

Windows Enterprise VPN Client 7.7

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	Potential breaking change.....	1
1.3	What's new in release 7.7	1
1.3.1	Certificate selection	1
1.3.2	Refined CRL cache management.....	2
1.3.3	Push response timeout is now configurable	2
1.3.4	Dynamic parameters have been removed	2
1.4	Other new features introduced in v7	3
1.4.1	Log format.....	3
1.4.2	TrustedConnect Panel forwards logs	3
1.4.3	Automatic certificate selection	3
1.4.4	Remediation tunnel opening notification.....	3
1.4.5	Implements Zero Trust Network Access	4
1.4.6	Filtering Mode	4
1.4.7	Cryptography	4
1.4.8	IKEv1 and vulnerable algorithms have been deprecated.....	5
1.4.9	SSL/OpenVPN	5
1.4.10	EAP	5
1.4.11	Certificate authentication and revocation.....	5
1.4.12	New features in the TrustedConnect Panel	6
1.4.13	New dynamic parameters have been added	7
1.4.14	Enhanced security	7
1.4.15	Improved smart card/token identification	7
2	Installing the software.....	8
2.1	Introduction	8
2.1.1	Minimum requirements.....	8
2.1.2	Digital signature and version	8
2.1.3	Vulnerabilities.....	9
2.2	Installation procedure	9
2.3	Canceling installation	16
2.4	Trial period	16
2.5	Configuring Windows	18



3	Activating the software.....	21
3.1	Step 1	21
3.2	Step 2	22
3.3	Activation errors	22
3.4	Manual activation	23
3.5	Activation using TAS.....	25
3.6	License and activated software.....	26
4	Updating the software.....	27
4.1	How to get an update	28
4.2	Update procedure.....	28
4.3	Updating the VPN configuration	29
4.4	Automation	30
5	Uninstalling the software.....	31
6	Getting started with the software.....	33
6.1	Introduction	33
6.2	Starting the software	33
6.3	Opening a test VPN tunnel from the Connection Panel.....	36
6.4	Configuring a VPN tunnel	39
6.5	Automating the opening of a VPN tunnel	39
6.6	Opening a VPN tunnel from the TrustedConnect Panel	40
7	Configuration Wizard	42
7.1	Step 1	43
7.2	Step 2	43
7.2.1	Configuring an IPsec/IKEv2 tunnel.....	43
7.2.2	For an SSL tunnel (OpenVPN)	44
7.3	Step 3	45
8	Connection Panel	46
9	Configuration Panel	48
9.1	Menus.....	49
9.2	Status bar.....	49

9.3	Shortcuts.....	50
9.4	VPN configuration tree.....	50
9.4.1	Usage	50
9.4.2	Contextual menus.....	51
9.4.3	Shortcuts.....	54
10	TrustedConnect Panel.....	55
10.1	Introduction	55
10.2	Interface.....	55
10.3	Notification area icon and color codes.....	56
10.4	Contextual menu.....	57
10.5	Usage.....	58
10.5.1	Workstation connected to corporate network.....	59
10.5.2	Workstation not connected to corporate network	59
10.6	Error cases.....	61
10.7	Generating logs and Console.....	62
10.8	Selecting the language	63
10.9	Choosing the connection	63
10.10	Current limitations.....	64
11	“About...” window	66
12	Importing and exporting the VPN configuration	67
12.1	Importing a VPN configuration	67
12.2	Exporting a VPN configuration	69
12.3	Merging VPN configurations.....	70
12.4	Splitting a VPN configuration.....	70
13	Configuring a VPN tunnel.....	71
13.1	SSL or IPsec IKEv2 VPN	71
13.2	Editing and saving a VPN configuration.....	71
13.3	Configuring an IPsec IKEv2 tunnel.....	72
13.3.1	IKE Auth: Authentication	72
13.3.2	IKE Auth: Protocol.....	75
13.3.3	IKE Auth: Gateway.....	78
13.3.4	IKE Auth: Certificate.....	79



13.3.5	Child SA: Overview	80
13.3.6	Child SA: Child SA.....	80
13.3.7	Child SA: Advanced.....	84
13.3.8	Child SA: Automation.....	85
13.3.9	Child SA: Remote sharing.....	85
13.4	Configuring an SSL/OpenVPN tunnel	86
13.4.1	Introduction	86
13.4.2	SSL: Authentication	86
13.4.3	SSL: Security	87
13.4.4	SSL: Gateway.....	89
13.4.5	SSL: Establishment.....	92
13.4.6	SSL: Automation.....	95
13.4.7	SSL: Certificate.....	95
13.4.8	SSL: Remote sharing.....	95
14	Redundant gateway	96
15	Automation.....	97
15.1	Tunnel fallback	98
15.2	Automatic Open mode	98
15.3	GINA mode.....	98
15.4	Scripts.....	99
16	Fallback tunnel.....	100
17	IPv4 and IPv6	101
18	Managing dynamic parameters	102
19	Managing certificates	104
19.1	Introduction	104
19.2	User certificate	105
19.2.1	Overview.....	105
19.2.2	Automatic certificate selection	106
19.3	Selecting a certificate (Certificate tab)	111
19.4	Importing a certificate to the VPN configuration.....	114
19.4.1	Importing a PEM/PFX certificate.....	114
19.4.2	Importing a PKCS #12 certificate.....	115
19.5	Using a certificate stored on a smart card or token.....	116

19.6	Using a certificate stored in the Windows Certificate Store	117
19.6.1	Required characteristics.....	117
19.6.2	Importing a certificate depending on the store used	118
19.7	PKI options: specifying the certificate and its storage device	118
19.8	VPN gateway certificate.....	119
19.8.1	Preventing or limiting CRL download or verification.....	119
19.8.2	Constraints on the Key Usage extension.....	126
19.8.3	Constraints on the Extended Key Usage extension	127
19.9	Managing certificate authorities	127
19.9.1	Overview.....	127
19.9.2	Importing a certificate authority.....	128
19.9.3	IPsec DR mode.....	128
20	Remote Desktop Sharing.....	130
21	Configuring the Connection Panel	132
22	Configuring the TrustedConnect Panel	135
22.1	Always-On.....	135
22.1.1	Operating principle	135
22.1.2	Configuring Always-On.....	136
22.2	Trusted Network Detection (TND)	137
22.2.1	Operating principle	137
22.2.2	Configuring TND.....	139
22.2.3	Disabling TND	145
22.3	Scripts.....	146
22.4	Hiding the panel automatically.....	146
22.5	Disabling the disconnect button.....	147
22.6	Removing menu items.....	147
22.7	Automatically restarting the TrustedConnect Panel	147
22.8	Purging logs.....	148
22.9	Behavior when smart card or token is removed.....	148
23	GINA mode.....	149
23.1	Overview	149
23.2	Configuring the GINA mode.....	150
23.3	Using the GINA mode.....	150



24	Filtering Mode.....	152
25	Options	153
25.1	View.....	153
25.1.1	Showing options in notification area menu	153
25.1.2	Showing the notification area fade-out pop-up.....	154
25.1.3	Restricting access to the Configuration Panel	154
25.2	General.....	155
25.2.1	VPN Client startup mode	155
25.2.2	Disabling detection of network interface disconnection	155
25.2.3	Show connection popup	156
25.2.4	Displaying more parameters.....	156
25.3	Managing logs.....	157
25.4	PKI Options.....	157
25.4.1	Certificate Check.....	159
25.4.2	Certificate Access.....	159
25.4.3	Token/Smart Card Reader choice	160
25.5	Managing languages.....	160
25.5.1	Choosing a language	160
25.5.2	Editing or creating a language	161
26	Audit logs, Console, and trace logs.....	163
26.1	Log format.....	163
26.2	Audit logs.....	164
26.3	Console	166
26.4	Trace mode	167
27	Security recommendations.....	169
27.1	Assumptions.....	169
27.1.1	Profile and responsibilities of administrators	169
27.1.2	Profile and responsibilities of users	169
27.1.3	Compliance with management rules for cryptographic elements.....	169
27.2	User workstation.....	169
27.3	VPN Client administration	170
27.4	VPN configuration	171
27.4.1	Sensitive information in the VPN configuration.....	171
27.4.2	User authentication	171

27.4.3	VPN gateway authentication	172
27.4.4	Protocol.....	172
27.4.5	“All through the tunnel” and “split tunneling” modes	172
27.4.6	GINA mode	173
27.4.7	ANSSI recommendations	173
28	Contact	174
28.1	Information.....	174
28.2	Sales.....	174
28.3	Support	174
29	Appendixes.....	175
29.1	Shortcuts.....	175
29.1.1	Connection Panel.....	175
29.1.2	VPN configuration tree.....	175
29.1.3	Configuration Panel.....	176
29.2	Audit logs.....	176
29.3	TrustedConnect Panel diagnostics.....	178
29.4	Activation error list.....	182
29.5	Basic cryptography concepts	184
29.5.1	SHA, RSA, ECDSA, and ECSDSA algorithms	184
29.5.2	Accessing certificates.....	185
29.5.3	Determining a certificate’s container type.....	186
29.5.4	Certificate format	187
29.5.5	Certificate authentication methods	192
29.6	Windows Enterprise VPN Client technical data.....	193
29.6.1	General.....	193
29.6.2	Operating mode.....	193
29.6.3	Connection/Tunnel.....	194
29.6.4	Cryptography and authentication.....	194
29.6.5	Miscellaneous.....	195
29.6.6	Administration.....	196
29.7	Third-party licenses.....	197
29.7.1	OpenSSL.....	197
29.7.2	LZ4.....	199



Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2026-04-07	All	Initial release	FBO, BBR
1.1	2026-05-11	18 19.2.1	Added missing link; refined link target Specified behavior if certificate does not conform to constraints	FGL, YLO, BBR
1.2	2026-07-06	1.2 1.3 2.2, 6, 10, 22, 25 & 26.3 18 19.2.2.2 27.4.7	Added a section on potential breaking changes Added links to the sections concerned by latest changes Specified behavior when minimizing or closing window Changed listing order of dynamic parameters <code>user_cert_keyusage</code> and <code>user_cert_dnpattern</code> Reorganized section and specified how the <code>user_cert_dnpattern</code> dynamic parameter works Updated external link	FBO, BBR
1.3	2026-09-29	10.1 10.5.1 22.2.1.1 22.2.1.2 22.2.1.3 22.2.2 All	Specified that TND relies on DNS suffixes and beacons (HTTPS method) or on domain names (AD method) Corrected a typo Specified that the detection method is selected in the TND tab; added the UDP 389 rule required with Filtering Mode Restricted DNS suffix and beacon requirements to the HTTPS method; corrected “methods” to “steps” Corrected behavior when the domain name list is empty; clarified GINA mode behavior Added a note on the lists used by each detection type; specified how to enter domain names (case, subdomains); reworded table introductions Minor corrections	JFG, BBR

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 Potential breaking change

If you update from a version earlier than 7.6, changes in the VPN Client's behavior may make your existing configuration incompatible.



If the user certificates you are using contain *Key Usage* or *Extended Key Usage* extensions that do not comply with the French National Cybersecurity Agency's (ANSSI) recommendations, update the certificates or use the `user_cert_keyusage` dynamic parameter to ensure that your VPN configuration continues to work with the new version of the VPN Client (see section 19.2 User certificate).

1.3 What's new in release 7.7

1.3.1 Certificate selection

This release introduces two new certificate selection methods:

- Using a regular expression
- Based on certificate authority



For more details, see section 19.2.2.2 Dynamic parameters for automatic certificate selection.

1.3.1.1 Using a regular expression

Regular expression (regex) matching on certificate subject substrings enables more precise certificate selection.



For more details, see paragraph `user_cert_dnpattern` in section 19.2.2.2 Dynamic parameters for automatic certificate selection.



1.3.1.2 Based on certificate authority

With the introduction of the `user_cert_issuerknown` dynamic parameter, user certificate selection can now be restricted to certificates issued by one of the certificate authorities (CAs) specified in the tunnel configuration.



For more details, see paragraph `user_cert_issuerknown` in section 19.2.2.2 Dynamic parameters for automatic certificate selection.

1.3.2 Refined CRL cache management

With the introduction of the following dynamic parameters, CRL caching can now be managed with more granular control:

- `crl_cache_check_period` and `crl_cache_lifetime` define whether the cached CRL must be updated
- `crl_download_retry` implements a CRL download retry mechanism



For more details, see section 19.8.1 Preventing or limiting CRL download or verification.

1.3.3 Push response timeout is now configurable

With the introduction of the `push_request_timer` dynamic parameter, a longer timeout can now be defined for receiving a push reply from an external authentication method for an SSL/OpenVPN tunnel.



For more details, see section 13.4.5.3 Tunnel Establishment Options.

1.3.4 Dynamic parameters have been removed

The following dynamic parameters have been removed, resulting in the following limitations:

- `enable_OCSP`: OCSP stapling is no longer available
- `VirtualInterfaceProfile`: the network profile type of the connection associated with the virtual network interface can no longer be changed



For more details, see section 18 Managing dynamic parameters.

1.4 Other new features introduced in v7

1.4.1 Log format

Logs sent by the Windows Enterprise VPN Client now conform to the [RFC 5424](#) Syslog message format specification.



For more details, see section 26.1 Log format.

1.4.2 TrustedConnect Panel forwards logs

The TrustedConnect Panel can now forward its logs to a Syslog server. Logs are formatted according to the [RFC 5424](#) Syslog message format specification.



For more details, see section 10 TrustedConnect Panel.

1.4.3 Automatic certificate selection

The automatic certificate selection feature has been updated to conform to ANSSI recommendations, particularly those related to the *Key Usage* and *Extended Key Usage* extensions.



If you update from a version earlier than 7.6, this change may prevent your existing configuration from working with the new version of the VPN Client (see section 19.2.2 Automatic certificate selection).

1.4.4 Remediation tunnel opening notification

The opening of a remediation tunnel is now clearly indicated by a yellow taskbar icon in the notification area and a yellow connection status indicator ring in the TrustedConnect Panel.



For more details, see section 10.3 Notification area icon and color codes.



1.4.5 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



For more details on the Filtering Mode, see section 24 Filtering Mode.



For more details on how to disable the **TrustedConnect Panel**'s disconnect button, see section 22.5 Disabling the disconnect button.



For more details on how to remove options from the **TrustedConnect Panel**'s contextual menu, see section 22.6 Removing menu items.

1.4.6 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



For more details, see section 24 Filtering Mode.

1.4.7 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



For more details on the cryptographic options available in Windows Enterprise VPN Client, see sections 13.3.1.3 Cryptography (IKE Auth) and 13.3.6.2 Cryptography (Child SA).

1.4.8 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 was 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)



For more details on IPsec mode, see section 19.9.3 IPsec DR mode.

1.4.9 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



For more details, see section 13.4 Configuring an SSL/OpenVPN tunnel.

1.4.10 EAP

The following variants of the Extensible Authentication Protocol (EAP) are now supported:

- EAP-MSCHAPv2
- EAP-GTC



For more details, see paragraph [EAP](#) in section 13.3.1 IKE Auth: Authentication.

1.4.11 Certificate authentication and revocation

Version 7 of the Windows Enterprise VPN Client introduces certificate restrictions due to increased security requirements, algorithm deprecations, and stricter certificate usage rules.



Refer to chapter 19 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

1.4.12 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)



For more details on how the **Console** works, refer to 26.3 Console.



For more information on how to use the MSI property `DIALERBEHAVIOR`, see section 10.9 Choosing the connection.



For more information on how to use the MSI property `RESTARTGUITC`, see section 22.7 Automatically restarting the TrustedConnect Panel.



For more information on how to use MSI properties, see the “Deployment Guide”.

1.4.13 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 more than one address
- `crl_cache_duration` allows you to implement a cache memory to store the CRL and define its expiration time
- `redundant_retry` allows you to define the maximum number of attempts to switch from the main gateway to the redundant gateway
- `user_cert_keyusage` allows you to select a certificate based on its Key Usage field
- `interface_metric` allows you to apply a metric to the virtual interface
- `timeout_to_open` allows you to define the timeout for the IKE service to open a tunnel
- `rekey_send_current_TSR` allows you to resend the list of traffic selectors (TSr) that the gateway had provided at the time of initial key establishment during Child SA rekeying



For more details, see section 18 Managing dynamic parameters.

1.4.14 Enhanced security

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



For more details, see the French National Cybersecurity Agency's (ANSSI) IPsec configuration document: [Recommendations for securing IPsec networks Traffic](#) (in French).

1.4.15 Improved smart card/token identification

When more than one smart card and/or token is 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.



For more details, see section 19.5 Using a certificate stored on a smart card or token.



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:

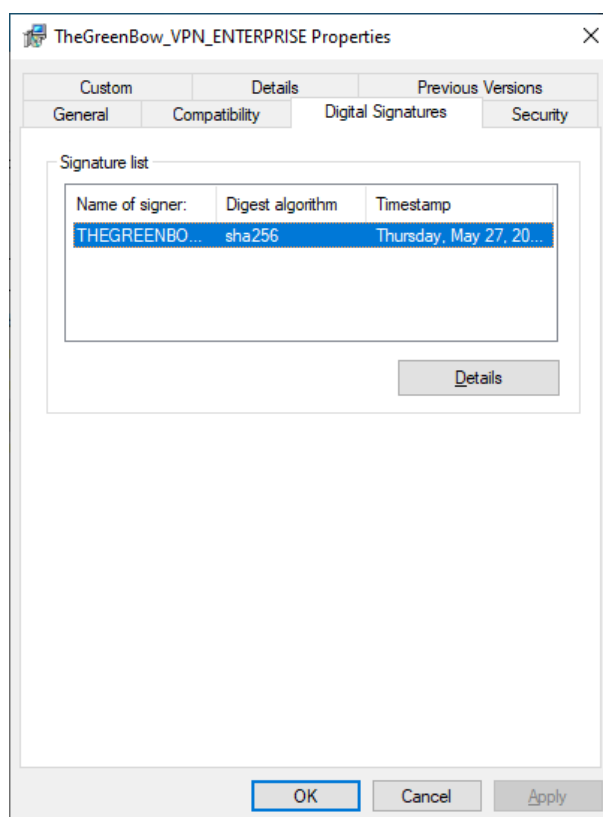
- Processor: 1 GHz or faster processor
- RAM: 2 GB
- Hard disk space available: 40 MB

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.



You 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.

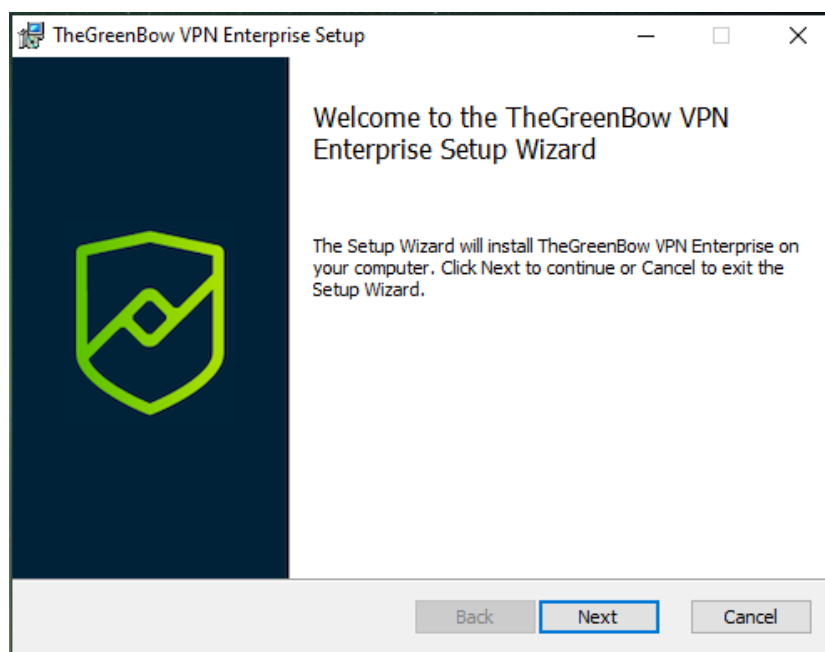


You can only update the software if your subscription is still valid (see section 4.1 How to get an update).



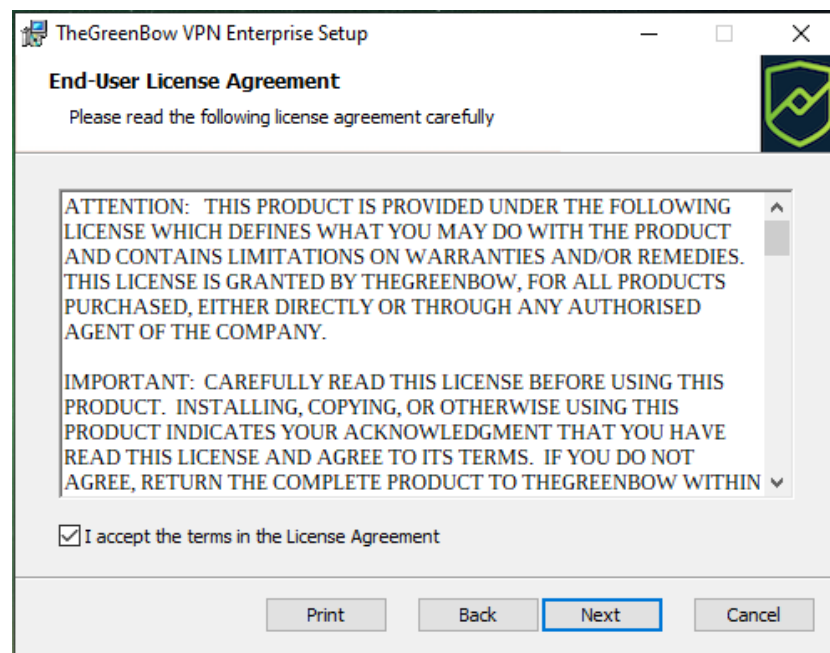
If you want to perform a silent installation, pass specific parameters during installation or perform a large-scale deployment, refer to the “Deployment Guide”.

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

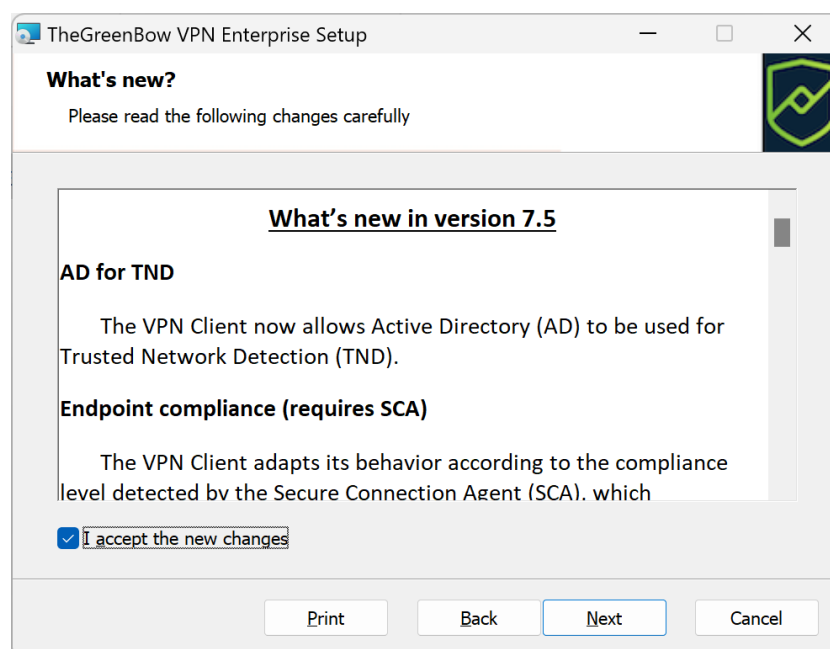


¹ In some cases, see section 4.3 Updating the VPN configuration.

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:

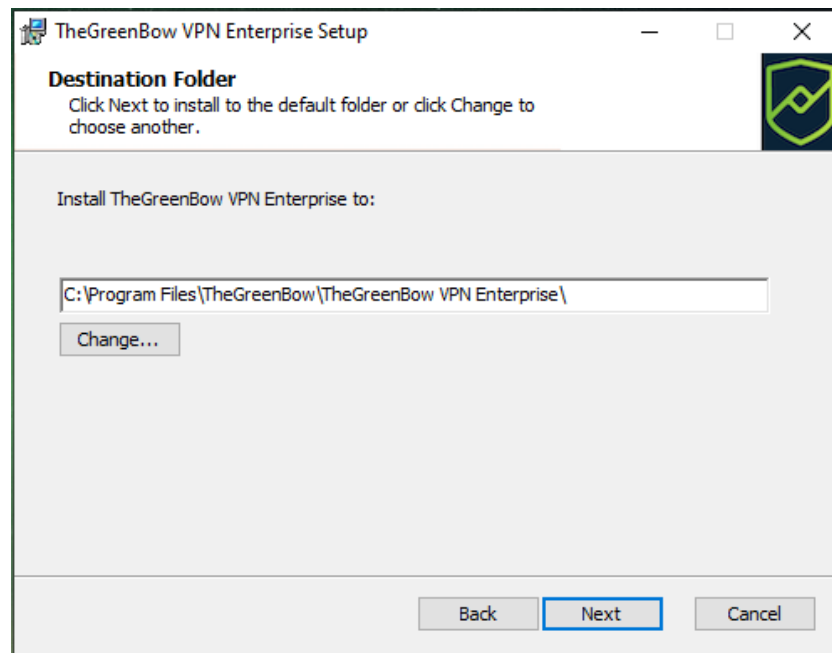


4. Carefully read the information about what's new and the note about how the existing VPN configuration will be converted during an update.



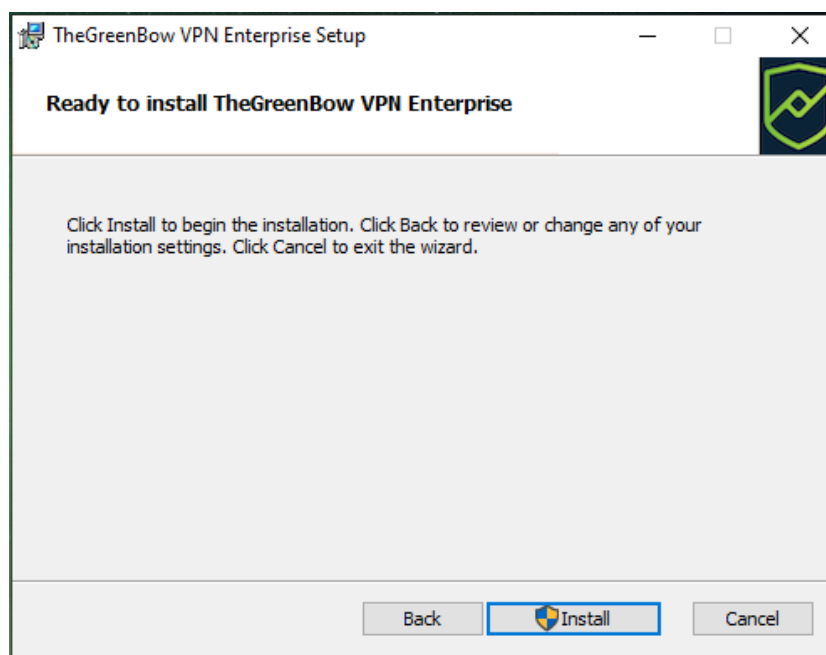
Once the installation is complete, you will not be able to revert to an earlier version of the software without manual intervention. If in doubt, back up your VPN configuration to a separate folder or to a removable storage medium.

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:

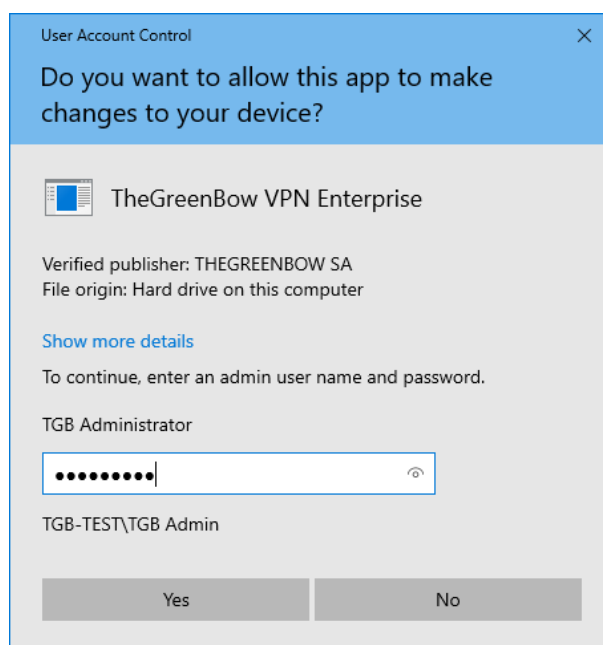


5. If you want to install the Windows Enterprise VPN Client in a specific directory, click **Change...** and select the desired directory. Otherwise, you can keep the default directory. Then, click **Next**.

