** tab in the **Connections Configuration** window allows you to configure the settings for the **Trusted Network Detection** feature.

Four radio buttons allow you to select the type of detection to be performed:

- HTTPS
- AD only
- LDAP
- LDAPS

¹ If the list is empty, any domain is accepted.


The following are the options detection type **HTTPS**:



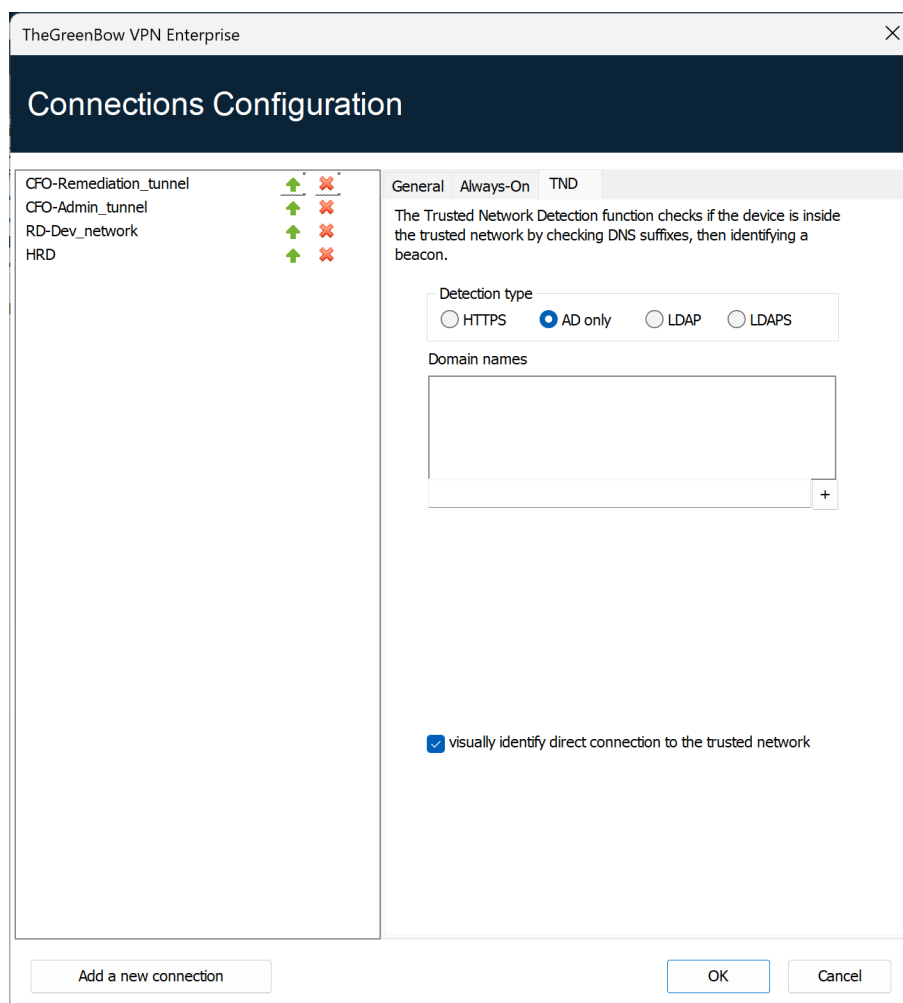
Trusted network DNS suffixes This parameter defines the list of trusted DNS suffixes. This list can contain several DNS suffixes.

To do this, enter the DNS suffix name you want to add, and then click the + button to the right of the input field. Repeat these steps as many times as necessary.



Trusted network beacons	<p>This parameter defines the list of IP addresses (or DNS names) of the trusted servers to be used.</p> <p>This list can contain several IP addresses (or DNS names). The VPN Client will then successively test all IP addresses (or DNS names) and all certificates associated with each server until it finds one that is accessible and valid.</p> <p>The IP addresses (or DNS names) must be separate by a comma in the list, without any blank spaces.</p> <p>You do not need to add the <code>https://</code> prefix to IP address (or DNS name).</p> <div data-bbox="464 656 1410 770"> By default, the TrustedConnect Panel tries to connect to the <code>/index.html</code> page. If this page does not exist on the server, the server cannot be used as a beacon.</div>
Beacons port	<p>This parameter defines the port to be used to reach trusted servers. Only a single port can be configured, and it will be used with all IP addresses (or DNS names).</p> <p>If this parameter is not configured, the VPN Client will use the port 443 by default.</p>
Visually identify direct connection to the trusted network	<p>This option adds a visual cue to the TrustedConnect Panel to indicate that the VPN Client is connected to the trusted network.</p> <p>If the box is checked, the taskbar icon and the color of the circle in the panel is blue when the machine is connected to the trusted network and green when a tunnel is open.</p> <p>If the box is unchecked, the taskbar icon and the color of the circle in the panel remains green in both cases. No distinction is made between the trusted network and an open tunnel.</p>

The following are the options detection type **AD only**:



Domain names

This parameter defines the list of trusted domain names. This list can contain several domain names.

To do this, enter the domain name you want to add, and then click the + button to the right of the input field. Repeat these steps as many times as necessary.

Domain names are not case sensitive.

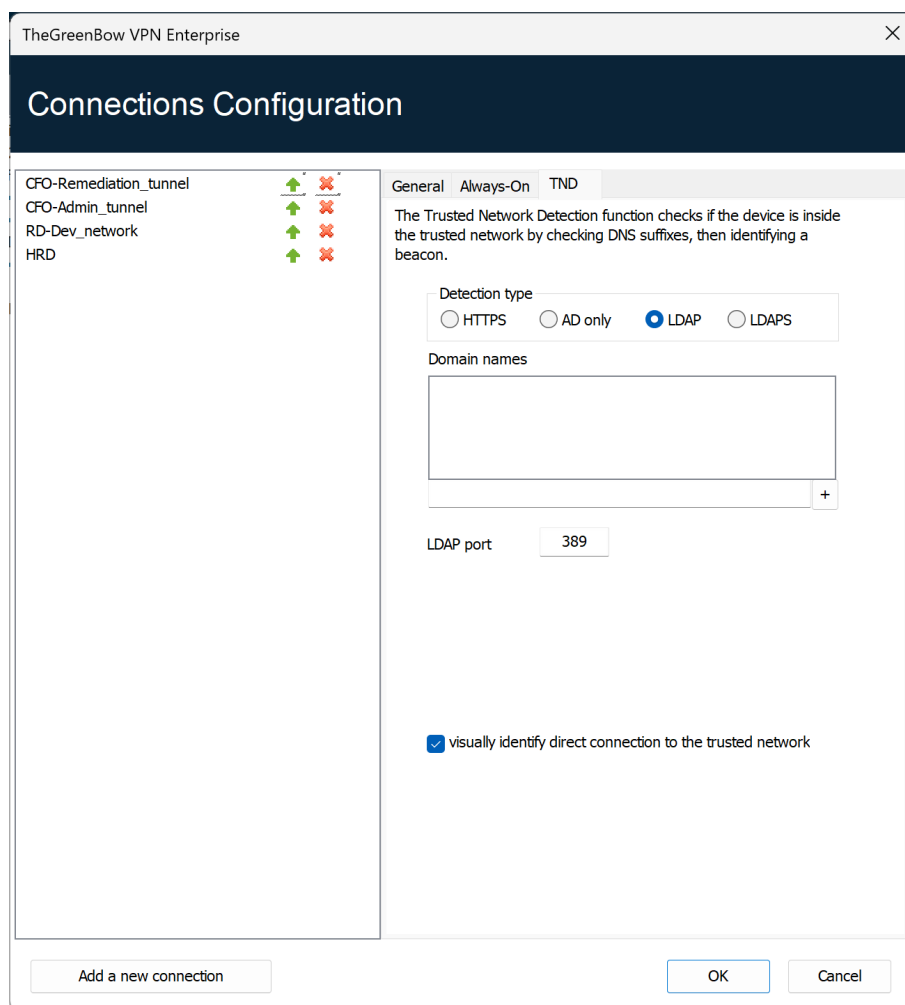
Visually identify direct connection to the trusted network

This option adds a visual cue to the **TrustedConnect Panel** to indicate that the VPN Client is connected to the trusted network.

If the box is checked, the taskbar icon and the color of the circle in the panel is blue when the machine is connected to the trusted network and green when a tunnel is open.

If the box is unchecked, the taskbar icon and the color of the circle in the panel remains green in both cases. No distinction is made between the trusted network and an open tunnel.

The following are the options detection type **LDAP**:



The screenshot shows the 'Connections Configuration' window for 'TheGreenBow VPN Enterprise'. The 'TND' tab is selected. On the left, a list of connections is shown: 'CFO-Remediation_tunnel', 'CFO-Admin_tunnel', 'RD-Dev_network', and 'HRD'. Each connection has a green up arrow and a red X icon. The main area on the right contains the 'TND' configuration. It includes a description: 'The Trusted Network Detection function checks if the device is inside the trusted network by checking DNS suffixes, then identifying a beacon.' Below this, the 'Detection type' is set to 'LDAP' (selected with a radio button). Other options are 'HTTPS', 'AD only', and 'LDAPS'. There is a 'Domain names' input field with a '+' button to its right. The 'LDAP port' is set to '389'. At the bottom, there is a checkbox labeled 'visually identify direct connection to the trusted network' which is checked. At the very bottom of the window are buttons for 'Add a new connection', 'OK', and 'Cancel'.

Domain names

This parameter defines the list of trusted domain names. This list can contain several domain names.

To do this, enter the domain name you want to add, and then click the + button to the right of the input field. Repeat these steps as many times as necessary.

Domain names are not case sensitive.

LDAP port

This parameter defines the port to use to reach the LDAP server.

You can only configure one port, which will be used for all domain names.

The default value is 389.

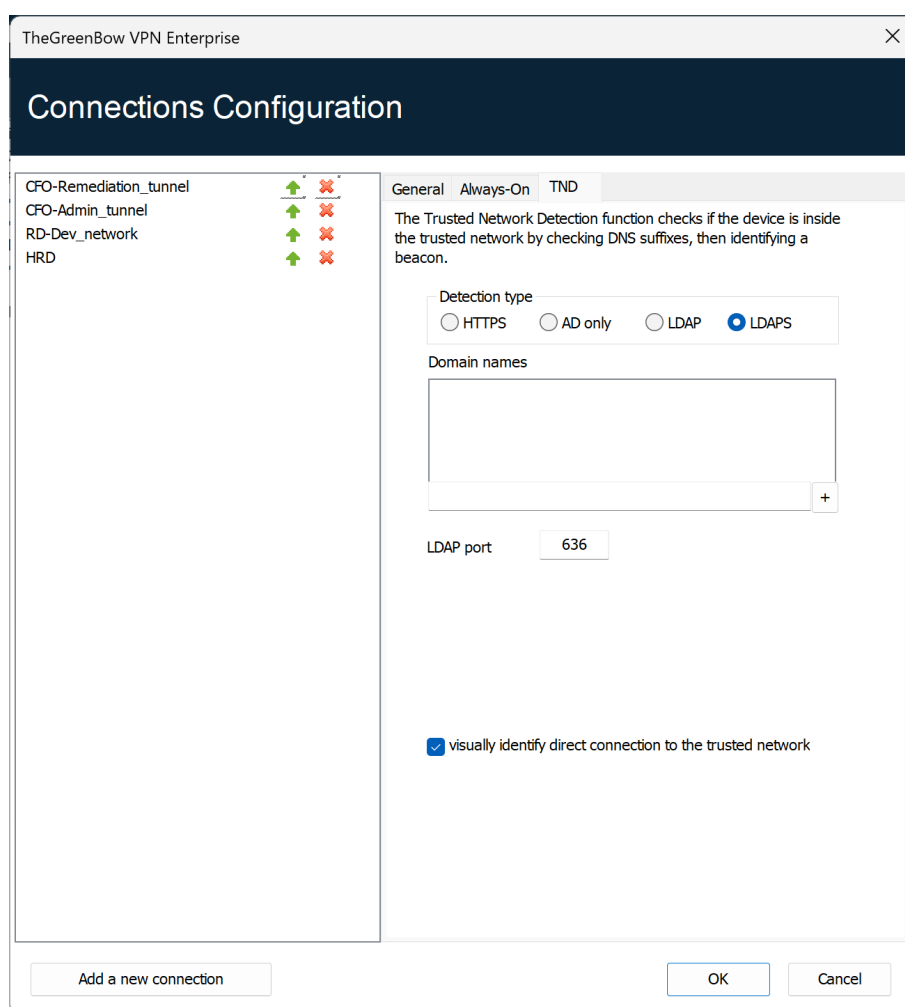
Visually identify direct connection to the trusted network

This option adds a visual cue to the **TrustedConnect Panel** to indicate that the VPN Client is connected to the trusted network.

