

macOS VPN Client 2.5

Administrator's Guide

TheGreenBow is a registered trademark.

Apple, the Apple logo, iPhone, iOS, Mac, and macOS are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

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	Introduction	1
1.1	TheGreenBow VPN Clients	1
1.2	Key features of the macOS VPN Client 2.5	2
1.3	Features introduced with v2	2
1.3.1	Support for IPsec DR mode according to latest changes to framework	2
1.3.2	IKEv1 and vulnerable algorithms have been deprecated	2
1.3.3	Enhanced security	3
1.3.4	Cryptography	3
1.3.5	Adopts OpenSSL 3.0	3
1.3.6	TLS/OpenVPN	3
1.3.7	Certificate authentication and revocation	3
1.3.8	Graphical interface and features	4
1.4	Current limitations	4
2	Installing the software	5
2.1	Installation and update procedure	5
2.1.1	Introduction	5
2.1.2	System requirements	5
2.1.3	Installation procedure	7
2.1.4	Initial launch	9
2.1.5	Previous installations of a VPN Client from the App Store	17
2.2	Trial period	18
2.3	Test configuration	19
2.4	Uninstalling the software	21
3	Activating the software	25
3.1	Step 1	25
3.2	Step 2	26
3.3	Activation errors	26
3.4	License and activated software	27
3.5	Displaying the activation window	28
4	User interface	29

4.1	Overview	29
4.2	Menus.....	30
4.3	Keyboard shortcuts	31
4.4	VPN configuration tree.....	31
4.4.1	Introduction	31
4.4.2	Contextual menus.....	33
4.4.3	Shortcuts.....	35
4.4.4	Buttons in the VPN configuration tree	35
5	About window	38
6	Importing and exporting VPN configurations	39
6.1	Importing a VPN configuration	39
6.2	Exporting a VPN configuration	39
7	Configuring a VPN tunnel.....	40
7.1	Editing and saving a VPN configuration.....	40
7.2	Configuring an IPsec IKEv2 tunnel.....	40
7.2.1	IKE Auth: Authentication	41
7.2.2	IKE Auth: Protocol.....	44
7.2.3	IKE Auth: Gateway.....	47
7.2.4	IKE Auth: Certificate.....	49
7.2.5	IKE Auth: More parameters.....	50
7.2.6	Child SA: Child SA.....	50
7.2.7	Child SA: Advanced.....	55
7.2.8	Child SA: More parameters	56
7.2.9	Child SA: Automation.....	57
7.3	Configuring an SSL/OpenVPN tunnel	57
7.3.1	SSL: Authentication	57
7.3.2	SSL: Security	59
7.3.3	SSL: Gateway.....	62
7.3.4	SSL: Establishment.....	64
7.3.5	SSL: Certificate.....	66
7.3.6	SSL: Automation.....	66
8	Redundant gateway	67
9	Automation	68
10	Managing dynamic parameters	70

11	Managing certificates	72
11.1	Introduction	72
11.2	User certificate	72
11.2.1	Overview.....	72
11.2.2	Dynamic parameters for automatic certificate selection.....	73
11.3	Selecting a certificate (Certificate tab)	73
11.4	Importing a certificate.....	75
11.4.1	Importing a PEM/PFX certificate.....	75
11.4.2	Importing a PKCS#12 certificate.....	76
11.5	VPN gateway certificate.....	77
11.5.1	Specify gateway certificate verification method.....	78
11.5.2	Constraints on the Key Usage extension.....	78
11.5.3	Constraints on the Extended Key Usage extension	79
11.6	Managing certificate authorities	79
11.6.1	Overview.....	79
11.6.2	Importing a certificate authority.....	80
11.6.3	IPsec DR mode.....	81
12	Logs.....	82
12.1	Console	82
12.2	Trace mode	83
12.3	System logs	83
13	Security recommendations.....	84
13.1	Assumptions.....	84
13.1.1	Profile and responsibilities of administrators	84
13.1.2	Profile and responsibilities of users	84
13.1.3	Compliance with management rules for cryptographic elements.....	84
13.2	User workstation.....	85
13.3	VPN configuration	85
13.3.1	Sensitive information in the VPN configuration.....	85
13.3.2	User authentication	86
13.3.3	VPN gateway authentication	86
13.3.4	Protocol.....	86
13.3.5	ANSI recommendations	86
14	Contact	87



- 14.1 Information..... 87
- 14.2 Sales..... 87
- 14.3 Support 87
- 15 Appendixes..... 88**
 - 15.1 Basic cryptography concepts 88
 - 15.1.1 SHA, RSA, and ECDSA algorithms..... 88
 - 15.1.2 Certificate format 89
 - 15.1.3 Certificate authentication methods..... 91
 - 15.2 macOS VPN Client technical data 92
 - 15.2.1 Main functions 92
 - 15.2.2 Languages..... 92
 - 15.2.3 Compatible OSes..... 92
 - 15.2.4 Cryptography and authentication..... 93

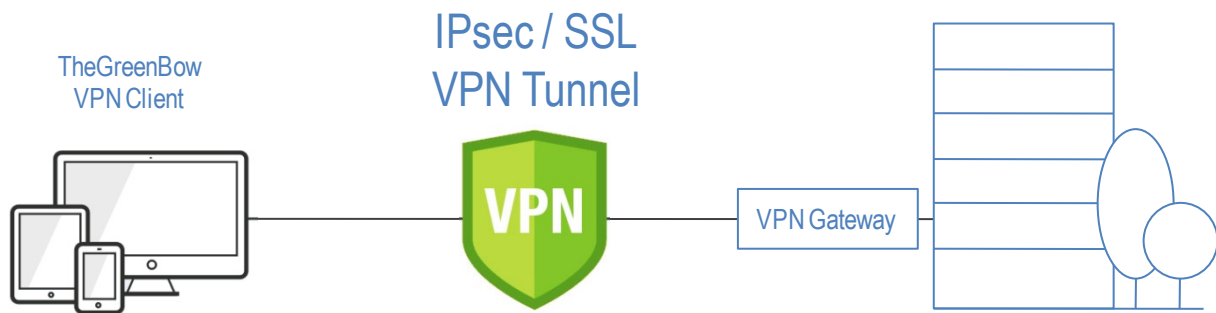
Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2025-09-11	All	Initial release	FBO, FHE, FAT, BBR

1 Introduction

1.1 TheGreenBow VPN Clients

TheGreenBow VPN Client software is designed to establish secure connections to your information system in any situation. Regardless of the network used, the authentication system you may have adopted, the equipment to be secured, the VPN gateway you use, TheGreenBow VPN Clients are particularly easy to deploy, configure, and use.



Available on all platforms

TheGreenBow VPN Clients have been certified for Windows and Linux, and are also available for macOS, iOS, and Android.

You can download the software from our website at www.thegreenbow.com and use it free of charge for a 30-day trial period.

Compatible with any gateway

TheGreenBow VPN Clients are compatible with any VPN gateway. Their unparalleled ergonomics and their ability to be quickly integrated make them unique trusted solutions on the market. A list of VPN configuration guides for various firewalls, gateways, routers, and TheGreenBow VPN clients is available here: www.thegreenbow.com/vpn_gateway.html.

Work with any type of network

Regardless of the context in which they are used, whatever the network or equipment used, TheGreenBow VPN Clients ensure a reliable and robust VPN connection, over 4G, 5G, Wi-Fi, wired networks, satellites, etc.

1.2 Key features of the macOS VPN Client 2.5

The macOS VPN Client includes the following features:

- Compatible with most IPsec and SSL gateways, including those that support the IPsec DR (Restricted) repository
- Protocols: SSL, IPsec IKEv2
- Authentication: PSK, EAP, X.509 certificates
- Multiple authentication (certificate + EAP)
- X.509 certificate management: PKCS#12, PFX, PEM
- IP fragmentation
- Support for NAT-T
- CP mode (Configuration Payload)
- Encryption: 128 / 192 / 256-bit AES CBC, CTR and GCM
- Hashing: SHA-2 256 / 384 / 512 bits
- DH Groups: 14-21 & 28
- Dead Peer Detection (DPD): Detection of gateway traffic interruption
- Redundant gateway
- IKEv2 fragmentation
- Local ID, Remote ID
- DNS suffixes
- Alternate DNS servers
- Secure management of VPN configurations (encryption and integrity)
- Comprehensive and intuitive configuration interface
- Display logs in real time
- Support for Certificate Authorities (CAs) and gateway certificate check
- Support for 25 languages (see full list in section 15.2.2 Languages)

1.3 Features introduced with v2

1.3.1 Support for IPsec DR mode according to latest changes to framework

Complies with ANSSI recommendations to ensure compatibility with gateways operating in “IPsec DR” (Restricted) mode, including use of SHA-2 hashing algorithm in the certificate request payload.