The following window is displayed:



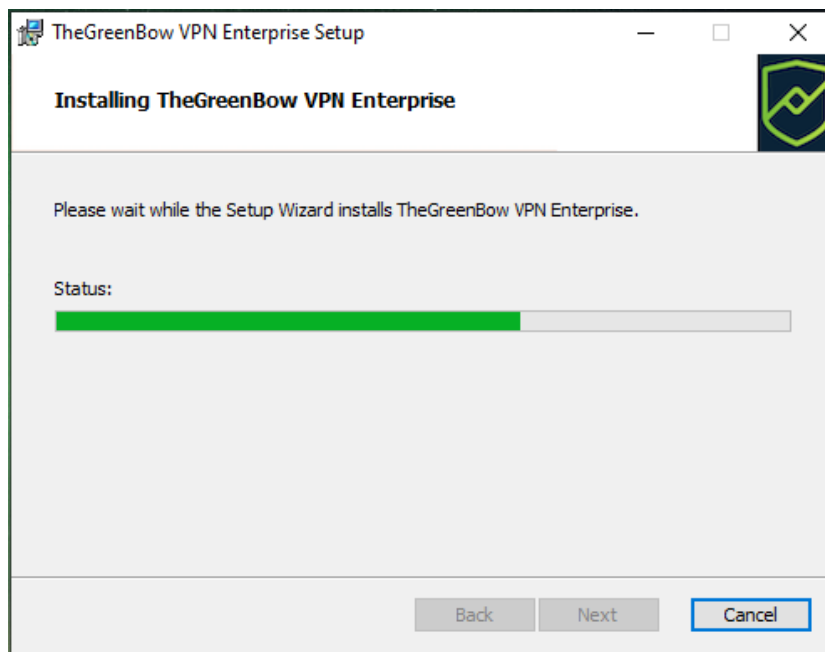
6. The program is ready to install. If you want to go back to check or change your installation settings, click **Back**. Otherwise, click **Install**. If you are installing from an account that does not have administrator rights, the following window is displayed:



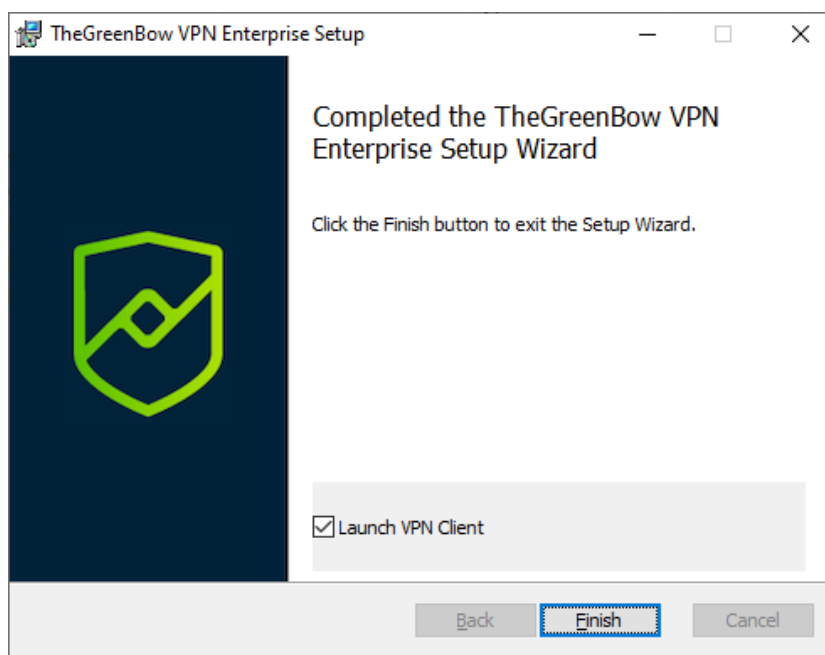
7. To proceed with the installation, you must enter an administrator name and password to allow the installation program to make changes to your computer. Otherwise, the software will not be installed.

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:



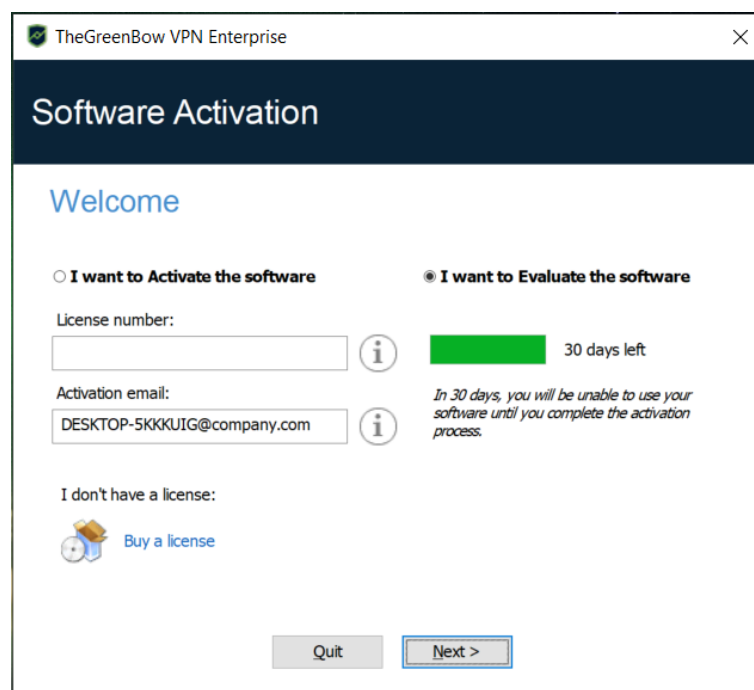
9. Wait for the installation of the Windows Enterprise VPN Client including all its components to complete. If installation has succeeded, the following window is displayed:



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 notification area. 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.

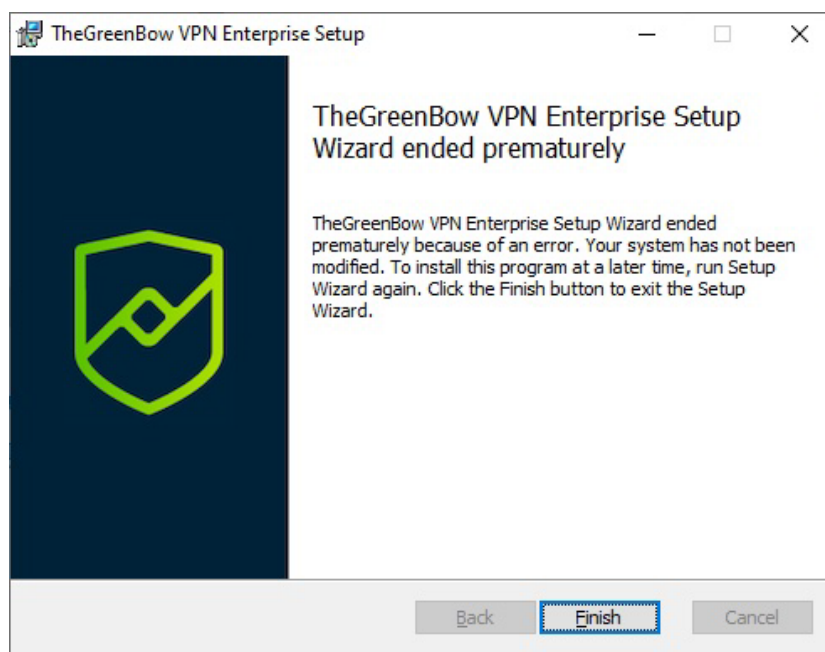
If you do not have a license and want to buy one, click **Buy a license**. TheGreenBow online store is displayed in a browser window. Here, you can buy one or more licenses. For further details on the activation procedure, refer to chapter 3 Activating the software.

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:



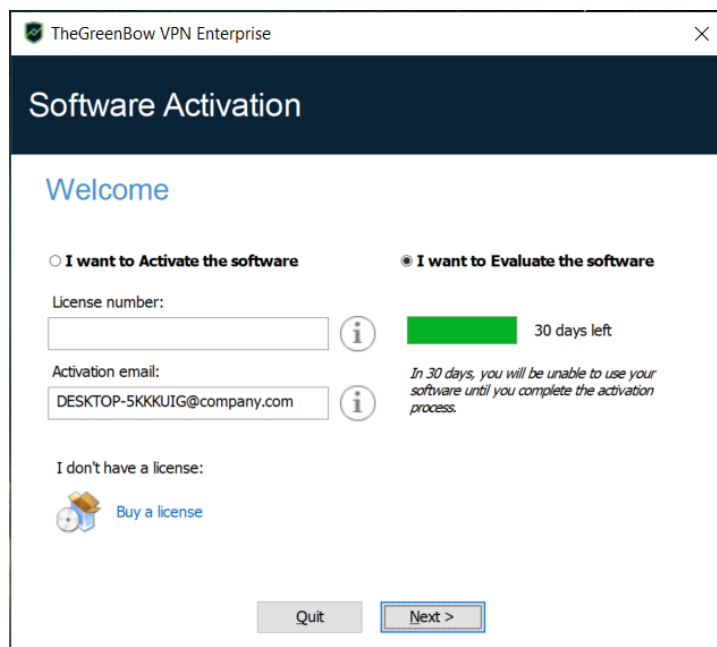
Your system has not been modified and you can resume installation at a later time.

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.

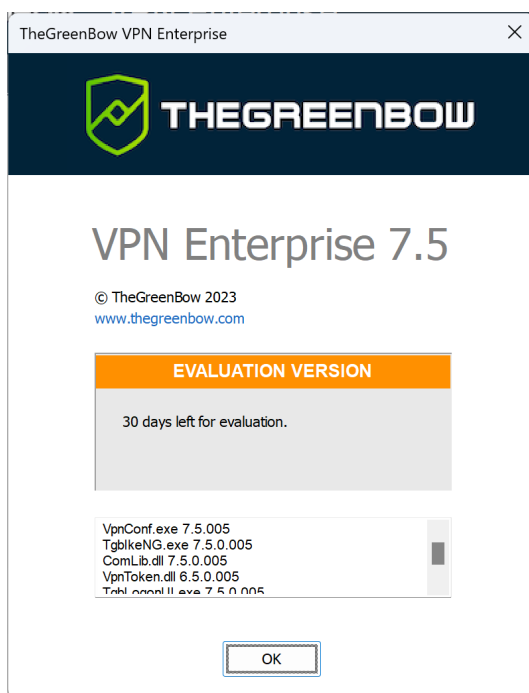
During this trial period, the VPN Client is fully operational, and all functions are unlocked.

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.

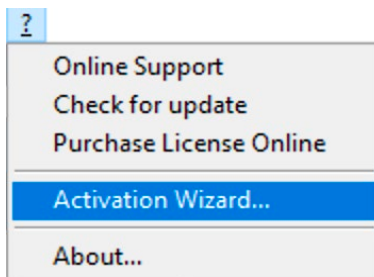


Select **I want to Evaluate the software**, then click **Next >** to run the software.

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

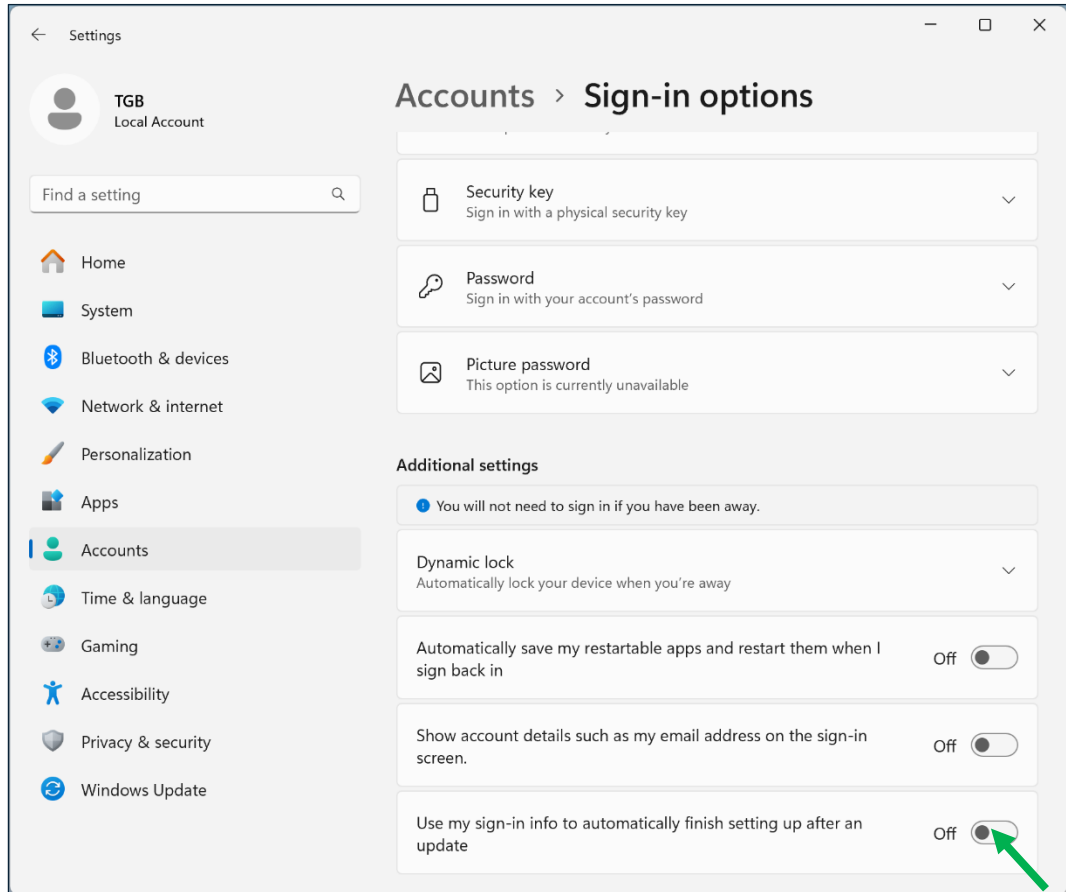
Once you have completed installation, you need to make sure that a Windows sign-in option is disabled.



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.

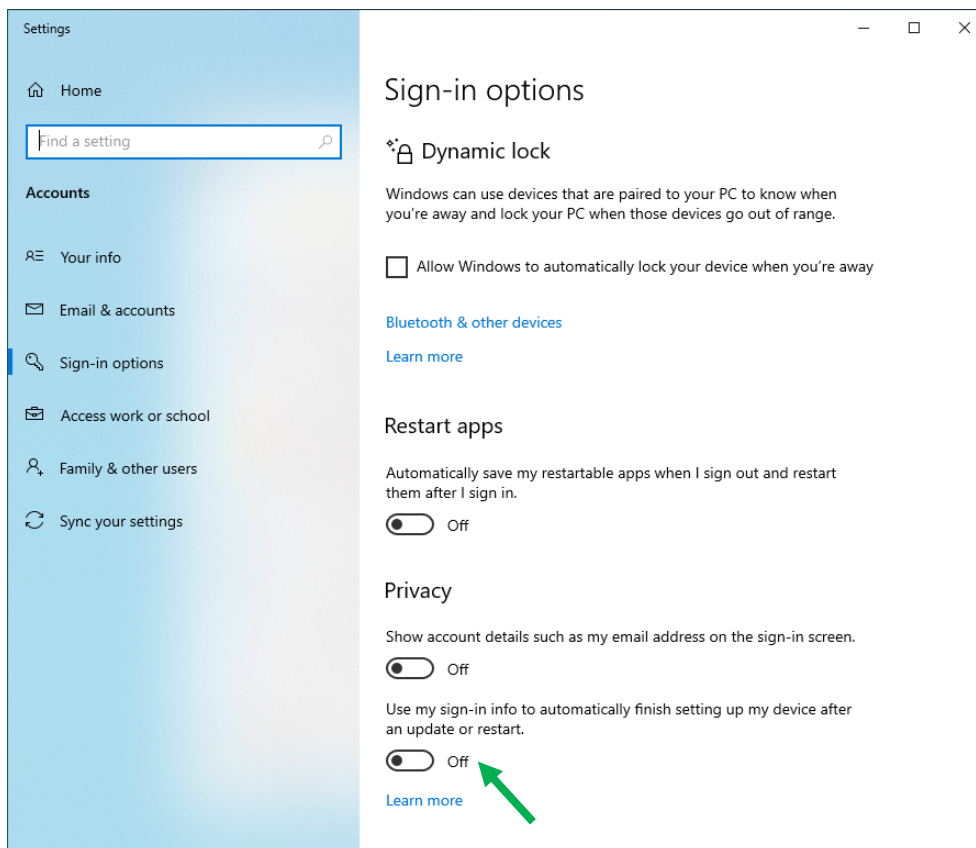
Windows 11

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.

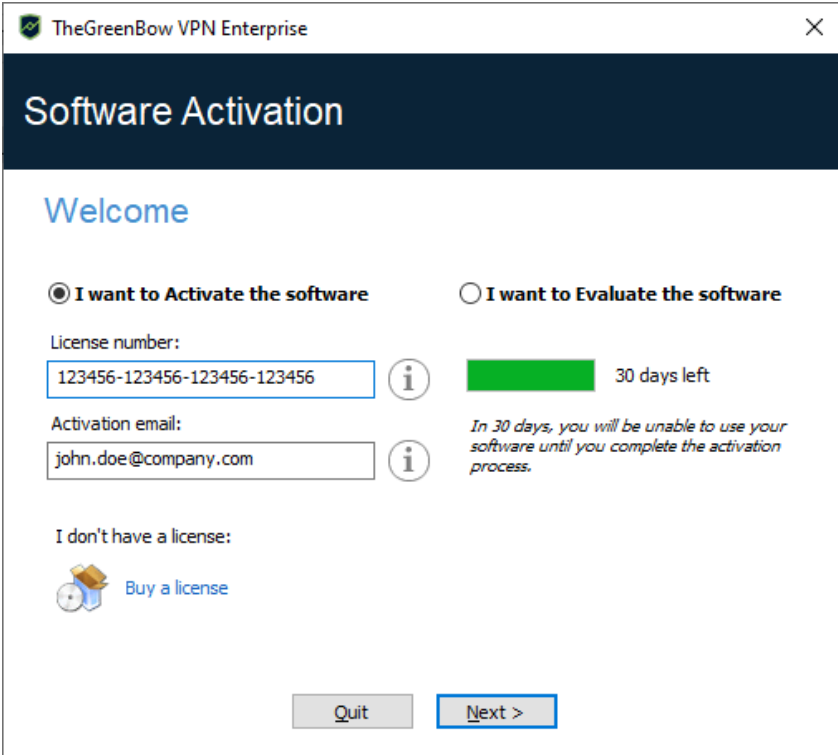
3.1 Step 1

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 more 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 of 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 these fields, there is a green progress bar and the text '30 days left'. Below the progress bar, 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.

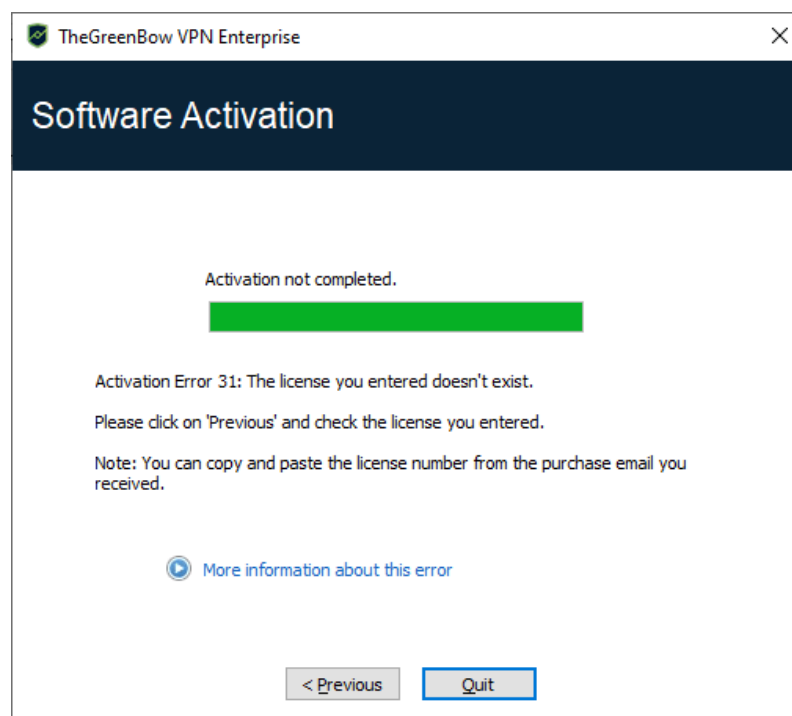
Once the activation has been carried out successfully, click **Run** to run the software.



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:

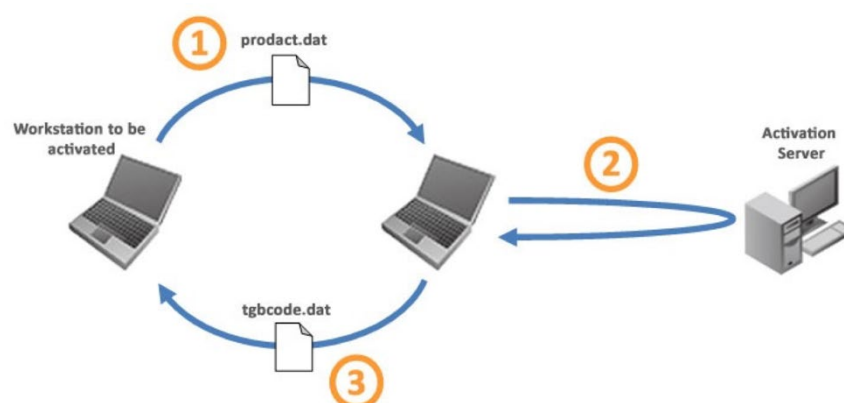
No.	Meaning	Troubleshooting
31	Wrong license number	Check license number.
33	The license number is already activated on a different workstation	Uninstall the software on the workstation with the activated license or contact TheGreenBow's Sales department.
53, 54	Communication with the activation server 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.



The full list of activation error codes can be found in the Appendix under section 29.4 Activation error list.

3.4 Manual activation

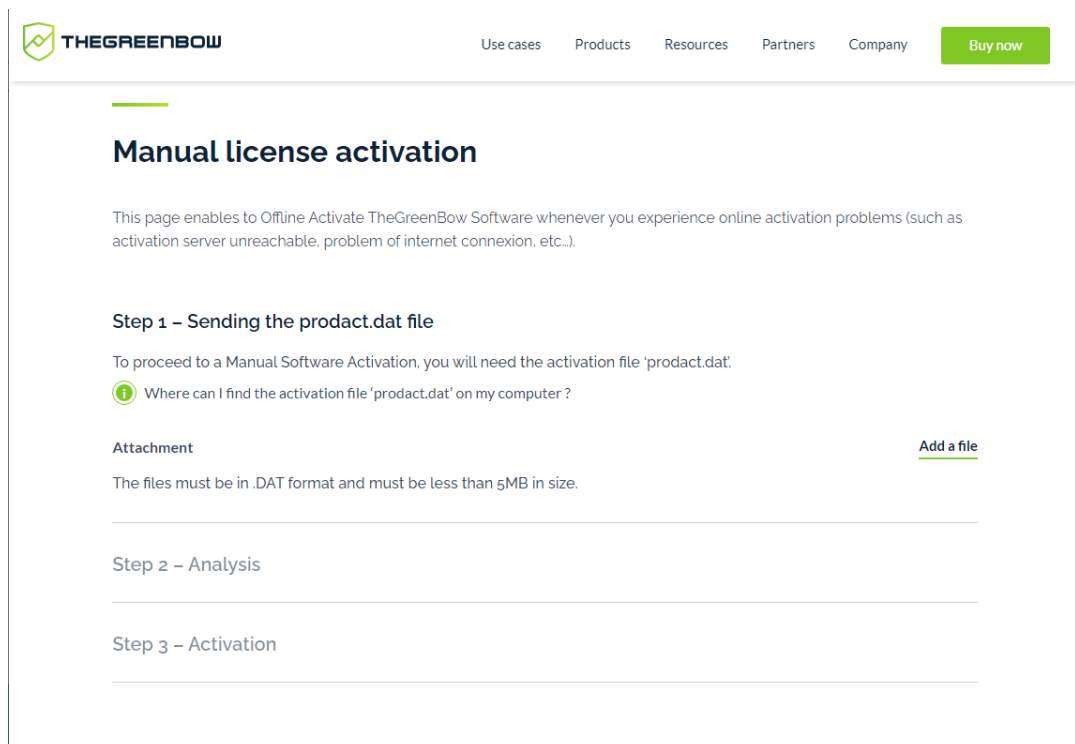
When activation fails due to a communication issue with the activation server, the software can be activated manually on [TheGreenBow's website](#). The procedure is as follows:



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 TheGreenBow's website. The page has a navigation bar with links for 'Use cases', 'Products', 'Resources', 'Partners', 'Company', and a 'Buy now' button. The main heading is 'Manual license activation'. Below it, a paragraph explains that this page enables offline activation for software 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'. Under Step 1, there is a question 'Where can I find the activation file 'product.dat' on my computer?' and an 'Attachment' section with a note that files must be in .DAT format and less than 5MB. An 'Add a file' button is visible next to the attachment section.

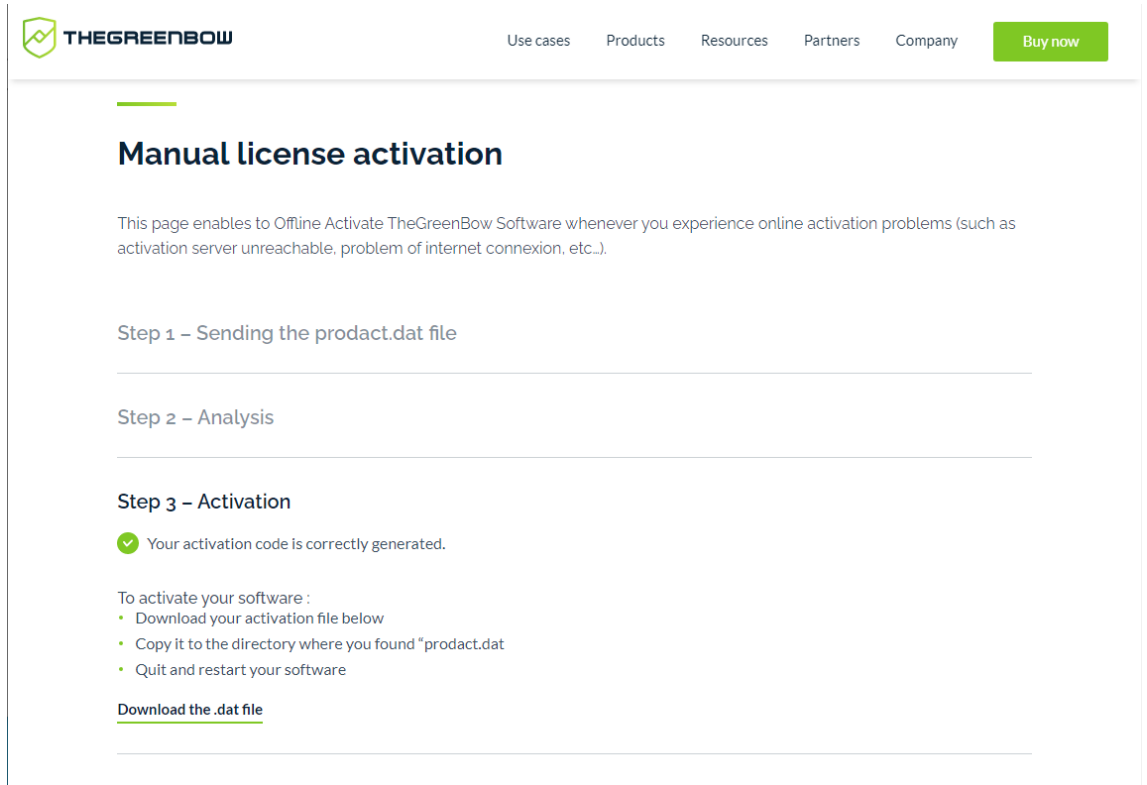
2. Click **Add a file** and open the `product.dat` file created on the workstation that you want to activate.

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 heading is 'Manual license activation'. Below it, a paragraph explains that this 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'. Under 'Step 3 – Activation', there is a green checkmark icon and the text 'Your activation code is correctly generated.' Below this, instructions for activation are listed: 'To activate your software :', followed by a bulleted list: 'Download your activation file below', 'Copy it to the directory where you found "product.dat"', and 'Quit and restart your software'. At the bottom of the activation section, there is a link 'Download the .dat file'.

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

3.5 Activation using TAS

You can activate the software using the TheGreenBow activation server (TAS, see TAS “Administrator’s Guide”). In this case, the TAS certificate must be stored in the Current User Certificate Store on the workstation you want to activate.



If you want to activate in GINA mode, the TAS certificate must be stored in the Local Machine Certificate Store on the workstation you want to activate.

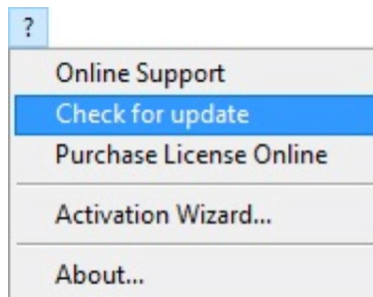
3.6 License and activated software

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

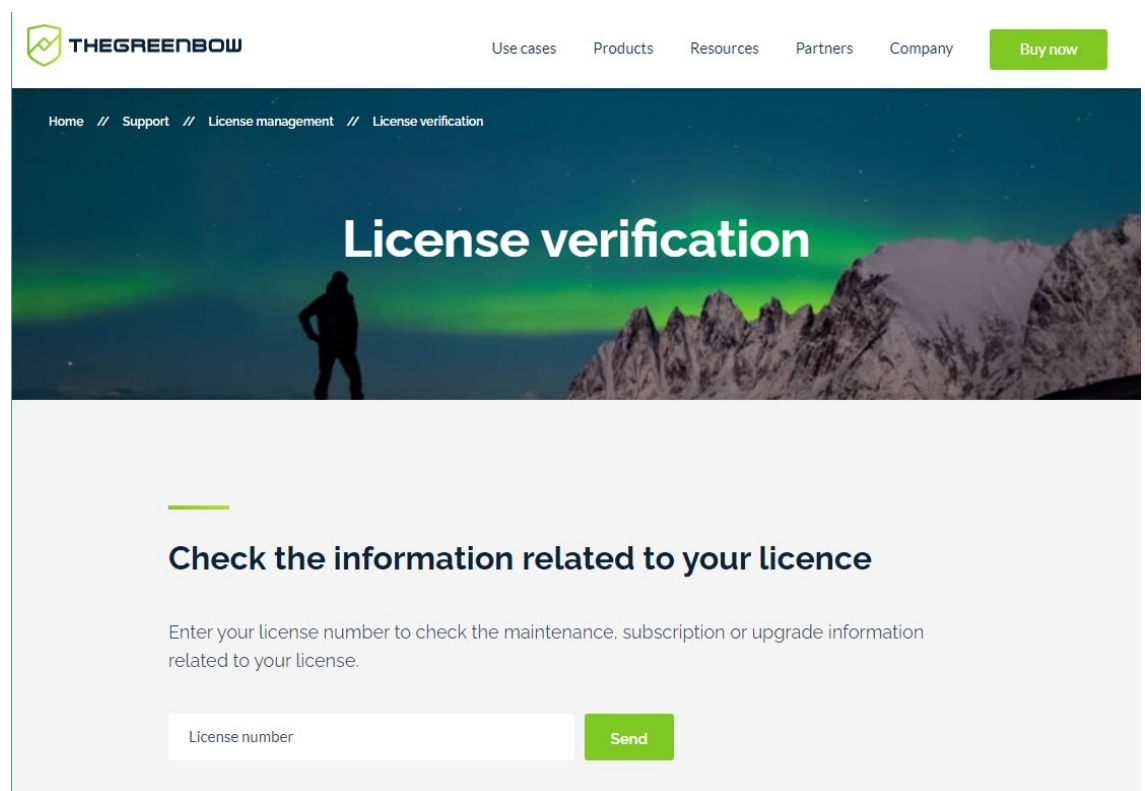
You can also check whether an update is available for the software at any time using the main interface menu ? > **Check for update**.