If the box is checked, the taskbar icon and the color of the circle in the panel is blue when the machine is connected to the trusted network and green when a tunnel is open.

If the box is unchecked, the taskbar icon and the color of the circle in the panel remains green in both cases. No distinction is made between the trusted network and an open tunnel.

The following are the options detection type **LDAPS**:



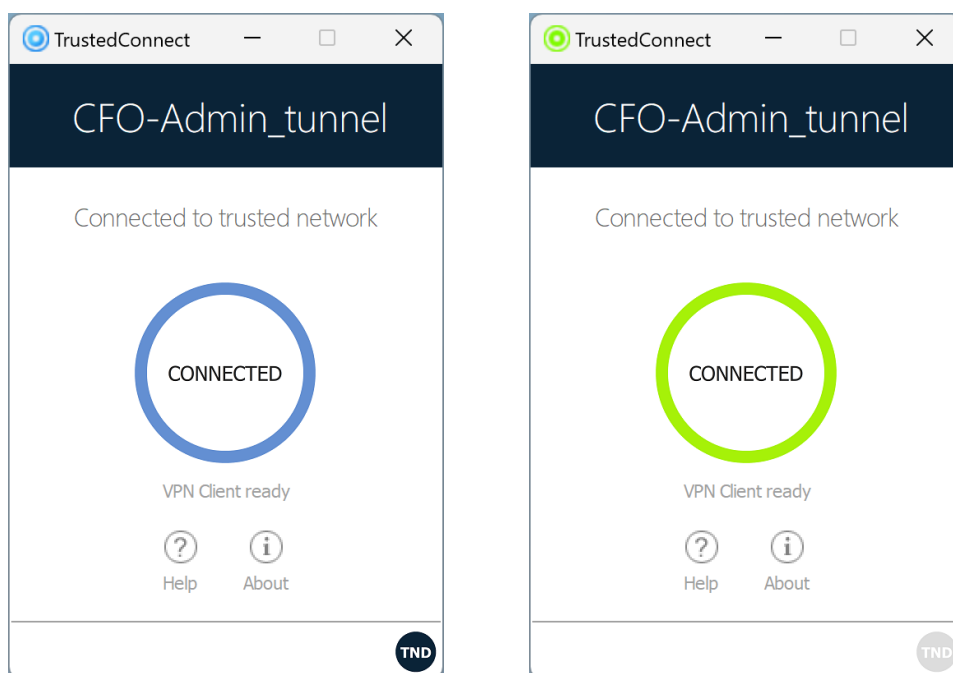


Domain names	<p>This parameter defines the list of trusted domain names. This list can contain several domain names.</p> <p>To do this, enter the domain name you want to add, and then click the + button to the right of the input field. Repeat these steps as many times as necessary.</p> <p>Domain names are not case sensitive.</p>
LDAP port	<p>This parameter defines the port to use to reach the LDAP server.</p> <p>You can only configure one port, which will be used for all domain names.</p> <p>The default value is 636.</p>
Visually identify direct connection to the trusted network	<p>This option adds a visual cue to the TrustedConnect Panel to indicate that the VPN Client is connected to the trusted network.</p> <p>If the box is checked, the taskbar icon and the color of the circle in the panel is blue when the machine is connected to the trusted network and green when a tunnel is open.</p> <p>If the box is unchecked, the taskbar icon and the color of the circle in the panel remains green in both cases. No distinction is made between the trusted network and an open tunnel.</p>

21.2.3 Disabling TND

In some cases, it may be useful to be able to open a tunnel to access certain resources even when the trusted network has been detected.

The MSI property `DIALERBEHAVIOR`, to be configured during installation, adds an option in the status bar that allows users to disable and later re-enable the TND function.



When the TND function is disabled (gray TND icon), the tunnel will be mounted systematically. When it is enabled (blue TND icon), no tunnel can be mounted when a trusted network has been detected (default behavior).



Refer to the “Deployment Guide” for the corresponding instructions.

21.3 Scripts

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

21.4 Minimizing the panel

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

You can set the time delay before the VPN Client's HMI is minimized, as well as the type of minimization. The **TrustedConnect Panel** can be minimized to the taskbar or to the notification area (systray, by default).



The time delay and minimization type only apply to automatic minimization of the **TrustedConnect Panel** when a connection to the trusted network is detected.



These configurations must be made using the properties of the VPN Client installer.



Refer to the “Deployment Guide” for the corresponding instructions.

21.5 Disabling the disconnect button

For better workstation protection, administrators can disable the disconnect button as soon as a connection is being established (TND check, opening a tunnel, etc.). To do this, you must use the MSI property `BTNBEHAVIORTC` or the corresponding parameter in the `vpnsetup.ini` file during installation.

When this option is enabled, clicking on the **Connecting** or **Connected** button on the **TrustedConnect Panel** will have no effect. Users cannot close the tunnel.



Refer to the “Deployment Guide” for the corresponding instructions.

21.6 Removing menu items

For better workstation protection, administrators can disable all or part of the menu options. To do this, you must use the MSI property `MENUIITEMTC` or the corresponding parameter in the `vpnsetup.ini` file during installation.

When this option is enabled, users will only have access to some menu options (to access logs, quit the interface, etc.), or will have no menu access at all.



Refer to the “Deployment Guide” for the corresponding instructions.

21.7 Automatically restarting the TrustedConnect Panel

To enhance workstation protection, administrators can force the **TrustedConnect Panel** to automatically restart when it is shut down. To do this, you must use the MSI property `RESTARTGUITC` or the corresponding parameter in the `vpnsetup.ini` file during installation.

When this option is enabled, the **TrustedConnect Panel** will be automatically restarted when users quit the software or if it crashes.



Refer to the “Deployment Guide” for the corresponding instructions.

21.8 Purging logs

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

This configuration must be made using the `VPNLOGPURGE` property of the VPN Client installer.



Refer to the “Deployment Guide” for the corresponding instructions.

21.9 Behavior when smart card or token is removed

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

This configuration must be made using the properties of the VPN Client installer.



Refer to the “Deployment Guide” for the corresponding instructions.

22 GINA mode

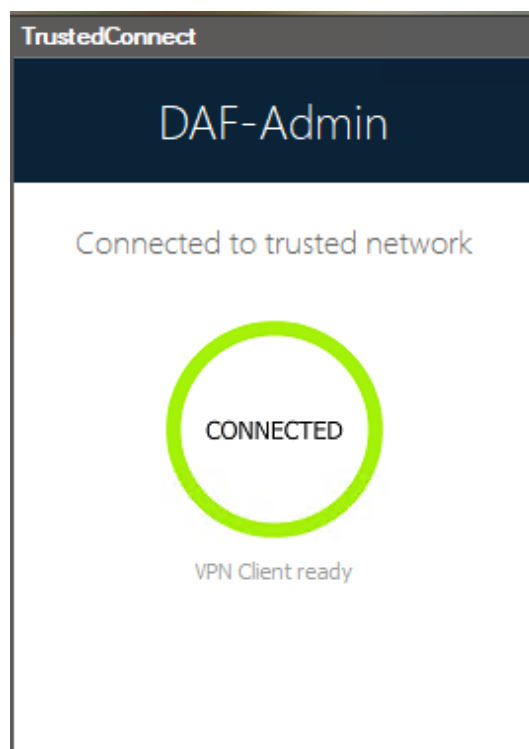
22.1 Overview

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.

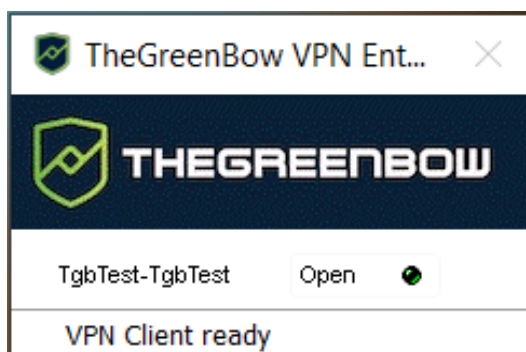
When a tunnel is configured “in GINA mode”, the following two situations are possible:

1. If the VPN Client is configured to start up in **TrustedConnect** mode (refer to section 25.2 General), then the **TrustedConnect Panel** will be displayed on the Windows logon screen and the VPN Client tries to automatically connect to the trusted network.



As of version 7.4 of the Windows Enterprise VPN Client, if you enabled the option that allows users to choose the connection in the **TrustedConnect Panel** using the MSI property `DIALERBEHAVIOR` when you installed the VPN Client (see “Deployment Guide”), users can choose the connection before they log on to Windows (see section 10.9 Choosing the connection).

2. Otherwise, a window allowing you to open a tunnel that is similar to the **Connection Panel** will be displayed on the Windows logon screen. It allows you to open a VPN tunnel manually or automatically.



As of version 7.5 of the Windows Enterprise VPN Client, the behavior of the GINA mode changes according to compliance level reported by the Secure Connection Agent (SCA), which determines whether a workstation should be allowed to access the corporate network (see section 24.2.3.3 In GINA mode).

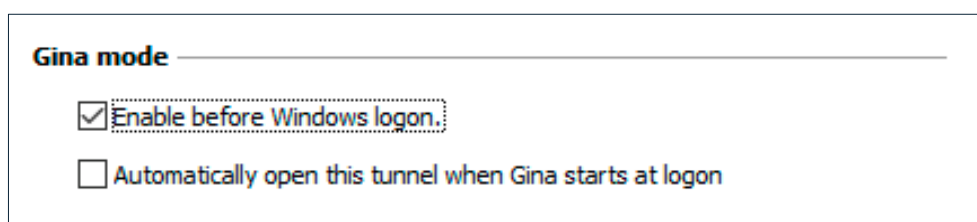
Special use case

If you want to use several tunnels, one of which for the GINA mode and another for connecting the user in TrustedConnect mode after Windows logon, the user tunnel must be the first in the list of connections.

This way, the GINA tunnel will be opened when the workstation starts up, and then a transition to the user tunnel will take place when the user logs on to Windows. Likewise, a transition from the user tunnel to the GINA tunnel will take place when the user logs off from Windows.

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

Security considerations

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



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 configured in GINA mode.



A VPN tunnel configured with a certificate stored in the Windows user certificate store cannot be used 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). The software simply cannot identify the user's certificate in the Windows machine certificate store.

23 Filtering Mode

TheGreenBow's Windows Enterprise VPN Client software includes advanced features called Filtering Mode and Captive Portal Detection (CPD) that are intended for a specific use and which must be added when installing the software before they can be used.

The Filtering Mode in the Windows Enterprise VPN Client is a function used to filter the workstation's inbound and outbound data flows. It is enabled as soon as the Windows Enterprise VPN Client is not connected to a trusted network. Consequently, it is only available with the **TrustedConnect Panel**.

The time users have to connect to the captive portal can be configured on the **CPD** tab in the **Connections Configuration** window. The default value is 180 s (3 min).



Refer to the "Filtering Mode User's Guide" for a detailed description of these features.



24 Secure Connection Agent

24.1 Overview

As of version 7.5 of the Windows Enterprise VPN Client, the VPN Client is able to communicate with a separately supplied add-on called Secure Connection Agent (SCA). It is part of the extended product offering and serves as a link between VPN Clients and the Connection Management Center (CMC).



Refer to the SCA's and the CMC's "Administration Guides" for more information about these products. You can find them on the Product documentation page on TheGreenBow's website:
<https://www.thegreenbow.com/fr/support/documentation-produits/>.

The SCA provides the following two functions:




1. Endpoint compliance monitoring: the SCA checks whether the endpoint should be allowed to access the corporate network. The VPN Client will adapt its behavior according to the reported compliance level.
2. Forwarding of the VPN Client's audit traces to the Connection Management Center (CMC).