1.3.2 IKEv1 and vulnerable algorithms have been deprecated

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

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

1.3.3 Enhanced security

The following have been added for enhanced security:

- Support for RFC 4304 Extended Sequence Numbers (ESNs) and RFC 6023 Childless IKE Initiation
- Systematic check of the gateway certificate each time a tunnel is opened

1.3.4 Cryptography

Support for the following using the BrainpoolP256r1 curve:

- Diffie-Hellman DH 28 (BrainpoolP256r1) [RFC 5639]
- ECDSA "BrainpoolP256r1" asymmetric signature mechanism with SHA-2

1.3.5 Adopts OpenSSL 3.0

All OpenSSL-based components in the VPN Client have been migrated to version 3.0

1.3.6 TLS/OpenVPN

The following changes have been introduced:

- End of support for vulnerable algorithms in TLS/OpenVPN: MD5, SHA-1, BF-CBC, TLS 1.1, "LOW" security suite for TLS V1.2
- Compression is no longer enabled by default

1.3.7 Certificate authentication and revocation

Due to increased security requirements, deprecation of certain algorithms, and stricter rules for using certificates, version 2 of the macOS VPN Client comes with certain restrictions on certificates.



Refer to chapter 11 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
- UDP encapsulation is forced for IKEv2 protocol
- Key Usage and Extended Key Usage of certificates is verified
- Verification of the user certificate CRL has become optional

1.3.8 Graphical interface and features

The following changes have been made to the GUI:

- Compliance with the new graphic charter
- Name of **More parameters** tab has been localized in French version

The following features have been added:

- New **Automation** tab and feature to execute scripts before and after opening the tunnel
- Added the **Popup when tunnel opens** option for SSL tunnels

1.4 Current limitations

The current version of the macOS VPN Client has the following limitations:

- The IPv6 protocol is not supported
- The activation screen is not displayed every time the software starts (see section 3.5 Displaying the activation window for a workaround)

2 Installing the software

2.1 Installation and update procedure

2.1.1 Introduction

The macOS VPN Client is now available as an Apple notarized disk image in DMG format.

Updates are performed in the same way as installations, except when updating an application installed from the Mac App Store (see section 2.1.5 Previous installations of a VPN Client from the App Store).

The VPN configuration is preserved during an update.



The macOS VPN Client can be installed on a Mac with Apple silicon (M1 or higher). In this case, if you have not already done so, you must install Rosetta 2 in order to run the software designed for an Intel processor. For more information about Rosetta 2, visit Apple's website:

<https://support.apple.com/en-us/HT211861>.

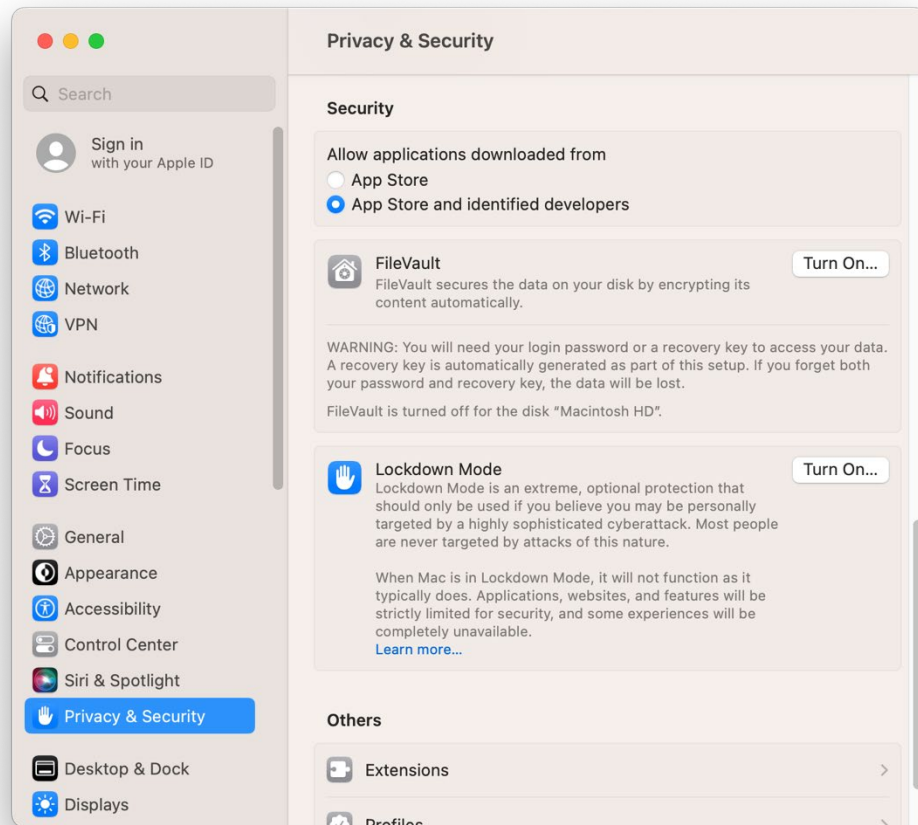
2.1.2 System requirements

The macOS VPN Client is designed for macOS 11 (Big Sur) and higher versions of Apple's operating system. However, it remains compatible with macOS 10.15 (Catalina).

Make sure that you are allowed to install third-party applications downloaded from the internet. To do this, proceed as follows:

In macOS 13 (Ventura) and later

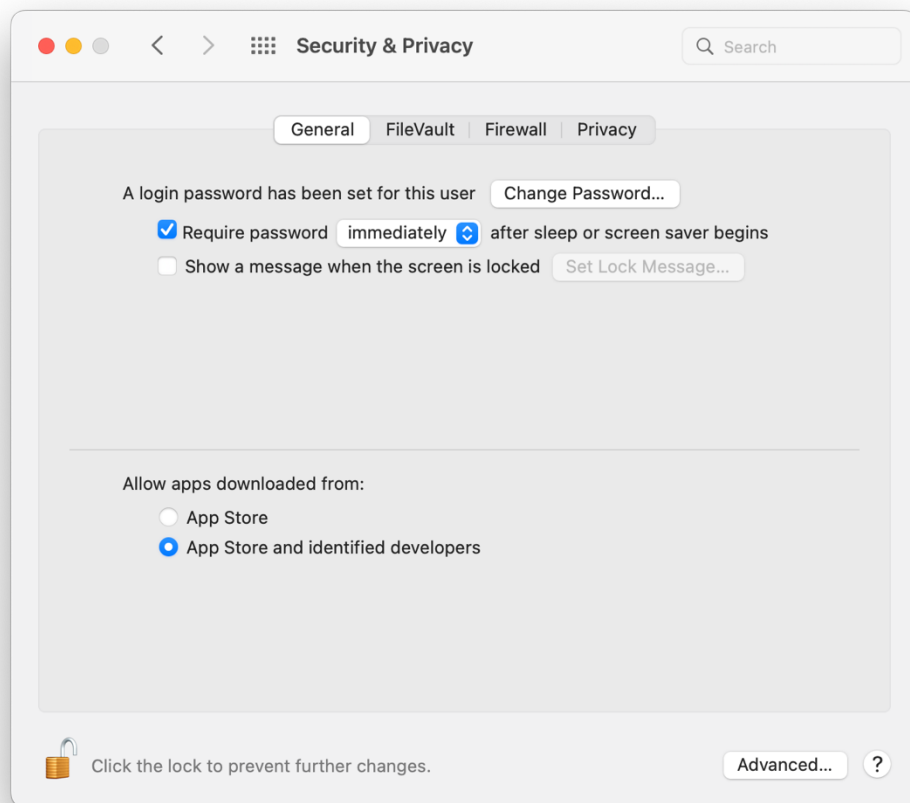
1. Open **System Settings...** > **Privacy & Security**, and then scroll down to the **Security** section.
2. Under **Allow applications downloaded from**, click **App Store and identified developers**.



Installing applications from identified developers is now allowed. You can now install the application.

In macOS 12 (Monterey) and earlier

1. Open **System Preferences... > Security & Privacy > General**.
2. Under **Allow apps downloaded from:**, click **App Store and identified developers**.

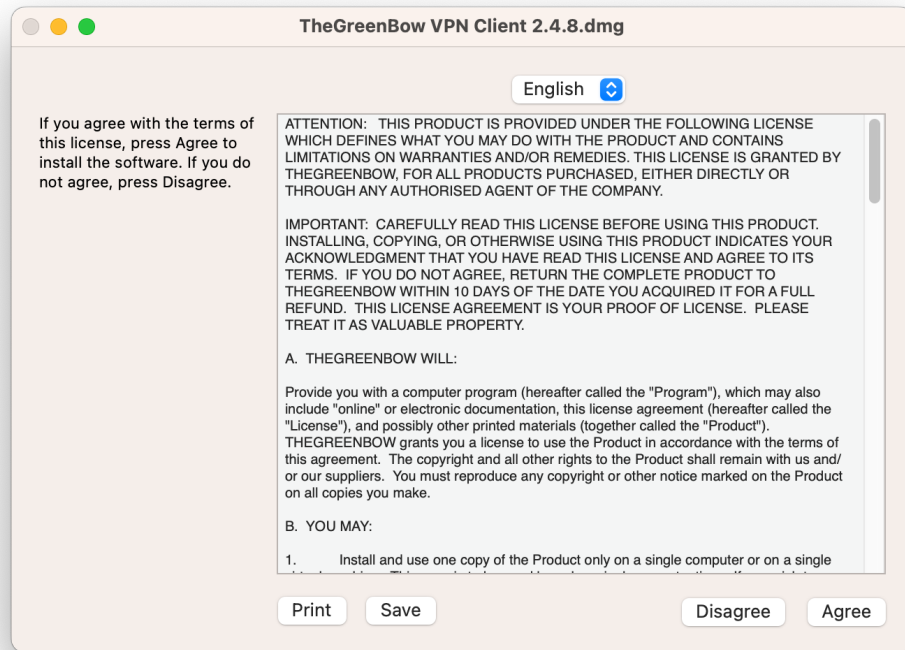


Installing applications from identified developers is now allowed. You can now install the application.