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

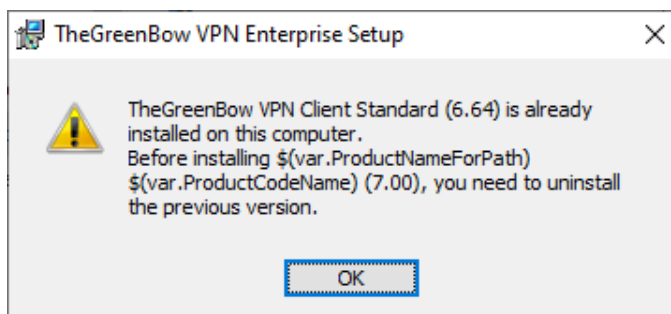


Performing an update from a Standard edition to an Enterprise edition and vice versa is not allowed. However, you can update from any previous version of the Enterprise VPN Client (including Premium and Certified).

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 7.7, updating will not be possible and the following screen is displayed:

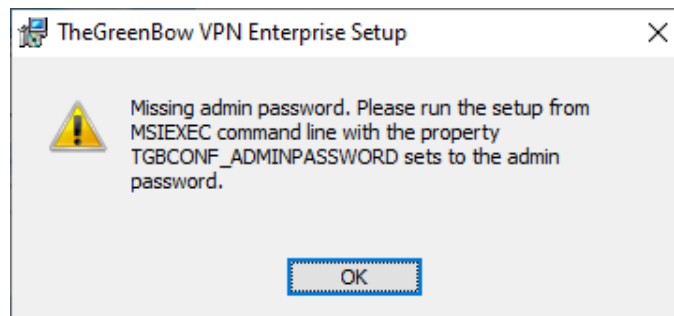


In this case, you will need to uninstall the previous version of the software before you install the new one.

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.

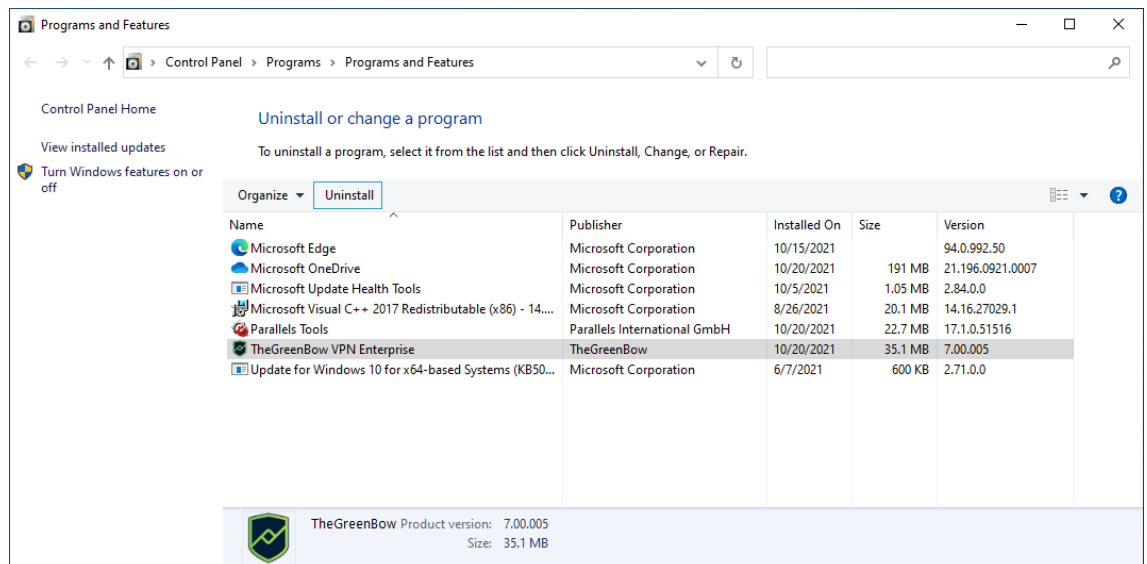


These options are described in the “Deployment Guide”.

5 Uninstalling the software

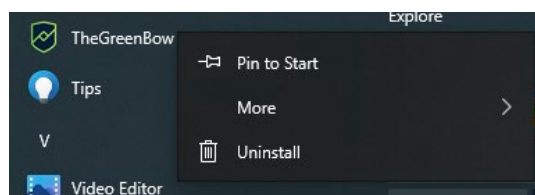
To uninstall the VPN Client, proceed as follows:

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.



You can also uninstall the program using the command line. This procedure is described in the "Deployment Guide".



If you launch the MSI installer and select the **Remove** option to uninstall the program, an error message appears specifying that this operation cannot be carried out. Please use one of the uninstallation methods described above.

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 from the icon in the notification area, 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](#) used for the Always-On and TND features (dedicated executable file)
- An icon in the notification area and its associated menu (both are different [for the TrustedConnect Panel](#) and [for the Connection and Configuration Panels](#))

6.2 Starting the software

Once the installation or update is complete, if you have left the **Launch VPN Client** checkbox selected and the software has not yet been activated, the activation window is displayed (see chapter 3 Activating the software). When the software has been activated or is in the trial period, the Windows Enterprise VPN Client starts without its graphical interface: only the TheGreenBow VPN Enterprise icon appears in the notification area. For a detailed description, see the [Notification area icon](#) subsection 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 any of the VPN Client's modules are corrupted, the software will not be operational. Depending on the situation, 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.

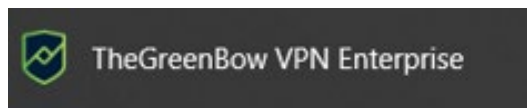
The Windows Enterprise VPN Client can be started directly by double-clicking on this icon.



The VPN Client starts without its graphical interface, and the TheGreenBow VPN Enterprise icon appears in the notification area (see the [Notification area icon](#) subsection 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.

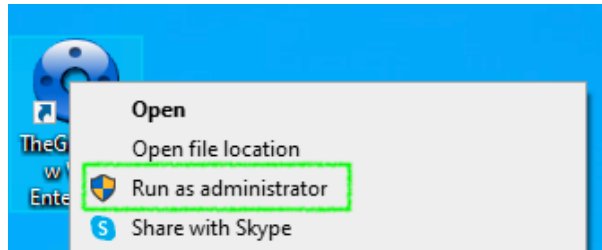


The VPN Client starts without its graphical interface, and the TheGreenBow VPN Enterprise icon appears in the notification area (see the [Notification area icon](#) subsection below).

Running the VPN Client as administrator

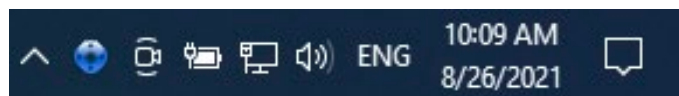
By default, access to the VPN Client's **Configuration Panel** is restricted to Windows administrators only.

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**.



Notification area icon

Under normal operating conditions, the notification area 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



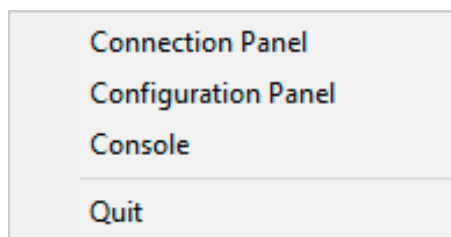
Green icon: at least one VPN tunnel is open

The tooltip for the icon always shows the software status:

- **VPN Tunnel opened** if one or more 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 notification area 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 notification area 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

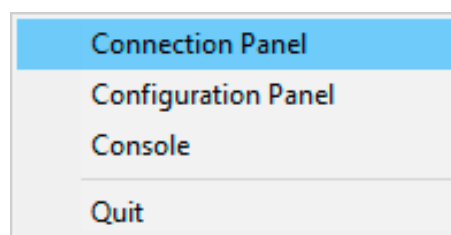


If the software has not been run as administrator and the **Restrict access to Configuration Panel to administrator** option has not been disabled, when the user selects the **Configuration Panel** option, a message is displayed indicating that the software must be run as administrator to access the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

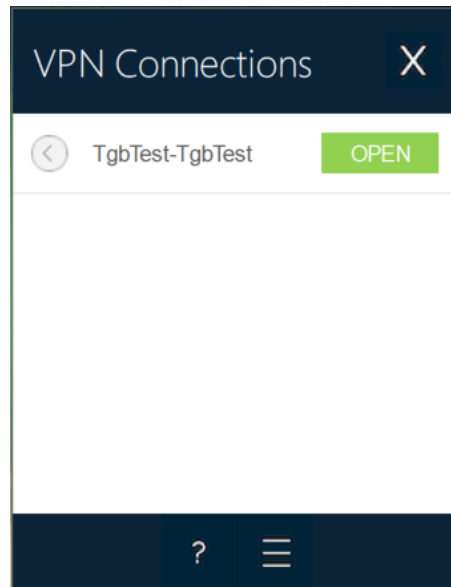
6.3 Opening a test VPN tunnel from the Connection Panel

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 notification area icon (see the [Notification area icon](#) subsection above), and then select the **Connection Panel** menu item. The **Connection Panel** is described in chapter 8 Connection Panel.

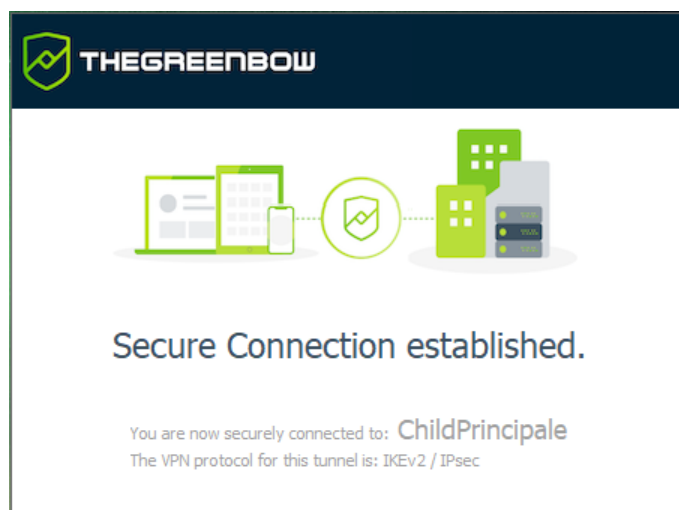


In the **Connection Panel**, click the **OPEN** button next to the **TgbTest-TgbTest** VPN tunnel.

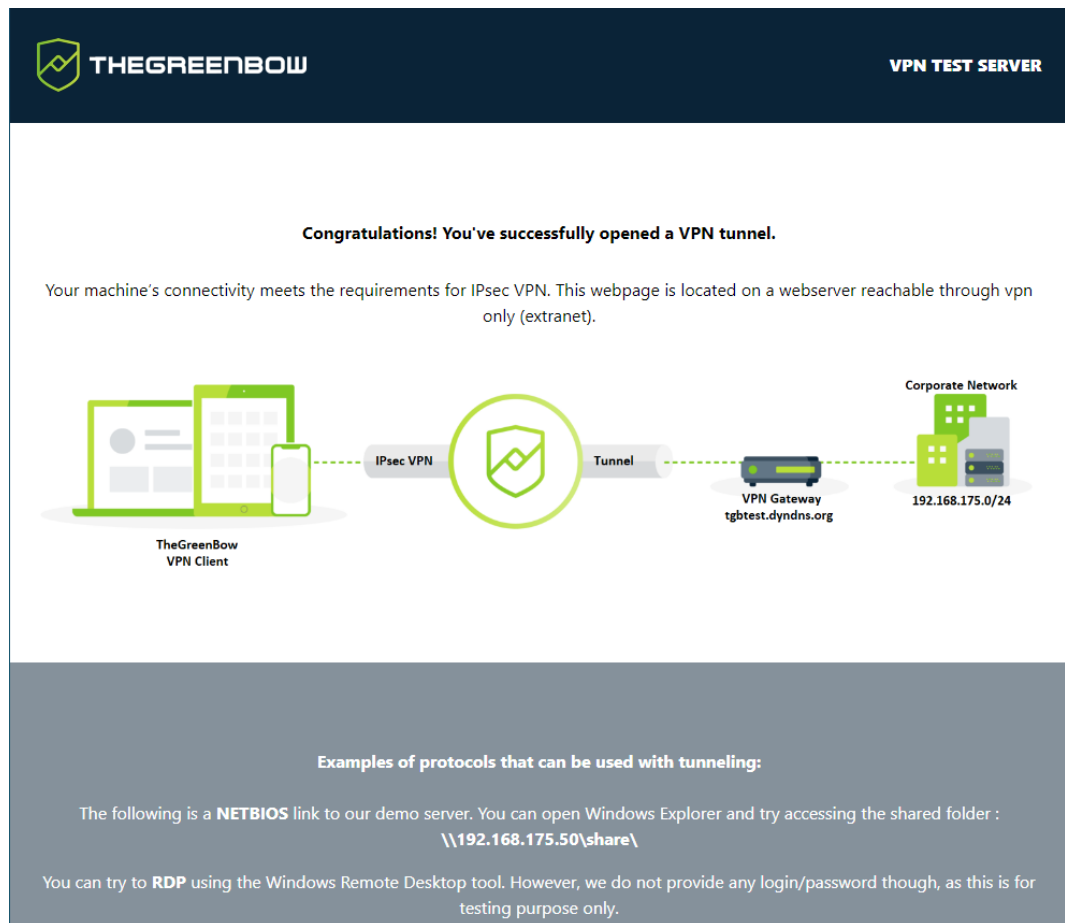


When the software has not been run as administrator and the **Restrict access to the Configuration Panel to administrator** option has not been disabled, the button with the three horizontal bars to the right of the question mark, which gives access to the **Configuration Panel**, is not displayed.

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



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



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:

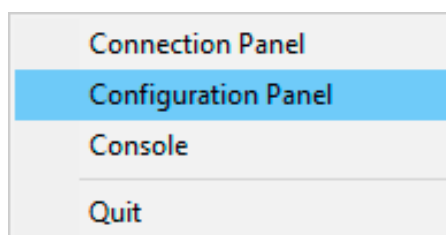
- Using the **Configuration Wizard**, see section 7 Configuration Wizard)
- By directly entering the settings in the **Configuration Panel**, see chapter 9 Configuration Panel)



The default timeout for opening a tunnel is 30 seconds. If this time elapses, the VPN Client considers the tunnel closed. When EAP is configured, this timeout also determines how long the user has to enter login credentials. The dynamic parameter `timeout_to_open` is used to define this timeout value, in seconds. Its minimum allowed value is 20 seconds. There is no maximum (see chapter 18 Managing dynamic parameters).

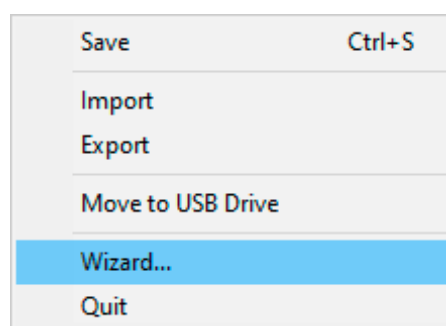
6.4 Configuring a VPN tunnel

To open the **Configuration Panel**, you must first have started the VPN Client as administrator (see the subsection entitled [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 notification area icon (see [Notification area 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.



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:

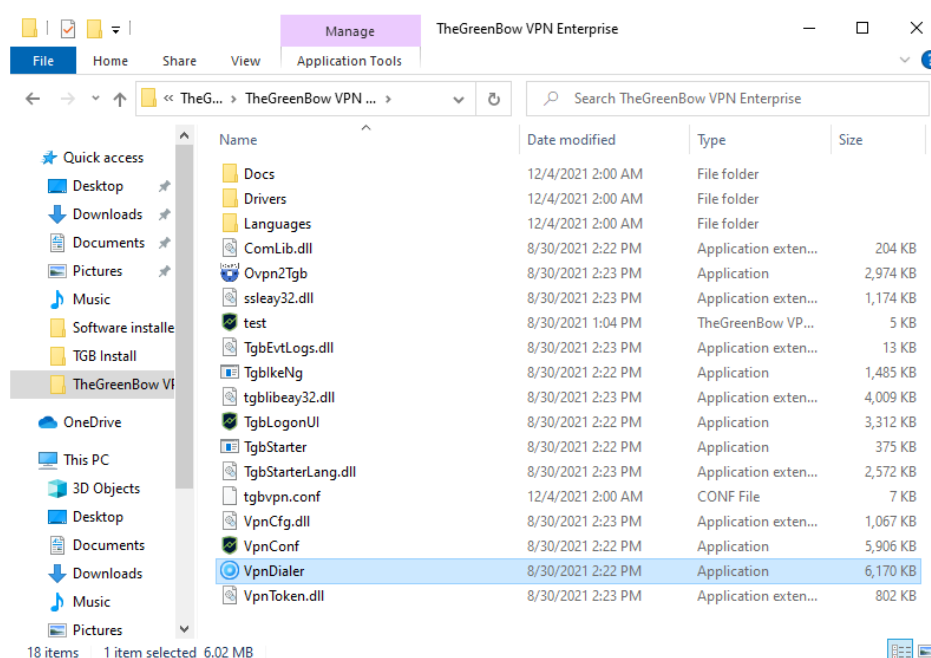
1. When Windows is started, before or after logging on
2. When traffic to the remote network is detected (see chapter 15 Automation)
3. When inserting the smart card or token containing the certificate used for this tunnel (see section 19.5 Using a certificate stored on a smart card or token)

4. When the **TrustedConnect Panel** is used, if the VPN Client detects that the workstation is not located in the trusted network (see chapter 22 Configuring the TrustedConnect Panel).

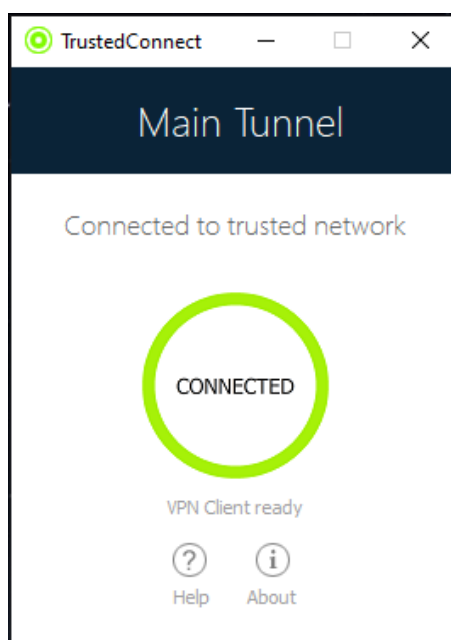
6.6 Opening a VPN tunnel from the TrustedConnect Panel

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`.

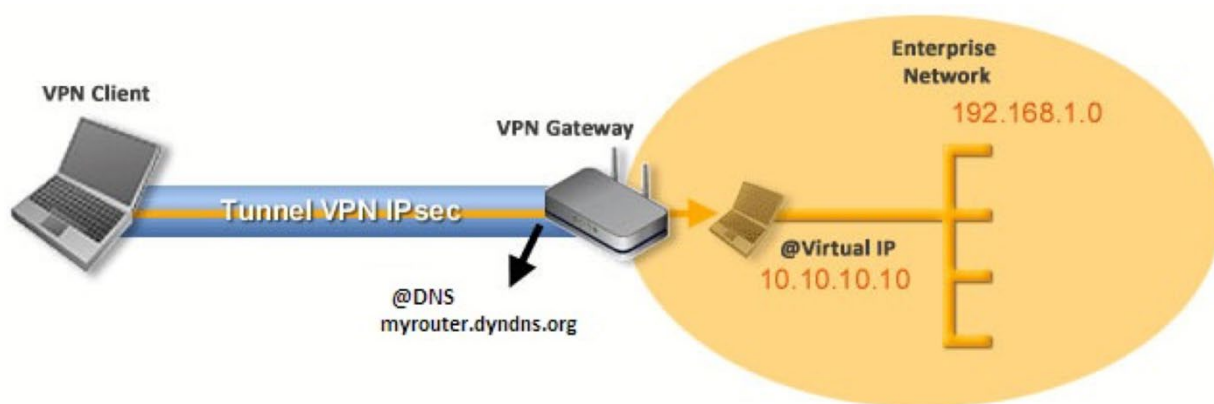


7 Configuration Wizard

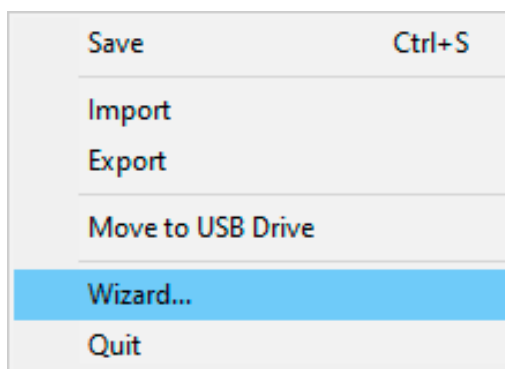
The **Configuration Wizard** is used to configure a VPN tunnel in three easy steps.

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



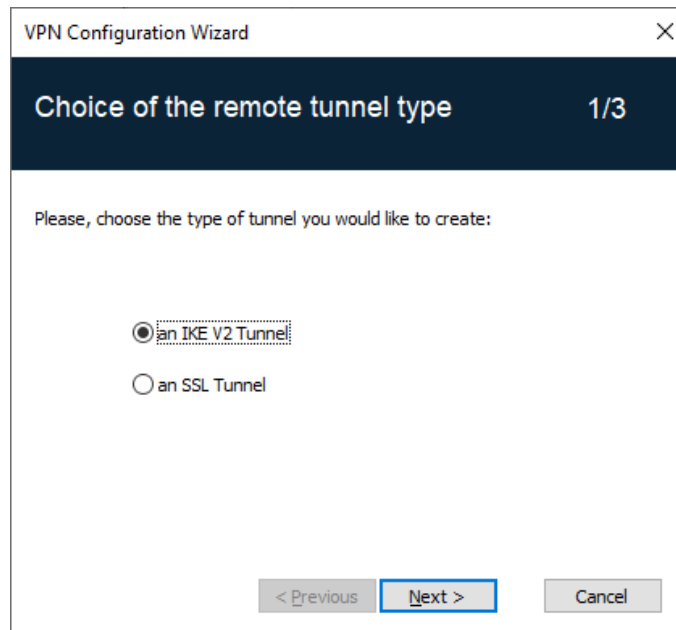
In the main interface, open the **VPN Configuration Wizard: Configuration > Wizard....**



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.

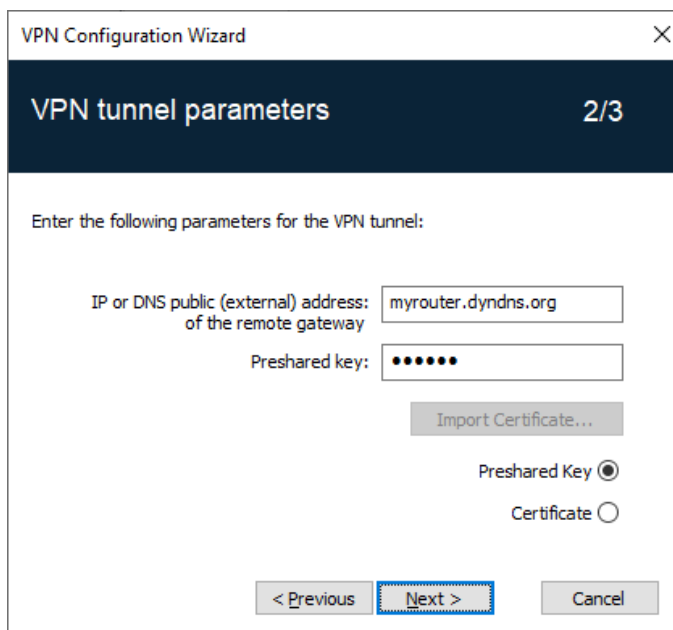


7.2 Step 2

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 19.4 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 19.4 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>

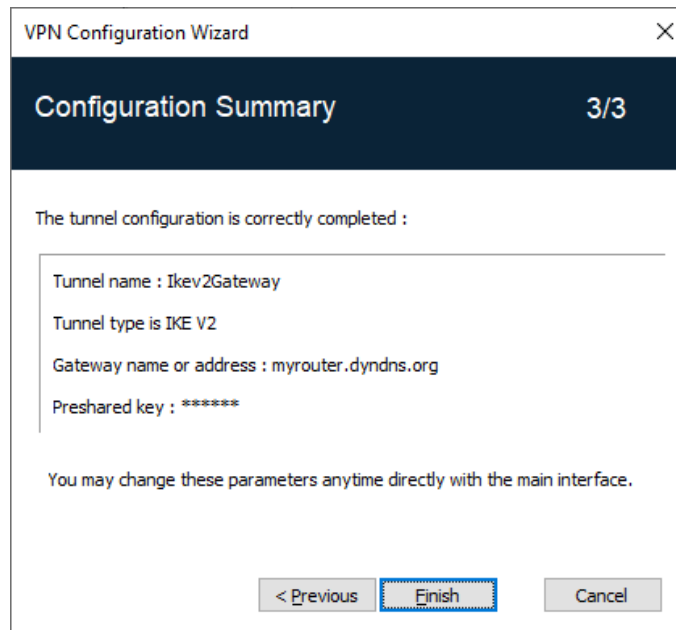
Import Certificate...

Login required ☐

< Previous Next > Cancel

7.3 Step 3

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



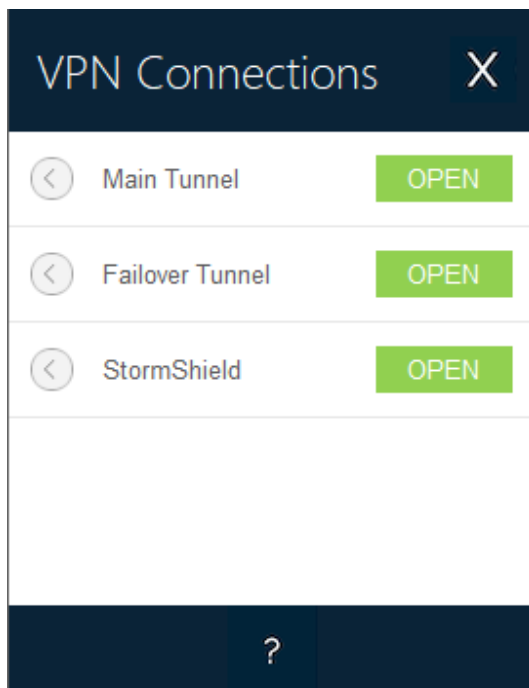
The tunnel that has just been configured now appears in the VPN configuration tree of the main interface.

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 21 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.

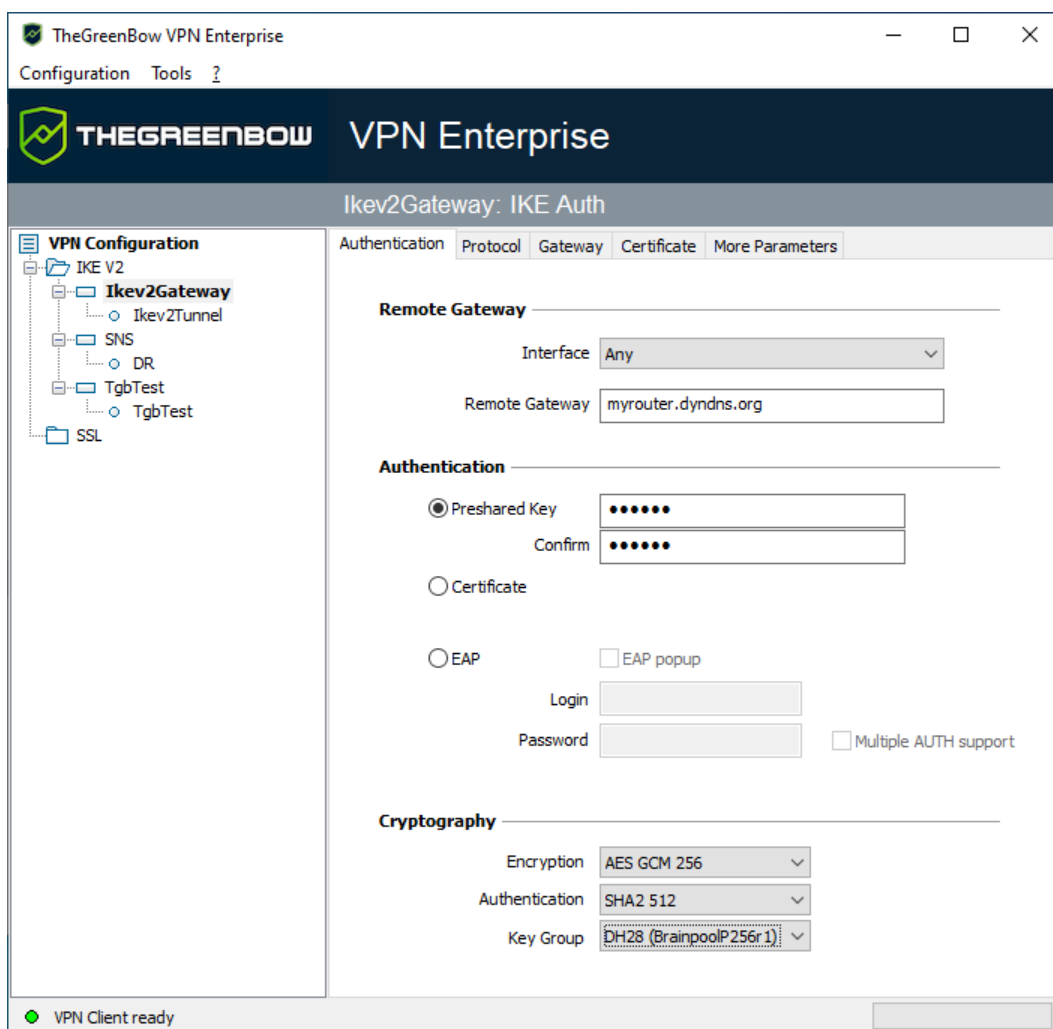
9 Configuration Panel

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 the subsection entitled [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



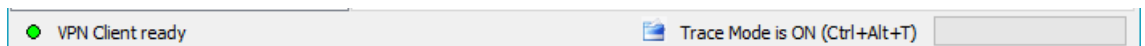
9.1 Menus

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 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 to the right of the status bar shows the progress when saving a configuration.

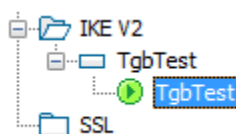
9.3 Shortcuts

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 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.