24.2 Endpoint compliance monitoring

24.2.1 Introduction

The endpoint compliance function checks the availability and status of the Windows firewall and of any antivirus provider that is registered with the Windows Security Center.

Currently there are three levels of compliance defined and the VPN Client will act differently according to each of these levels, as described in the truth table below.

Virus & threat protection		Firewall & network protection		Result
0	+	0	=	 Cannot open any tunnel
1	+	0	=	 Switch to a remediation area
0	+	1		
1	+	1	=	 Access sensitive network

A remediation VPN connection should be considered as a VPN tunnel with restricted access. It could for example allow a system administrator to take control over the PC from the corporate network.



After logging on to Windows, the Secure Connection Agent will use the last known compliance level until the Windows Security Center service has started.

24.2.2 Configuring the VPN Client

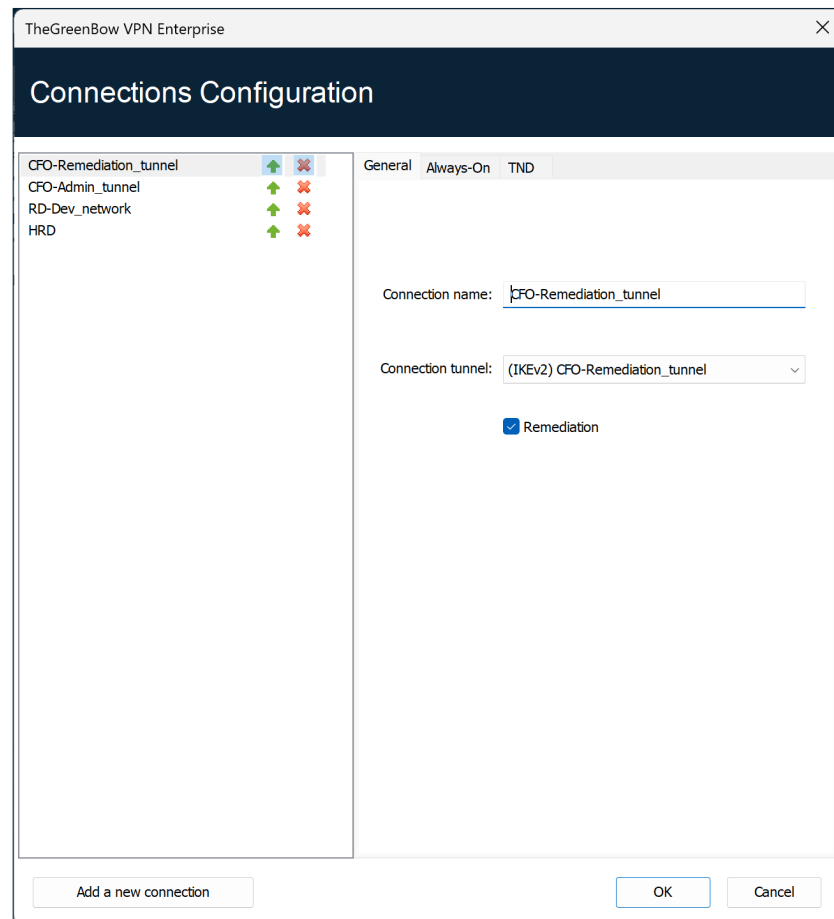
When the Secure Connection Agent (SCA) detects near compliance, a remediation connection will be opened if such a connection has been configured.

To configure a remediation connection, proceed as follows:

1. Access the Windows Enterprise VPN Client's **Configuration Panel**.
2. From the **Tools** menu, choose **Connections Configuration** to open the **Connections Configuration** window.
3. On the **General** tab, check the **Remediation** box for the connection to be used as a remediation connection.



This information is stored in the configuration file.



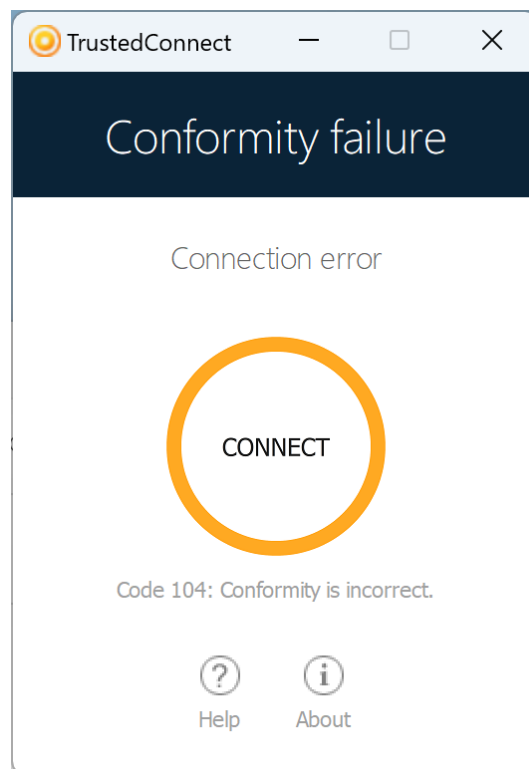
The **Remediation** box must only be checked for a single connection. If the **Remediation** box is checked for several connections, it will be impossible to know which connection will be used.

24.2.3 Selecting the tunnel to open according to the compliance level

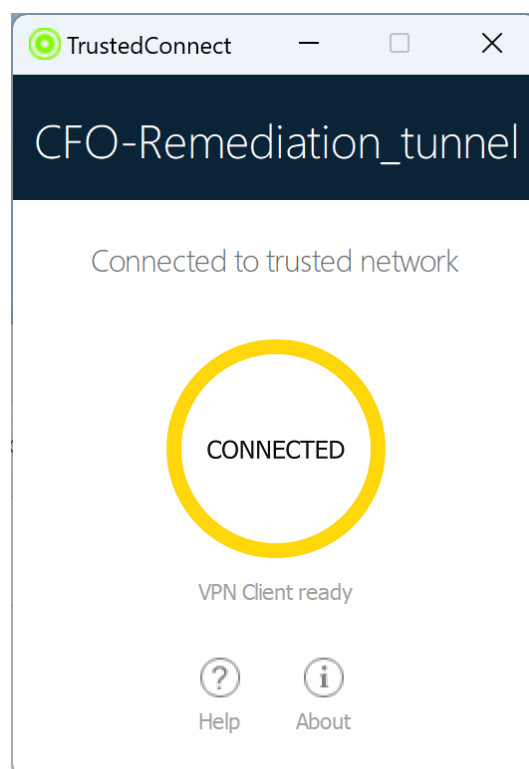
24.2.3.1 In the TrustedConnect Panel

The **TrustedConnect Panel** uses the compliance level when a tunnel is selected.

When the compliance check fails, the following message is displayed:



When the workstation must go over a remediation area and a remediation tunnel has been configured, the following message is displayed:



The **TrustedConnect Panel** takes into account compliance changes on the fly. The **TrustedConnect Panel**'s behavior can be configured using the MSI property `DIALERBEHAVIOR` (see the "Deployment Guide") in order to cause an automatic switchover to the following:

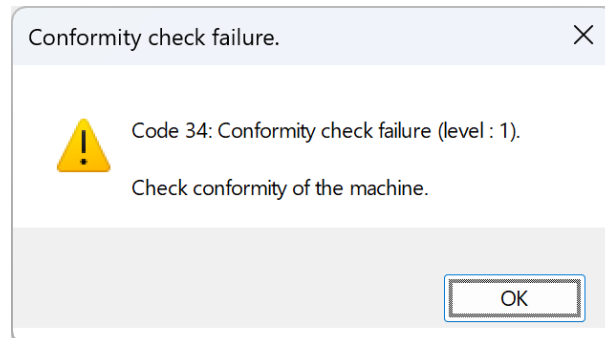
- A compliance error or a remediation tunnel when the compliance level is no longer satisfactory
- A normal tunnel when compliance level becomes satisfactory again
- The remediation tunnel when the compliance level requires switching to a remediation area

24.2.3.2 In the Connection Panel

The compliance check can be performed in the **Connection Panel** in a similar fashion to how it works in the **TrustedConnect Panel** (see section 24.2.3.1 In the TrustedConnect).

The main difference with the **TrustedConnect Panel** resides in the fact that there is no automation in the **Connection Panel**. The verification to decide whether the tunnel should be opened according to the compliance level is only made when the tunnel is actually being opened.

When the tunnel should not be opened, an error is displayed on the screen and a message is recorded in the **Console**:



If a remediation tunnel is configured, the user will be able to open it in order to bring the workstation into compliance.

When the SCA is not installed and therefore the compliance check is not enabled, any tunnel linked to any connection can be opened.



The compliance level is only available at the connection level, not at the tunnel level. The compliance check therefore is only handled in the **Connection Panel** mode.

Any user who can access the VPN Client's **Configuration Panel** can mount any tunnel regardless of the compliance level.

24.2.3.3 In GINA mode

Because the information required to switch to a remediation tunnel is not available before logging on to Windows, opening a remediation tunnel is not possible in GINA mode. However, it won't be possible to open any tunnel as long as the workstation does not meet any of the compliance criteria.

24.3 Forwarding audit traces from the VPN Client to the CMC

24.3.1 Introduction

Audit trace forwarding is used to collect the audit traces generated by the VPN Client (stored in the `LogFiles\System` sub-folder) and forward them to the Connection Management Center (CMC).



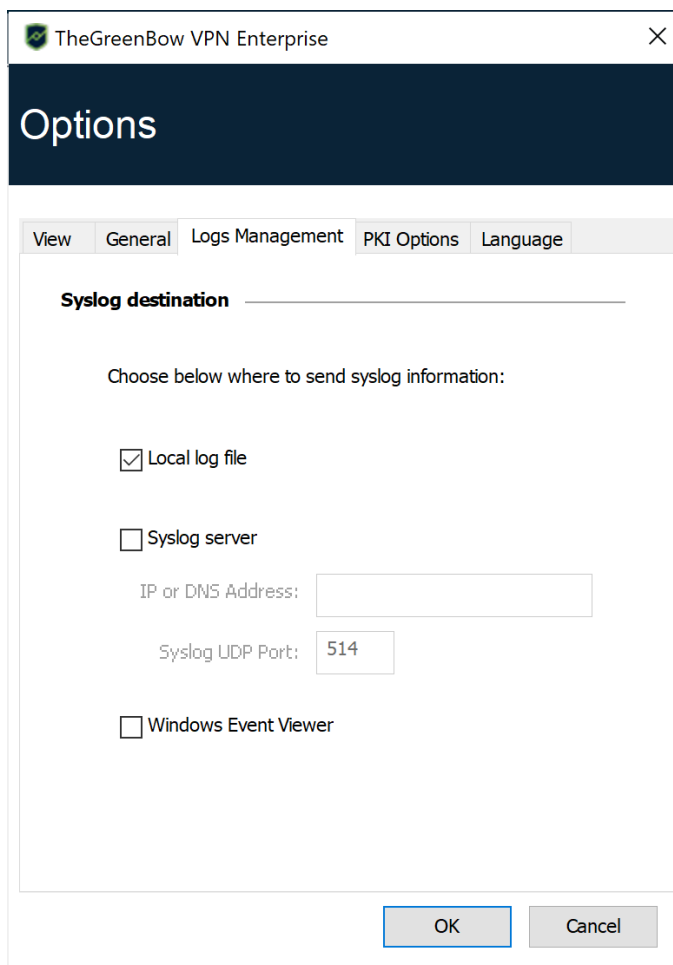
To find out how to configure the agent, refer to the SCA's "Administrator's Guide" available on [TheGreenBow](#)'s website.

24.3.2 Configuring the VPN Client

Audit traces can only be forwarded if the VPN Client generates audit traces in the first place!

To enable audit traces, proceed as follows:

1. Access the Windows Enterprise VPN Client's **Configuration Panel**.
2. From the **Tools** menu, choose **Options...**
3. Select the **Logs Management** tab.
4. Check the **Local log file** box.
5. Click **OK**.