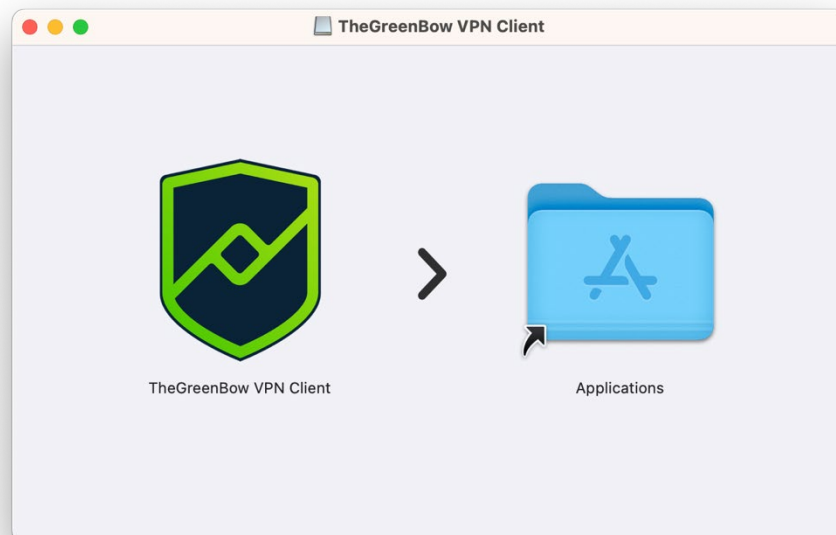
2.1.3 Installation procedure

To install the application, download the DMG file from our website at thegreenbow.com, or copy it to the Mac workstation on which it is to be installed, then double-click it.

The terms of the user license will be displayed, and you will need to accept them to use the software.



Once you click **Accept** to confirm your agreement, the disk image will be mounted, and the following screen will be displayed:

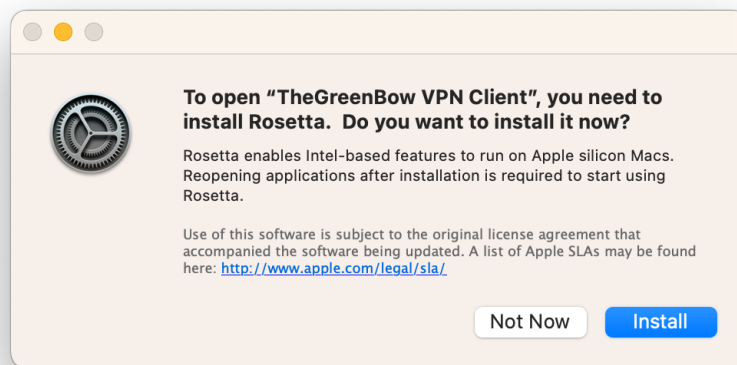


To install the app, drag the **TheGreenBow VPN Client** icon onto the **Applications** folder icon. This will copy the app to the **Applications** folder on your workstation.

You can now unmount the DMG file by dragging it to the **Trash**, as it is no longer required.

2.1.4 Initial launch

The first time you launch the app on a Mac with Apple silicon (M1 or higher) and if you have not yet installed Rosetta 2, a dialog box is displayed asking you whether you want to install it now:

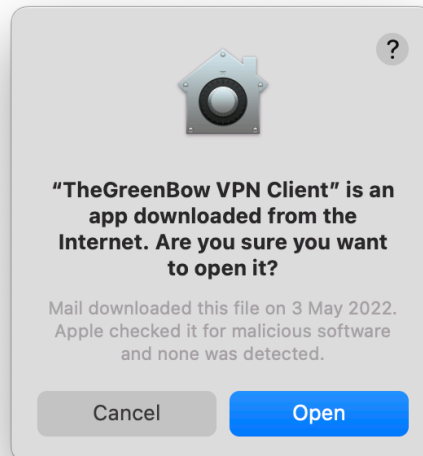


Click **Install**. The installation is performed automatically and generally does not last more than a few seconds.



For more information about Rosetta 2, visit Apple's website:
<https://support.apple.com/en-us/HT211861>.

The first time you start the app, a dialog box is displayed asking you to confirm that you want to open an app that has been downloaded from the internet.

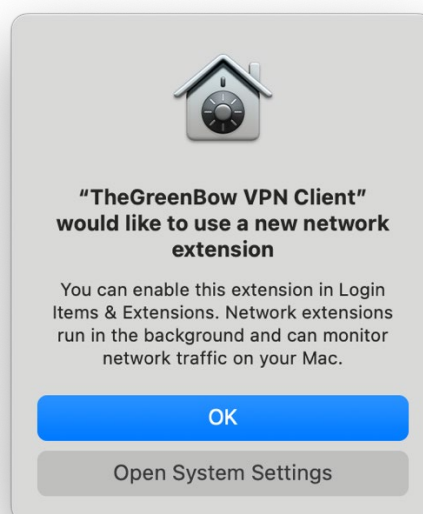


Click **Open** to confirm that you want to open the app.

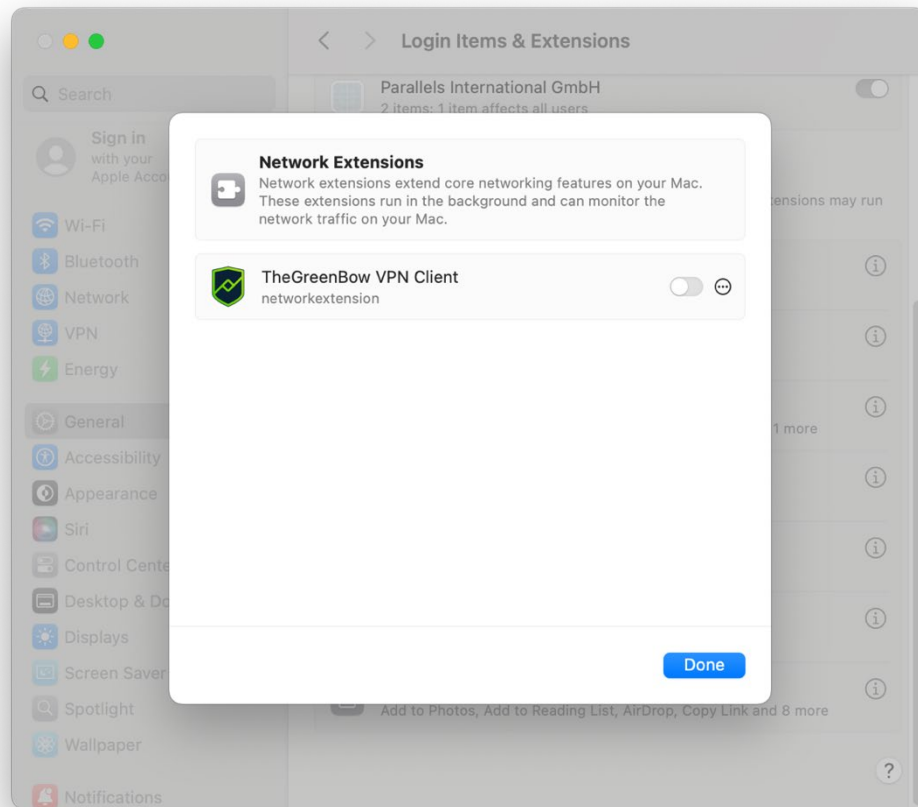
Another dialog box is then displayed requesting your permission to enable a system extension. This system extension has been developed by TheGreenBow and is required to manage VPN tunnels and implement VPN protocols. Therefore, if you do not enable the system extension, you will not be able to open any VPN tunnels.