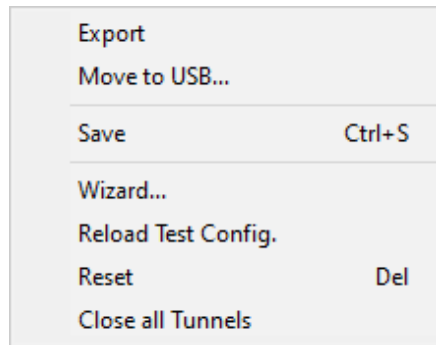
Two items in the tree cannot have the same name. The software displays a message to the user if the name entered is already in use.

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.

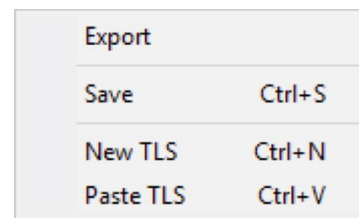


9.4.2.2 IKEv2, SSL

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:



IKEv2 menu



SSL menu

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

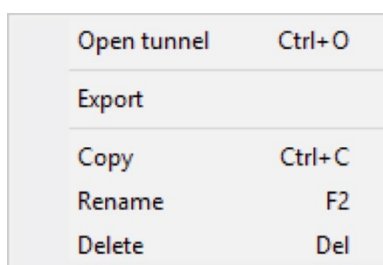
Right-clicking an IKE Auth displays the following contextual menu:



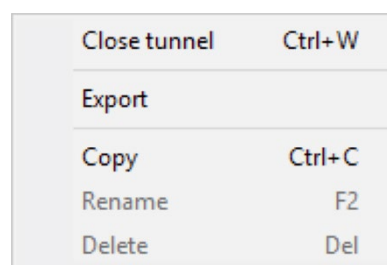
Copy	Copies the selected IKE Auth to the clipboard.
Rename¹	Renames the IKE Auth.
Delete²	Deletes the IKE Auth, including any associated Child SAs, after confirmation by the user.
New Child SA	Adds a new Child SA to the selected IKE Auth.
Paste Child SA	Adds the Child SA that has been copied to the clipboard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

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 ditto



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, either from DNS suffixes and beacons (HTTPS method) or from Active Directory domain names (AD method)
- **Always-On:** Ensures that the connection remains secure whenever the network interface changes, for example, between Ethernet, Wi-Fi and 4G/5G

10.2 Interface

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

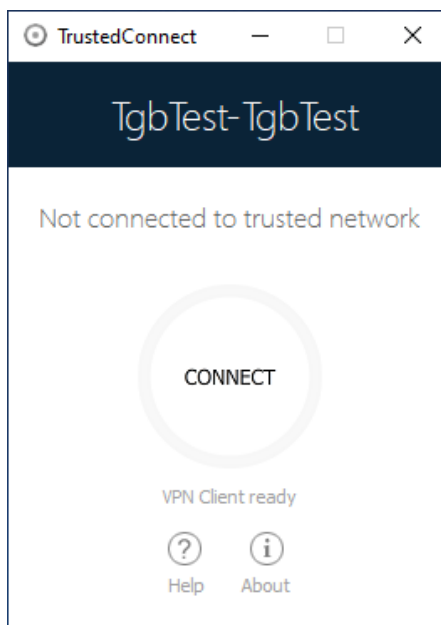
For subsequent uses, the **TrustedConnect Panel** memorizes the place to which the user has moved it.

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

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



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).



At any time, you can minimize the **TrustedConnect Panel** to the taskbar or close it using the **Minimize** and **Close** buttons in the title bar. Closing the panel does not shut down the application: it continues to run in the background. To redisplay the panel, click the **TrustedConnect** icon in the taskbar or in the notification area.

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 22.5 Disabling the disconnect button for more details.

10.3 Notification area icon and color codes

The notification area icon of the **TrustedConnect Panel** is slightly different from that of the **Configuration Panel** and the **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.



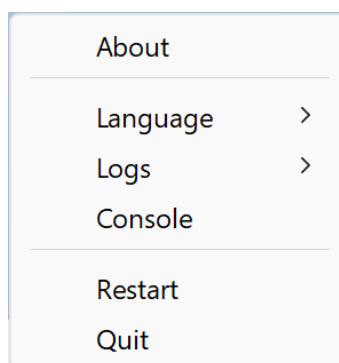
This state means that the **TrustedConnect Panel** has opened a remediation tunnel.



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

10.4 Contextual menu

Right-clicking the **TrustedConnect Panel** icon in the notification area opens its contextual menu:



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 22.6 Removing menu items for more details.

10.5 Usage

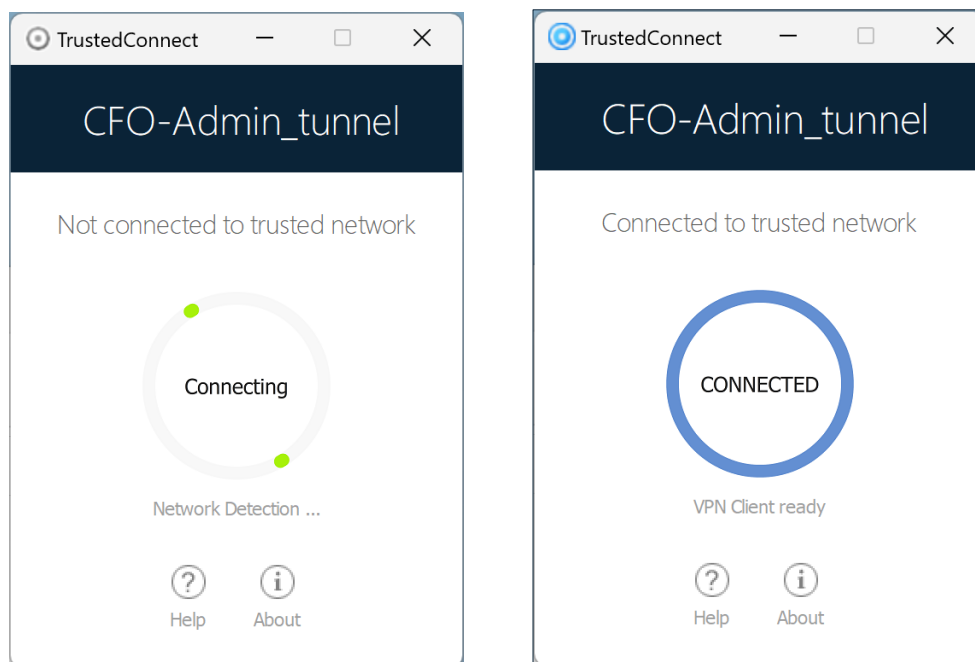
There are two types of use depending on whether the workstation is already connected to the corporate network or not.



As of version 7.3 of the Windows Enterprise VPN Client, you can disable the TND feature to open a tunnel even when the workstation is located on the trusted network. Refer to section 22.2.3 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 **TrustedConnect Panel** then is automatically either minimized to the taskbar or closed, depending on the behavior the administrator has configured. In either case, the panel remains available from the notification area.



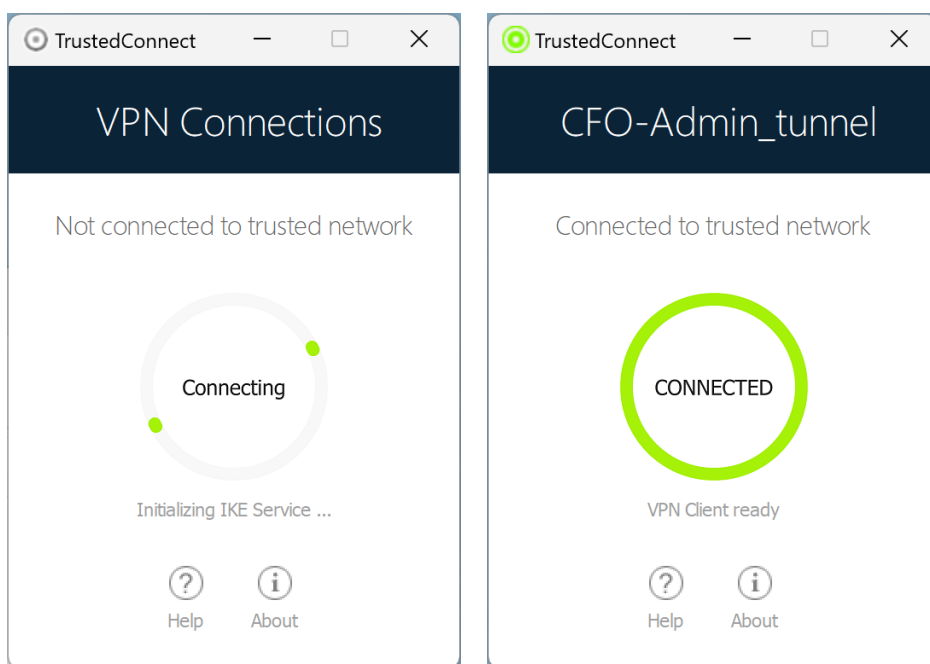
Refer to the “Deployment Guide”.

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

10.5.2 Workstation not connected to corporate network

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

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

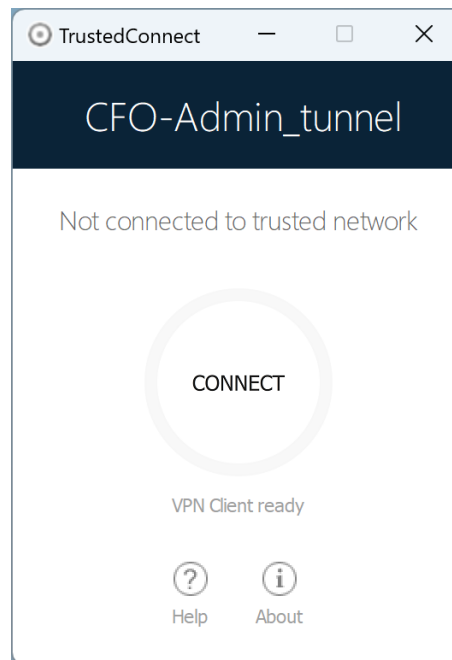


Once the connection is established, the **TrustedConnect Panel** is automatically either minimized to the taskbar or closed, depending on the behavior the administrator has configured. In either case, the panel remains available from the notification area.

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.

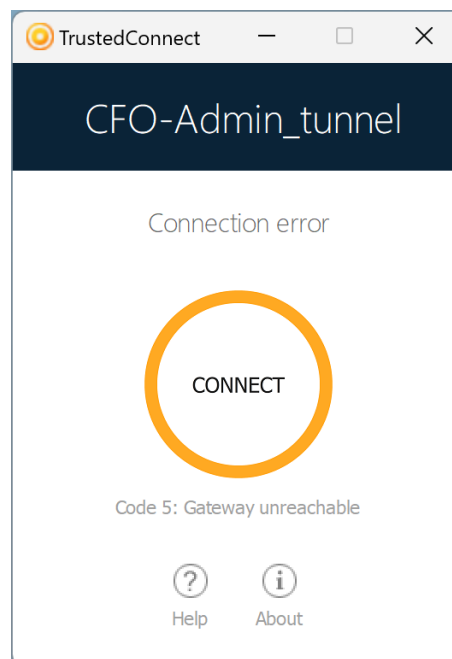
When the tunnel is mounted and the workstation is shown as being on the corporate network, you can click inside the connection status indicator ring to stop the tunnel.

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

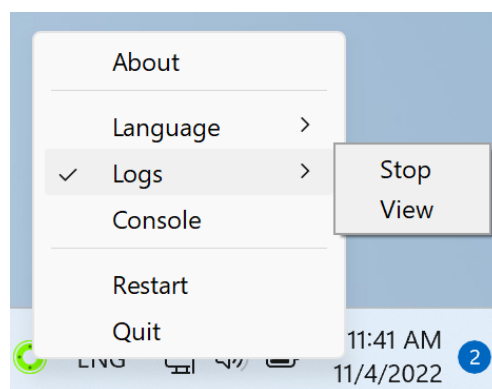
the administrator requests the logs, refer to the procedure described in the next section.

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

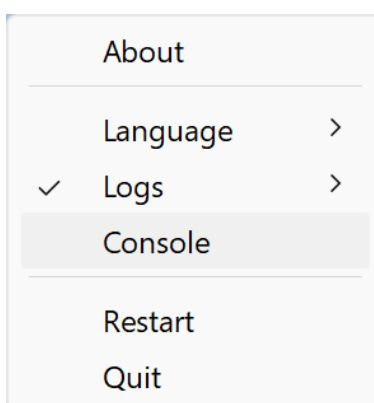
The **TrustedConnect Panel** allows you to create and view logs.

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.

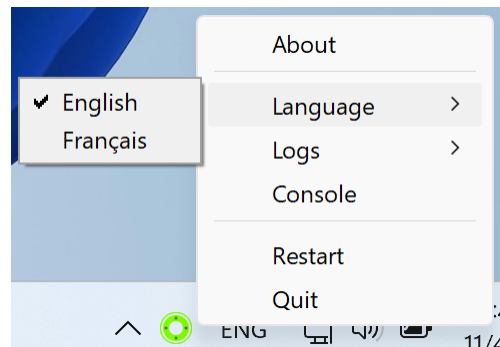
You can now also display the **Console** window with VPN traces directly from the **TrustedConnect Panel's** contextual menu.



To find out how to use the **Console** window, refer to section 26.3 Console.

10.8 Selecting the language

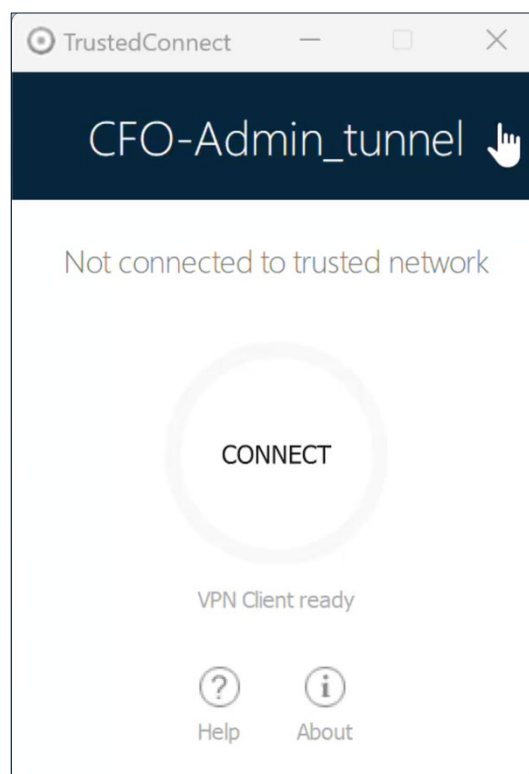
The **TrustedConnect Panel** allows you to select the software's display language: French or English. To select the language, access the menu and select the **Languages** item. In the submenu, select **English** or **Français**:



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:

1. If the **TrustedConnect Panel** is not displayed on the screen, click its icon in the notification area to display it.
2. 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**.
3. 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.
4. Click the **CONNECT** button. The VPN Client attempts to establish the connection. If it succeeds, the connection status indicator ring turns green, and the button label changes to **CONNECTED**. The **TrustedConnect Panel** is then automatically either minimized to the taskbar or closed, depending on the behavior the administrator has configured. In either case, the panel remains available from the notification area.



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 subsection entitled [Special use case](#) in section 23.1 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`.

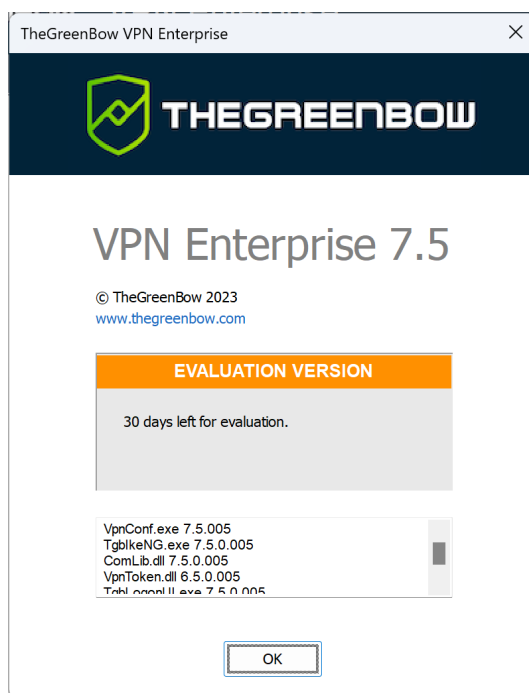
The **TrustedConnect Panel** (`VpnDialer.exe`) is currently only available in French and English.



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.

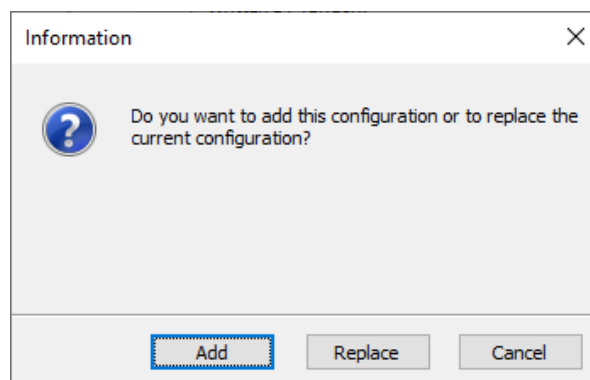


As of version 6.8 of the Windows Enterprise VPN Client, the function that allows you to double-click on a VPN configuration file to import it is no longer available.



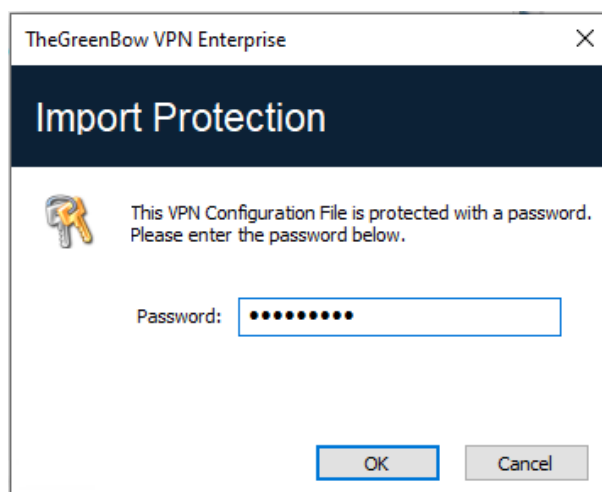
The Windows Enterprise VPN Client can check the integrity of the VPN configuration file (see MSI property `SIGNFILE` in the “Deployment Guide”). In this case, a signature is generated during export and the integrity of the file is checked during import.

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:

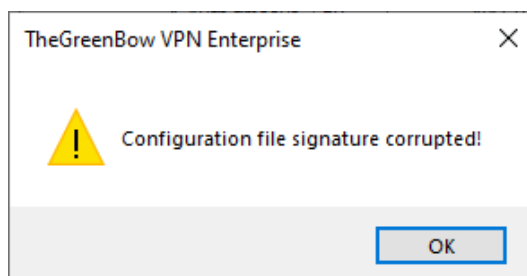


¹ The use of command-line options within the software is covered in the “Deployment Guide”. In particular, it details all the options available for importing a VPN configuration: `/import`, `/add`, `/replace` or `/importonce`.

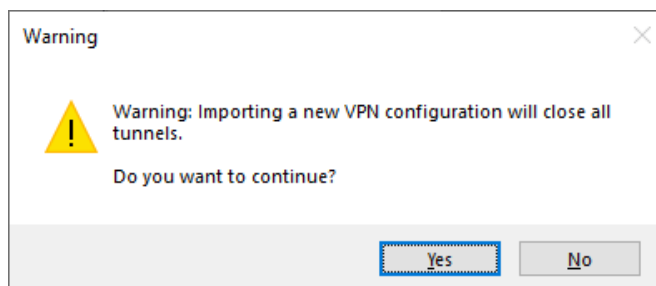
If the imported VPN configuration has been exported with password protection (see section 12.2 Exporting a VPN configuration below), users will have to provide the password.



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 more 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



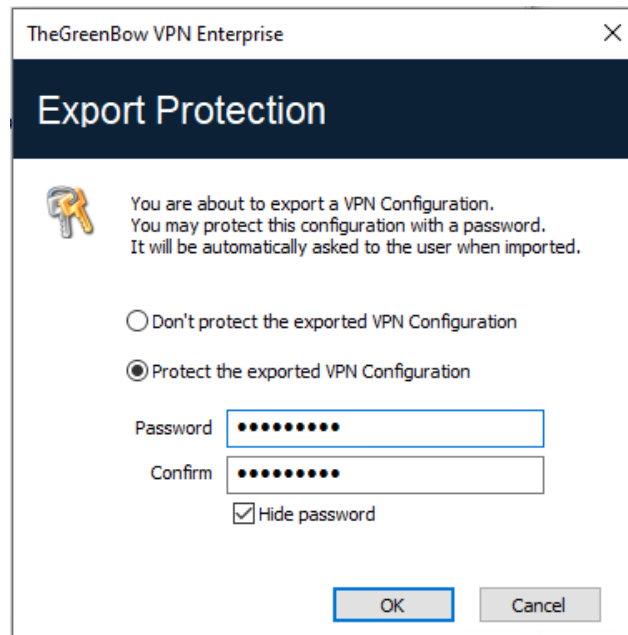
By default, the extension of exported VPN configuration files is `.tgb`.



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 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 tunnel.

It also allows you to open them simultaneously.

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

- 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.



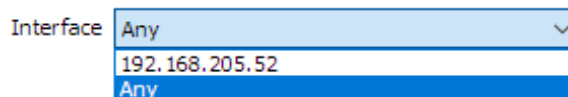
13.3 Configuring an IPsec IKEv2 tunnel

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**.



The screenshot shows a dropdown menu for the 'Interface' field. The current selection is 'Any'. Below it, two other options are visible: '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 more than one IP address, you can specify the address using the dynamic parameter `local_subnet` (see chapter 18 Managing dynamic 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 19 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.

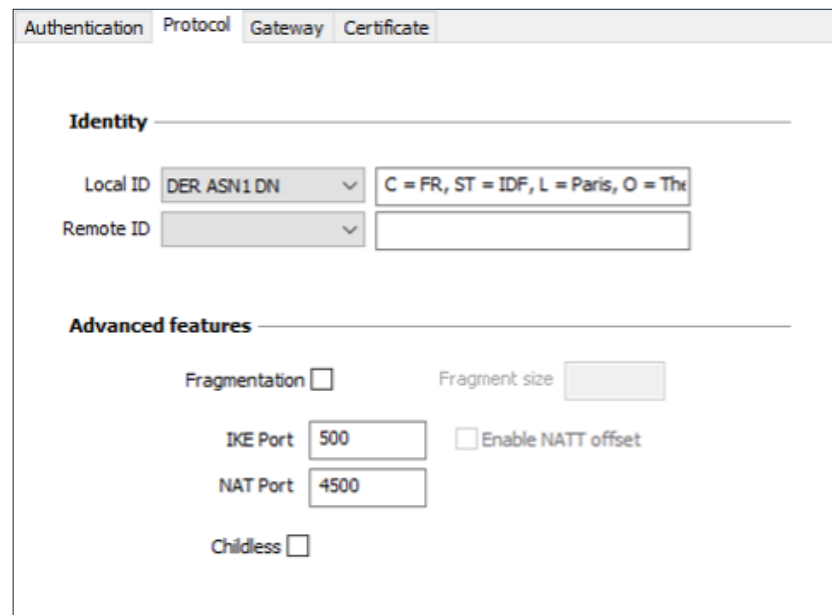
⁴ See note 1.

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 (unchecked), 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 (unchecked), and a 'Childless' checkbox (unchecked).



If you use an IPsec DR gateway, you must add the dynamic parameter `nonce_size` (see section see chapter 18 Managing dynamic 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.

Depending on 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 chapter19 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.

Depending on 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	Enables IKEv2 packet fragmentation in accordance with RFC 7383. This function prevents IKEv2 packets from being fragmented by the IP network they're passing through. The fragment size must generally be set to a value that is 200 bytes smaller than the MTU of the physical interface, e.g. 1300 bytes for a typical 1500-byte MTU.
IKE Port	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.  The remote VPN gateway must also be able to perform the IKE Auth exchanges on a port other than 500.
NAT Port	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.  The remote VPN gateway must also be able to perform the IKE Child SA exchanges on a port other than 4500.
Enable NATT offset	When the IKE port is different from 500, it may be necessary to check this option for the gateway to accept the connection.
Childless	When this mode is enabled, the VPN Client will attempt to initiate IKE exchanges without creating any Child SA in accordance with RFC 6023. We recommend using this mode.



13.3.3 IKE Auth: Gateway

Authentication	Protocol	Gateway	Certificate	More Parameters
Dead Peer Detection (DPD)				
Check interval 30 sec.				
Max. number of retries 5				
Delay between retries 15 sec.				
Lifetime				
Lifetime 1800 sec.				
Gateway related parameters				
Redundant Gateway				
Retransmissions 3				
Gateway timeout 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 19 Managing certificates.

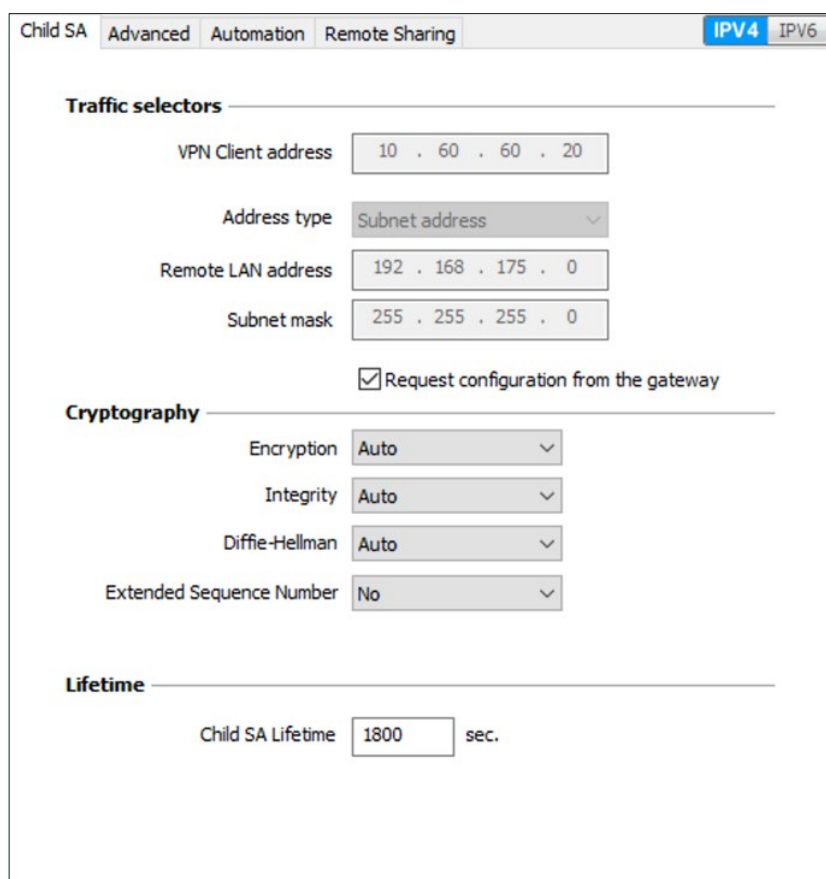
13.3.5 Child SA: Overview

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.



Traffic selectors can be configured using dynamic parameters. See [Dynamic parameters for traffic selectors](#) at the end of this section.

Address type	The endpoint of the tunnel can be a network or a remote workstation. Refer to section 13.3.6.5 Configuring the address type below.
Request configuration from the gateway	This option (also called “Configuration Payload” or “Mode CP”) lets the VPN Client get all the information required for the VPN connection from the gateway: VPN Client address, remote LAN address, subnet mask, and DNS addresses. When this option is checked, all corresponding fields are disabled (uneditable). They are filled in dynamically as the tunnel is opened with the values sent by the VPN gateway during the Mode CP exchange. 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. If more than 16 subnetworks are configured by the gateway, only the first 16 will be taken into account.

Dynamic parameters for traffic selectors

The two dynamic parameters `rekey_send_current_TSr` and `local_virtual_network_size`, described below, are used to configure traffic selectors.

rekey_send_current_TSr

This parameter is used to define the VPN Client’s behavior during Child SA rekeying.

False or undefined	The value 0.0.0.0 is sent again.
True	The list of traffic selectors (TSr) the gateway sent during initial key establishment is sent again for compatibility with IPsec DR gateways that strictly follow this recommendation.



The default behavior of Stormshield gateways is `True`.

local_virtual_network_size

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 chapter 18 Managing dynamic parameters

13.3.6.2 Cryptography

Encryption	Encryption algorithm negotiated during the IPsec phase ¹ : Auto ² , AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Integrity	Integrity algorithm negotiated during the IPsec phase ³ : Auto ⁴ , SHA2 256, SHA2 384, SHA2 512.
Diffie-Hellman	Length of Diffie-Hellman key ⁵ : Auto ⁶ , 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): Auto ⁷ , 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.

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.

⁶ See note 2.

⁷ See note 2.

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.

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



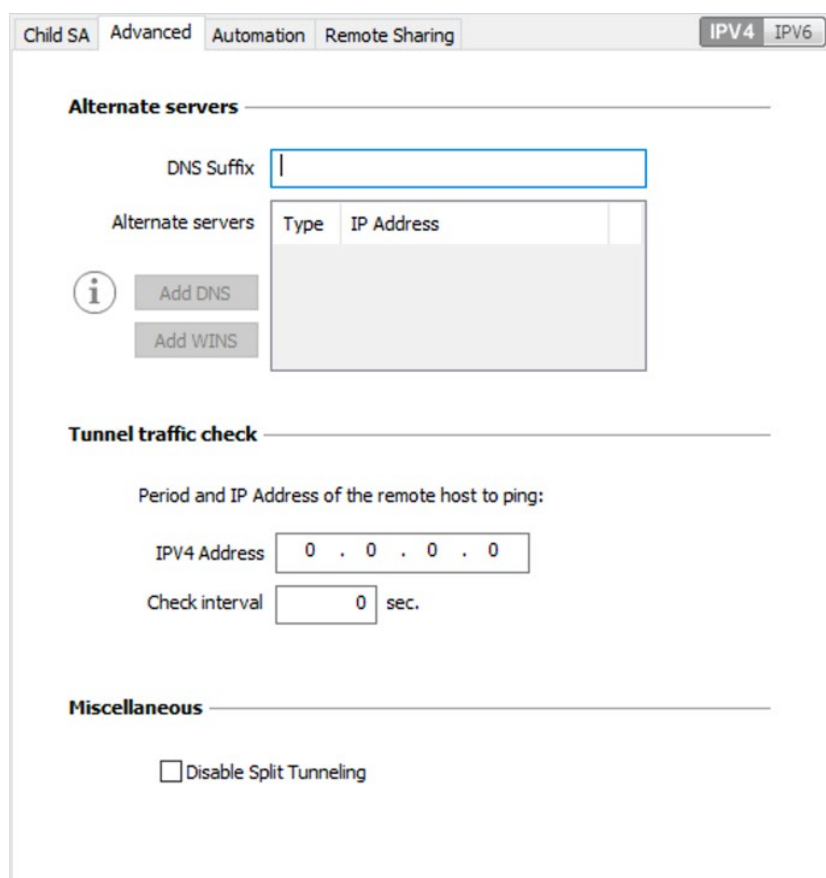
The function [Automatically open this tunnel on traffic detection](#) is used to automatically open a tunnel when traffic with one of the addresses specified in the address range is detected (provided that this address range is authorized in the VPN gateway configuration).