The screenshot shows the 'Options' dialog box for 'TheGreenBow VPN Enterprise'. The 'Syslog destination' tab is selected. The dialog has a dark blue header with the title 'Options'. Below the header is a tab bar with 'View', 'General', 'Logs Management', 'PKI Options', and 'Language'. The 'Logs Management' tab is active. The main content area is titled 'Syslog destination' and contains the instruction 'Choose below where to send syslog information:'. There are three options: 'Local log file' (checked), 'Syslog server' (unchecked), and 'Windows Event Viewer' (unchecked). The 'Syslog server' option has two input fields: 'IP or DNS Address:' and 'Syslog UDP Port: 514'. At the bottom right are 'OK' and 'Cancel' buttons.



Refer to chapter 26 Administrator logs, Console, and traces for a complete description of the various types of logs available.

25 Options

25.1 View

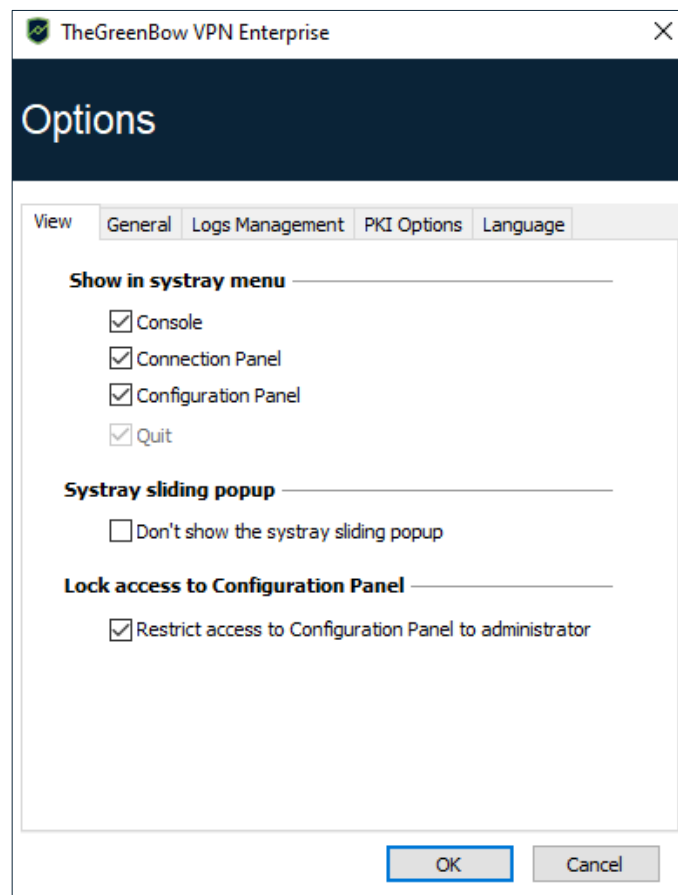
Using the options listed on the **View** tab in the **Options** window, you can hide nearly all of the software's interfaces:

- Options in the taskbar menu
- Fade-out pop-up in the taskbar
- Access to the **Configuration Panel**

25.1.1 Showing options in systray menu

You can choose to hide the **Console**, **Configuration Panel** and **Connection Panel** options in the taskbar (systray) menu. The menu can thus be reduced to the single item **Quit**.

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



25.1.2 Showing the systray fade-out pop-up

When the **Don't show the systray sliding popup** option is disabled, a fade-out pop-up appears above the VPN Client icon in the taskbar when a VPN tunnel is opened or closed.

This pop-up 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 open



Tunnel is closed



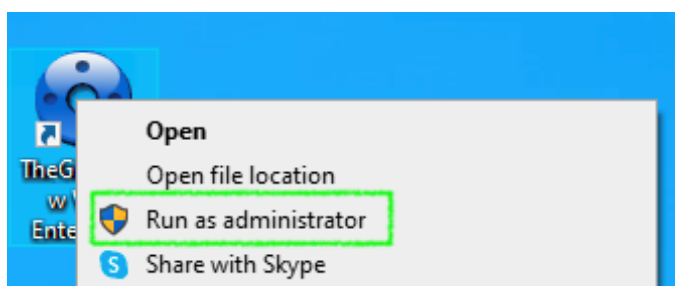
Failed to open the tunnel: the window will briefly explain what happened and provide a hyperlink for more information about the incident.



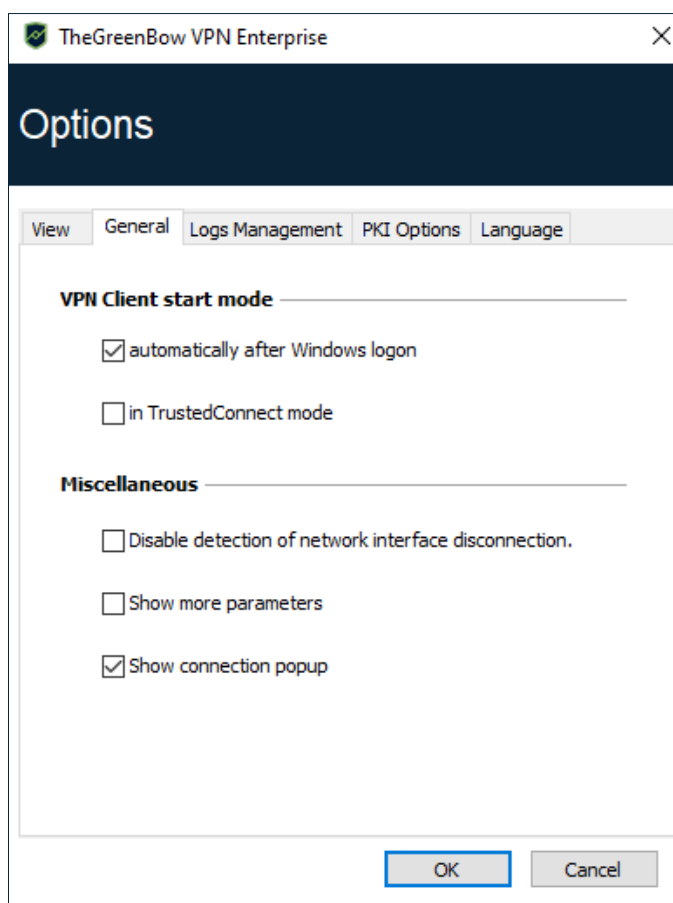
25.1.3 Restricting access to the Configuration Panel

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

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



25.2 General



25.2.1 VPN Client startup mode

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

If the option is not checked, the user must start the VPN Client manually, either by double-clicking on the desktop icon or by selecting the software in the Windows **Start** menu.



Refer to section 6.2 Starting the software for further details.

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

25.2.2 Disabling detection of network interface disconnection

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

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

When the **Disable detection of network interface disconnection** box is checked, the VPN Client will not close tunnels as soon as a disconnection is observed. This guarantees a very stable VPN tunnel, even on unreliable physical networks, typically wireless networks such as Wi-Fi, 4G, 5G or satellite.

25.2.3 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.

25.2.4 Displaying more parameters

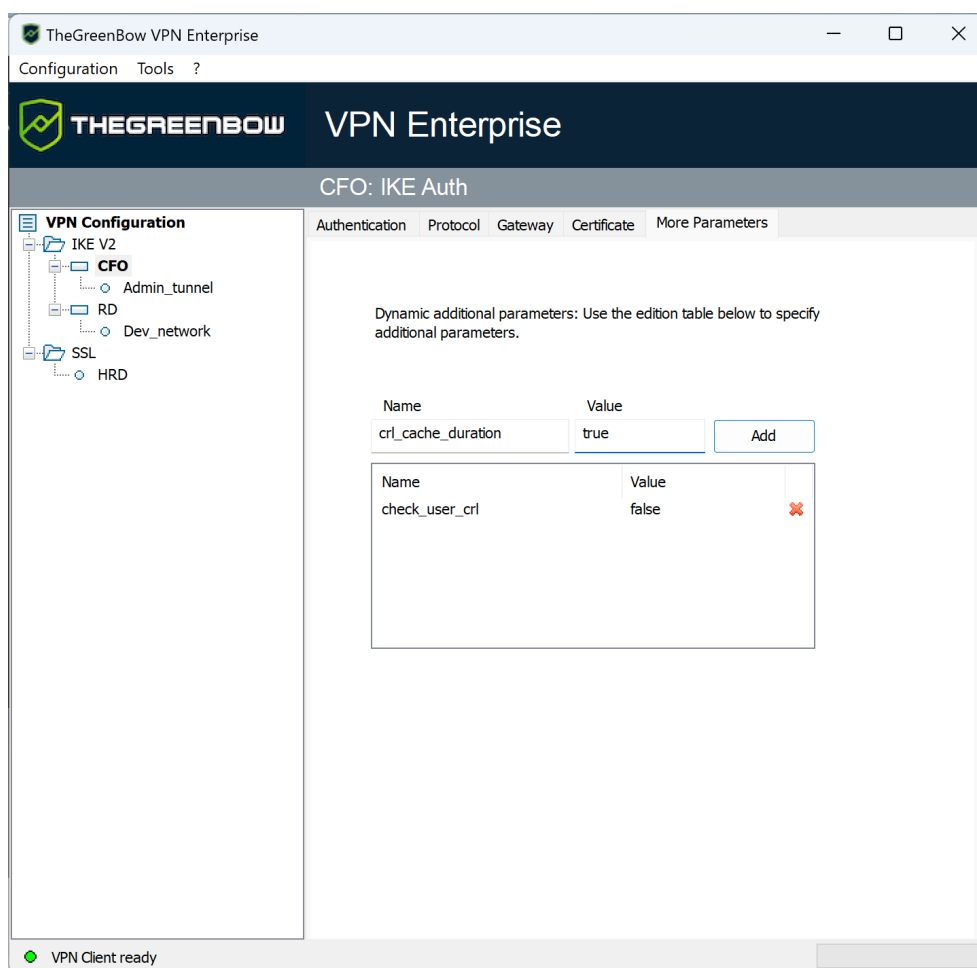
If required, you can configure additional dynamic parameters for the Windows Enterprise VPN Client under its IKE Auth configuration. Only the following dynamic parameters are documented in this guide:

- Specify IP address of network interface
 - `local_subnet` (see section 13.3.1.1)
- Specify nonce size for IPsec DR gateways
 - `nonce_size` (see section 13.3.2)
- Specify the size of the virtual local network
 - `local_virtual_network_size` (see section 13.3.6.1)
- Select a certificate based on its subject
 - `user_cert_dnpattern` (see section 18.2.2.1)
- Select a certificate based on its “key usage” field
 - `user_cert_keyusage` (see section 18.2.2.2)
- Select the token/smart card reader to be used for automatic user certificate selection
 - `reader_pattern` (see section 18.2.2)
- Define certificate store to use at tunnel level
 - `MachineStore` (see section 18.6.1)
- Enable the Online Certificate Status Protocol (OCSP)
 - `enable_OCSP` (see section 18.8)

- Prevent or limit CRL download
 - `check_user_crl` (see section 18.8.1)
 - `crl_cache_duration` (see section 18.8.1)
- Validate the certificate even if it does not comply with the constraints on the Key Usage extension
 - `allow_server_extra_keyusage` (see section 18.8.2)
- Validate the certificate even if it does not comply with the constraints on the Extended Key Usage extension
 - `allow_server_and_client_auth` (see section 18.8.3)
- Use the SHA-2 hash algorithm in the certificate request payload
 - `sha2_in_cert_req` (see section 18.9)
- Use other certificate authentication methods
 - `Method14_RSASSA_PKCS1` (see section 29.4.5)
 - `Method1_PKCS1v15_Scheme` (see section 29.4.5)
- Use method 214 or method 14 to authenticate Brainpool user certificates
 - `use_method_214` (see section 29.4.5)
- Display a customized message in the PIN code request pop-up window
 - `user_smartcard_tip` (see section 18.5)

Under certain circumstances, TheGreenBow's support team may ask you to add other dynamic parameters (Name, Value) that are not documented in this guide. These are intended to manage specific use cases, either in the installed version of the software or in patches that will be provided to you.

To enable the **More parameters** tab in the VPN tunnel configuration window as shown below, check the **Show more parameters** option on the **General** tab in the **Options** window.



25.3 Managing logs



Refer to section 26.1 Administrator logs.