You can enable the system extension as follows:

In macOS 15 (Sequoia) and later

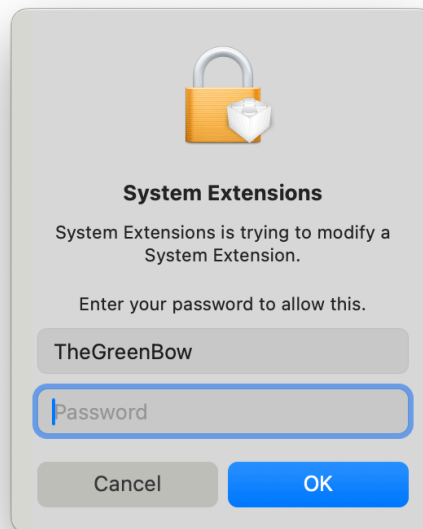


1. Click **Open System Settings**, or click **OK**, and then open **System Settings... > General > Login Items & Extension**. In the extensions list, click the info button ⓘ to the right of **Network Extensions**. The **Network Extensions** modal window opens over the system settings:



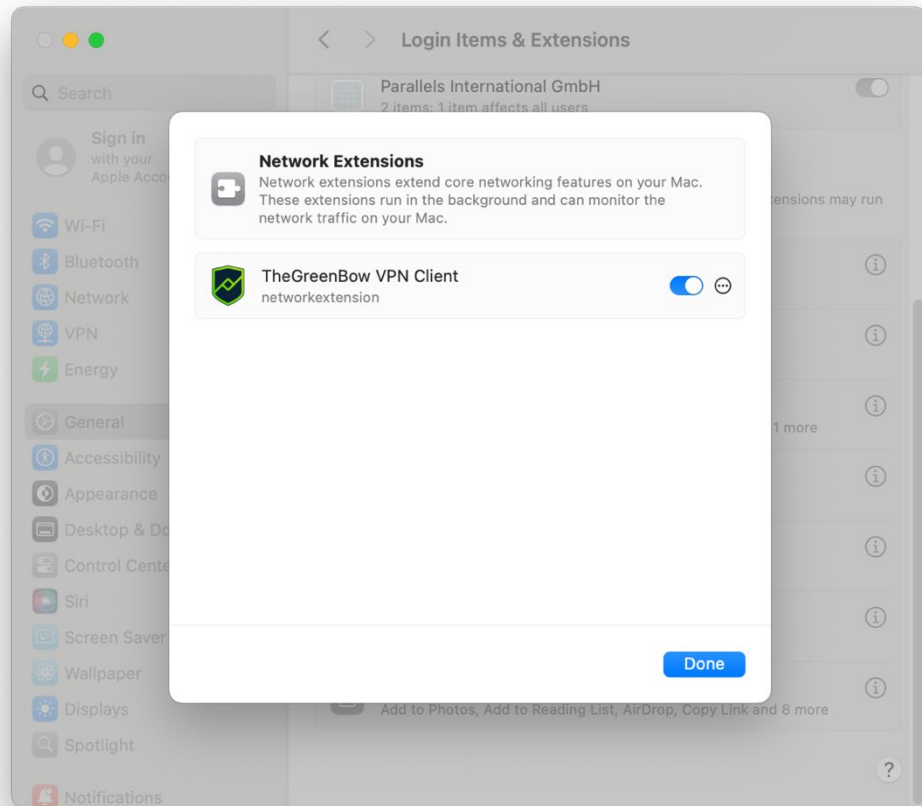
2. Toggle the switch to the right of the name TheGreenBow VPN Client.

The **System Extensions** dialog box appears, prompting you to enter an administrator password:



3. Enter the password, then click sur **OK**.

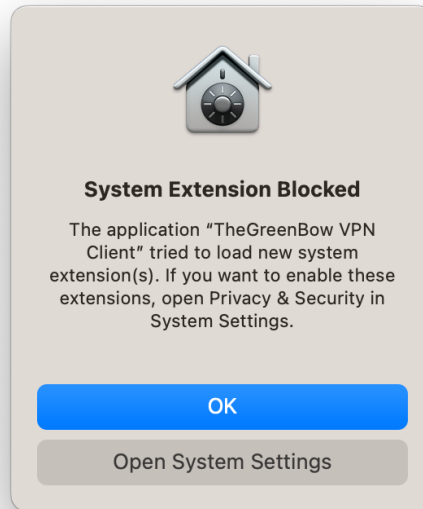
The **Network Extensions** modal window appears again, with the toggle switch to the right of TheGreenBow VPN Client enabled:



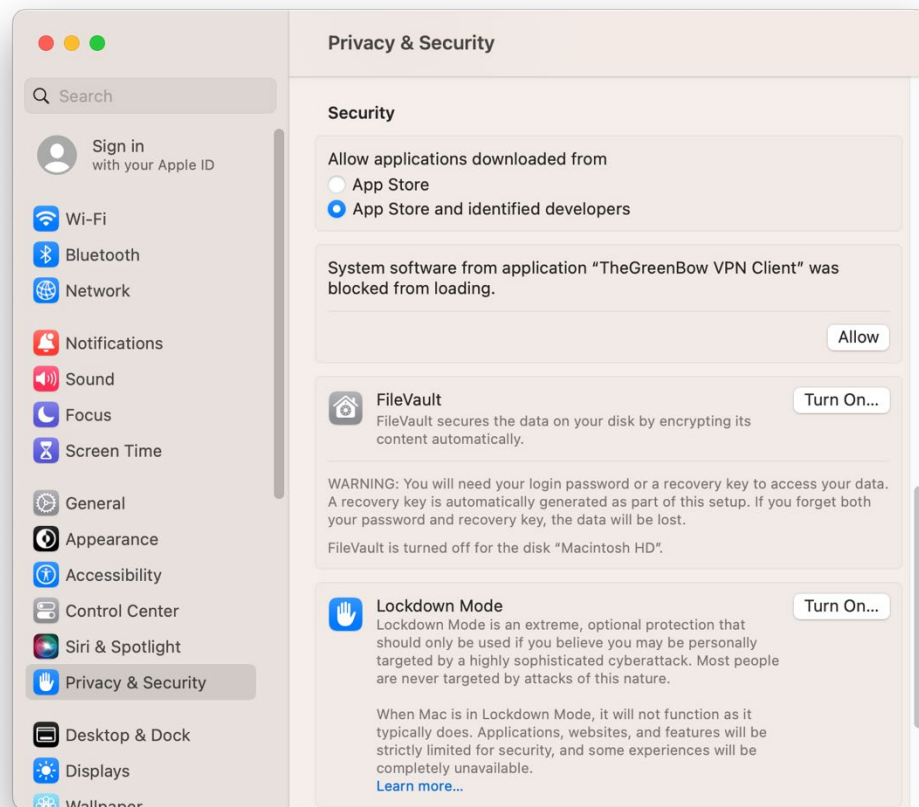
4. In the **Network Extensions** window, click **Done**.

The network extension is now enabled. You can close the **System Settings**.

In macOS 13 (Ventura) and macOS 14 (Sonoma)



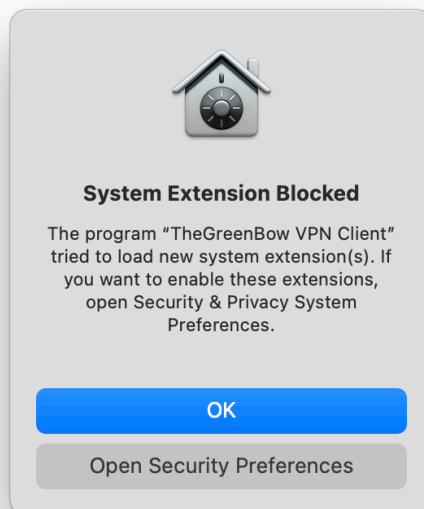
1. Click **Open System Settings**, or click **OK**, open **System Settings...** > **Privacy & Security**, and then scroll down to the **Security** section.
2. Under the option to allow downloaded applications, there should be a message stating that **System software from application "TheGreenBow VPN Client" was blocked from loading**, followed by an **Allow** button.



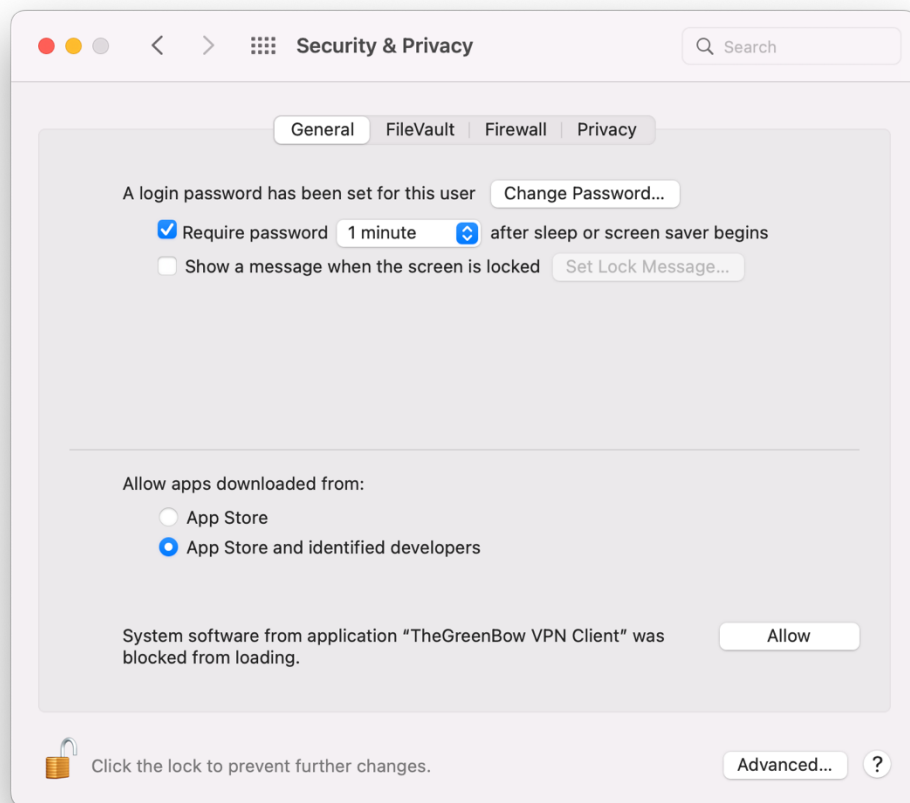
3. Click **Allow**.
4. A message is displayed asking you to confirm the changes to your **System Settings**. Enter your password to allow this.