“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**.

13.3.7 Child SA: Advanced



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 20 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.

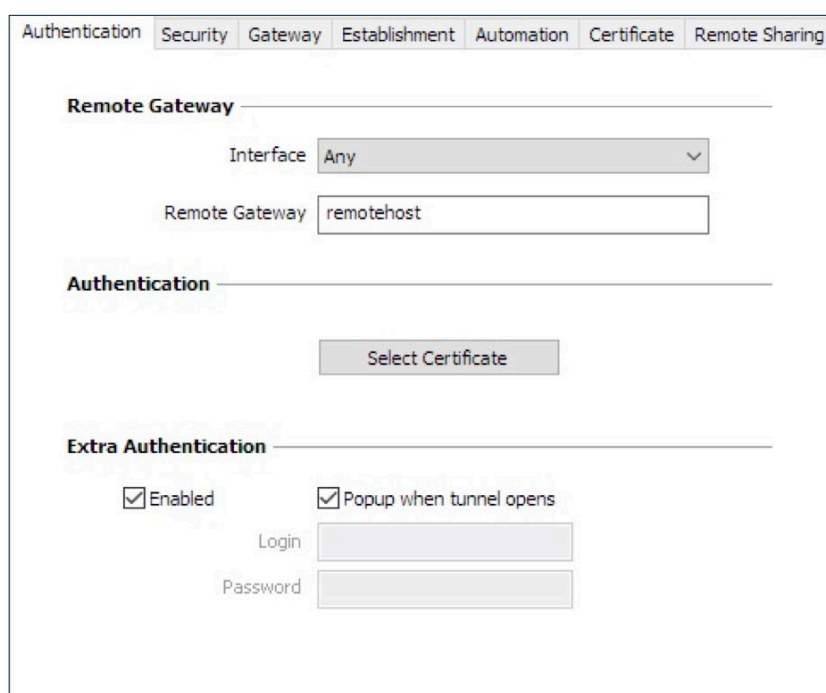
13.4 Configuring an SSL/OpenVPN tunnel

13.4.1 Introduction

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

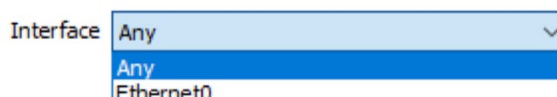
SSL VPN tunnels established by the Windows Enterprise VPN Client are compatible with OpenVPN and can establish secure connections with all gateways implementing this protocol.

13.4.2 SSL: Authentication



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**.



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 19 Managing certificates.

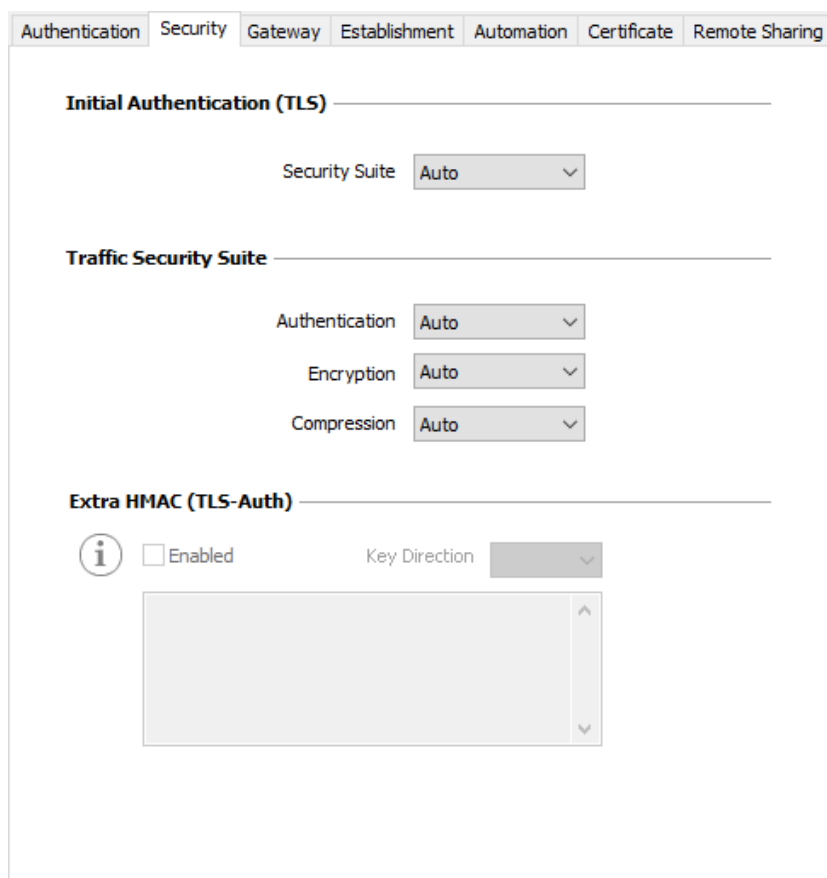
13.4.2.3 Extra Authentication

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





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 ditto

³ ditto

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' configuration tab. It includes the following settings:

- Dead Peer Detection (DPD)**:
 - Ping Gateway (s): 0
 - Detect Gateway (s): 0
 - On Dead Peer Detection: ☐ Close tunnel, ☐ Re-open tunnel
- Gateway related parameters**:
 - ☐ Explicit Exit
 - Check Gateway Certificate: Yes
 - Check Gateway Options: Apply
 - Validate the subject of the gateway certificate: [Empty text field]
 - Redundant Gateway: [Empty text field]
- 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 This parameter configures the VPN Client to send a specific VPN tunnel closing frame to the gateway when closing the tunnel.
If this option is not selected, the gateway will use DPD to close the tunnel at its end, which is less effective.

Check Gateway Certificate Specifies the control level applied to the gateway certificate.
In the current version, two levels are available:

- **Yes** (the certificate's validity is checked)
- **No** (the certificate's validity is not checked)

The **Lite** option is reserved for future use. In this version, it is equivalent to the **Yes** option.
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**.



The dynamic parameter `check_gateway_crl` is used to prevent the verification of the CRL used for gateway certificate validation (see 19.8.1.5) and the dynamic parameter `check_pki` is used to specify the gateway certificate verification method (see 19.8.1.6).

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.

Check Gateway Options	Used to determine the level of consistency between the VPN tunnel and gateway parameters (encryption algorithms, compression, etc.). • 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.
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) Lifetime (sec)

Packets

Tunnel Options

Physic.If MTU Tunnel IPV4

Tunnel MTU Tunnel IPV6

Tunnel Establishment Options

Port ☐ TCP Authentication timeout

Retransmissions Traffic setup timeout

Traffic

Traffic detection to open tunnel

IPV4 /

IPV6 /

Tunnel traffic check

IPV4

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 Virtual interface MTU.

When values have been entered, we recommend setting a lower value for the tunnel MTU than that of the physical interface MTU.

The default value for MTU is 0, meaning that the software will use the MTU value of the physical interface.

Tunnel IPV4 Defines the VPN Client's behavior when it receives an IPv4 configuration from the gateway:

- **Auto:** Accepts the information sent by the gateway
- **Yes:** Checks whether the information sent by the gateway matches the configured behavior. If it does not, 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 Defines the VPN Client's behavior when it receives an IPv6 configuration from the gateway:

- **Auto:** Accepts the information sent by the gateway
- **Yes:** Checks whether the information sent by the gateway matches the configured behavior. If it does not, 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 Port number used to establish the tunnel. The default port value is set to 1194.

The tunnel will use UDP by default. The **TCP** option is used to transport the tunnel over TCP.



Authentication timeout Time allowed to establish the authentication phase. When this time expires, it is assumed that the tunnel will not open. When this timeout expires, the tunnel is closed.



When an external authentication method is used, the default timeout for a push reply is 2 seconds. If this timeout is too short, you can increase it using the `push_request_timer` dynamic parameter (see chapter 18 Managing dynamic parameters).

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

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

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 19 Managing certificates.

13.4.8 **SSL: Remote sharing**



Refer to chapter 20 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 owing to a DNS resolution issue.



The dynamic parameter `redundant_retry` defines the maximum number of attempts to switch from the main gateway to the redundant gateway. The default value is 0, which means the number of attempts is unlimited (see chapter 18 Managing dynamic parameters).



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 of the Windows Enterprise VPN Client configuration window. The tab is selected among others: Authentication, Security, Gateway, Establishment, Automation, Certificate, and Remote Sharing. The 'Automation' section is divided into four main areas: 'Tunnel fallback', 'Automatic Open mode', 'Gina mode', and 'Scripts'. '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' has 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' has two checkboxes: 'Enable before Windows logon.' and 'Automatically open this tunnel when Gina starts at logon'. 'Scripts' has 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 23 GINA mode below).
-----------------------------	---

Automatically open this tunnel when GINA starts at logon	When this option is enabled, the tunnel will automatically open before the Windows logon. This option is enabled if the option Enable before Windows logon is selected.
--	--

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



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



18 Managing dynamic parameters

If necessary, the Windows Enterprise VPN Client allows the inclusion of additional dynamic parameters when configuring an IPsec/IKEv2 or OpenVPN tunnel.

The following table lists the dynamic parameters documented in this guide and specifies their use and their scope:

Parameter	Usage	Scope
local_subnet	Specify IP address of network interface (see 13.3.1.1)	IKE Auth and TLS
nonce_size	Specify nonce size for IPsec DR gateways (see 13.3.2)	IKE Auth
local_virtual_network_size	Specify virtual local network size (see 13.3.6.1)	Child SA
user_cert_keyusage	Select a certificate based on its Key Usage field (see 19.2.2.2)	IKE Auth and TLS
user_cert_dnpattern	Select a certificate based on its subject (see 19.2.2.2)	IKE Auth and TLS
user_cert_issuerknown	Restrict certificate selection to certificates whose issuer is included in the CA configuration for the tunnel (see 19.2.2.2)	IKE Auth
reader_pattern	Select the token/smart card reader to be used for automatic user certificate selection (see 19.2.2.1)	IKE Auth and TLS
MachineStore	Define the certificate store to be used at the tunnel level (see 19.6.1)	IKE Auth and TLS
check_user_crl	Prevent download of CRL used for user certificate validation (see 19.8.1.2)	IKE Auth and TLS
crl_cache_duration	Limit download of CRL used for gateway certificate validation (see 19.8.1.3)	IKE Auth and TLS
crl_cache_check_period	Define how often the cached CRL is updated (see 19.8.1.4)	IKE Auth and TLS
crl_cache_lifetime	Define the lifetime of the cached CRL (see 19.8.1.4)	IKE Auth and TLS
check_gateway_crl	Prevent the verification of the CRL used for gateway certificate validation (see 19.8.1.5)	IKE Auth and TLS
check_pki	Specify gateway certificate verification method (see 19.8.1.6)	IKE Auth and TLS
crl_download_retry	Implement a CRL download retry mechanism (see 19.8.1.7)	IKE Auth and TLS
allow_server_extra_keyusage	Validate the certificate even if it does not comply with the constraints on the Key Usage extension (see 19.8.2)	IKE Auth and TLS

Parameter	Usage	Scope
<code>allow_server_and_client_auth</code>	Validate the certificate even if it does not comply with the constraints on the Extended Key Usage extension (see 19.8.3)	IKE Auth and TLS
<code>sha2_in_cert_req</code>	Use the SHA-2 hash algorithm in the certificate request payload (see 19.9.3)	IKE Auth
<code>Method14_RSASSA_PKCS1</code>	Use other certificate authentication methods (see 29.5.5)	IKE Auth
<code>Method1_PKCS1v15_Scheme</code>	Use other certificate authentication methods (see 29.5.5)	IKE Auth
<code>use_method_214</code>	Use method 214 or method 14 for Brainpool user certificate authentication (see 29.5.5)	IKE Auth
<code>user_smartcard_tip</code>	Display a custom message in the PIN code entry popup (see 19.5)	IKE Auth
<code>interface_metric</code>	Apply a metric to the virtual interface (see 27.4.5)	Child SA and TLS
<code>rekey_send_current_TSR</code>	Resend the list of traffic selectors (TSr) that the gateway had provided at the time of initial key establishment during Child SA rekeying (see 13.3.6.1)	Child SA
<code>redundant_retry</code>	Define the maximum number of attempts to switch from the main gateway to the redundant gateway (see 14)	IKE Auth and TLS
<code>timeout_to_open</code>	Define the timeout for the IKE service to open a tunnel (see 6.3)	Child SA and TLS
<code>pincode_lifetime</code>	Define the duration that a token or smart card PIN code remains in memory (see 19.5)	Child SA
<code>push_request_timer</code>	Define the push reply timeout for an external authentication method in an SSL/OpenVPN tunnel (see 13.4.5.3)	TLS

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 find out how to enable the **More Parameters** tab, see section 25.2.4 Displaying more parameters.



19 Managing certificates

19.1 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 29.5.5 Certificate authentication methods)
- RSASSA-PSS with SHA-2 (only if the corresponding dynamic parameter has been configured, see section 29.5.5 Certificate authentication methods)
- ECDSA “secp256r1” with SHA-2 (256 bits)
- ECDSA “BrainpoolP256r1” with SHA-2 (256 bits)
- ECDSA “secp384r1” with SHA-2 (384 bits)
- ECDSA “secp521r1” with SHA-2 (512 bits)



To find out more about the authentication methods and cryptography used in the Windows Enterprise VPN Client, refer to section 29.5 Basic cryptography concepts in the appendix.

19.2 User certificate

19.2.1 Overview

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

The certificate must conform to the following constraints (ANSSI security recommendations):

- The Key Usage extension must be present, marked as critical, and only contain the value `digitalSignature` and/or `nonRepudiation`.
- The Extended Key Usage extension can be absent. If it is present, it must be marked as non-critical and only contain the value `id-kp-clientAuth`.



Behavior if certificate does not conform to constraints

If the user certificate does not meet the above constraints, the VPN Client's behavior depends on the certificate selection mode and on the value of the dynamic parameter `user_cert_keyusage`:

Case	Conditions	Warning displayed in Console	Connection to the gateway
Default settings	Automatic selection enabled and <code>user_cert_keyusage</code> undefined or set to its default value (4)	Yes	Blocked
Custom settings	Manual selection, or automatic selection enabled and <code>user_cert_keyusage</code> set to a value other than 4	Yes	Authorized ¹



For more information on automatic certificate selection, see section 19.2.2 Automatic certificate selection. The dynamic parameter `user_cert_keyusage` is described in section 19.2.2.2 Dynamic parameters for automatic certificate selection under [user cert keyusage](#).

19.2.2 Automatic certificate selection

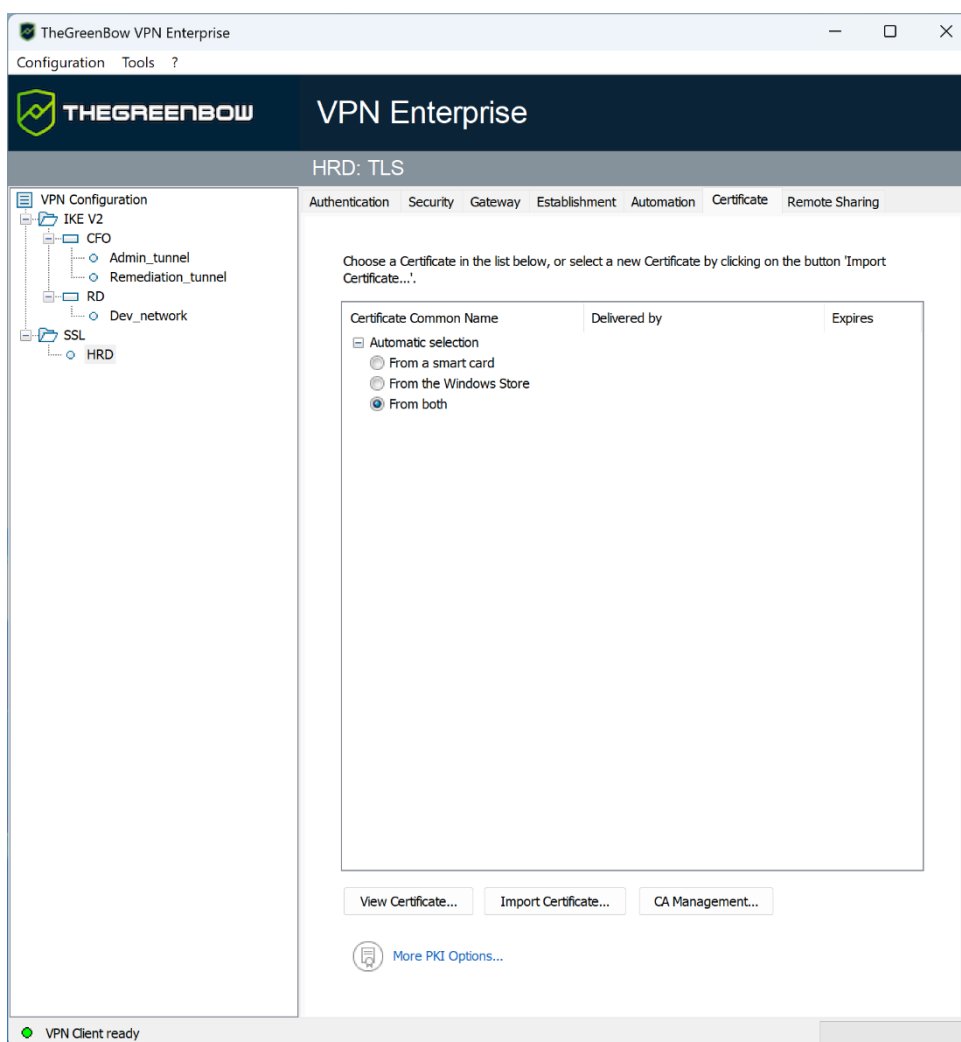
19.2.2.1 Overview

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

¹ If the gateway is configured with strict settings, it will refuse to authenticate the VPN Client.



Only valid certificates are considered during automatic selection. The following checks are performed to ensure certificate validity:

- The certificate's start date is earlier than the current date
- The certificate's expiration date is later than the current date
- The key size is greater than or equal to 2048 bits
- Key Usage and Extended Key Usage (EKU) extensions comply with ANSSI recommendations

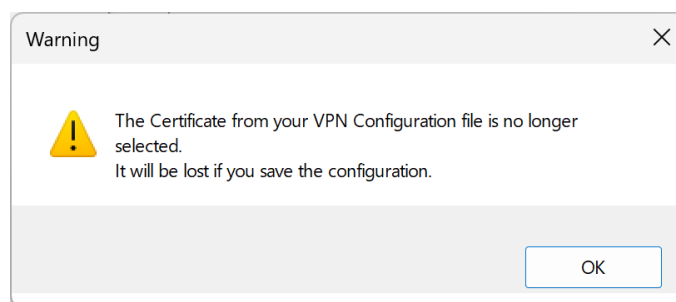
If you choose **From both**, the software will first look for the user certificate on a token/smart card. If it cannot find any, it will continue to search for a certificate in the Windows Certificate Store.

If you choose **From a smart card** or **From both** and you use more than one token/smart card reader, you must configure the dynamic parameter `reader_pattern` to specify the reader from which the certificate should be selected (see section see chapter 18 Managing dynamic 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 chapter 18 Managing dynamic 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.



19.2.2.2 Dynamic parameters for automatic certificate selection

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 configuration and apply to a given tunnel, whereas the MSI properties apply to all tunnels.

user_cert_keyusage

The dynamic parameter `user_cert_keyusage` is used to select a certificate based on its Key Usage (KU) field:



As of version 7.6 of the Windows Enterprise VPN Client, this dynamic parameter supports a new value that complies with ANSSI recommendations and is now the new default.

0	The certificate is not selected based on the Key Usage field.
1	The certificate is selected based on the Key Usage field, which must include the attribute <code>digitalSignature=1</code> .
2	The certificate is selected based on the Key Usage field, which must include the attributes <code>digitalSignature=1</code> and <code>keyEncipherment=1</code> .
4 or undefined	The certificate is selected based on the Key Usage and Extended Key Usage (EKU) extensions allowed by ANSSI: only <code>digitalSignature</code> and/or <code>nonRepudiation</code> in Key Usage, and either no EKU extension or only <code>id-kp-clientAuth</code> . If multiple certificates meet these criteria, the one with the most recent start date is selected.

user_cert_dnpattern

The dynamic parameter `user_cert_dnpattern` is used to select a certificate based on its subject.

When defined, the Windows Enterprise VPN Client searches tokens, smart cards, and the Windows certificate store for a certificate whose subject matches the specified regular expression.

Regular expressions follow the ECMAScript 2025 syntax.



For more information, see the ECMAScript® 2025 Language Specification (ECMA-262): <https://ecma-international.org/publications-and-standards/standards/ecma-262/>.



For more information about the ECMAScript regular expression grammar, see the ECMAScript regular expression syntax reference on the following page: <https://en.cppreference.com/w/cpp/regex/ecmascript.html>.

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



In previous versions of the software, this parameter contained only text to match against part of the certificate subject. Existing configurations therefore remain compatible without intervention.

The following examples demonstrate how regular expressions can be applied to the certificate subject shown below:

```
C = FR, ST = IDF, L = PARIS, O = TGB, OU = DT, CN =
TEST_CLIENT1_RSA2048_DEC24, emailAddress =
test@thegreenbow.com
```



Regular expression	Description	Example of matching string	Example of non-matching string
<code>^.*TEST_CLIENT1_RSA2048_DEC24.*\$</code>	Matches any string containing the substring TEST_CLIENT1_RSA2048_DEC24 anywhere in the subject.	CN = TEST_CLIENT1_RSA2048_DEC24, OU = DT	CN = TEST_CLIENT1_RSA2048_DEC26, OU = DT
<code>^(?!.*PREFIX-TEST_CLIENT1_RSA2048_DEC24).*</code>	Uses a negative lookahead assertion <code>(?!...)</code> . Matches only strings that do not contain PREFIX-TEST_CLIENT1_RSA2048_DEC24. Once the negative lookahead assertion succeeds, <code>.*</code> consumes the entire string.	CN = TEST_CLIENT1_RSA2048_DEC24, OU = DT	CN = PREFIX-TEST_CLIENT1_RSA2048_DEC24, OU = DT
<code>^(?!.*CN = PREFIX-TEST_CLIENT1_RSA2048_DEC24).*</code>	Does not match strings containing the exact substring CN = PREFIX-TEST_CLIENT1_RSA2048_DEC24.	C = FR, CN = TEST_CLIENT1_RSA2048_DEC24	C = FR, CN = PREFIX-TEST_CLIENT1_RSA2048_DEC24
<code>^C = [A-Z]{2}.*test@thegreenbow.com\$</code>	The string must start with C = followed by exactly two uppercase letters <code>[A-Z]{2}</code> . It may then contain any number of characters <code>(.*)</code> and must end with test@thegreenbow.com.	C = FR, L = PARIS, emailAddress = test@thegreenbow.com	C = fr, emailAddress = test@thegreenbow.com
<code>^C\s=\s[A-Z]{2}.*test@thegreenbow.com\$</code>	Same logic as the previous example, but explicitly requires whitespace around the equals sign <code>(\s=\s)</code> , matching the format C = FR ... test@thegreenbow.com.	C = FR, L = PARIS, emailAddress = test@thegreenbow.com	C=FR,L=PARIS,emailAddress=test@thegreenbow.com
<code>^(?!.*TEST_CLIENT1_RSA2048_DEC26).*</code>	Uses a negative lookahead to exclude strings containing TEST_CLIENT1_RSA2048_DEC26.	CN = TEST_CLIENT1_RSA2048_DEC24	CN = TEST_CLIENT1_RSA2048_DEC26

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

user_cert_issuerknown

The dynamic parameter `user_cert_issuerknown` restricts user certificate selection to certificates whose issuer (Issuer field) is specified in the tunnel's CA configuration.

When it is defined, the Windows Enterprise VPN Client searches on a token or smart card, or in the Windows certificate store, for a certificate issued by one of the certificate authorities (CAs) specified in the tunnel configuration.



If the issuing certificate authority (CA) specified in this parameter is not included in the VPN configuration file, user certificate filtering does not work (see section 19.9 Managing certificate authorities).

19.3 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 19.4 Importing a certificate to the VPN configuration)
- On a smart card or token (see 19.5 Using a certificate stored on a smart card or token)
- In the Windows Certificate Store (see 19.6 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 card readers, the reader is displayed with a warning icon in front, if the smart card is not inserted.



Certificate Common Name	Delivered by	Expires
[-] Windows Personal Certificat...		
☐ Automatic selection		
 ☐ 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

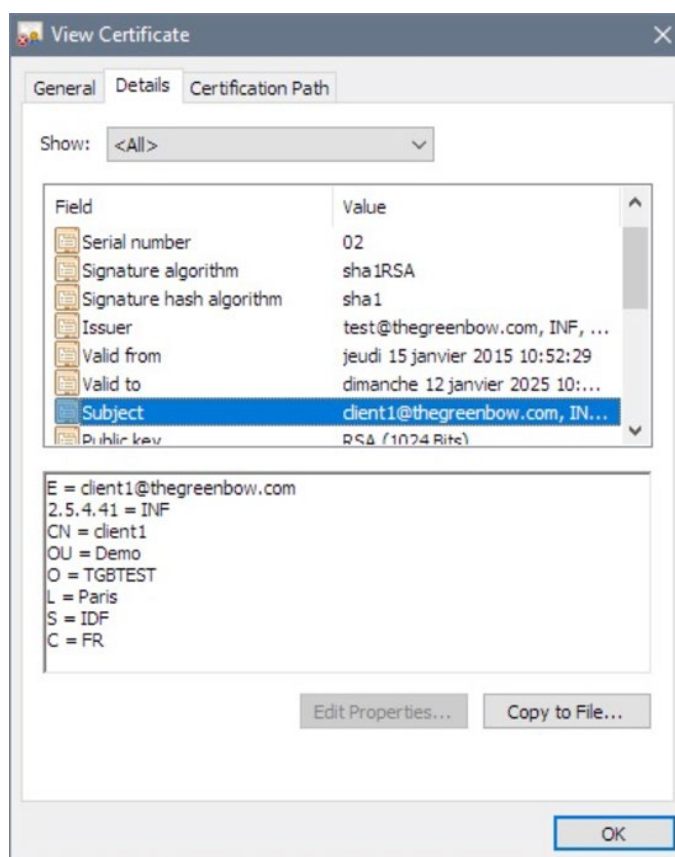
Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...'.

Certificate Common Name	Delivered by	Expires
☐ Automatic selection ☐ From a smart card ☐ From the Windows Store ☐ From both		
☐ VPN Configuration File ☒ CLIENT1_RSA_OCT2022 FGCAINTER2MAY2022 04-06-2032		
☐ Windows Personal Certifica... ☐ CLIENT1_RSA_OCT2022 FGCAINTER2MAY2022 04-06-2032		
☐ Badgeo ID 2.0 ☐ 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
Identity _____ Local ID DER ASN1 DN ▼ Remote ID ▼			

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 19.2.2 Automatic certificate selection).

19.4 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.

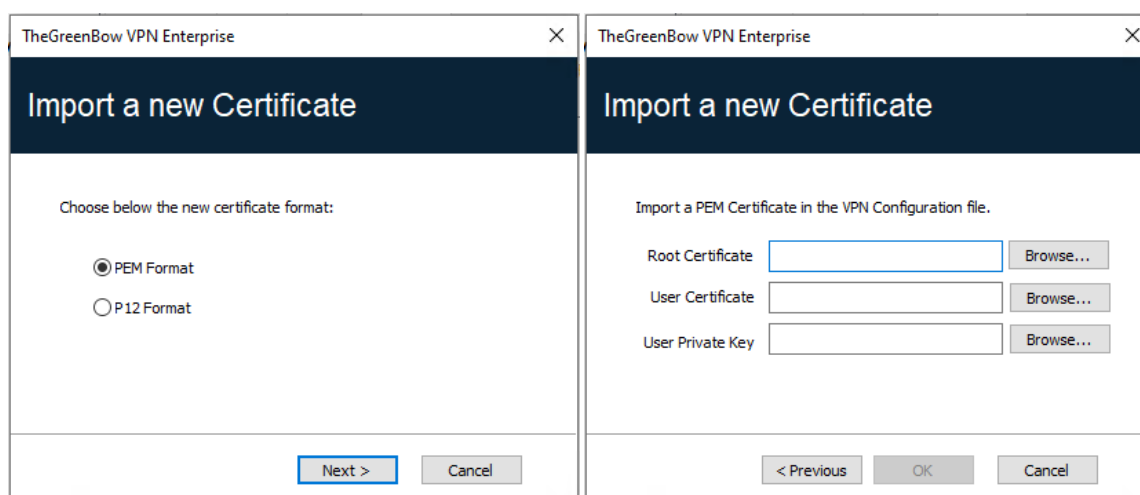
Nevertheless, the disadvantage of transporting certificates in a VPN configuration is that each configuration then becomes user-specific. We therefore do not recommend this solution for a substantial deployment.



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.

19.4.1 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.