25.4 PKI Options

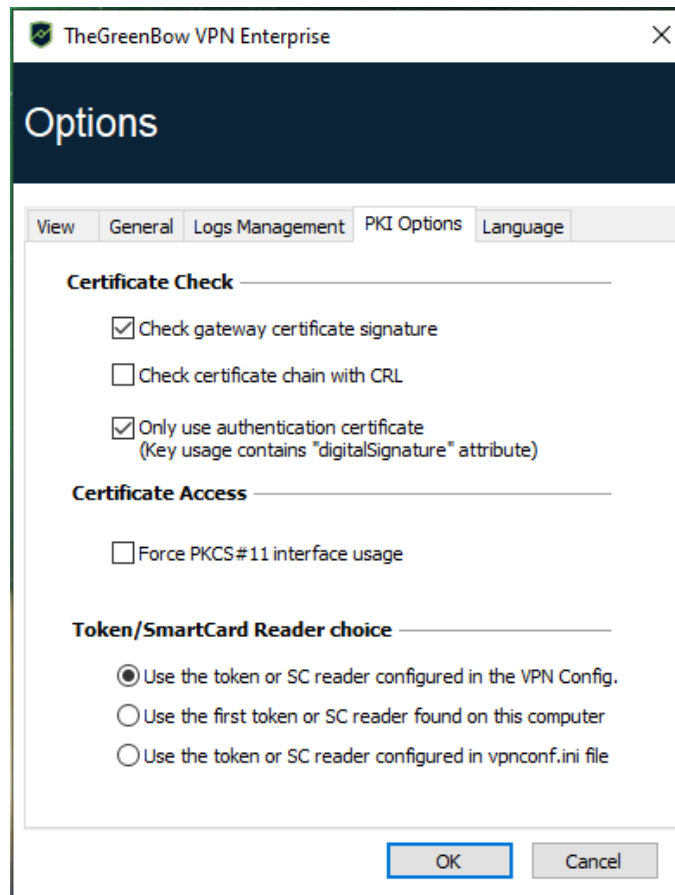
The **PKI Options** tab is used to fine-tune smart card and token management and to further specify certificate access.

PKI options include the following:

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



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





25.4.1 Certificate Check

Check gateway certificate signature

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



When this option is selected, the subject of the gateway certificate must be entered in the Remote ID of the tunnel concerned to prevent vulnerability [2018 7293](#) from being exploited.

Check certificate chain with CRL

When this option is selected, the VPN Client checks the Certificate Revocation List (CRL) of the VPN gateway certificate, as well as the CRL of all certificates in the certificate chain down to the root certificate.

The root and intermediate certificates must be imported into the configuration or available in the Windows Certificate Store. Likewise, the CRLs must also be accessible, either in the Windows Certificate Store or available for download.



As of version 7.5 of the Windows Enterprise VPN Client, you can check the revocation of the gateway certificate using Online Certificate Status Protocol Stapling (OCSP Stapling). To do this, you must add the dynamic parameter `enable_OCSP` set to the value `true` (see section 25.2.4 Displaying more parameters).

Certs of Gateway and Client are issued by different CA

If the VPN Client and the VPN gateway use certificates from a different certificate authority, this box must be checked.

Only use authentication certificate

When this option is checked, the VPN Client will only take into account **Authentication** certificates (i.e. certificates whose Key Usage extension contains the `digitalSignature` attribute).


This function allows you to automatically select a certificate when several are stored on the same smart card or token.

The checkbox is grayed out when the MSI property `KEYUSAGE` is set to 2 or 3 during installation (refer to the "Deployment Guide").

25.4.2 Certificate Access

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

25.4.3 Token/Smart Card Reader choice

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



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

25.5 Managing languages

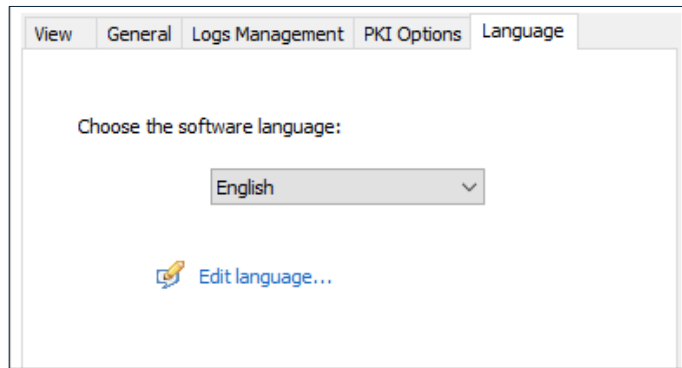
25.5.1 Choosing a language

The Windows Enterprise VPN Client can run in several languages.

You can change languages while running the software.

To choose another language, open the **Tools > Options** menu, then select the **Language** tab.

Choose the desired language in the drop-down menu:

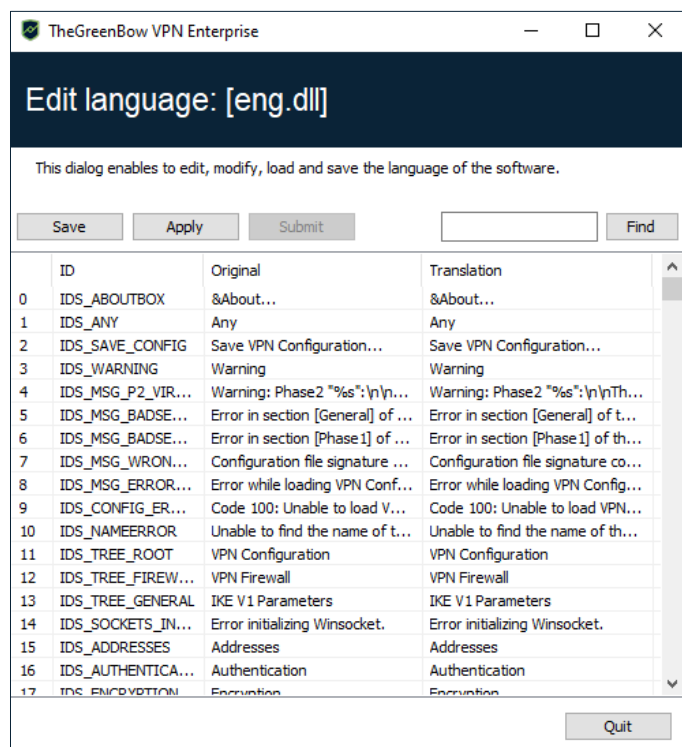


The list of languages available in the standard version of the software is provided in an appendix in section 29.5 Windows Enterprise VPN Client technical data.

25.5.2 Editing or creating a language

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

On 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:

- Translate each character string by clicking on the corresponding row.
- 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).
- Save the changes (**Save** button).

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

- 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).
- Send a new translation to TheGreenBow (**Submit** button).

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



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



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

%s	the software will replace it by a character string
%d	the software will replace it by a digit
\n	indicates a carriage return
&	indicates that the following character should 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 `IDS_SC_P11_3` string must be left as is.



26 Administrator logs, Console, and traces

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

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

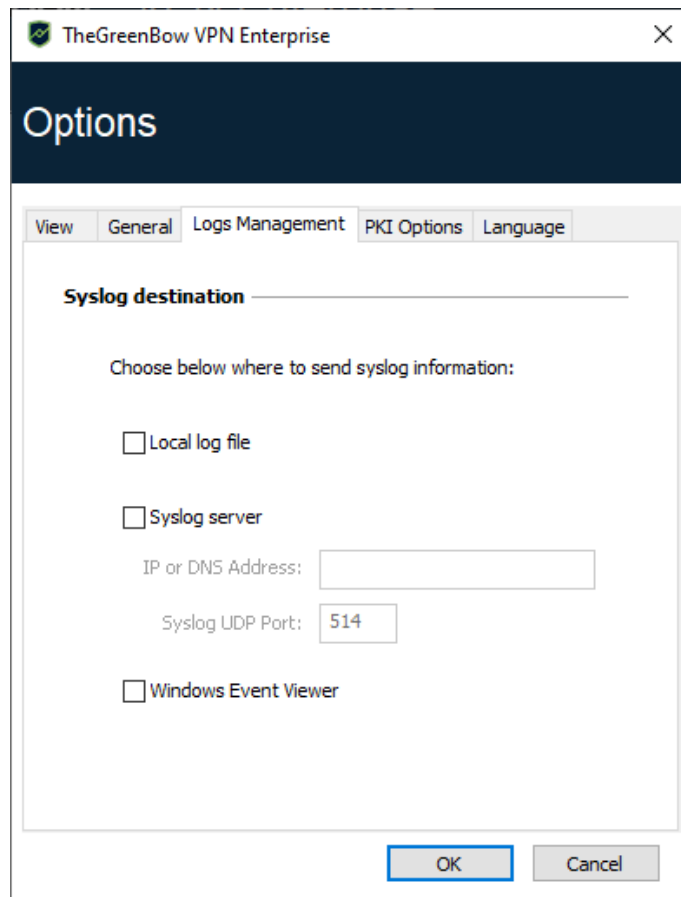
26.1 Administrator logs

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

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

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

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



Administrator logs are listed in section 29.2 Administrator logs in the appendixes.



Administrator logs are only available in English. They are not localized into any other language.

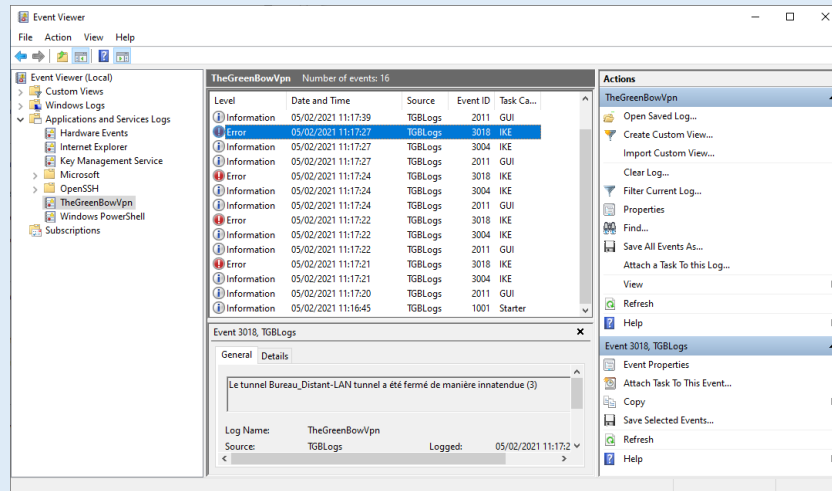


When administrator logs are stored in a local file, the path to these logs is the **System** sub-directory in the logging directory:

C:\ProgramData\TheGreenBow\TheGreenBow VPN Enterprise\LogFiles\System.

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

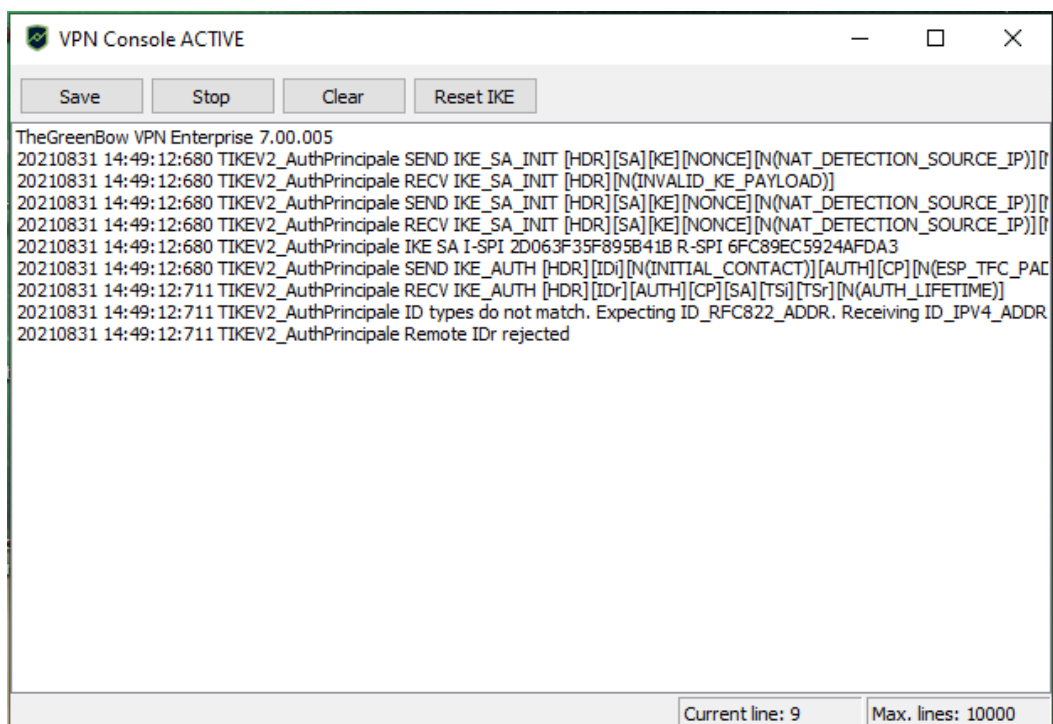
The path for Windows Enterprise VPN Client logs in the Windows Event Viewer is the following:



26.2 Console

Access the **Console** using either of the following methods:

- **Tools > Console** menu in the **Configuration Panel** (main interface)
- **Console** option in the **TrustedConnect Panel**'s contextual menu
- 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

26.3 Trace mode

Trace mode is enabled using the following shortcut: Ctrl+Alt+T.