The system extension is now enabled. You can close **System Settings**.

In macOS 12 (Monterey) and earlier



1. Click **Open Security preferences**, or click **OK**, then open **System Preferences... > Security & Privacy > General**.



2. To edit the settings, make sure the padlock at the bottom left of the window is open. If it is locked, click the padlock and enter your password.
3. At the bottom of the window, a message should appear indicating that **System software from application "TheGreenBow VPN Client" was blocked from loading**, followed by an **Allow** button.
4. Click **Allow**.

The system extension is now enabled. You can close **System Preferences**.

2.1.5 Previous installations of a VPN Client from the App Store

In case you installed a previous version of the macOS VPN Client from the Mac App Store, you must uninstall it before you install the new version.

To uninstall an app acquired from the Mac App Store, proceed as follows:

1. Run the **Launchpad**.
2. Move the mouse pointer over the app icon.
3. Click and hold until all icons start to wiggle.
4. Click the cross above the app icon.
5. Click **Delete** to confirm.

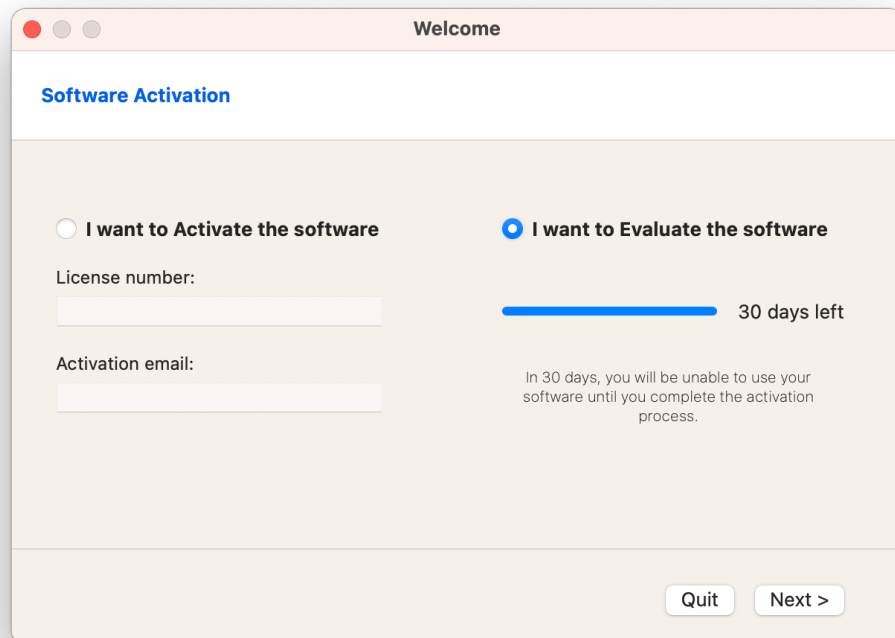
We also recommended that you manually remove all the tunnels that the app has added to the **System Preferences/Settings**.

To delete a tunnel that has been added to the **System Preferences/Settings**, go to **System Preferences/Settings... > Network** and search for tunnels whose **VPN Application** is `TheGreenBow VPN Client`.

2.2 Trial period

You can try the macOS VPN Client free of charge for 30 days. During this trial period, the VPN Client is fully operational, and all functions are unlocked.

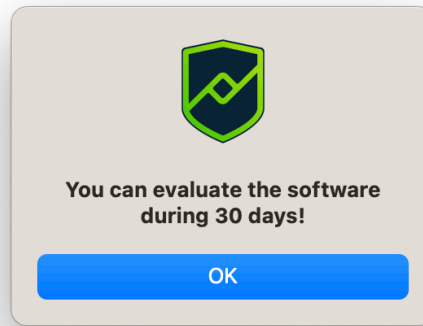
An activation window will be shown the first time you run the software. It allows you to either activate or evaluate the software and shows the number of days remaining in the trial period.



If you want to evaluate the software, select **I want to Evaluate the software**, then click **Next >** to run the software.

You can find the number of days remaining in the trial period at any time in the **About** window (see section 5 About window).

During the trial period, a window showing the number of days remaining in the trial period will be shown every time you start the software.



When the trial period expires, you must activate the app to continue using it.



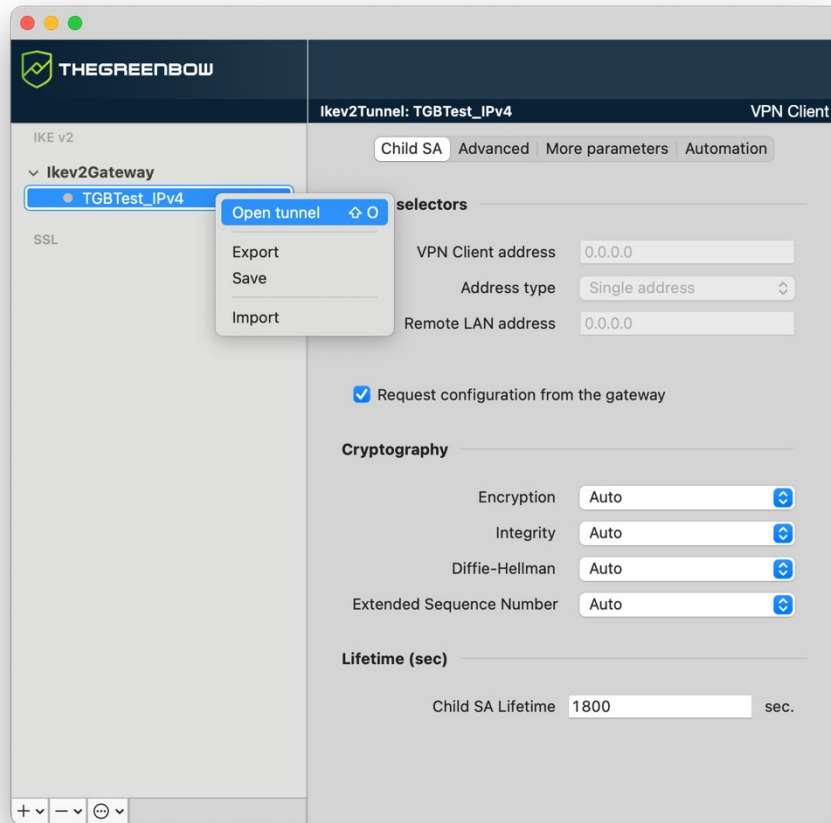
In the current version of the software, the activation window is only shown the first time you start the software. To find out how to display it again, refer to section 3.5 Displaying the activation window.



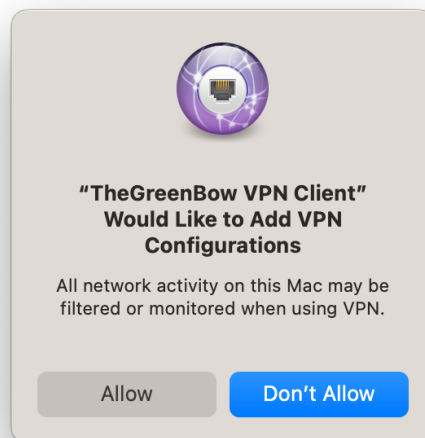
To find out how to activate the software, refer to chapter 3 Activating the software.

2.3 Test configuration

Once the app is installed, a test VPN configuration is automatically added to the list of VPN configurations. The test configuration can be used to check whether the macOS VPN Client is operational.



To open the tunnel TGBTest_IPv4, double-click the name or select the tunnel, and then open the contextual menu and select **Open Tunnel** or use the ⌘O shortcut. A window is displayed prompting you to add VPN configurations.



Click **Allow**. The tunnel should then open.