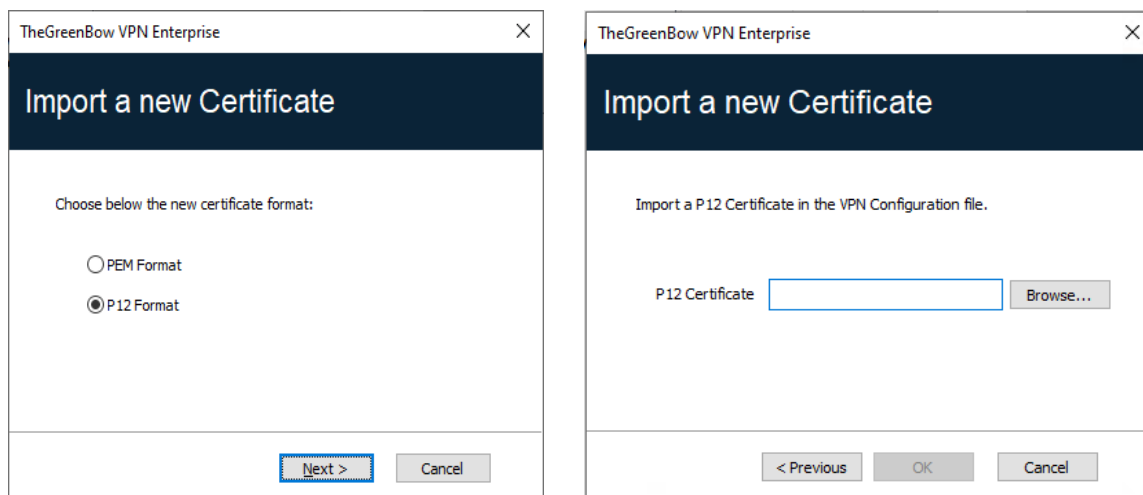
19.4.2 Importing a PKCS #12 certificate

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.

19.5 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 19.6.2 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 19.2.2 Automatic certificate 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 chapter 18 Managing dynamic parameters).



As of version 7.7 of the Windows Enterprise VPN Client, the dynamic parameter `pincode_lifetime` allows the PIN code to remain in memory for up to 8 hours (28,800 s). In the event of an unstable Wi-Fi connection, users are not required to re-enter the PIN during this period (see chapter 18 Managing dynamic parameters).

The PIN cache timeout is triggered when a tunnel configured for PIN authentication is successfully established. The timeout applies only to the current tunnel, even if the same token or smart card is used to establish multiple tunnels.

Resetting the IKE daemon clears the PIN code from the cache, even if the configured timeout has not expired.

19.6 Using a certificate stored in the Windows Certificate Store

19.6.1 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 Current User Certificate Store (it represents the personal identity of the user who wants to open a VPN tunnel to the corporate network) To use the Local Machine Certificate Store, add dynamic parameter `MachineStore` set to the value `true` (see chapter 18 Managing dynamic 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.

19.6.2 Importing a certificate depending on the store used

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

- Current User Certificate Store or user store:

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

- Local Machine Certificate Store or 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 19.2.2 Automatic certificate selection).

19.7 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.

19.8 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.



Some gateways automatically send intermediate certificates. In such cases, you do not need to include them in the configuration—only the certificate authority's root certificate is required.

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 Local Machine 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

19.8.1 Preventing or limiting CRL download or verification

19.8.1.1 Introduction

In some cases, Certificate Revocation Lists (CRLs) can be relatively large (several MB). Downloading or verifying them may take time and slow down tunnel establishment, especially when many users contact the HTTP server simultaneously.

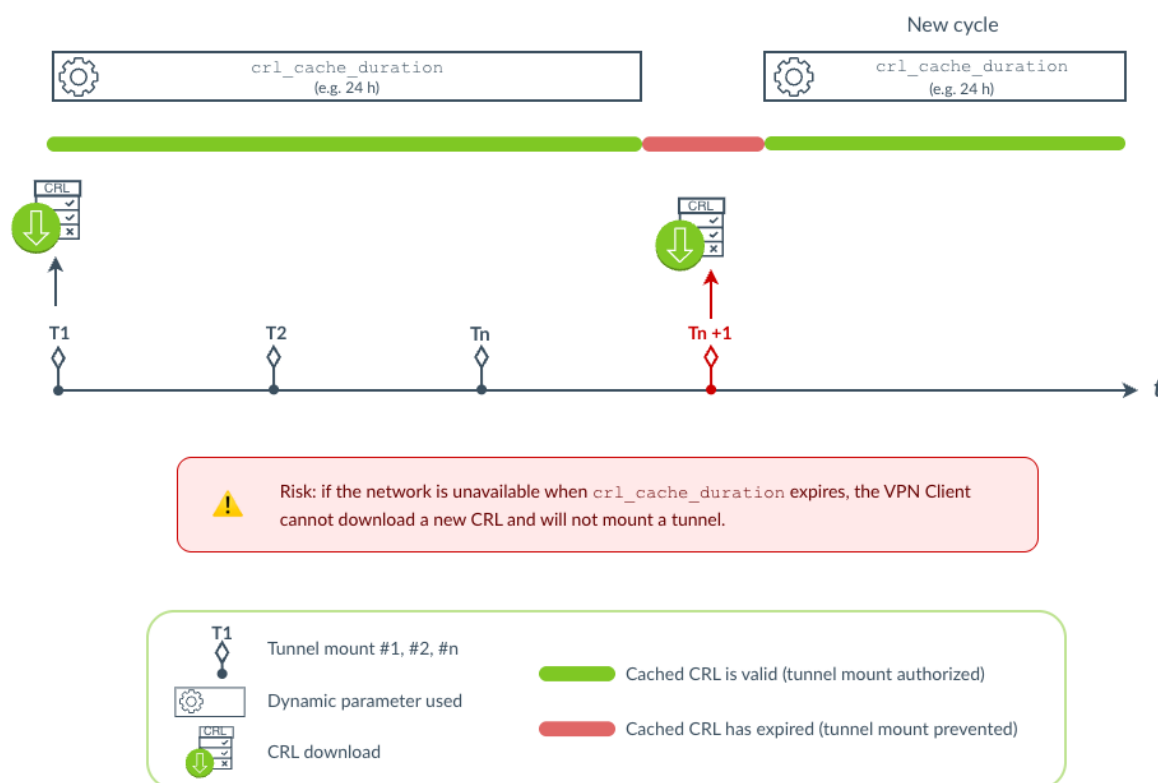
The Windows Enterprise VPN Client provides seven dynamic parameters described below to speed up tunnel establishment. These parameters work independently from one another and can be combined:

- `check_user_crl`: prevents the download of the CRL the user certificate (see 19.8.1.2)
- `crl_cache_duration`: limits the download of the CRL used to validate the gateway CRL (see 19.8.1.3)
- `crl_cache_check_period` and `crl_cache_lifetime` define whether the cached CRL must be updated (see 19.8.1.4)
- `check_gateway_crl`: prevents the verification of the CRL used to validate the gateway certificate (see 19.8.1.5)
- `check_pki`: specifies the gateway certificate verification method (see 19.8.1.6)
- `crl_download_retry`: implements a CRL download retry mechanism (see 19.8.1.7)



A Certificate Revocation List (CRL) lists all the certificates that are no longer trustworthy: expired certificate, compromised private key, modification of a field relating to the owner, etc. CRLs are defined in [RFC 5280](#) and [RFC 6818](#), and are published by Certificate Authorities (CAs) and Public Key Infrastructures (PKIs).

When `crl_cache_duration` is used alone, the VPN Client caches the downloaded CRL for the configured duration, reusing it for all subsequent tunnel connections without triggering a new download. Once the duration expires, the next attempt to mount a tunnel triggers a fresh CRL download and resets the cache timer, as illustrated in the diagram below.

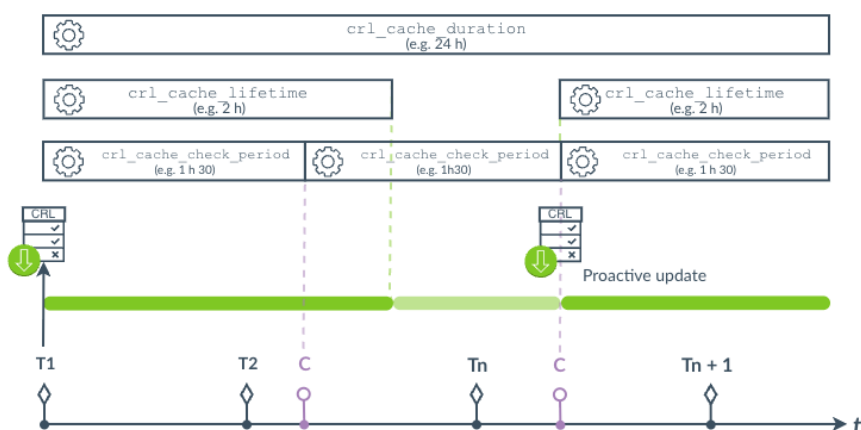
Scenario 1 – `crl_cache_duration` used alone

However, if a network disruption occurs when the cache has expired (`crl_cache_duration`) and a new CRL download is required, the VPN Client cannot download a new CRL and blocks the tunnel from mounting. The dynamic parameters `crl_cache_check_period` and `crl_cache_lifetime` work together to prevent this scenario, as illustrated in the diagram below:

- `crl_cache_lifetime` defines a validity period shorter than `crl_cache_duration`, determining when the cached CRL becomes eligible for renewal
- `crl_cache_check_period` sets the frequency at which the cached CRL validity is checked and, if necessary, triggers a fresh download

Together, these two parameters ensure the cached CRL is refreshed before `crl_cache_duration` expires, so that it never expires at the critical moment of connection.

Scenario 2 – Proactive update ($crl_cache_check_period + crl_cache_lifetime$)



- ✓ The CRL is updated proactively while the tunnel is active.
It is never expired at the critical moment when a tunnel is mounted.
- ⚠ Residual risk: network failure during proactive update.

T1 Tunnel mount #1, #2, #n

Periodic check:
- OK = cached CRL is still valid (no download)
- Not OK ($crl_cache_lifetime$ has expired)
= new CRL is downloaded

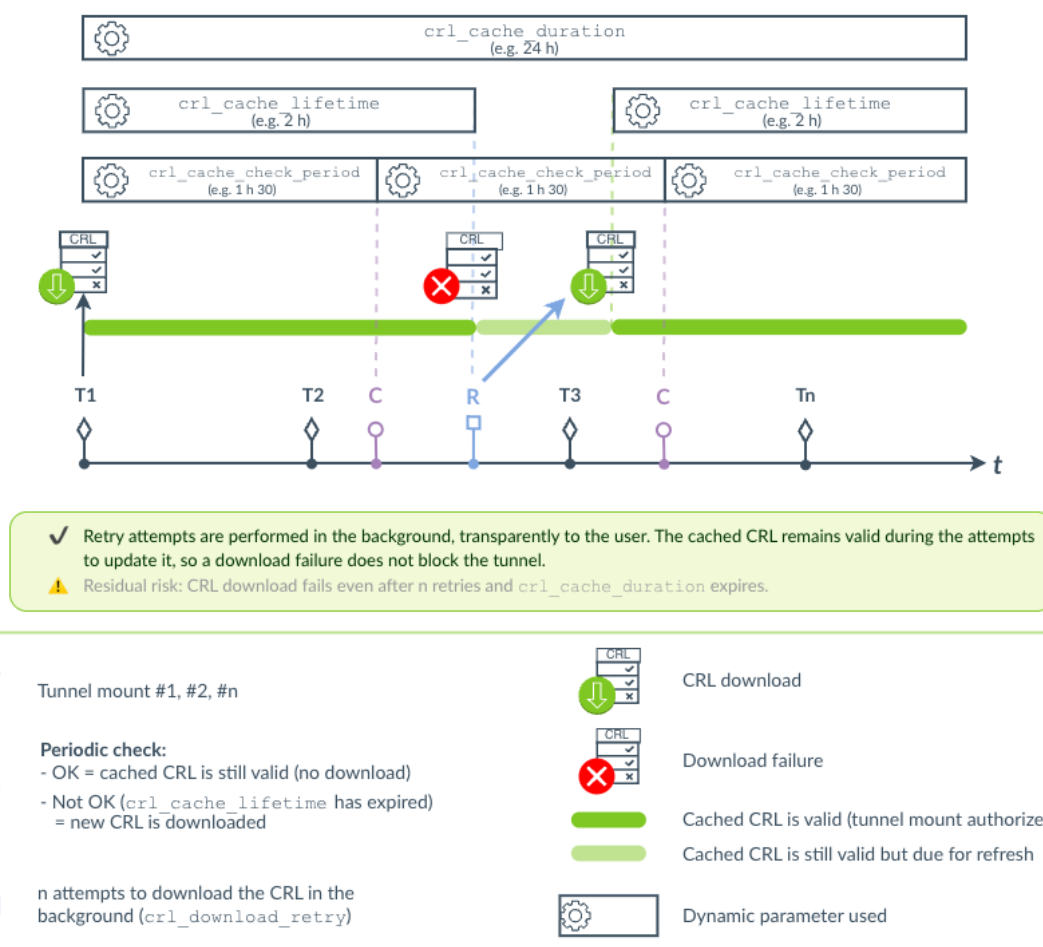
 Dynamic parameter used

 CRL download

 Cached CRL is valid (tunnel mount authorized)

 Cached CRL is still valid but due for refresh

Even when $crl_cache_check_period$ and $crl_cache_lifetime$ are active, a network disruption can prevent the CRL from being downloaded on the first attempt. The $crl_download_retry$ parameter completes this setup by implementing an automatic retry mechanism: if the first attempt fails, further attempts are launched in the background, transparently to the user. As illustrated in the diagram below, the cached CRL remains valid in the meantime, preventing a download failure from blocking the tunnel.

Scenario 3 – Retry mechanism (`crl_download_retry`)

To find out more about how to add dynamic parameters, refer to chapter 18 Managing dynamic parameters.

19.8.1.2 Preventing CRL downloads for user certificate validation

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`. In this case, the user certificate CRL is not verified. The gateway will handle this verification.



19.8.1.3 Limiting CRL downloads for gateway certificate validation

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.

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.

19.8.1.4 Updating the cached CRL

When a CRL has been cached using the `crl_cache_duration` dynamic parameter (see 19.8.1.3 Limiting CRL downloads for gateway certificate validation), the `crl_cache_check_period` and `crl_cache_lifetime` dynamic parameters determine, while the tunnel is established, whether the cached CRL must be updated and trigger an update if necessary.



The check and update apply only to certificates stored in the VPN configuration of the current tunnel. Certificates associated with other tunnels, whether using a different PKI or different cache entries, are not checked or updated.

The dynamic parameter `crl_cache_check_period` defines the check interval, in seconds. The recommended value is 5,400 seconds (i.e. 1.5 hours).

The dynamic parameter `crl_cache_lifetime` defines the CRL cache lifetime, in minutes. Once this period has expired, the CRL is updated at the next check performed by `crl_cache_check_period`.



Verifying and updating the cached CRL requires both dynamic parameters to be configured.

19.8.1.5 Preventing CRL verification for gateway certificate validation

Similarly as for the user certificate validation CRL, the dynamic parameter `check_gateway_crl` is used to enable or disable the verification of the CRL used for VPN gateway certificate validation at the tunnel level.

Possible values:

False	The CRL for VPN gateway certificate validation is not verified.
True	The CRL for VPN gateway certificate validation is verified (default value).

19.8.1.6 Specifying gateway certificate verification

Similarly as for MSI property `PKICHECK` (see Deployment Guide), which performs this check at an overall level, the dynamic parameter `check_pki` is used to verify the VPN gateway certificate at the tunnel level.



This parameter is prohibited (or forced to `True`) in IPsec DR mode.

Possible values:

False	The VPN gateway certificate is not verified.
True	The following characteristics of the VPN gateway certificate are verified: validity date, certificate chain, signature and CRL of each certificate in the certificate chain—default value.



Verifying the VPN gateway certificate is essential in all circumstances. Certificate verification should be disabled only temporarily, and only in a controlled test environment under strict supervision.

19.8.1.7 Implementing a retry mechanism

In some situations, a failure to download the CRL prevents the VPN Client from validating the certificate and establishing the tunnel. The user must then attempt to establish the tunnel again.

To address this issue during unstable network conditions, a CRL download retry mechanism can be implemented to automatically retry the download if it fails. Configure the `crl_download_retry` dynamic parameter to specify the maximum number of CRL download attempts. If this parameter is not defined or set to 0, no retry is performed.

The CRL download is retried regardless of the type of error encountered. If a cache duration is configured using `crl_cache_duration` (see section 19.8.1.3 Limiting CRL downloads for gateway certificate validation) or a lifetime is configured using `crl_cache_lifetime` (see section

19.8.1.4 Updating the cached CRL), the retry is performed only after the configured duration has expired.

19.8.2 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 chapter 18 Managing dynamic 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_server_extra_keyusage`.



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

19.8.3 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 chapter 18 Managing dynamic 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`

19.9 Managing certificate authorities

19.9.1 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 (256 bits)
- ECDSA "BrainpoolP256r1" with SHA-2 (256 bits)
- ECDSA "secp384r1" with SHA-2 (384 bits)
- ECDSA "secp521r1" with SHA-2 (512 bits)

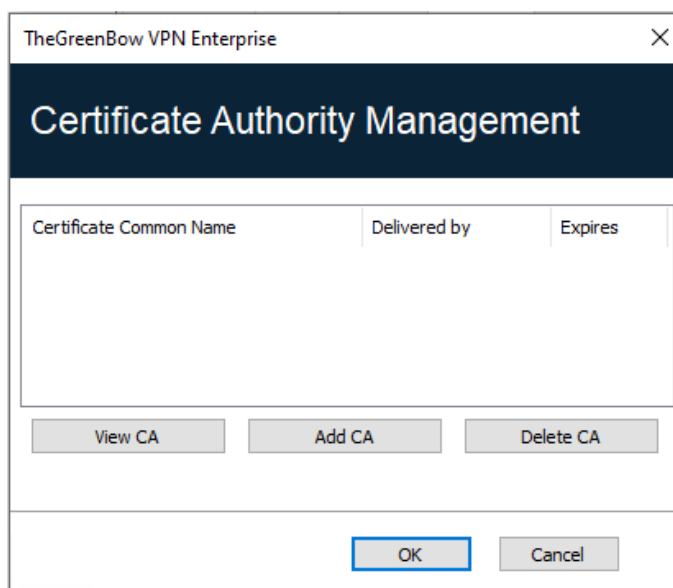
The following root CA types are supported:

- RSASSA-PKCS1-v1.5 with SHA-2
- RSASSA-PSS with SHA-2
- ECDSA “secp256r1” with SHA-2 (256 bits)
- ECDSA “BrainpoolP256r1” with SHA-2 (256 bits)
- ECDSA “secp384r1” with SHA-2 (384 bits)
- ECDSA “secp521r1” with SHA-2 (512 bits)



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

19.9.2 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.

19.9.3 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 see chapter 18 Managing dynamic 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.

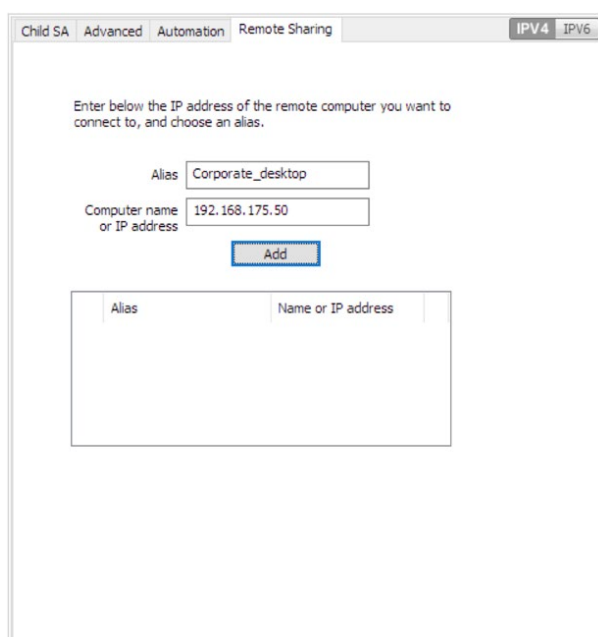
20 Remote Desktop Sharing

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

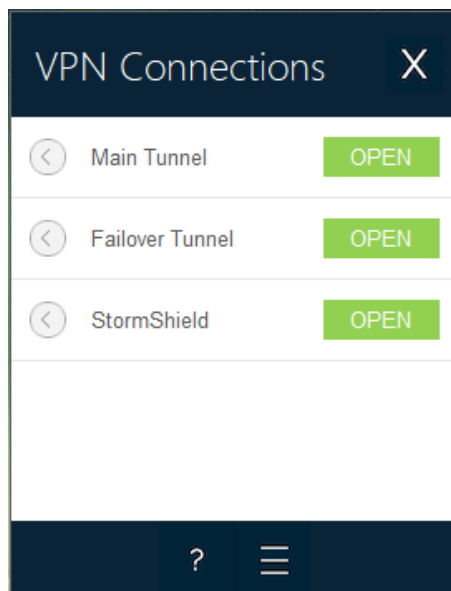
Alias	Name or IP address	
Corporate_desktop	192.168.175.50	

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.



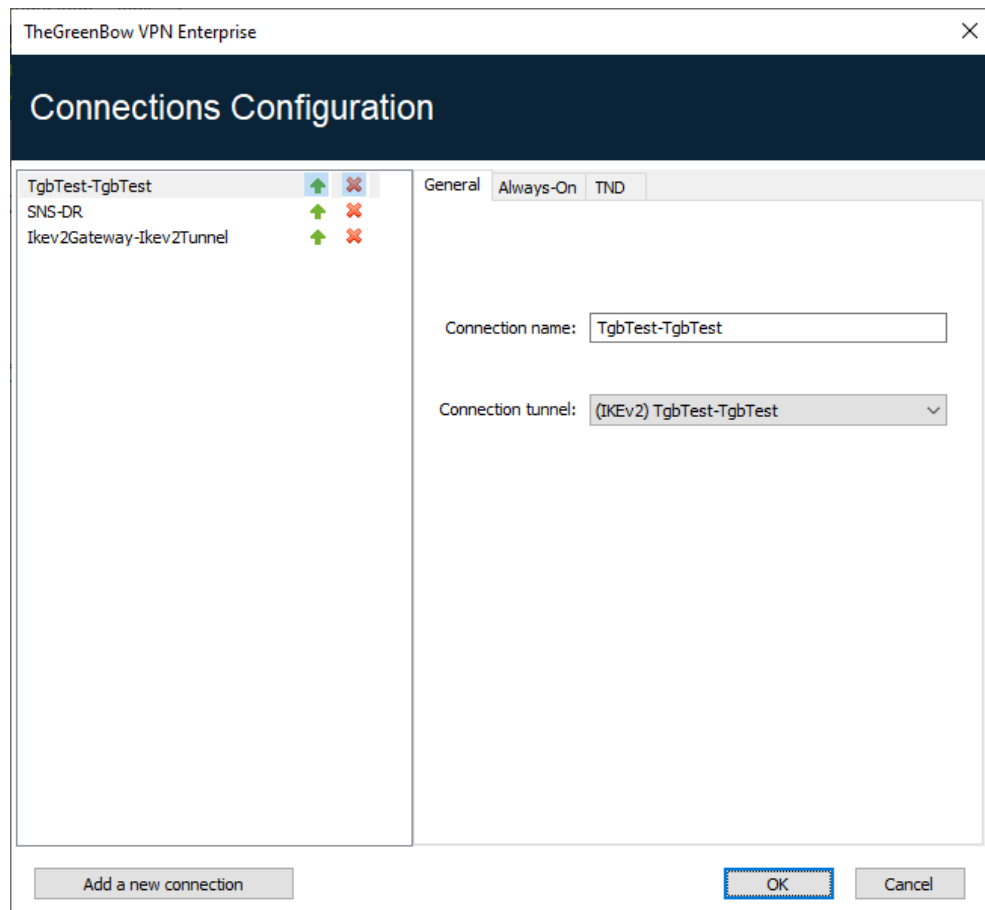
21 Configuring the Connection Panel

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 21 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.

22 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 21 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 graphical interface
- Purge log files

22.1 Always-On

22.1.1 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)

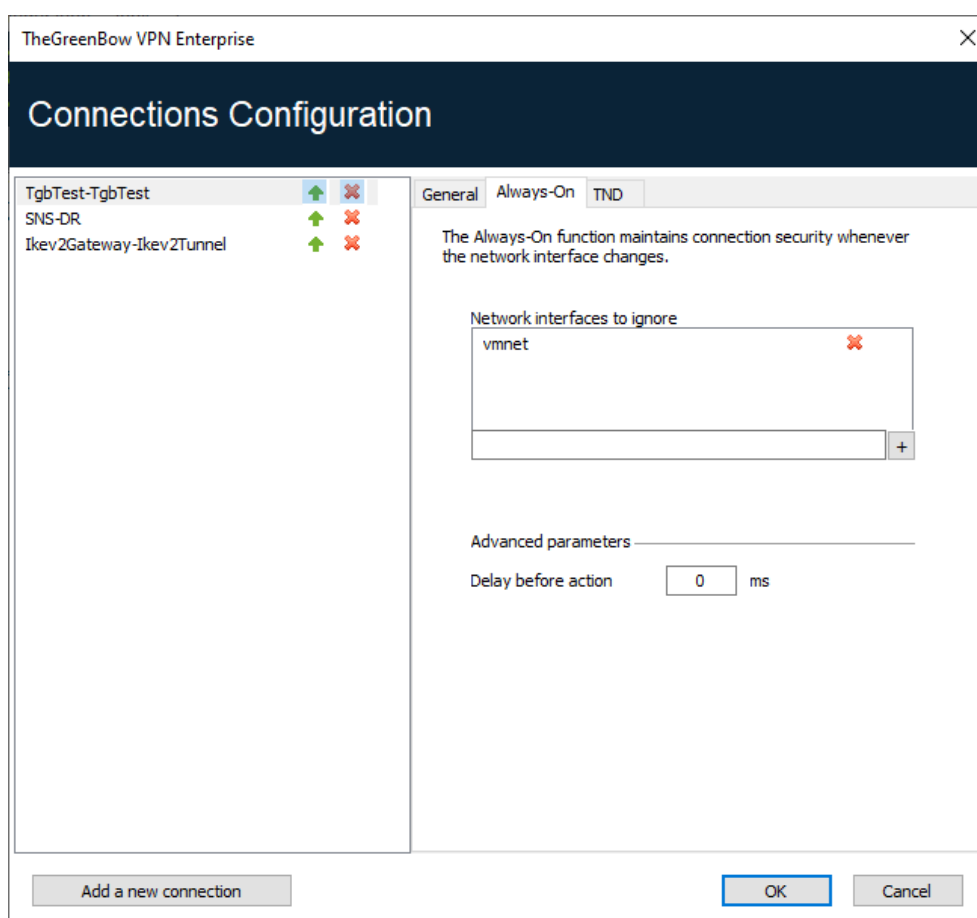
The following network events trigger automatic tunnel reconnection (and, where appropriate, detection of the trusted network), unless they have been explicitly excluded (see section 22.1.2 Configuring Always-On):

- 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

22.1.2 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.

22.2 Trusted Network Detection (TND)

22.2.1 Operating principle

22.2.1.1 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, selected in the **TND** tab, to detect whether the workstation is on a trusted network:

1. **HTTPS method:** it checks for a trusted DNS suffix, then verifies whether it can access a trusted web server and whether the server's certificate is valid (see section 22.2.1.2 HTTPS method)
2. **AD method:** it checks whether the workstation is joined to an Active Directory (AD) domain whose name is in the list of trusted domain names (see section 22.2.1.3 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. Moreover, you must add a rule to the `BLOCK_ALL` ruleset that allows outbound UDP traffic on port 389 to the domain controllers. Without this rule, Trusted Network Detection (TND) cannot detect the trusted network.

22.2.1.2 HTTPS method

The HTTPS method 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 steps 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

To enable TND with the HTTPS method, 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).

22.2.1.3 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 is considered to be outside the trusted network until a user logs on to Windows.

22.2.2 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, detection cannot succeed.



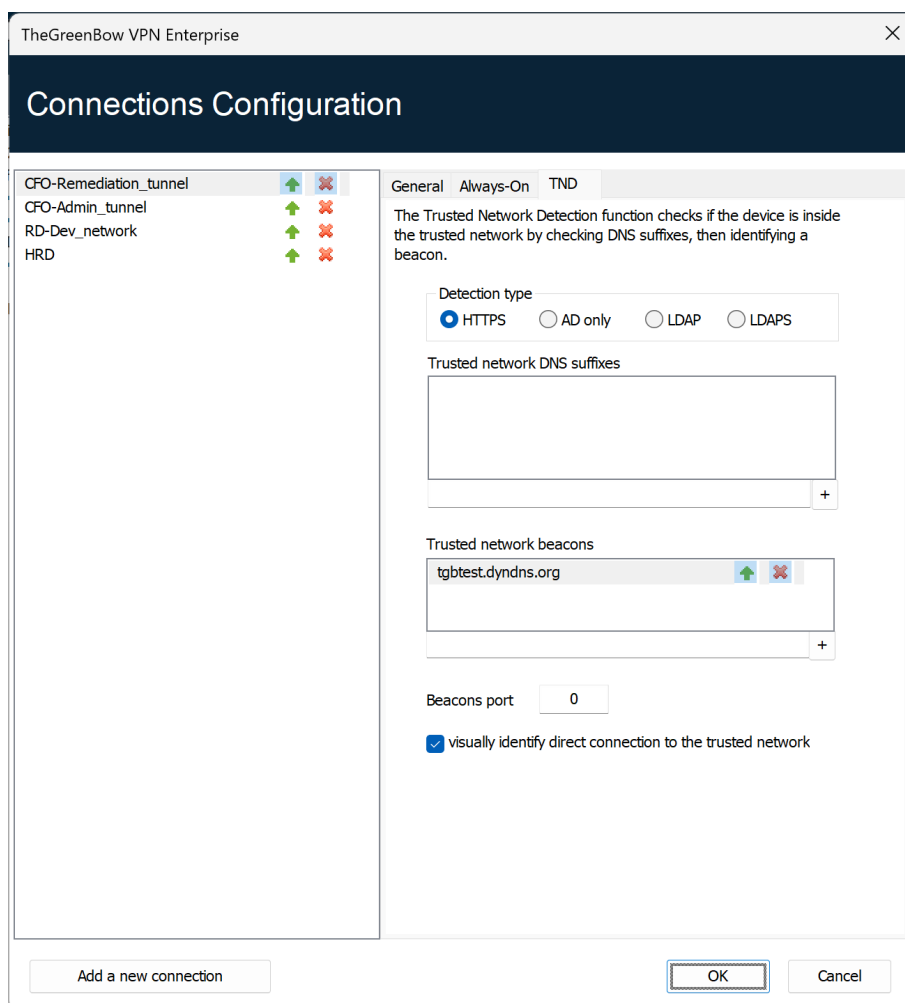
With the **AD only**, **LDAP**, or **LDAPS** detection type, the **Trusted network DNS suffixes** list is not used: only the **Domain names** list is taken into account.

Make sure it is filled in; if it is empty, detection cannot succeed.

Enter each domain name exactly as your directory reports it, including case, and list every domain individually: a parent domain does not cover its subdomains.

DNS suffixes remain fully operational with the **HTTPS** detection type, provided at least one beacon is configured.