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

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



Trace logs can only be enabled on the **Configuration Panel** and access to the **Configuration Panel** can be restricted to administrators.



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



Log files are generated every day and kept for 10 days by default. The software automatically deletes any files that are older than this. The period during which logs are kept can be configured using the `VPNLOGPURGE` property of the VPN Client installer (refer to the "Deployment Guide").



Administrator logs stored in a local file will not be deleted (see section 26.1 Administrator logs).



27 Security recommendations

27.1 Assumptions

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

27.1.1 Profile and responsibilities of administrators

The system and network administrator as well as the security administrator, respectively tasked with installing the software and defining the VPN security policies, are nonhostile. They are trained to carry out the tasks for which they are responsible and follow administrative manuals and procedures.

The security administrator regularly ensures that the product's configuration is in line with the one that he or she has set up and performs the necessary updates when necessary.

The product's logging function is enabled and properly configured. Administrators are responsible for regularly reviewing the logs.

27.1.2 Profile and responsibilities of users

Users of the software are nonhostile and have been properly trained on how to use it. More specifically, users execute the tasks for which they are responsible to ensure proper operation of the product and do not reveal the information used for their authentication with the VPN gateway.

27.1.3 Compliance with management rules for cryptographic elements

Bi-keys and certificates used to open the VPN tunnel are generated by a trustworthy certificate authority that guarantees compliance with management rules for these cryptographic elements and, more specifically, with the specifications laid out by your local cybersecurity agency, e.g. [\[RGS B1\]](#) and [\[RGS B2\]](#) in France (only available in French).

27.2 User workstation

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

- Antivirus software must be installed, and its signature database must be updated on a regular basis.

- 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.
- Its operating system is up to date with the various security patches.
- Its configuration is such that it is protected against local attacks (memory forensics, patch, or binary corruption).

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

- [Computer health guide](#) (Guide d'hygiène informatique, document only available in French)
- [Configuration guide](#) (Guide de configuration, document only available in French)
- [Password](#) (Mot de passe, document only available in French)

27.3 VPN Client administration

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

We recommend that you protect access to the VPN configuration with a password and restrict the software's visibility to end users (default behavior of the Windows Enterprise VPN Client) as detailed in section 25.1.3 Restricting access to the Configuration Panel.

We recommend that you enable the hash integrity check for the VPN configuration file using the MSI property `SIGNFILE` set to 1 when installing the software (see MSI `SIGNFILE` property in the “Deployment Guide”). When the property is not specified during installation, its default value is 0 (disabled).

The software must therefore be run as administrator to be able to access the **Configuration Panel**.

We recommend keeping the **Start VPN Client after Windows Logon** mode enabled, which is the default mode upon installation.

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



27.4 VPN configuration

27.4.1 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:

- Do not use the EAP (password/login) mode alone, but only in combination with a certificate.
- If EAP is used, do not store the EAP login name/password in the VPN configuration (function described in section 13.3.1.2 Authentication).
- Do not import any certificates to the VPN configuration (function described in section 18.4 Importing a certificate to the VPN configuration) and preferably use certificates stored on removable devices (tokens) or in the Windows Certificate Store.
- Do not use the “Preshared key” mode (function described in section 13.3.1 IKE Auth: Authentication”) and preferably use the “Certificate” mode with certificates stored on removable media (tokens) or in the Windows Certificate Store.
- Do not export the VPN configuration without encrypting it, i.e. not password-protected (function described in section 12.2 Exporting a VPN configuration).

27.4.2 User authentication

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

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

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

27.4.3 VPN gateway authentication

We recommend that you implement a check on the VPN gateway certificate as described in section 25.4 PKI Options.

We recommend that you do not configure the VPN Client to validate certificates that do not comply with the constraints on the Extended Key Usage and Key Usage extensions (do not use dynamic parameters `allow_server_and_client_auth` and `allow_server_extra_keyusage`).

27.4.4 Protocol

We recommend that you only configure IPsec/IKEv2 tunnels (and no SSL/OpenVPN tunnels).

27.4.5 “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 13.3.6.5 Configuring the address type and 13.3.7.3 Miscellaneous.

27.4.6 GINA mode

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



27.4.7 ANSSI recommendations

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

28 Contact

28.1 Information

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

28.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

28.3 Support

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

Online help

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

FAQ

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

Contact form

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



29 Appendixes

29.1 Shortcuts

29.1.1 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.

29.1.2 VPN configuration tree

F2	Used to edit the name of the selected.
Del	Deletes 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 Child SA is selected.
Ctrl+W	Closes the corresponding VPN tunnel if a Child SA 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 IKE Auth. If an IKE Auth is selected, creates a Child SA.
Ctrl+S	Saves the VPN configuration.

29.1.3 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 trace mode (log generation).
Ctrl+S	Saves the VPN configuration.

29.2 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_TGBIKESTARTED	3001	Notice	IKE has started (status %d).
LOGID_TGBIKESTOPPED	3002	Notice	IKE has stopped.
LOGID_TUNNELOPEN	3004	Info	Tunnel %s is asked to open.
LOGID_VPNCONFCRASHED	2003	Notice	GUI crashed (state %d).
LOGID_TGBIKECRASHED	3003	Notice	IKE crashed (state %d).
LOGID_STARTERSTOP	1002	Notice	Starter service is stopped.
LOGID_RESETIKE	2007	Warning	IKE is asked to reset.
LOGID_VPNCONFSTARTED	2008	Notice	GUI has started from user %s.
LOGID_VPNCONFSTOPPING	2009	Notice	GUI is stopping from user %s.
LOGID_VPNCONFLOADERROR	2010	Error	Configuration couldn't load (reason: %s).
LOGID_VPNCONFOPENTUNNEL	2011	Info	GUI opens tunnel (source: %s).
LOGID_VPNCONFCLOSETUNNEL	2012	Info	GUI closes tunnel (source: %s).
LOGID_VPNCONFSAVE	2013	Notice	New configuration is saved.
LOGID_VPNCONFIMPORT	2014	Info	%s has been imported.
LOGID_VPNCONFIMPORTERR	2015	Error	%s could not be imported (status %d).
LOGID_VPNCONFEXPORT	2016	Info	%s has been exported.
LOGID_TOKENINSERT	2017	Info	Token %s has been inserted.
LOGID_TOKENEXTRACT	2018	Info	Token %s has been extracted.
LOGID_USBININSERT	2019	Info	USB Key has been inserted.



ID Log define	ID Log value	Severity	Log string
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 %s Ok
LOGID_TUNNELAUTH_NOK	3007	Error	Tunnel authentication failed (reason %d).
LOGID_TUNNELTRAFFIC_NOK	3008	Error	Tunnel %s failed (reason %d).
LOGID_AUTHREKEYING	3009	Info	Tunnel %s initiated rekey (source %d).
LOGID_AUTHREKEYED	3010	Info	Tunnel %s rekeyed.
LOGID_TUNNELREKEYING	3011	Info	Tunnel %s initiated rekey (source %d).
LOGID_TUNNELREKEYED	3012	Info	Tunnel %s rekeyed.
LOGID_PINCODE	3013	Notice/Error	Pin code is entered (status %d).
LOGID_DRIVERNOK	3014	Critical	Driver could not be loaded (status %d).
LOGID_IKEEXT_STOP	1003	Warning	IKEEXT service is stopped.
LOGID_IKEEXT_RESTART	1004	Notice	IKEEXT service is restarted.
LOGID_IKEEXT_ERROR	1005	Critical	IKEEXT could not be stopped (status %d).
SYSTEMLOGID_VIRTIFOK	3015	Info	Virtual interface created successfully (instance %d).
SYSTEMLOGID_VIRTIFNOK	3016	Error	Virtual interface could not be created (error %d).
LOGID_TUNNELCLOSED	3017	Notice	%s tunnel successfully closed (%d min).
LOGID_TUNNELCLOSED_ERR	3018	Error	%s tunnel closed unexpectedly (%d).
LOGID_CERTERROR	3019	Error	Error %d when handling certificate %s.

29.3 TrustedConnect Panel diagnostics

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

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

Code	Diagnostics	Solution
0	VPN configuration issue VPN connection not found in configuration	<ul style="list-style-type: none"> Make sure that the <code>tgvpn.conf</code> file is available in the VPN Client installation directory.
1	Issue with a certificate The VPN configuration uses a certificate whose private key cannot be found.	<ul style="list-style-type: none"> Check the VPN Client's configuration and any possible associated authentication devices (smart card reader, token, or Windows Certificate Store). Reimport the VPN configuration and then reimport the certificate concerned. Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
3	Configuration issue The message No proposal chosen has been received during an IKE exchange: the cryptographic algorithm suite configured for the IKE_SA_INIT sequence does not match the one configured on the gateway.	<ul style="list-style-type: none"> Verify that the cryptographic algorithm suite for THE IKE_SA_INIT sequence of the VPN connection matches that of the gateway (refer to IKE Auth in the Configuration Panel).
4	Configuration issue The message "No proposal chosen" has been received during an IKE exchange: the cryptographic algorithm suite of the ESP protocol does not match the one configured on the gateway.	<ul style="list-style-type: none"> Verify that the cryptographic algorithm suite of the ESP protocol (refer to Child SA in the Configuration Panel) matches that of the gateway.
5	Cannot access gateway The gateway address ("Remote Router Address") specified in the VPN configuration is not reachable. If it is an IP address, it cannot be found or cannot be reached. If it is a DNS address it may be inaccessible, indefinite, or cannot be resolved.	<ul style="list-style-type: none"> Check the address of the gateway/remote workstation. For example, try "pinging" this address.
6	Configuration issue The message Remote ID other than expected has been received. This means that the value of the Remote ID does not match the value expected by the remote VPN gateway.	<ul style="list-style-type: none"> Make sure that the Local ID parameter on the VPN client's Protocol tab matches the Remote ID of the remote gateway (or workstation). Caution: The Remote ID on the router is the Local ID on the VPN Client and vice versa.



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

Code	Diagnostics	Solution
16	Network configuration An error occurred while creating the virtual interface used for the VPN connection.	<ul style="list-style-type: none"> Retrieve the user log files. They must be analyzed. Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
24	Configuration issue The gateway did not accept the cryptographic algorithm suite provided by the VPN Client.	<ul style="list-style-type: none"> Make sure that the VPN Client's cryptographic algorithm suites match those of the gateway. Check the Local ID and Remote ID. Caution: The Local ID on the router is the Remote ID on the VPN Client and vice versa.
25	Configuration issue The gateway did not accept the remote network configured in the VPN Client or the virtual IP address provided by the VPN Client.	<ul style="list-style-type: none"> Make sure that the virtual IP address (VPN Client address parameter) specified in the VPN Client's configuration is acceptable at the gateway end. Make sure that the remote network (Remote network address parameter) specified in the VPN Client's configuration is acceptable on the gateway end.
26	Configuration issue The VPN client provides its own traffic selectors, while the gateway is configured to provide them.	<ul style="list-style-type: none"> Check the Request configuration from the gateway parameter on the Child SA tab.
27	Gateway error The gateway reported an error not supported by the VPN Client.	<ul style="list-style-type: none"> Analyze the logs on the gateway end. Retrieve the user log files. They must be analyzed. Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
28	Login/password error The gateway has rejected the EAP authentication while establishing the VPN connection.	<ul style="list-style-type: none"> Check the EAP authentication parameters in the VPN Client's configuration. Make sure that the user knows his or her credentials, should he or she need them while establishing the connection.
30	Smart card or token error Cannot access the certificate stored on the smart card or token.	<ul style="list-style-type: none"> Check that the smart card reader or token is correctly configured on the workstation, and that the VPN Client can access it.
31	Captive portal authentication timeout expired No session has been opened on the captive portal. The workstation therefore has no internet connectivity.	<ul style="list-style-type: none"> Click the Connect button in order to authenticate on the captive portal.
100	Cannot load the VPN configuration No VPN connection has been found in the configuration file.	<ul style="list-style-type: none"> Make sure that at least one tunnel is configured in the Connection Panel. Go to Tools > Connections Configuration, then add a tunnel and save the configuration.