Once the tunnel is open, you should be able to ping the IP address 192.168.175.50 or open the web page at <http://192.168.175.50/> in your browser. You should then see TheGreenBow's test website:



2.4 Uninstalling the software

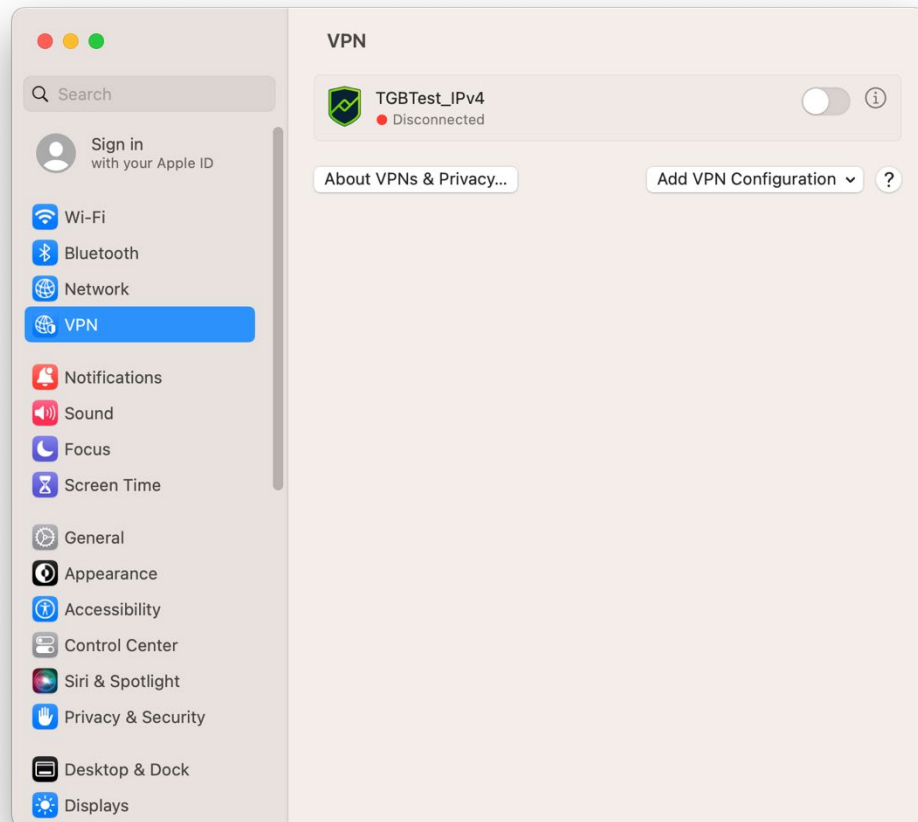
You can uninstall the app by dragging its icon from the **Applications** folder to the **Trash**.

Once you have uninstalled the app, tunnels may still be shown in the **Network** section of the **System Preferences/Settings**. These tunnels have the name `TheGreenBow VPN Client` under **VPN Application**.

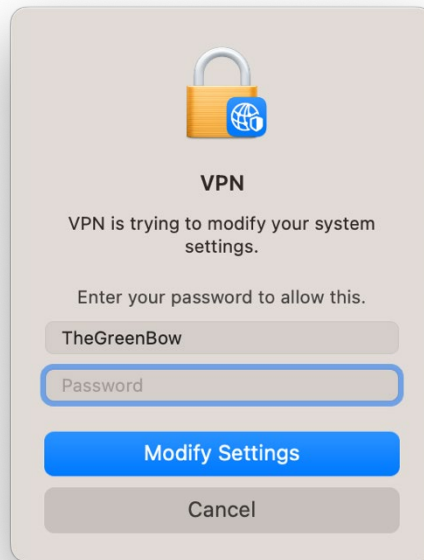
To delete them, proceed as follows:

In macOS 13 (Ventura) and later

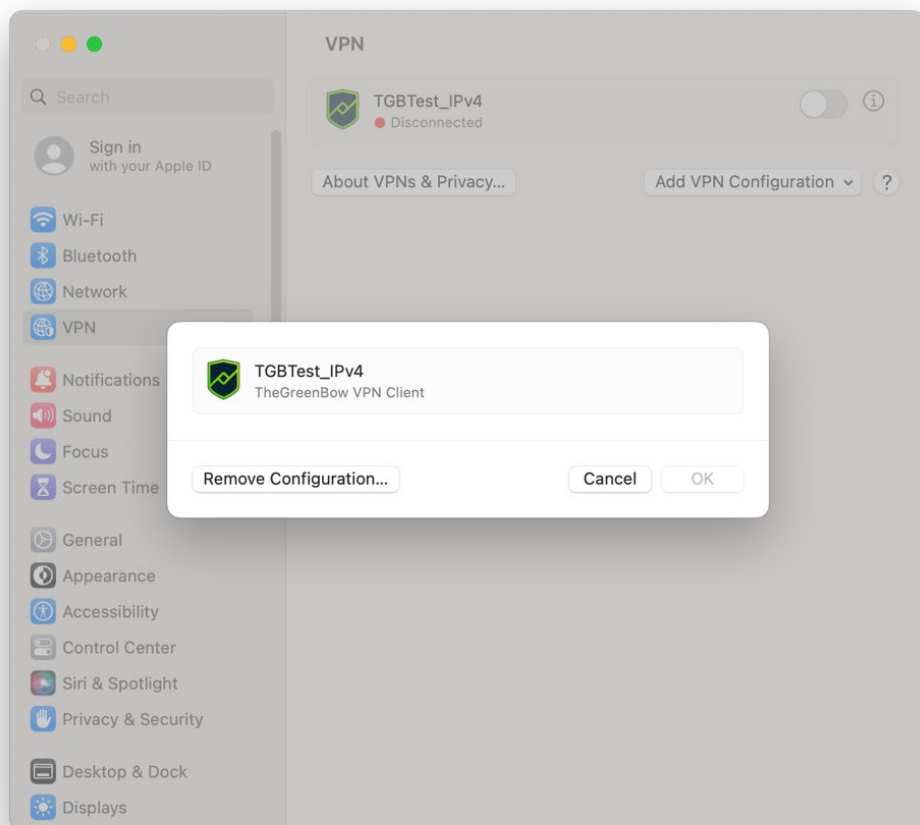
1. Open **System Settings...** > **VPN** (when network filters are installed, the menu is called **VPN & Filters**).



2. Click the info button (i) to the right of the toggle button. The first time you click this button, a window is displayed prompting you to allow modifications to your system settings.



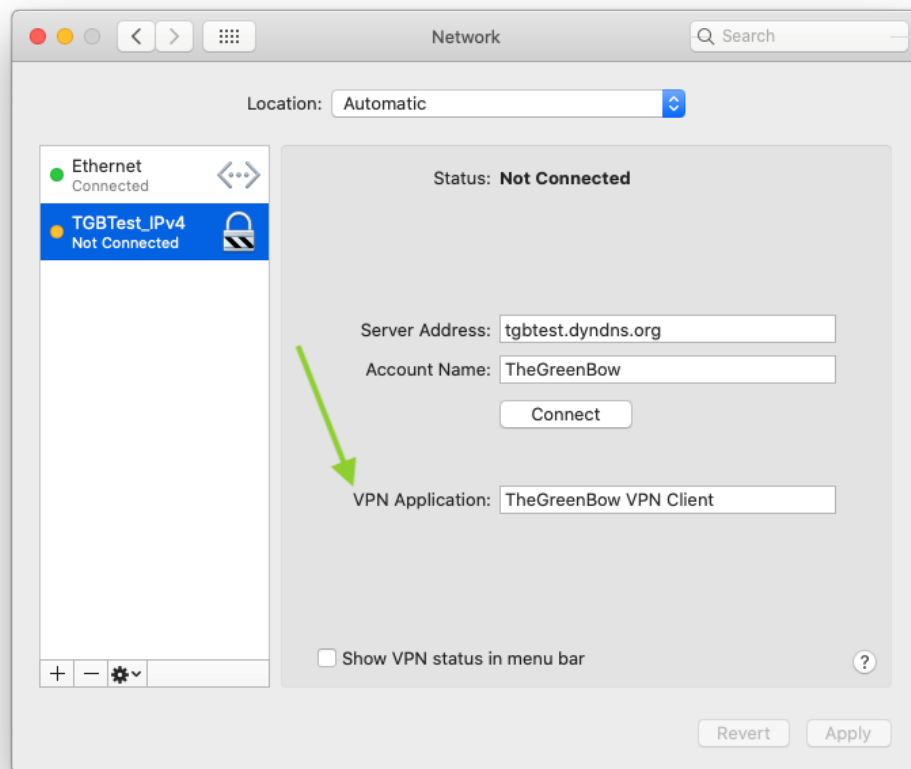
3. Enter your password, and then click **Modify Settings**. A dialog box is displayed.