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



TheGreenBow VPN Enterprise

Connections Configuration

Connection Name	Status
CFO-Remediation_tunnel	Up (Green arrow)
CFO-Admin_tunnel	Down (Red X)
RD-Dev_network	Down (Red X)
HRD	Down (Red X)

General | Always-On | TND

The Trusted Network Detection function checks if the device is inside the trusted network by checking DNS suffixes, then identifying a beacon.

Detection type

☒ HTTPS ☐ AD only ☐ LDAP ☐ LDAPS

Trusted network DNS suffixes

Trusted network beacons

tgtest.dyndns.org

Beacons port 0

☒ visually identify direct connection to the trusted network

Add a new connection OK Cancel

Trusted network DNS suffixes

This parameter is used only with the HTTPS detection type. It defines the list of trusted DNS suffixes. This list can contain more than one DNS suffix.

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 This parameter defines the list of IP addresses (or DNS names) of the trusted servers to be used.

This list can contain more than one IP address (or DNS name). 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.

The IP addresses (or DNS names) must be separated by a comma in the list, without any blank spaces.

You do not need to add the `https://` prefix to IP address (or DNS name).



By default, the **TrustedConnect Panel** tries to connect to the `/index.html` page. If this page does not exist on the server, the server cannot be used as a beacon.

Beacons port 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).

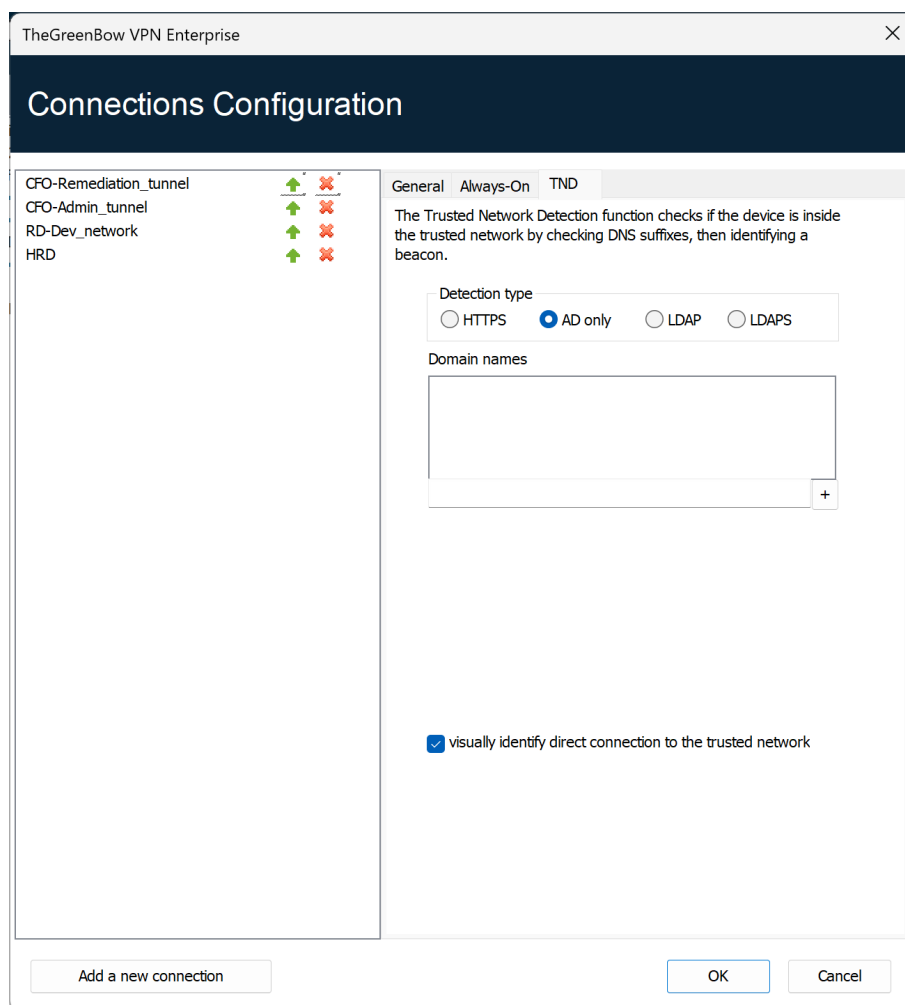
If this parameter is not configured, the VPN Client will use the port 443 by default.

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

If the box is checked, the notification area icon and the panel's status indicator ring are blue when the machine is connected to the trusted network and green when a tunnel is open.

If the box is unchecked, the notification area icon and panel's status indicator ring remain green in both cases. No distinction is made between the trusted network and an open tunnel.

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



Domain names

This parameter defines the list of trusted domain names. This list can contain more than one domain name.

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.

Enter each domain name exactly as your directory reports it, including case. A parent domain does not cover its subdomains: list each domain individually. If the list is empty, detection cannot succeed.

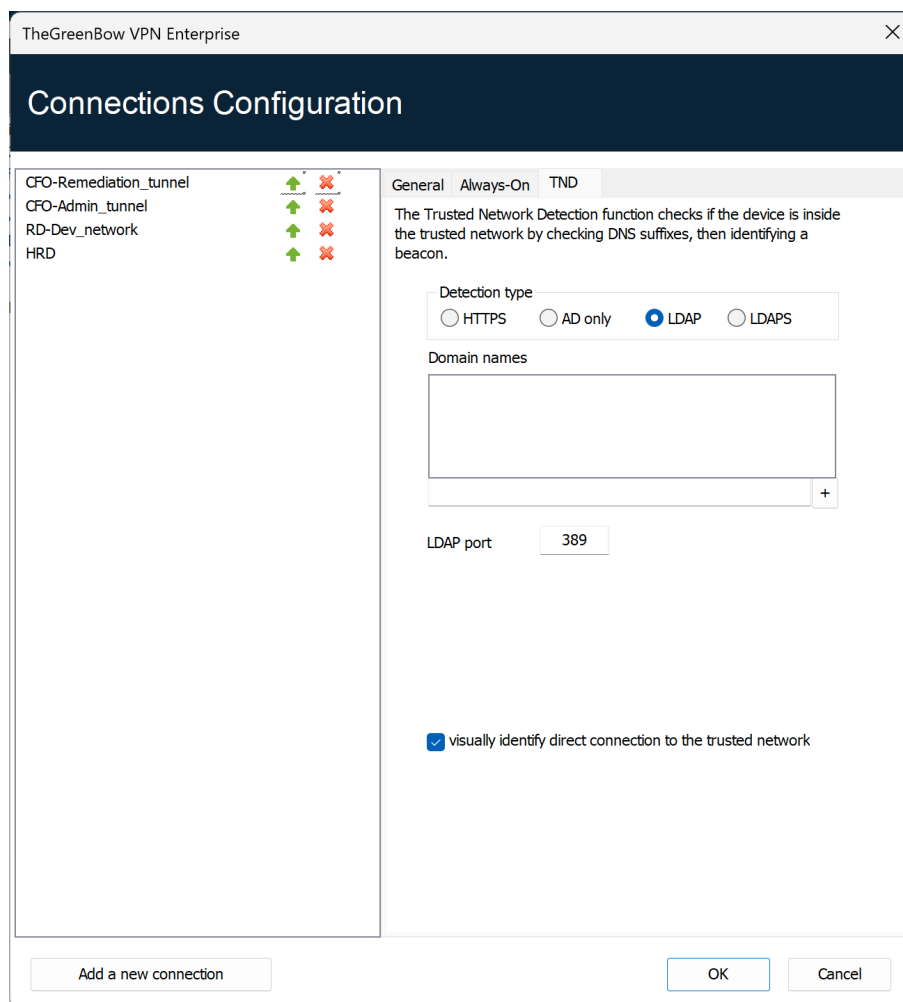
Visually identify direct connection to the trusted network

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 notification area icon and the panel's status indicator ring are blue when the machine is connected to the trusted network and green when a tunnel is open.

If the box is unchecked, the notification area icon and panel's status indicator ring remain green in both cases. No distinction is made between the trusted network and an open tunnel.

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



Domain names

This parameter defines the list of trusted domain names. This list can contain more than one domain name.

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.

Enter each domain name exactly as your directory reports it, including case. A parent domain does not cover its subdomains: list each domain individually. If the list is empty, detection cannot succeed.

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.

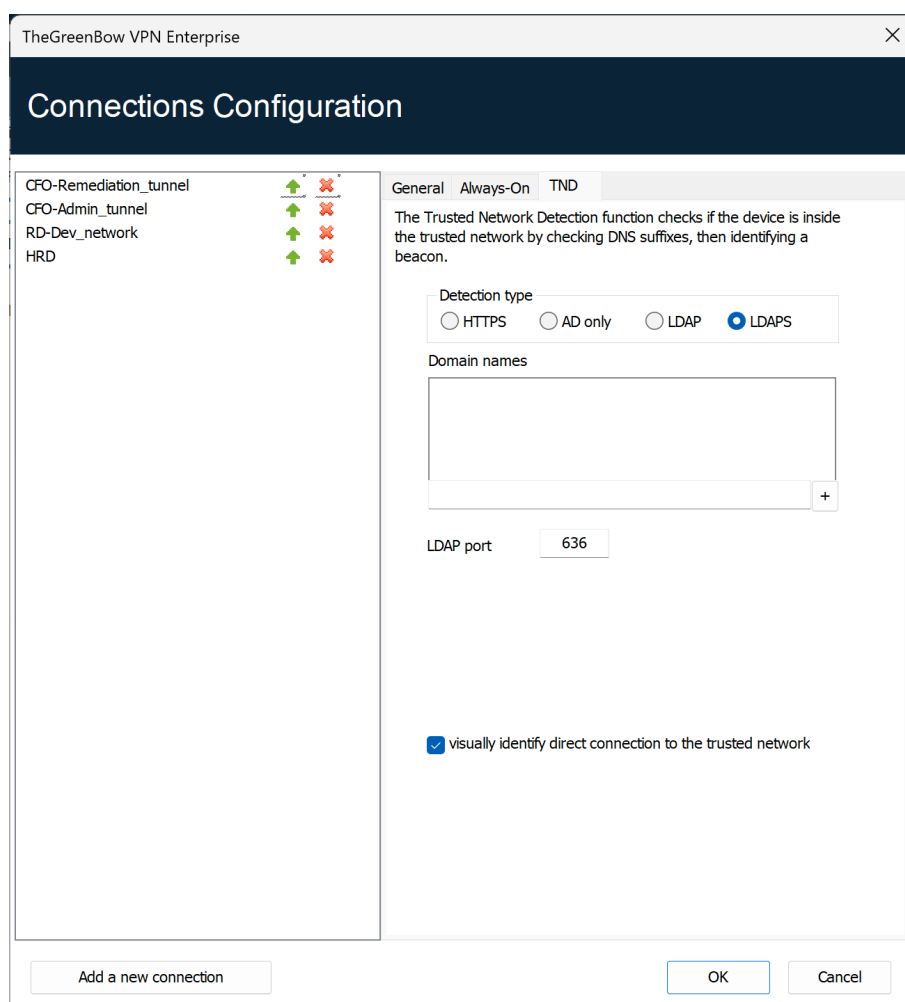
Visually identify direct connection to the trusted network

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 notification area icon and the panel's status indicator ring are blue when the machine is connected to the trusted network and green when a tunnel is open.

If the box is unchecked, the notification area icon and panel's status indicator ring remain green in both cases. No distinction is made between the trusted network and an open tunnel.

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



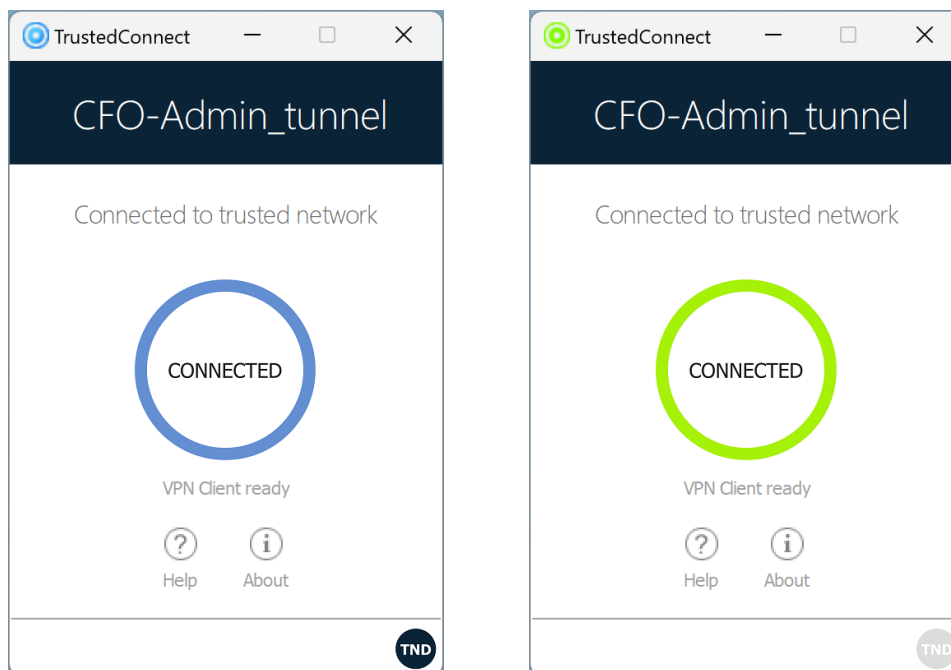
The screenshot shows the 'Connections Configuration' window of TheGreenBow VPN Enterprise. The window has a title bar 'TheGreenBow VPN Enterprise' and a close button. The main title is 'Connections Configuration'. On the left, there is a list of connections: 'CFO-Remediation_tunnel', 'CFO-Admin_tunnel', 'RD-Dev_network', and 'HRD'. Each connection has a green up arrow and a red X icon next to it. On the right, there are tabs: 'General', 'Always-On', and 'TND'. The 'TND' tab is selected. Below the tabs, there is 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, there is a 'Detection type' section with four radio buttons: 'HTTPS', 'AD only', 'LDAP', and 'LDAPS'. The 'LDAPS' radio button is selected. Below this is a 'Domain names' section with a text input field and a '+' button. Below that is an 'LDAP port' section with a text input field containing '636'. At the bottom, there is a checkbox labeled 'visually identify direct connection to the trusted network' which is checked. At the very bottom, there are three buttons: 'Add a new connection', 'OK', and 'Cancel'.

Domain names	This parameter defines the list of trusted domain names. This list can contain more than one domain name. 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. Enter each domain name exactly as your directory reports it, including case. A parent domain does not cover its subdomains: list each domain individually. If the list is empty, detection cannot succeed.
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 636.
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 notification area icon and the panel's status indicator ring are blue when the machine is connected to the trusted network and green when a tunnel is open. If the box is unchecked, the notification area icon and panel's status indicator ring remain green in both cases. No distinction is made between the trusted network and an open tunnel.

22.2.3 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.

22.3 Scripts

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

22.4 Hiding the panel automatically

Two seconds after the workstation is detected as connected to the trusted network (either physically or through the VPN tunnel), the **TrustedConnect Panel** is automatically hidden: by default it is closed, but you can have it minimized to the taskbar instead. Whether minimized or closed, the panel remains available from its icon in the notification area (system tray).

You can also change the time delay (two seconds by default) before the panel is hidden.



The time delay and the hide action (minimize or close) apply only when the **TrustedConnect Panel** is hidden automatically upon detection of the trusted network. They do not apply when you minimize or close the panel manually.

These settings can only be defined using the MSI properties of the VPN Client installer.



Refer to the “Deployment Guide” for instructions on setting these MSI properties.

22.5 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.

22.6 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.

22.7 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.



22.8 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.

22.9 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.

23 GINA mode

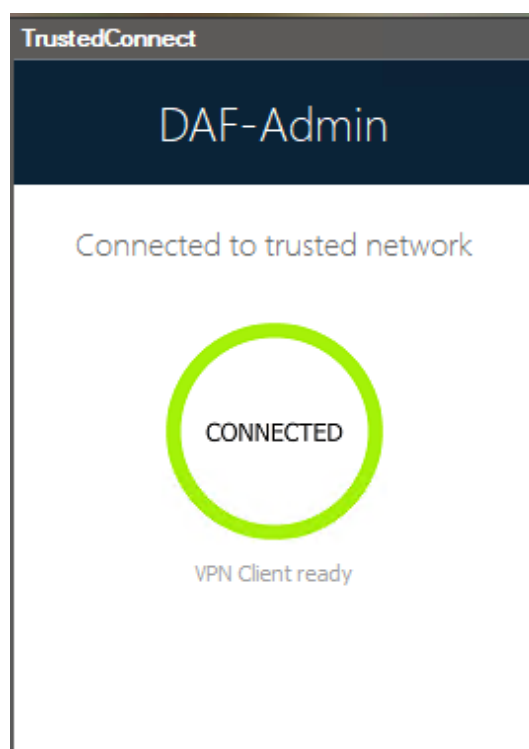
23.1 Overview

The GINA mode allows you to open VPN connections before the Windows logon.

This function can, for example, create a secure connection to an access rights management server so that the user workstation access rights can be obtained before opening a user session.

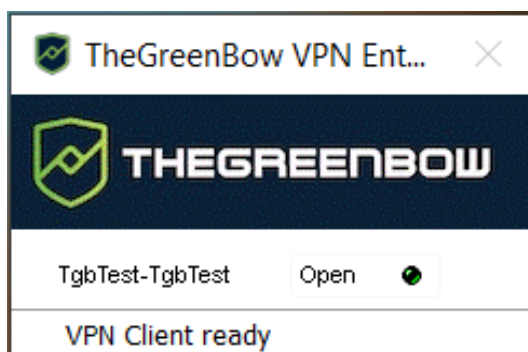
When a tunnel is configured “in GINA mode”, the following two situations are possible:

1. If the VPN Client is configured to start up in **TrustedConnect** mode (refer to section 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.



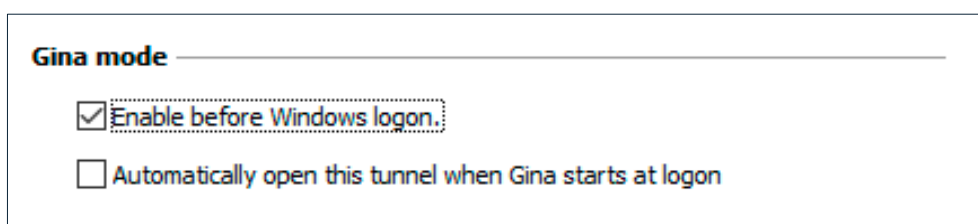
Special use case

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.

23.2 Configuring the GINA mode

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



Refer to chapter 15 Automation.

23.3 Using the GINA mode

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

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

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 Current 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 Local Machine Certificate Store.



24 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.

25 Options

25.1 View

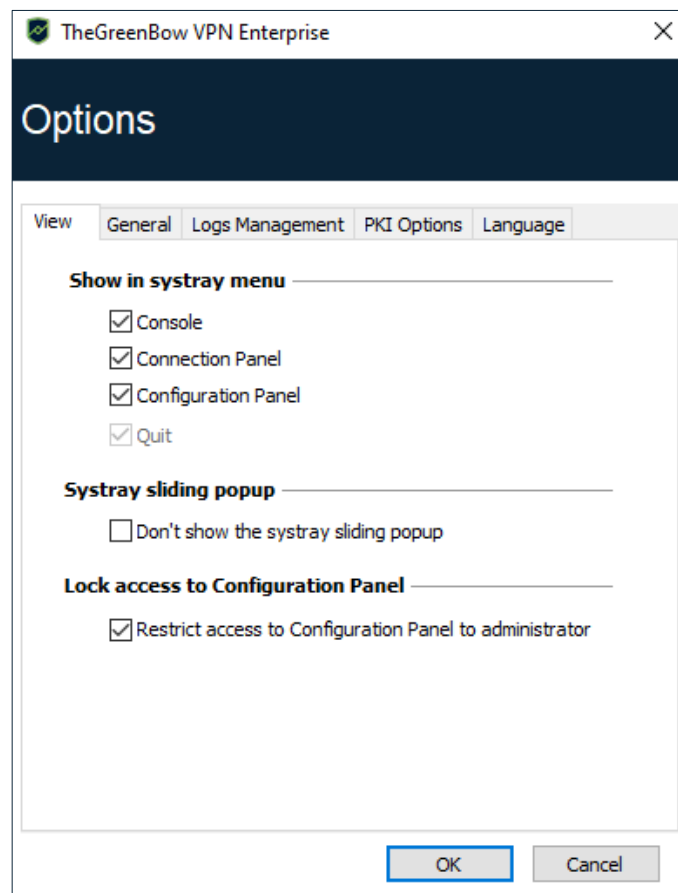
Using the options listed on the **View** tab in the **Options** window, you can hide nearly all of the software's interfaces:

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

25.1.1 Showing options in notification area menu

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

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



25.1.2 Showing the notification area 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 notification area (system tray) 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



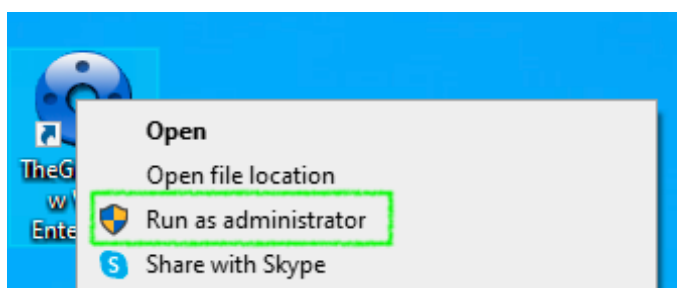
Failed to open the tunnel: the window will briefly explain what happened and provide a hyperlink for more information about the incident.



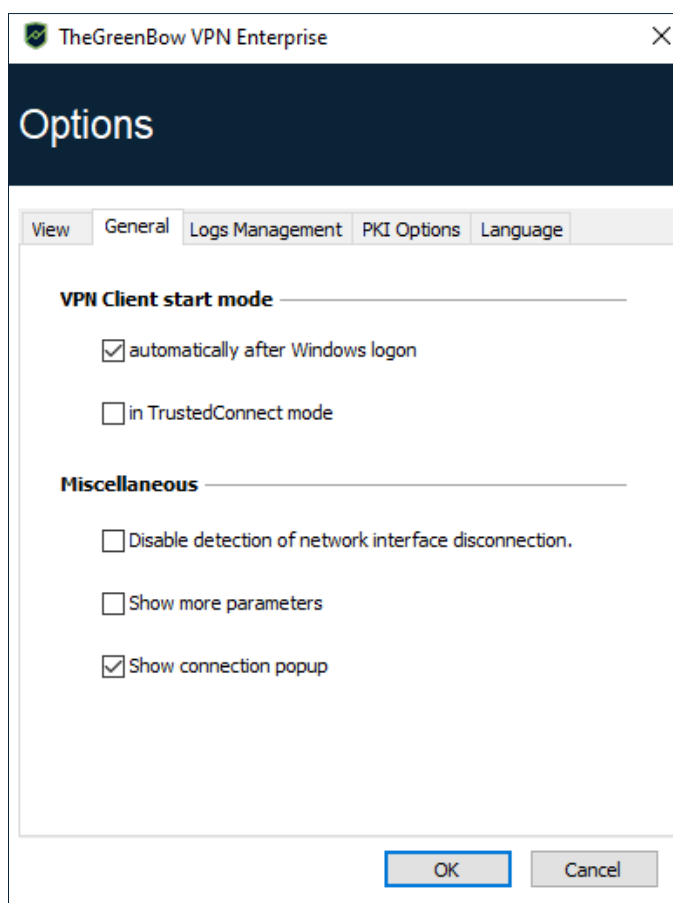
25.1.3 Restricting access to the Configuration Panel

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.

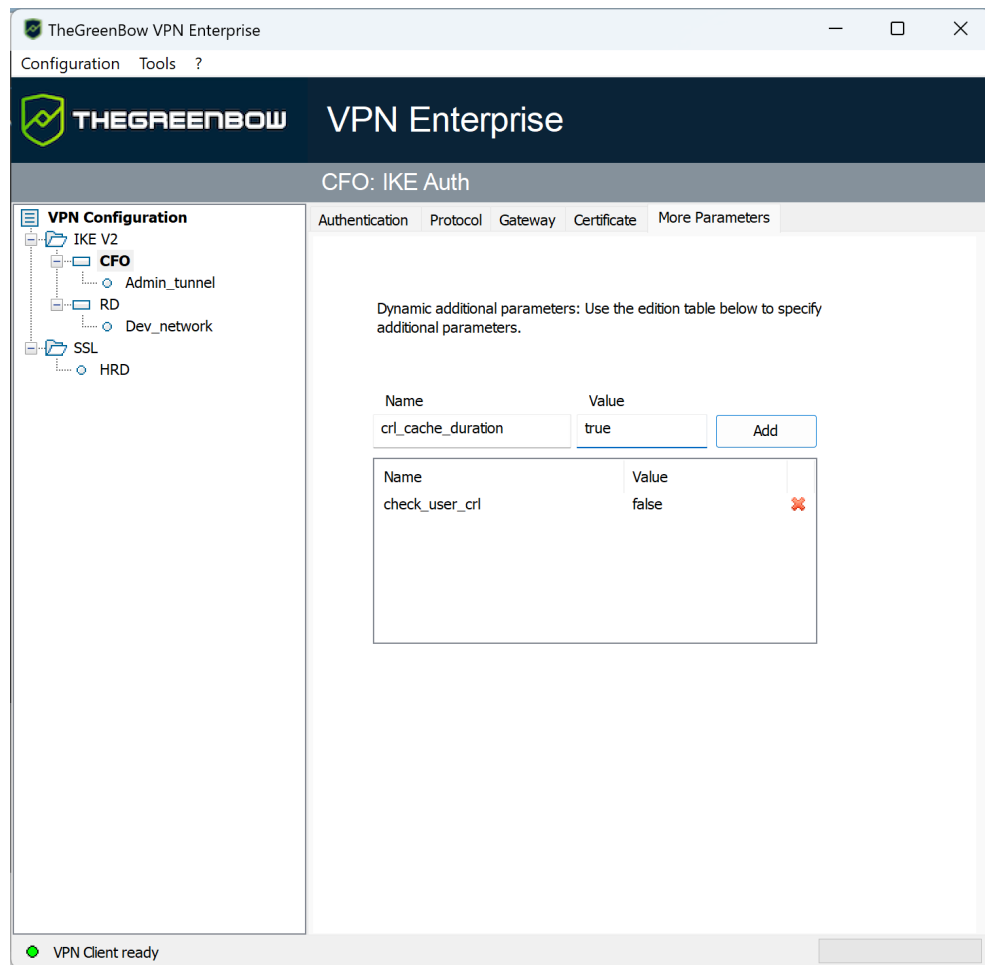
25.2.3 Show connection popup

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

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.



To find out how to add dynamic parameters, see chapter 18 Managing dynamic parameters.

25.3 Managing logs



Refer to section 26.2 Audit logs.

25.4 PKI Options

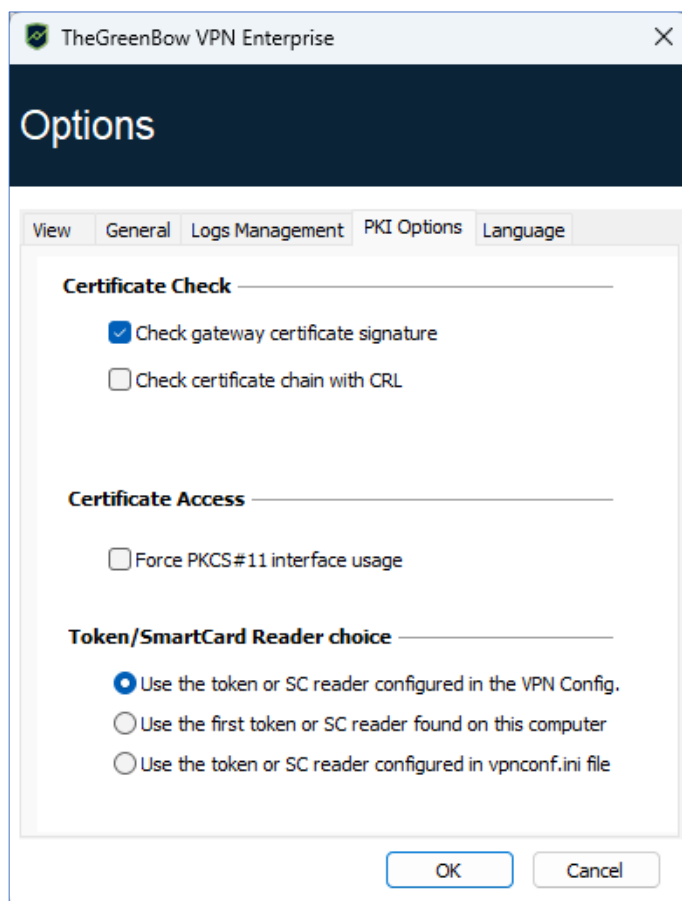
The **PKI Options** tab is used to fine-tune smart card and token management and to further specify certificate access.

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. CRLs must also be accessible, either in the Local Machine Certificate Store or available for download.

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.



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

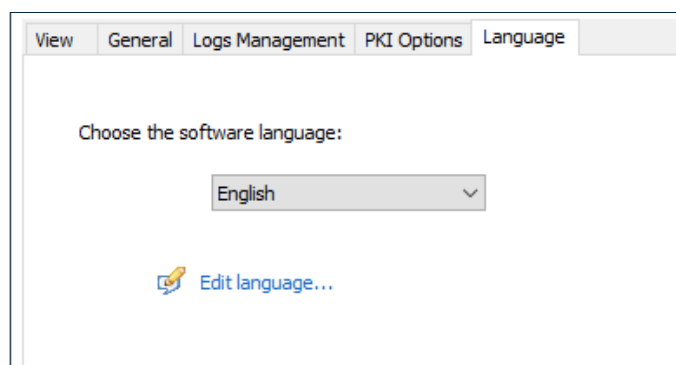
25.5.1 Choosing a language

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:

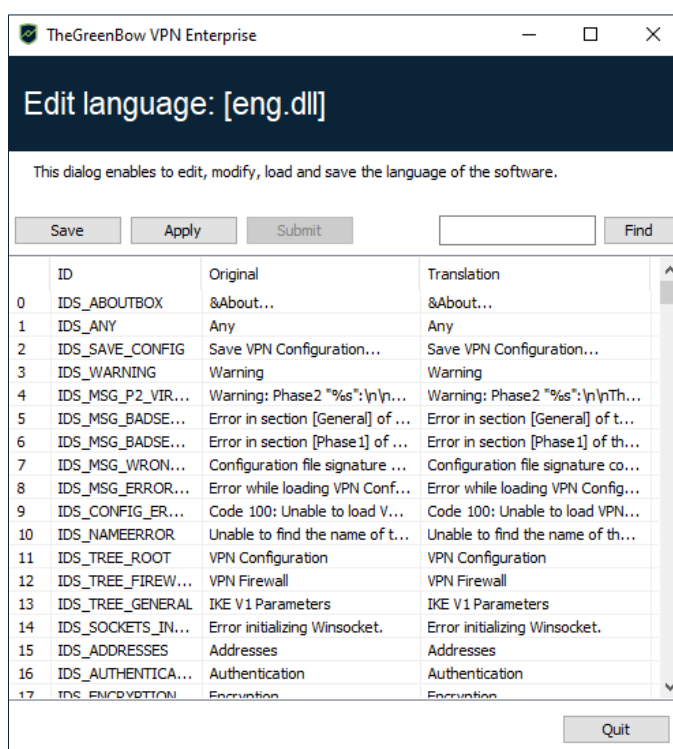


The list of languages available in the standard version of the software is provided in an appendix in section 29.6 Windows Enterprise VPN Client technical data.