Code	Diagnostics	Solution
101	GINA configuration error A tunnel is active before logon, but has not been configured to be used by the TrustedConnect Panel .	<ul style="list-style-type: none">Make sure that the tunnel which is active before logon is also configured in the Connection Panel. Go to Tools > Connections Configuration, then add a tunnel and save the configuration.
102	IKE initialization error An error occurred while initializing the IKE daemon.	<ul style="list-style-type: none">Retrieve the user log files.Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
103	DNS error A DNS name could not be resolved in the set of rules for the Filtering Mode.	<ul style="list-style-type: none">Make sure that the workstation can access the internet.Make sure that the Filtering Mode does not itself block access to DNS queries.Replace DNS names with IP addresses.
200	Software activation The software is not activated, and the trial period has expired.	<ul style="list-style-type: none">Retrieve the user log files.Check software activation.

29.4 Basic cryptography concepts

29.4.1 SHA, RSA, ECDSA, and ECSDSA algorithms

Digital signatures generally involve two different types of algorithms:

- A hash algorithm (SHA: Secure Hash Algorithm)
- A signature algorithm (RSA: initials of the three inventors, ECDSA: Elliptic Curve Digital Signature Algorithm or ECSDSA: Elliptic Curve Schnorr Digital Signature Algorithm)

The strength of RSA encryption depends on the size of the key used. With every doubling of the key length, decryption is six to seven times slower.

According to the NIST and the ANSSI, the recommended minimum key size is 2048 bits.

Hash algorithms can be attacked in either of the following two ways:

- Hash collision
- Preimage

A collision occurs when two distinct files produce the same hash value, and it thus becomes possible to substitute one for the other.

Preimage consists in determining the value of a file from its hash value. A second preimage consists in starting out from the hash value to produce a value that is different from the one originally used with the hash function.

According to the ANSSI, the family of SHA-1 hash functions no longer complies with its general security reference system (RGS) and the SHA-2 family should therefore be used. The NIST similarly encourages US federal agencies to switch from SHA-1 to SHA-2.

The rules applied by the Windows Enterprise VPN Client follow NIST and ANSSI recommendations. However, if the implemented PKI does not meet these requirements, some of these restrictions can be removed from the software using dynamic parameters.



There are several notations in use for the SHA-2 family of algorithms. For example, SHA-2 (256 bits) is also written SHA-256, SHA-2 (384 bits) is also written SHA-384, and so on.

The same applies to elliptic curves. For example, secp256r1 is also referred to as the “P-256 curve”, secp384r1 as the “P-384 curve”, and secp521r1 as the “P-521 curve”.

29.4.2 Accessing certificates

29.4.2.1 CSP, CNG, and PKCS #11: what are the differences?

Certificate management in Windows involves a variety of software and standards regardless of whether certificates are stored in a certificate store, on a token, or on a smart card.



Certificates stored on smart cards or tokens are usually copied to the current user's certificate store when the card is inserted into the reader or when the token is connected to the computer.

CSP, CNG, and PKCS #11 are related concepts that all use application programming interfaces (APIs) for certificate management, but the technology implemented is different in each case.

29.4.2.2 CSP and KSP

In Windows, certificate management traditionally used independent software modules called Cryptographic Service Providers (CSPs). CSPs actually perform algorithms for authentication, encoding, and encryption.

Today, there is a new generation of independent software modules called Key Storage Providers (KSPs). A KSP is used to create, manage, store, and retrieve private keys.



29.4.2.3 CAPI and CNG

Changing security standards have led Microsoft to deprecate the API associated with CSPs, called Cryptography API (CryptoAPI or CAPI). It has now been replaced with Cryptography API: Next Generation (CNG), which separates cryptographic service providers from key storage providers.

For this reason, versions 7.2 and higher of the Windows Enterprise VPN Client do not support CSPs and only support the CNG API. You therefore need to ensure that the certificate is imported into the Windows Certificate Store with the correct library (see section 29.4.3 Determining a certificate's container type below).

29.4.2.4 Machine store and user store

It should also be noted that there are two certificate stores in Windows:

- The machine store that is available to all users of a machine
- The user store that is only available to the current user of a machine



In command lines, the `-user` option of the `certutil` command is used to specify the user store. When it is omitted, the machine store will be used by default.

29.4.2.5 PKCS #11

In cryptography, PKCS stands for Public Key Cryptography Standards. They are a set of specifications developed by RSA Security.

The PKCS #11 standard provides applications with a method of accessing hardware peripherals (smart cards or tokens), regardless of the type of device. It therefore includes an API serving as a generic interface for a device driver that supports the PKCS #11 standard. This API is supported both by versions 6.8x and 7.x of the Windows Enterprise VPN Client if a corresponding middleware is installed.

29.4.2.6 Summary

In summary, there are several types of middleware used to access certificates stored on tokens, on smart cards, and in certificate stores (`certmgr.msc`):

- **CSP** stands for **Cryptographic Service Provider** (deprecated and replaced with CNG): supported up to versions 6.8x
- **CNG** stands for **Cryptography API: Next Generation**: only API supported in versions 7.x. In this case, you must import the certificate into the Windows store using the right library.
- **PKCS #11** stands for **Public-Key Cryptography Standards**: supported by both versions 6.8x and 7.x

29.4.3 Determining a certificate's container type

CSP and CNG are Microsoft middleware. In Windows, certificates are stored in containers of CNG or CSP type.

To find out the container used for certificates stored in the certificate store, on a token, or on a smart card, you can list the certificates contained in the (user or machine) store. The information returned specifies the type of supplier based on which you can infer the container type (CSP or CNG). The latter will then allow you to determine whether the certificate is compatible with version 7.2 or higher of the Windows Enterprise VPN Client.

- To list the certificates contained in the user store, run the following command:

```
certutil -verifystore -user My
```

- To list the certificates contained in the machine store, run the following command:

```
certutil -verifystore My
```

Based on the information returned, you can determine the container type as follows. If the supplier is:

- Microsoft Smart Card Key Storage Provider, the container is of CNG type (compatible with versions 7.2 and higher)
- Microsoft Base Smart Card Crypto Provider, the container is of CSP type (not compatible with versions 7.2 and higher)



For certificates using the PKCS #11 middleware, the container type is irrelevant since it is compatible with both versions of the Windows Enterprise VPN Client.

29.4.4 Certificate format

As of version 7 of the Windows Enterprise VPN Client, certificates must be in a format that conforms to a specific key size and hash algorithm.

Mandatory

- Key length: must be at least 2048 bits for RSA certificates
- Digest algorithm: must be SHA-256, SHA-384, or SHA-512

Optional

CRL checking for user certificates



As of version 7.5 of the Windows Enterprise VPN Client, you can check the revocation of the gateway certificate using Online Certificate Status Protocol Stapling (OCSP Stapling). To do this, you must add the dynamic parameter `enable_OCSP` set to the value `true` (see section 25.2.4 Displaying more parameters).

29.4.4.1 Gateway certificate

Key Usage extension part

- Must be present
- Must be marked as critical, and
- Must only contain the values `digitalSignature` and/or `nonRepudiation`



If this is not the case, refer to the dynamic parameter `allow_server_extra_keyusage` described in section 18.8.2 Constraints on the Key Usage extension.



In accordance with security requirements, the `keyEncipherment` value of the Key Usage extension has been deprecated and replaced with the `nonRepudiation` value, which is now accepted by default. However, version 7.5 of the Windows Enterprise VPN Client continues to accept the `keyEncipherment` value without needing to use dynamic parameter `allow_extra_keyusage`.



We recommend that you give preference to the `nonRepudiation` value over the `keyEncipherment` value of the Key Usage extension.

Extended Key Usage extension part

- Can be present or not
- If it is present, it must:
 - Be marked as non-critical, and
 - Only contain either of the following values
 - `id-kp-serverAuth` or
 - `id-kp-serverAuth` and `id-kp-ipsecIKE`

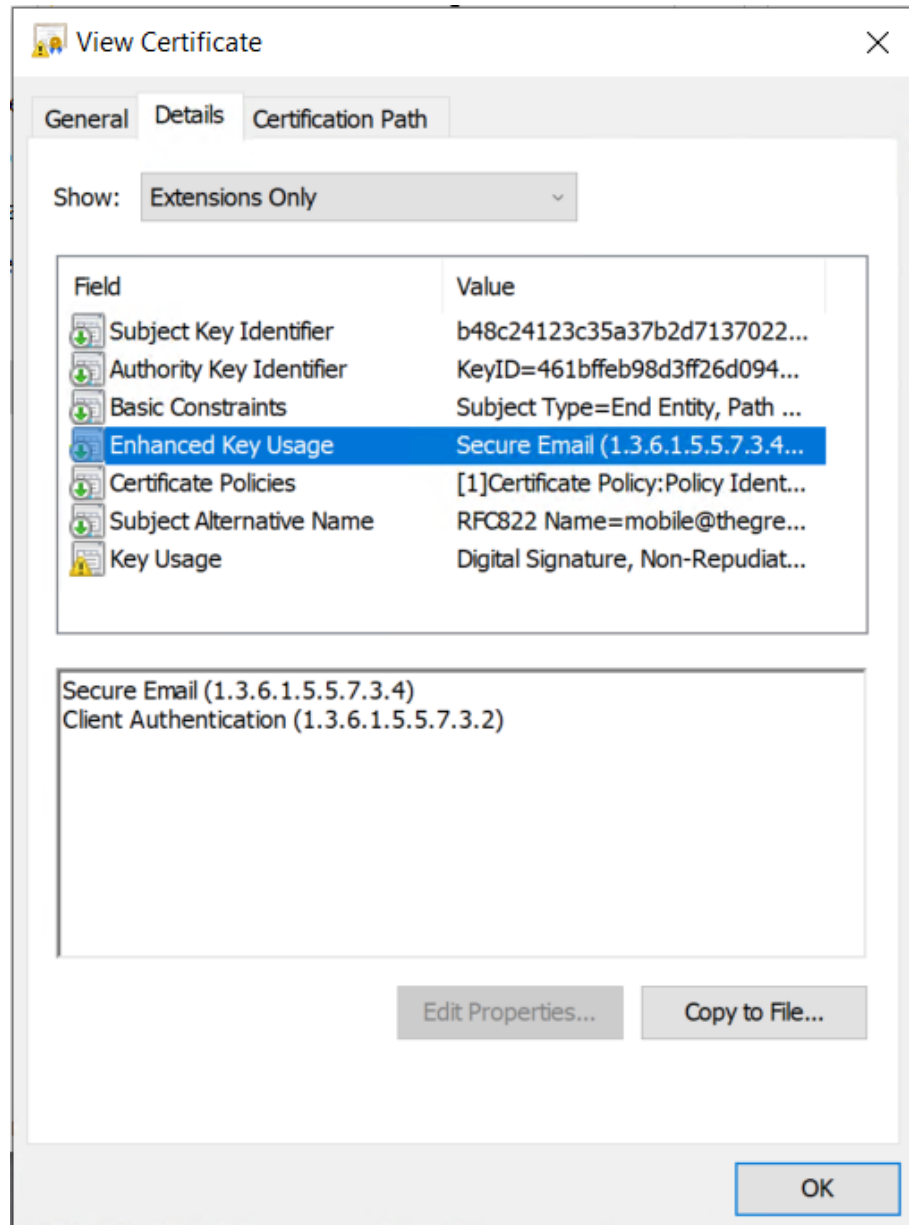


If this is not the case, refer to the dynamic parameter `allow_server_and_client_auth` described in section 18.8.3 Constraints on the Extended Key Usage extension.