4. Click **Remove Configuration...**
5. Repeat for all tunnels that you want to remove from **System Settings**.

In macOS 12 (Monterey) and earlier

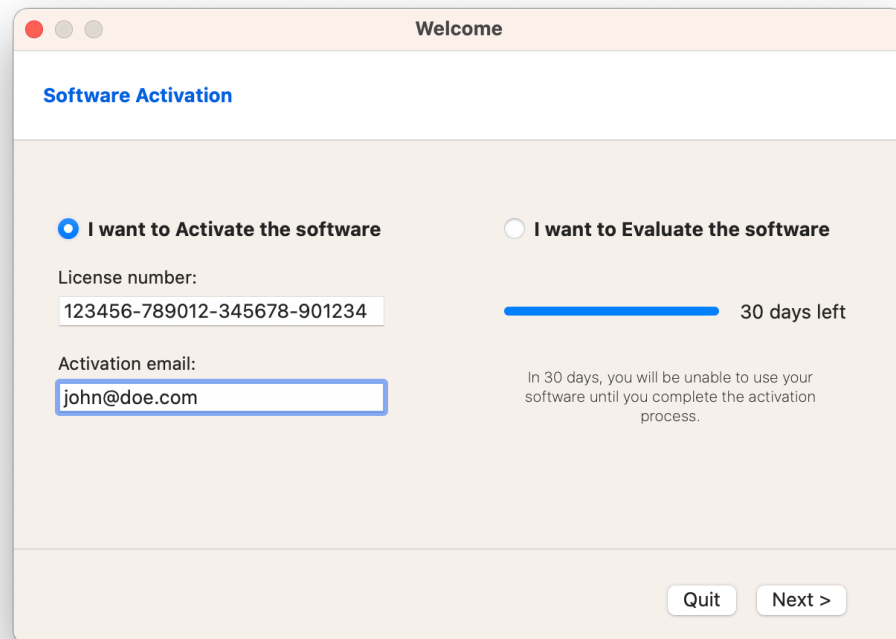
1. Open **System Preferences...** > **Network**.
2. In the left column, select the tunnel to delete.
3. Click the **minus** button.
4. Then, click **Apply** to confirm that you want to delete the tunnel.



3 Activating the software

You can activate the macOS VPN Client the first time you run the software or at any time during the trial period (see section 2.2 Trial period).

If you chose to evaluate the software before activating it, you must follow the procedure described in section 3.5 Displaying the activation window to access the activation window.



To activate the software, follow the steps described in the sections below.

3.1 Step 1

If you do not yet have a license, access TheGreenBow's online store at <https://store.thegreenbow.com/en/>. Select macOS. Click **Buy**, and then follow the instructions to buy one or several licenses.

In the **License number** field, enter the license number you received by e-mail. The license number can be copy-pasted directly from the purchase confirmation e-mail into this field.

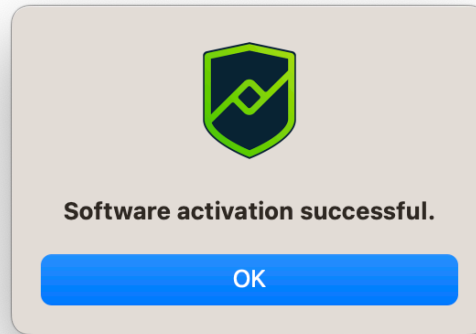
The license number consists of the characters [0..9] and [A..F], possibly grouped 6 by 6 and separated by hyphens.

In the **Activation email** field, enter the e-mail used to identify your activation. This information is used for recovering the activation information if it is lost.

3.2 Step 2

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

Once the activation has been carried out successfully, click **OK** 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

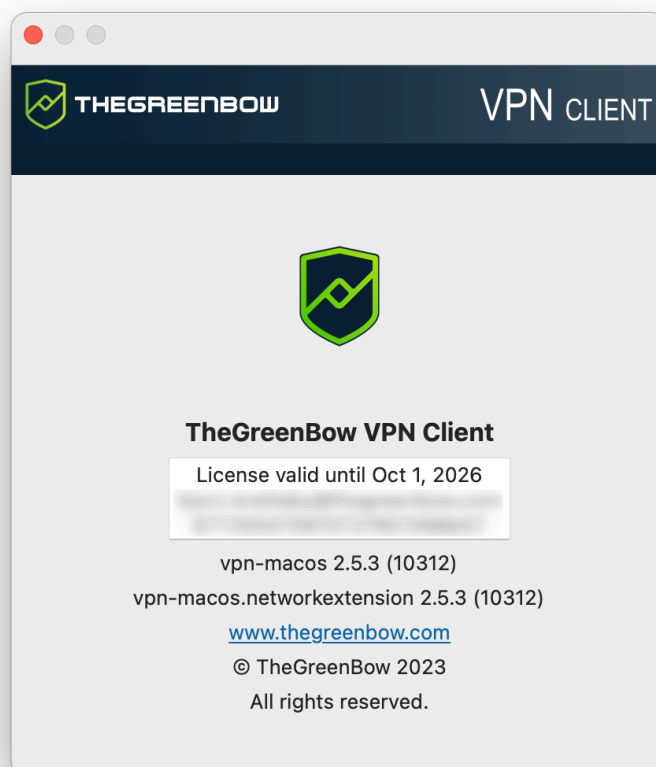
Software activation may fail for various reasons. The error is always displayed in the activation window. It is sometimes followed by a link that displays more information about the error or suggests actions to solve the problem.

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

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

3.4 License and activated software

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



3.5 Displaying the activation window

In the current version of the software, the activation window is only shown the first time you start the software. If you have chosen to evaluate the software before activating it, follow the procedure described below to display the activation window when the trial period has expired or as soon as you are ready to activate the software.

1. If the software is already running, quit it.
2. In the **Finder**, hold down the Option key and select the **Go > Library** menu item.
3. Access the
Group Containers/HCZ5L8U556.group.com.thegreenbow.vpn/Library/Application Support/ **folder**.
4. In this folder, delete all files that have a `.dat` or `.json` extension.
5. If necessary, repeat these steps in the
Group Containers/HCZ5L8U556.group.com.thegreenbow.vpn/Library/Caches/ **folder**.

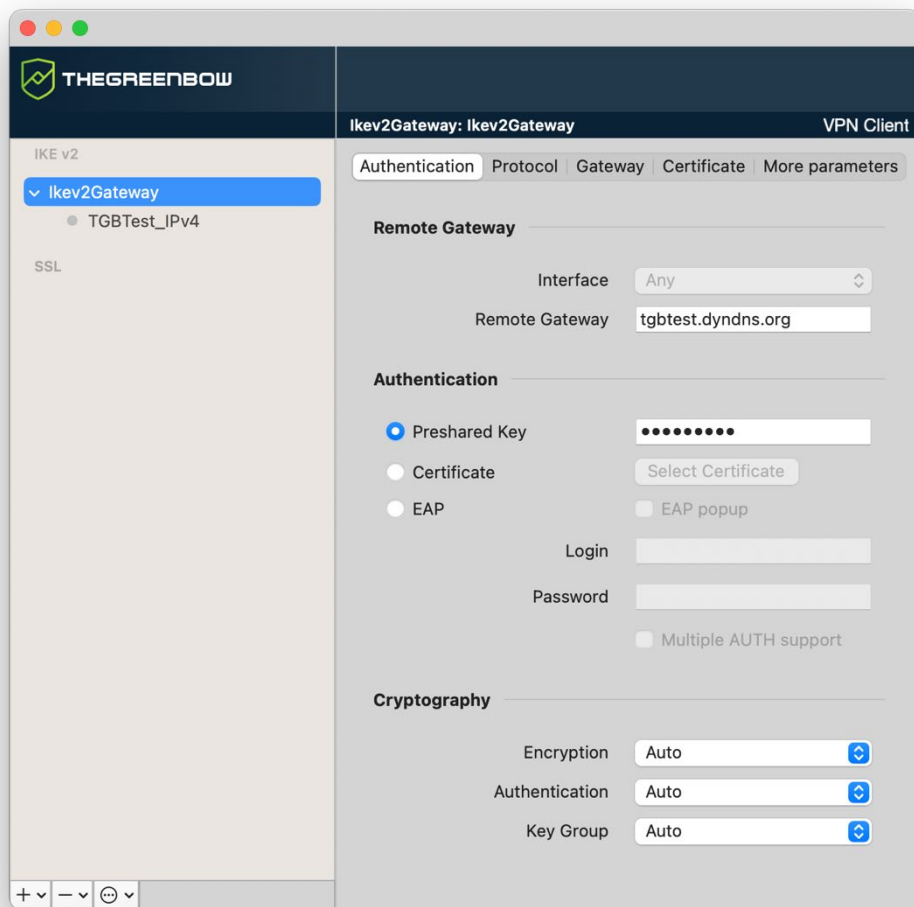
The activation window will be shown the next time you run the software. You can proceed with activation by following the steps described in section 3.1 Step 1 above.

4 User interface

4.1 Overview

When you start the VPN Client, the **Configuration Panel** and the menus are shown. The **Configuration Panel** consists of the following elements:

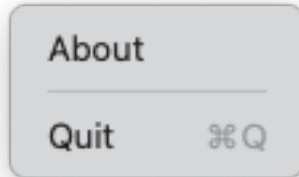
- The VPN configuration tree on the left side of the panel
- The VPN tunnel configuration tabs on the right side of the panel



The content of the configuration tab changes according to the item selected in the VPN configuration tree.