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](https://thegreenbow.com)'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 Audit logs, Console, and trace logs

The Windows Enterprise VPN Client features three types of logs:

1. Audit logs¹ 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. 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 Log format

As of version 7.6 of the Windows Enterprise VPN Client, the various logs and audit logs it generates meet the specifications of [RFC 5424](#) on the Syslog format. Moreover, fields of structured data type (SD/STRUCTURED-DATA) have been added to send information regarding endpoint compliance, software activation, and tunnel names.

The new log format is as follows:

```
<facility+severity>VERSION TIMESTAMP MACHINENAME APPNAME  
THREADID MSGID \[TGB@PENID name="valeur" ...\) Trace
```

Where:

- `facility` is the driver name:
 - `local0` (Starter)
 - `local1` (GUI)
 - `local2` (IKE)
- `severity` is the severity level:
 - Informational
 - Notice
 - Error
 - Warning
 - Critical
- `VERSION` = 1
- `TIMESTAMP` complies with the format specified in [RFC 5424](#)

¹ Also known as “administrator logs” in previous versions of this guide and referred to as “syslog information” in the VPN Client’s interface.

- MACHINENAME is the machine name
- APPNAME is the module name

Example:

```
<133>1 2024-06-06T13:13:42.319Z WIN-LHH6PVM13CQ TgbStarter 3876  
1001 Starter service is started (logs 3).
```

26.2 Audit logs

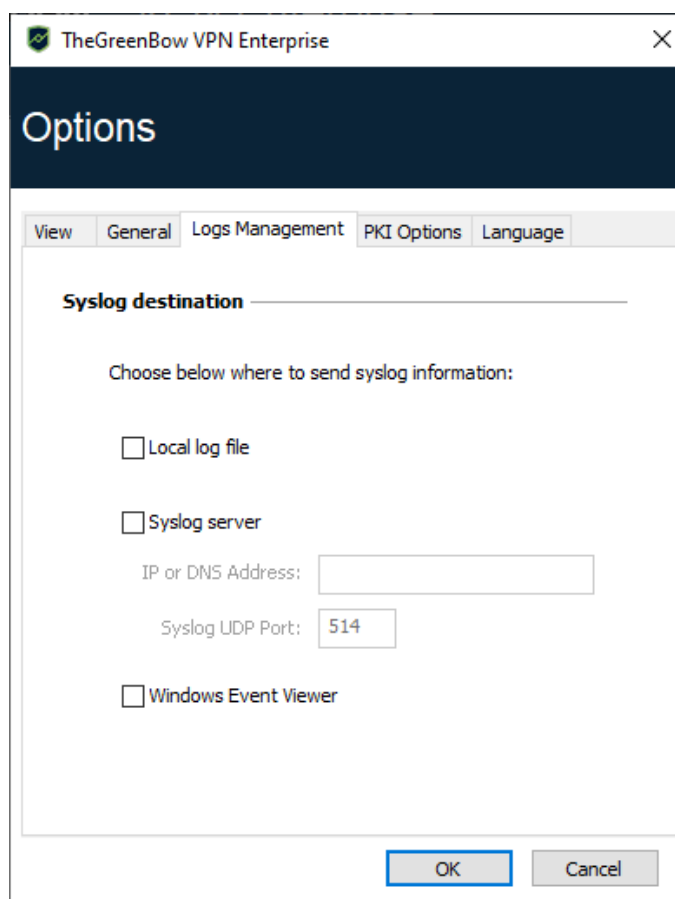
The Windows Enterprise VPN Client can collect audit logs¹: tunnel opening, expired certificate, connection duration, wrong login/password, changes to the VPN configuration, import or export of this configuration, etc. Audit logs provide a first level of analysis for any issues that may be encountered.

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 or a log sink

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

¹ Also known as “administrator logs” in previous versions of this guide and referred to as “syslog information” in the VPN Client’s interface.



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



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



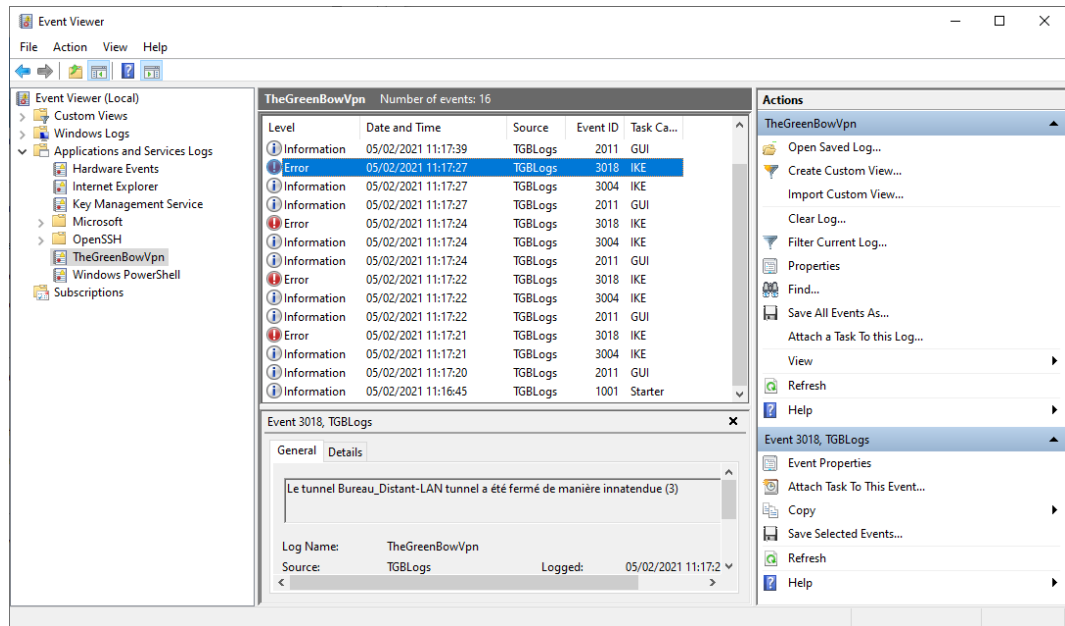
When audit logs are stored in a local file, the path to these logs is the **System** sub-directory in the logging directory:

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.



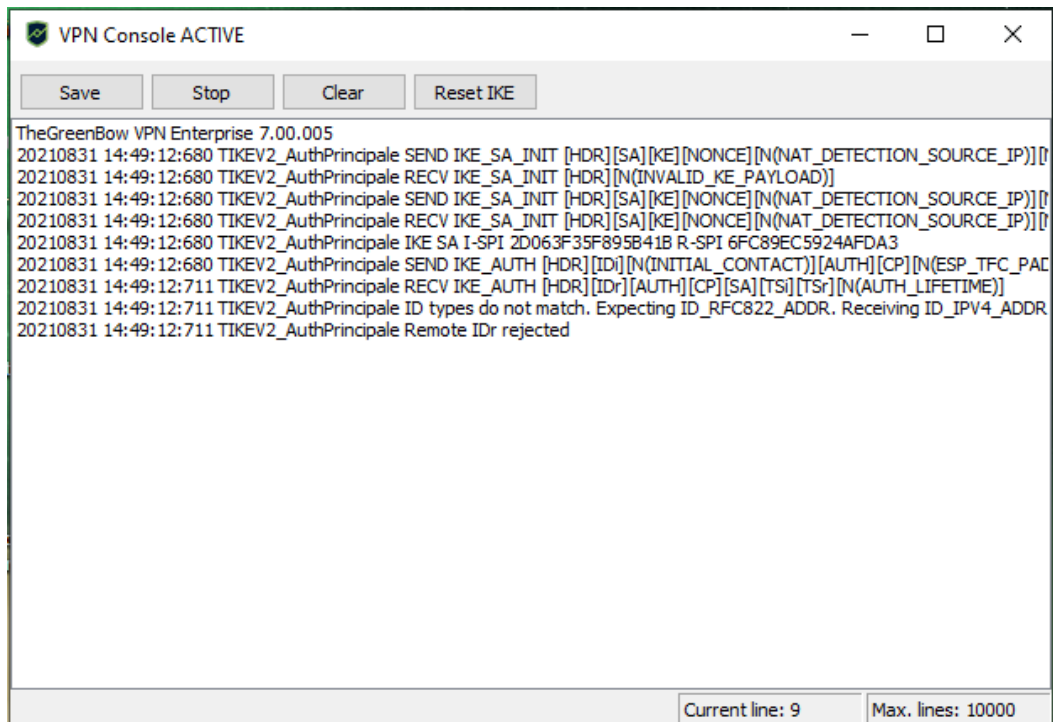
The path for Windows Enterprise VPN Client logs in the Windows Event Viewer is the following: **Applications and Service Logs > TheGreenBowVpn.**



26.3 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 notification area 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

26.4 Trace mode

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

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

When 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").



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



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 19.4 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.



In “All traffic through the tunnel” mode, the interface metric is set to 1 by default, allowing for packets to be routed through the tunnel.

However, administrators can define an interface metric value for their specific needs using the dynamic parameter `interface_metric`.

Maximum value: 50

Additionally, the dynamic parameter `VirtualInterfaceProfile` can be used to change the network profile type of the connection associated with the virtual card. This is only applicable in “All traffic through the tunnel” mode.



Possible values:

0 or undefined	Public
1	Private



Refer to sections 13.3.6.5 Configuring the address type, 13.3.7.3 Miscellaneous and 18 Managing dynamic parameters.

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 Audit 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.



ID Log define	ID Log value	Severity	Log string
LOGID_TOKENEXTRACT	2018	Info	Token %s has been extracted.
LOGID_USBININSERT	2019	Info	USB Key has been inserted
LOGID_USBEXTRACT	2020	Info	USB Key has been extracted
LOGID_INSTALLATION	2021	Info	VPN running for the 1st time.
LOGID_UPDATE	2022	Info	VPN software has been updated.
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 done.
LOGID_TUNNELTRAFFIC_OK	3006	Info	Tunnel is opened.
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.
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).
LOGID_VIRTIFOK	3015	Info	Virtual interface created successfully (instance %d).
LOGID_VIRTIFNOK	3016	Error	Virtual interface could not be created (error %d).
LOGID_TUNNELCLOSED	3017	Notice	Tunnel successfully closed.
LOGID_TUNNELCLOSED_ERR	3018	Error	Tunnel closed unexpectedly (%d)
LOGID_CERTERROR	3019	Error	Error %d when handling certificate %s.
LOGID_TUNNELDATA_UL	3020	Info	%d bytes sent inside the tunnel.
LOGID_TUNNELDATA_DL	3021	Info	%d bytes received inside the tunnel.
LOGID_VPNCONFLOAD_CONF	2024	Info	GUI loading configuration.

ID Log define	ID Log value	Severity	Log string
LOGID_VPNCONFCERTIMPORTERR	2025	Error	Certificate import failed
LOGID_TC_POSTURE_TRUSTED	2026	Info	Workstation is on trusted network
LOGID_TC_POSTURE_NOTTRUSTED	2027	Info	Workstation is not on trusted network (%s)
LOGID_TC_POSTURE_CPD	2028	Info	Captive portal has been detected
LOGID_TC_CONFORMITY	2029	Info	Conformity is set to level %d
LOGID_ACTIVATION_OK	2030	Info	Product is activated.
LOGID_ACTIVATION_NOK	2031	Notice	Product is not activated.
LOGID_ACTIVATION_EVAL	2032	Notice	Product is under evaluation.
LOG_ACTIVATION_EXPIRED	2033	Warning	Product subscription has expired
LOGID_ACTIVATION_ERROR	2034	Error	Product could not activate error %d
LOGID_TUNNEL_ALIVE	2035	Info	Tunnel is alive

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	Make sure that the <code>tgbvpn.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.	- 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	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).



Code	Diagnostics	Solution
	sequence does not match the one configured on the gateway.	
4	Configuration issue The message “No proposal chosen” has been received during an IKE exchange: the cryptographic algorithm suite of the ESP protocol does not match the one configured on the gateway.	• Verify that the cryptographic algorithm suite of the ESP protocol (refer to Child SA in the Configuration Panel) matches that of the gateway.
5	Cannot access gateway The gateway address (“Remote Router Address”) specified in the VPN configuration is not reachable. If it is an IP address, it cannot be found or cannot be reached. If it is a DNS address it may be inaccessible, indefinite, or cannot be resolved.	• Check the address of the gateway/remote workstation. For example, try “pinging” this address.
6	Configuration issue The message Remote ID other than expected has been received. This means that the value of the Remote ID does not match the value expected by the remote VPN gateway.	• Make sure that the Local ID parameter on the VPN client's Protocol tab matches the Remote ID of the remote gateway (or workstation). Caution: The Remote ID on the router is the Local ID on the VPN Client and vice versa.
7	Gateway certificate Checking the certificate chain of the certificate received from the VPN gateway is enabled. The gateway certificate chain could not be validated.	• Check the gateway certificate expiration date. • Check the validity start date of the gateway certificate. • Check the signatures of all certificates in the certificate chain (including root certificate, intermediate certificates, and gateway certificate). • Check whether the CRLs of all certificate issuers in the certificate chain are up to date. • Make sure that none of the certificates concerned have been revoked in the corresponding CRL lists. • Make sure that the root certificate and all certificates in the certificate chain (root 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.	• Check whether the gateway is still accessible from the workstation.

Code	Diagnostics	Solution
10	Authentication issue The gateway has declined the user's authentication credentials.	- Check the user certificate. - Check that the Local ID on the Protocol tab of the Configuration Panel matches the value and type defined on the gateway. Caution: The Local ID on the VPN Client is the Remote ID on the router and vice versa. - Check the logs on the remote gateway to get more information about this issue.
13	Configuration issue An error occurred while establishing the VPN connection. Establishing the VPN connection has been abandoned.	- Retrieve the user log files. They must be analyzed. - Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
14	Network configuration An error occurred while creating the virtual interface used for the VPN connection.	- Retrieve the user log files. They must be analyzed. - Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
15	Network configuration The virtual IP address assigned during the VPN connection already exists on one of the workstation's interfaces.	- Change the virtual IP address (VPN Client address parameter) specified in the VPN Client's configuration. - Change the IP address provided by the gateway to the VPN Client.
16	Network configuration An error occurred while creating the virtual interface used for the VPN connection.	- Retrieve the user log files. They must be analyzed. - Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
24	Configuration issue The gateway did not accept the cryptographic algorithm suite provided by the VPN Client.	- Make sure that the VPN Client's cryptographic algorithm suites match those of the gateway. - Check the Local ID and Remote ID. Caution: The Local ID on the router is the Remote ID on the VPN Client and vice versa.
25	Configuration issue The gateway did not accept the remote network configured in the VPN Client or the virtual IP address provided by the VPN Client.	- Make sure that the virtual IP address (VPN Client address parameter) specified in the VPN Client's configuration is acceptable at the gateway end. - Make sure that the remote network (Remote network address parameter) specified in the VPN Client's configuration is acceptable on the gateway end.
26	Configuration issue The VPN client provides its own traffic selectors, while the gateway is configured to provide them.	Check the Request configuration from the gateway parameter on the Child SA tab.
27	Gateway error The gateway reported an error not supported by the VPN Client.	- Analyze the logs on the gateway end. - Retrieve the user log files. They must be analyzed.



Code	Diagnostics	Solution
		Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.
28	Login/password error The gateway has rejected the EAP authentication while establishing the VPN connection.	- Check the EAP authentication parameters in the VPN Client's configuration. - Make sure that the user knows his or her credentials, should he or she need them while establishing the connection.
30	Smart card or token error Cannot access the certificate stored on the smart card or token.	Check that the smart card reader or token is correctly configured on the workstation, and that the VPN Client can access it.
31	PIN code cancelled by user The tunnel aborted because the user clicked on Cancel when the PIN code was requested.	Click Connect to authenticate on the captive portal.
32	Gateway not authenticated The tunnel aborted because the gateway certificate could not be validated.	- CAs are missing, or are expired in the configuration, or CRL can't be retrieved, or gateway certificate was revoked. - A retry can be performed in some cases, i.e. when the CRL can't be retrieved.
33	Crypto failure Failed to initialize OpenSSL cryptographic library.	If the problem persists, restart the computer. If the issue continues, contact the administrator. The machine may be compromised by malware.
35	No valid certificate found Automatic certificate selection failed: no valid certificate found.	- If a token or smart card is used, ensure that it is connected or inserted correctly. Try disconnecting and reconnecting it. - If the certificate is being read from the Windows certificate store, contact your administrator.
36	Network interface initialization issue Driver is no longer installed.	Some major Windows updates uninstall the TheGreenBow driver. You must reinstall the VPN Client when this happens.
100	Cannot load the VPN configuration No VPN connection has been found in the configuration file.	Make sure that at least one tunnel is configured in the Connection Panel. Go to Tools > Connections Configuration, then add a tunnel and save the configuration.
101	GINA configuration error A tunnel is active before logon, but has not been configured to be used by the TrustedConnect Panel .	Make sure that the tunnel which is active before logon is also configured in the Connection Panel. Go to Tools > Connections Configuration, then add a tunnel and save the configuration.
102	IKE initialization error An error occurred while initializing the IKE daemon.	- Retrieve the user log files. - Create a ticket and send it to support@thegreenbow.com making sure to attach all log files.

Code	Diagnostics	Solution
103	DNS error A DNS name could not be resolved in the set of rules for the Filtering Mode.	- Make sure that the workstation can access the internet. - Make sure that the Filtering Mode does not itself block access to DNS queries. - Replace DNS names with IP addresses.
104	Compliance error Secure Connection Agent reported a compliance issue.	Ensure your firewall and antivirus are enabled and up to date.
105	Driver initialization error An error occurred while initializing the driver.	Drivers have been uninstalled. The VPN Client must be reinstalled.
106	Captive portal authentication timeout No session has been established on the captive portal. Therefore the endpoint has no internet connectivity.	Click Connect to authenticate on the captive portal.
200	Software activation The software is not activated, and its trial period has expired.	- Retrieve user log files. - Verify software activation.

29.4 Activation error list

The following table lists error codes reported by the activation server and displayed in the VPN Client in the event of failed activation:

Code	Diagnostics	Solution
0x30	Activation process failed Activation server encountered an internal error.	Check logs on the activation server.
0x31	License number not found The activation server didn't find the license requested by the VPN Client.	Check that the license number is correct both on the VPN Client and on the activation server.
0x33	Quota exceeded No available license on the activation server.	- Reset unused licenses on the activation server. - or - Buy new licenses.
0x34	License doesn't match product An Enterprise license is used on the standard edition, or vice versa.	- Install the edition of the MSI matching the license. - or - Use the license matching the installed product.



Code	Diagnostics	Solution
0x35	License doesn't match customization A partner license is used on a TGB product or on another partner product.	• Install the MSI of the partner matching the license. or • Use the correct partner or TGB license for the installed product.
0x36	Maintenance expired The maintenance period has expired.	• Use a new license. or • Buy an extension for the current license.
0x37	Unknown release The server does not recognize the version reported by the VPN Client.	• On the server, import XML with the right Product Release Information.
0x39	Activation not allowed The license is blocked on the activation server.	• Check the status of the license number on the activation server.
0x50	Invalid server response The server responded with an incorrect message.	• Check that the activation server address is correct on the VPN Client.
0x51	The response doesn't match the license number Internal error.	• Contact TGB Support.
0x52	The response doesn't contain an activation code No activation code was found in the response.	• Check the activation server address is correct. • Check the activation server version matches the VPN Client version.
0x53	Response "401" HTTP communication reported 401.	• Retry the activation procedure. • Contact TGB Support.
0x54	Unable to connect to the activation server The HTTPS connection could not be established.	• Check that OSACert is properly configured on the VPN Client. • Check that the CA and CRL are up to date on the VPN Client. • Send VPN Client logs to TGB Support.
0x55	Unable to decode activation code The server provided an activation code the VPN Client is unable to decode.	• Check that OSACert is correct on the VPN Client.
0x56	Activation code is incorrect An activation code was found but is incorrect.	• Perform the activation procedure again. • Contact TGB Support.
0x57	Temporary license expired The temporary license is no longer valid.	• Buy a new license. • Ask for a new temporary license.

Code	Diagnostics	Solution
0x58	License has expired The current subscription has expired.	Buy a license extension.
0x70	No activation code found Activation code was not found.	- Retry the activation procedure. - Contact TGB Support.

29.5 Basic cryptography concepts

29.5.1 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”.

29.5.2 Accessing certificates

29.5.2.1 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 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.

29.5.2.2 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.

29.5.2.3 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 29.5.3 Determining a certificate's container type below).

29.5.2.4 Machine store and user store

It should also be noted that there are two certificate stores in Windows:

- The Local Machine Certificate Store or machine store that is available to all users of a machine
- The Current User Certificate Store or 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.

29.5.2.5 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.

29.5.2.6 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 **C**ryptographic **S**ervice **P**rovider (deprecated and replaced with CNG): supported up to versions 6.8x
- **CNG** stands for **C**ryptography **A**PI: **N**ext **G**eneration: 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 **P**ublic-**K**ey **C**ryptography **S**tandards: supported by both versions 6.8x and 7.x

29.5.3 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.

29.5.4 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

29.5.4.1 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 19.8.2 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_server_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`

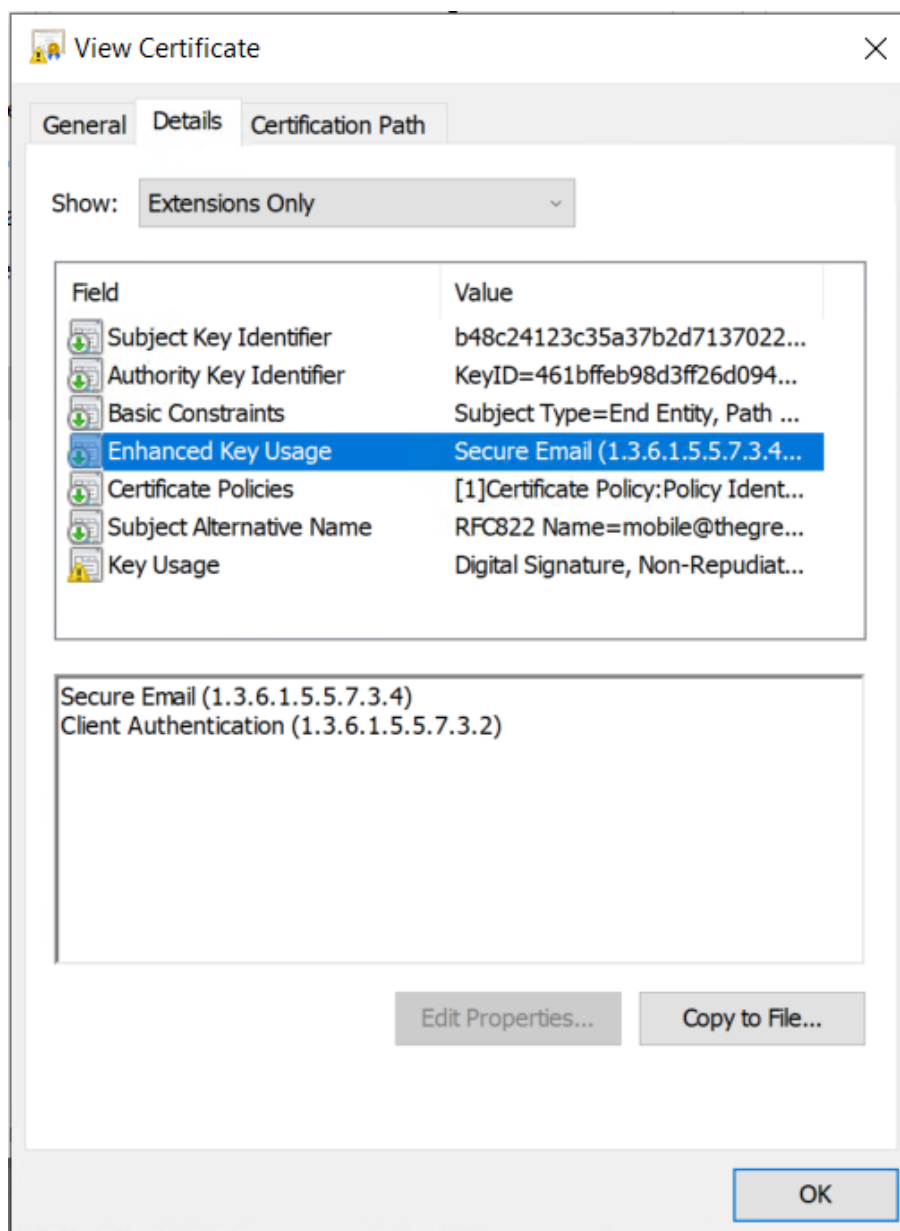


If this is not the case, refer to the dynamic parameter `allow_server_and_client_auth` described in section 19.8.3 Constraints on the Extended Key Usage extension.

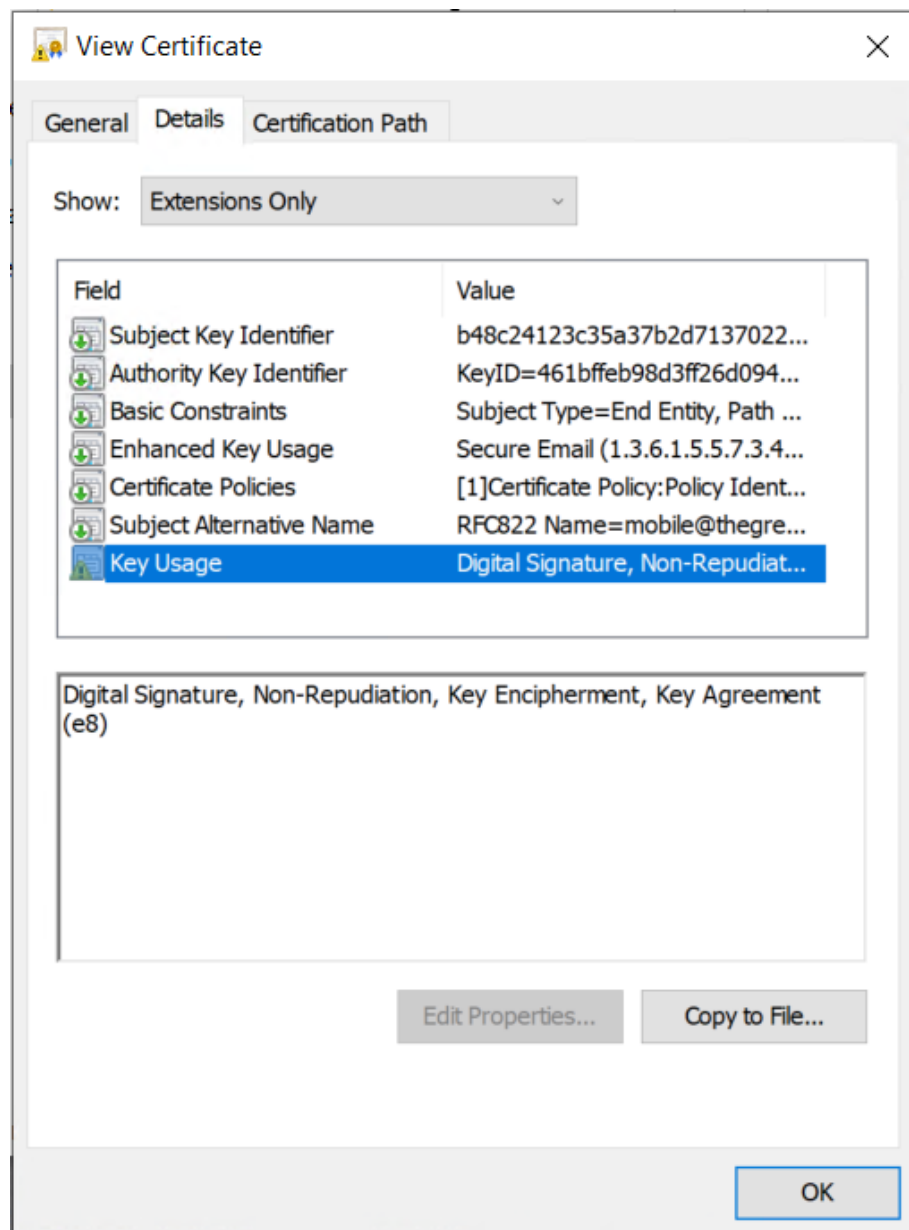
29.5.4.2 Example of a certificate in Windows

In a Windows PKI, the following is the relationship between a certificate and its extensions:

- Extended Key Usage:



- Key Usage:





29.5.4.3 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
```

29.5.4.4 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.

29.5.5 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 chapter 18 Managing dynamic 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 chapter 18 Managing dynamic 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 chapter 18 Managing dynamic 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.

29.6 Windows Enterprise VPN Client technical data

29.6.1 General

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

29.6.2 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 and 11
Scripts	Run configurable scripts when opening or closing a VPN tunnel
Remote Desktop Sharing	Open a remote computer with a single click via RDP and VPN tunnel
TrustedConnect Panel	Automatically open tunnel with Always-On and trusted network detection (TND)

29.6.3 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

29.6.4 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: • 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	• Preshared key • EAP-MSCHAPv2 • EAP-GTC • X.509 certificates • Multiple Auth



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]; ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) on the BrainpoolP256r1 curve • Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) on the BrainpoolP256r1 curve
PKI	• 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 Lists (CRLs) • 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

29.6.5 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)

29.6.6 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 Audit 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



29.7 Third-party licenses

29.7.1 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

29.7.2 LZ4

LZ4 is licensed under the BSD 2-Clause License, reproduced below.

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.

Secure your connections
in all circumstances