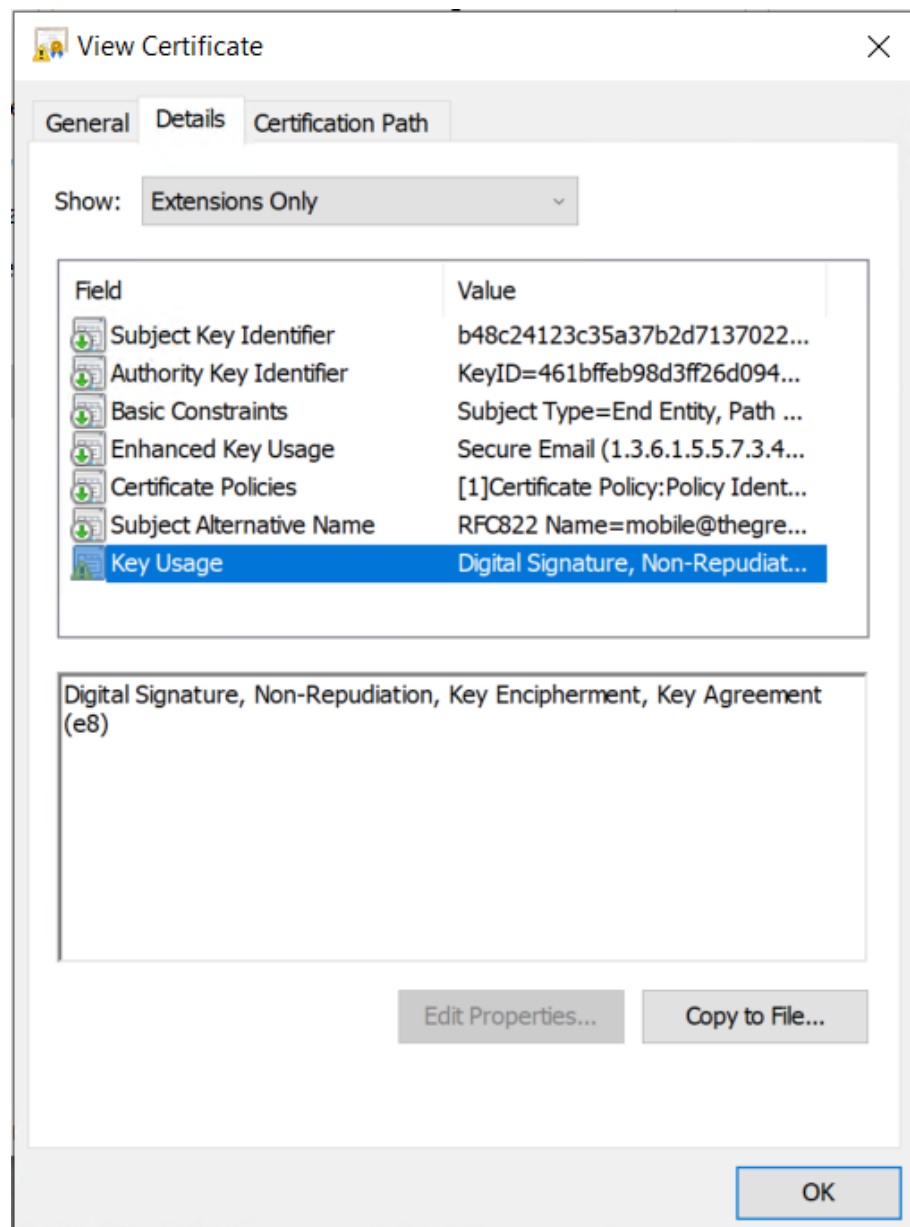
29.4.4.2 Example of a certificate in Windows

In a Windows PKI, the following is the relationship between a certificate and its extensions:

- Extended Key Usage:



- Key Usage:





29.4.4.3 Example of a certificate log

The extensions are included in a certificate log (file named `tgbikeng.log`):

```
20220826 17:20:23:953      Local0.Info      [11204]
X509v3 extensions
20220826 17:20:23:956      Local0.Info      [11204]
Basic constraints :
20220826 17:20:23:960      Local0.Info      [11204]
CA:FALSE
20220826 17:20:23:965      Local0.Info      [11204]
Netscape Certificate comment :
20220826 17:20:23:968      Local0.Info      [11204]
TheGreenBow PKI generated server certificate
20220826 17:20:23:971      Local0.Info      [11204]
Subject key identifier :
20220826 17:20:23:974      Local0.Info      [11204]
FB:D6:5A:EF:FE:1B:DC:68:90:66:B9:D7:47:45:EA:B5:86:97:4
A:B3
20220826 17:20:23:978      Local0.Info      [11204]
Authority key identifier :
20220826 17:20:23:981      Local0.Info      [11204]
keyIdentifier:
6F:6D:B8:A5:0B:EA:64:82:2E:B4:5F:0A:35:53:8B:80:05:4C:7
B:0E
20220826 17:20:23:984      Local0.Info      [11204]
authorityCertIssuer: C = FR, ST = Ile-de-France, L =
Paris, O = TheGreenBow, OU = QA40, CN = Root CA
20220826 17:20:23:988      Local0.Info      [11204]
authorityCertSerialNumber: 10:00
20220826 17:20:23:990      Local0.Info      [11204]
Key usage : critical
20220826 17:20:23:995      Local0.Info      [11204]
Digital signature
20220826 17:20:24:000      Local0.Info      [11204]
Extended key usage :
20220826 17:20:24:003      Local0.Info      [11204]
Server authentication
```

29.4.4.4 User certificate

Warning messages may be displayed in the **Console** for a user certificate, but you do not need to remove any restrictions from the VPN Client.

29.4.5 Certificate authentication methods

The Windows Enterprise VPN Client supports the following certificate authentication methods:

- Method 1: RSA Digital Signature with SHA-2 [RFC 7296]
- Method 9: ECDSA “secp256r1” with SHA-2 (256 bits) on the P-256 curve [RFC 4754]
- Method 10: ECDSA “secp384r1” with SHA-2 (384 bits) on the P-384 curve [RFC 4754]
- Method 11: ECDSA “secp521r1” with SHA-2 (512 bits) on the P-521 curve [RFC 4754]
- Method 14: Digital Signature RSASSA-PSS, RSASSA-PKCS1-v1_5, and Brainpool with SHA-2 (256/384/512 bits) [RFC 7427]
- Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) on the BrainpoolP256r1 curve (only available with gateways that support this method)

The default authentication method used for RSA certificates (RSASSA-PSS or RSASSA-PKCS1-v1_5) is method 14 with an RSASSA-PSS signature. If the gateway/firewall uses method 14 with an RSASSA-PKCS1-v1.5 signature, the VPN Client will reject the certificate and the following message will be displayed in the **Console**:

```
RSASSA-PKCS1-v1_5 signature scheme not supported with  
authentication method 14
```

In the event that the gateway does not support method 14 with an RSASSA-PSS signature, you can configure the VPN Client to use method 14 with an RSASSA-PKCS1-v1_5 signature, by adding the dynamic parameter `Method14_RSASSA_PKCS1` with a value set to `true` or `yes` (see section see section 25.2.4 Displaying more parameters).

In the event that the gateway does not support method 14 with an RSASSA-PKCS1-v1_5 signature, you can configure the VPN Client to use method 1 with an RSA and SHA-2 digital signature, by adding the dynamic parameter `Method1_PKCS1v15_Scheme` with a value set to 04 (SHA-256), 05 (SHA-384) or 06 (SHA-512) (see section 25.2.4 Displaying more parameters). The VPN Client will reject any other value entered.

The authentication method used for ECDSA certificates (elliptical curves) depends on the elliptical curve used in the certificate: ECDSA with SHA-256 on the P-256 curve, ECDSA with SHA-384 on the P-384 curve, ECDSA with SHA-512 on the P-521 curve or ECDSA with SHA-256 on the BrainpoolP256r1 curve.

When the VPN Client needs to create a signature for a Brainpool user certificate, authentication method 14 is used by default, which is appropriate for a gateway that is not running in Restricted mode. If this type of certificate



is to be used with a gateway running in Restricted mode, the dynamic parameter `use_method_214` must be added and set to the value `true` (see section 25.2.4 Displaying more parameters). The `NID_sha256`, `NID_sha384`, or `NID_sha512` message digest algorithm is used for signature depending on the key size.



The SHA-1 algorithm cannot be used in digital signatures.



The Windows Enterprise VPN Client will reject RSA certificates with a key size of less than 2048 bits.



The Windows Enterprise VPN Client will reject ECDSA certificates with a key size of less than 256 bits.

29.5 Windows Enterprise VPN Client technical data

29.5.1 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

29.5.2 Operating mode

Invisible mode	Automatically open tunnel when traffic is detected Control access to VPN configurations Hide part or all the interfaces
Gina	Open a tunnel before Windows logon using: GINA/Credential providers on Windows 10
Scripts	Run configurable scripts when opening or closing a VPN tunnel
Remote Desktop Sharing	Open a remote computer with a single click via RDP and VPN tunnel
TrustedConnect Panel	Automatically open tunnel with Always-On and trusted network detection (TND)

29.5.3 Connection/Tunnel

Connection mode	Peer-to-gateway
Networks	IPv4 and IPv6
Protocols	IPsec/IKEv2 SSL/OpenVPN
Mode CP	Automatically retrieve network settings from the VPN gateway

29.5.4 Cryptography and authentication

Encryption, Key group, Hashing (IKEv2)	Symmetric: AES CBC/CTR/GCM 128/192/256 bits Diffie-Hellman: DH 14 (MODP 2048), DH 15 (MODP 3072), DH 16 (MODP 4096), DH 17 (MODP 6144), DH 18 (MODP 8192), DH 19 (ECP 256), DH 20 (ECP 384), DH 21 (ECP 521), DH 28 (BrainpoolP256r1) Hashing: SHA-2 (256/384/512 bits)
TLS security suites (OpenVPN)	TLS 1.2—Medium TLS 1.2—High TLS 1.3: <ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256
Encryption, Hashing (OpenVPN)	Symmetric: AES-128-CBC, AES-192-CBC, AES-256-CBC Hashing: SHA-2 (224/256/384/512 bits)
Authentication	<ul style="list-style-type: none"> • Preshared key • EAP-MSCHAPv2 • X.509 certificates • Multiple Auth



Certificate authentication methods	<ul style="list-style-type: none">• Method 1: RSA Digital Signature with SHA-2 [RFC 7296]• Method 9: ECDSA “secp256r1” with SHA-2 (256 bits) on the P-256 curve [RFC 4754]• Method 10: ECDSA “secp384r1” with SHA-2 (384 bits) on the P-384 curve [RFC 4754]• Method 11: ECDSA “secp521r1” with SHA-2 (512 bits) on the P-521 curve [RFC 4754]• Method 14: Digital Signature RSASSA-PSS, RSASSA-PKCS1-v1_5, and Brainpool with SHA-2 (256/384/512 bits) [RFC 7427]• Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) on the BrainpoolP256r1 curve (only available with gateways that support this method)
PKI	<ul style="list-style-type: none">• Support for certificates in X.509 format• Importing PKCS #12, PEM/PFX certificates• Multiple media: Windows Certificate Store, smart card, token, configuration file• Support for Certificate Revocation List (CRL) and OCSP stapling• Automatically detect a smart card reader or token according to criteria• PKCS #11 and CNG access to tokens and smart cards• Complete check of the “user” and “gateway” certificate chain

29.5.5 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	RFC 3706. Detection of inactive IKE endpoints.
Redundant gateway	Redundant gateway management, automatically selected when DPD is triggered (inactive gateway)

29.5.6 Administration

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



29.6 Third-party licenses

29.6.1 OpenSSL

OpenSSL is licensed under the Apache License 2.0 license, reproduced here.

Apache License
Version 2.0, January 2004
<https://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise

designated in writing by the copyright owner as "Not a Contribution."

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

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

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



the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

29.6.2 LZ4

LZ4 is licensed under the Simplified BSD License, reproduced here.

LZ4 Library
Copyright (c) 2011-2020, Yann Collet
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 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 COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT HOLDER 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.

Protect your connections
in any situation