4.2 Menus

TheGreenBow VPN Client

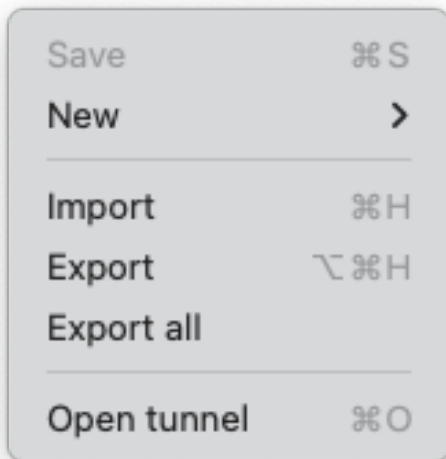


- **About:** Displays the software version number, the license number, and its validity period
- **Quit:** Closes the app



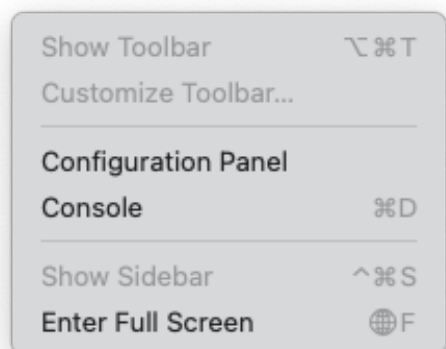
Closing the app does not close any open tunnel.

Configuration



- **Save:** Saves the configurations
- **New:** Creates a new **IKE Auth**, **Child SA**, or **TLS** configuration
- **Import:** Imports a configuration from a `.tgb` file
- **Export:** Exports the selected configuration
- **Export all:** Exports all configurations
- **Open/Close tunnel:** Opens or closes the selected tunnel

View

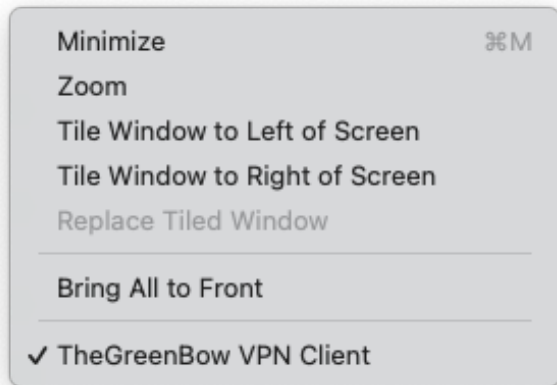


- **Configuration Panel:** Opens the VPN configuration window
- **Console:** Opens the macOS Console



The **Show Toolbar**, **Customize Toolbar...** and **Show Sidebar** options are grayed out as they are not available in this version.

Window



- Contains the usual system options used to manage application windows.

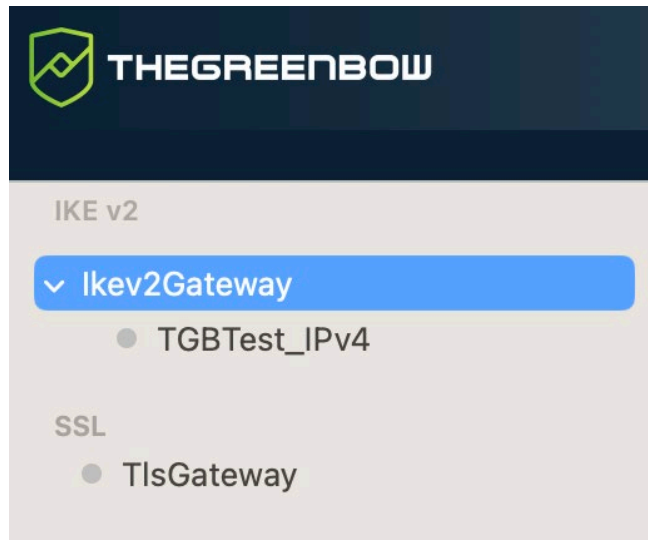
4.3 Keyboard shortcuts

⌘S	Saves all the configurations
⌘H	Imports a new VPN configuration
⌘Q	Quits the app
⌘D	Opens the log Console
⌘O	Opens the selected tunnel
⌘W	Closes the selected tunnel

4.4 VPN configuration tree

4.4.1 Introduction

The left side of the **Configuration Panel** shows the VPN configuration in the form of a tree structure. It can contain an infinite number of tunnels.



Under the root of the VPN configuration, used 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 item in the VPN configuration tree 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 entry at the root level allows you to view, edit, or create IPsec configurations using IKEv2 with multiple IKE Auth¹ and Child SA² connections. Each IKE Auth can contain more than one Child SA.

The icon to the left of the tunnel indicates its status:

	Tunnel is closed. Double-click to open it if no other tunnel is mounted.
	Tunnel is open. Double-click to close it.
	Tunnel being opened or closed.

To rename an item, select it, then click it or press the Enter key on the keyboard.

¹ Default name: Ikev2Gateway.

² Default name: Ikev2Tunnel.

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

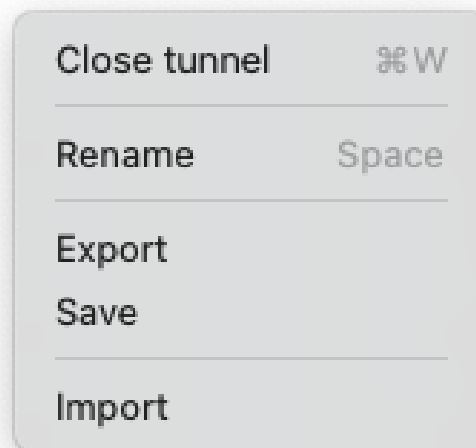


The **Save** command saves all the configurations, not specific configurations.

4.4.2 Contextual menus

4.4.2.1 IKEv2 and SSL

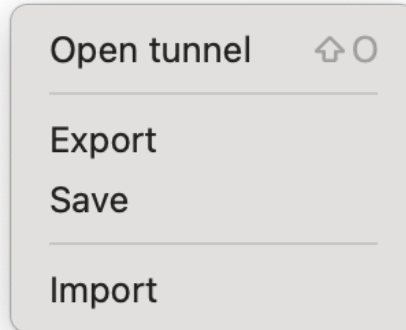
Press and hold the Control key while you click the IKEv2 or SSL item to display the following contextual menu:



Open/Close Tunnel	Opens the selected tunnel / Closes the open tunnel (IKEv2 or SSL).
Rename	This menu item is not active.
Export	Exports all IKEv2/SSL configurations.
Save	Saves all the changes made to the configurations (IKEv2 and SSL).
Import	Imports a <code>.tgb</code> configuration file.

4.4.2.2 IKE Auth

Press and hold the Control key while you click an IKE Auth¹ item to open the following contextual menu:

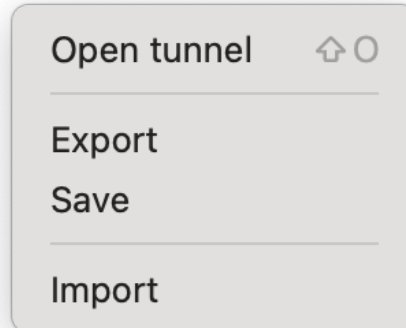


Open/Close tunnel	Opens the selected tunnel / Closes the open tunnel.
Export	Exports the IKE Auth node and all its Child SA nodes.
Save	Saves all the changes you have made.
Import	Imports a .tgb configuration file.

¹ Default name: Ikev2Gateway.

4.4.2.3 Child SA

Press and hold the Control key while you click a Child SA¹ item to display the following contextual menu:



Open/Close tunnel	Opens the selected tunnel / Closes the open tunnel.
Export	Exports the IKE Auth node and all its Child SA nodes.
Save	Saves all the changes you have made.
Import	Imports a .tgb configuration file.

4.4.3 Shortcuts

The following shortcuts are available:

⌘S	Saves all the configurations.
⌘W	Closes the open tunnel.
⌘⇧O	Opens the selected tunnel.

4.4.4 Buttons in the VPN configuration tree

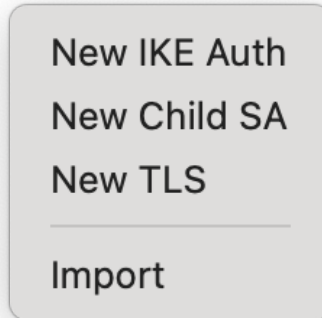
You will find the following buttons at the bottom of the VPN configuration tree:

¹ Default name: Ikev2Tunnel.



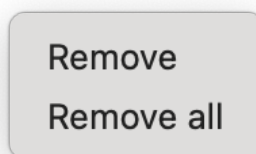
Click one of the buttons to open the corresponding contextual menus. The menu associated with each button is described in the following subsections.

4.4.4.1 + button



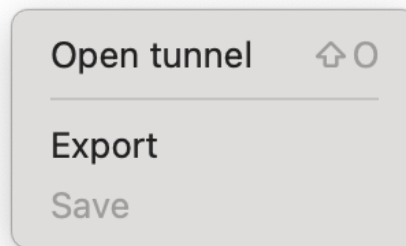
New IKE Auth	Creates a new IKE Auth node.
New Child SA	Creates a new Child SA node. If an IKE Auth node was selected in the VPN configuration tree, then the newly created Child SA node will be a child item of the selected IKE Auth node. Otherwise, a pair of new IKE Auth and Child SA nodes will be created simultaneously.
New TLS	Creates a new SSL node.
Import	Imports a .tgb configuration file.

4.4.4.2 - button



Delete	Removes the selected node (and all its child items) from the VPN configuration tree.
Remove all	Removes all nodes in the VPN configuration tree

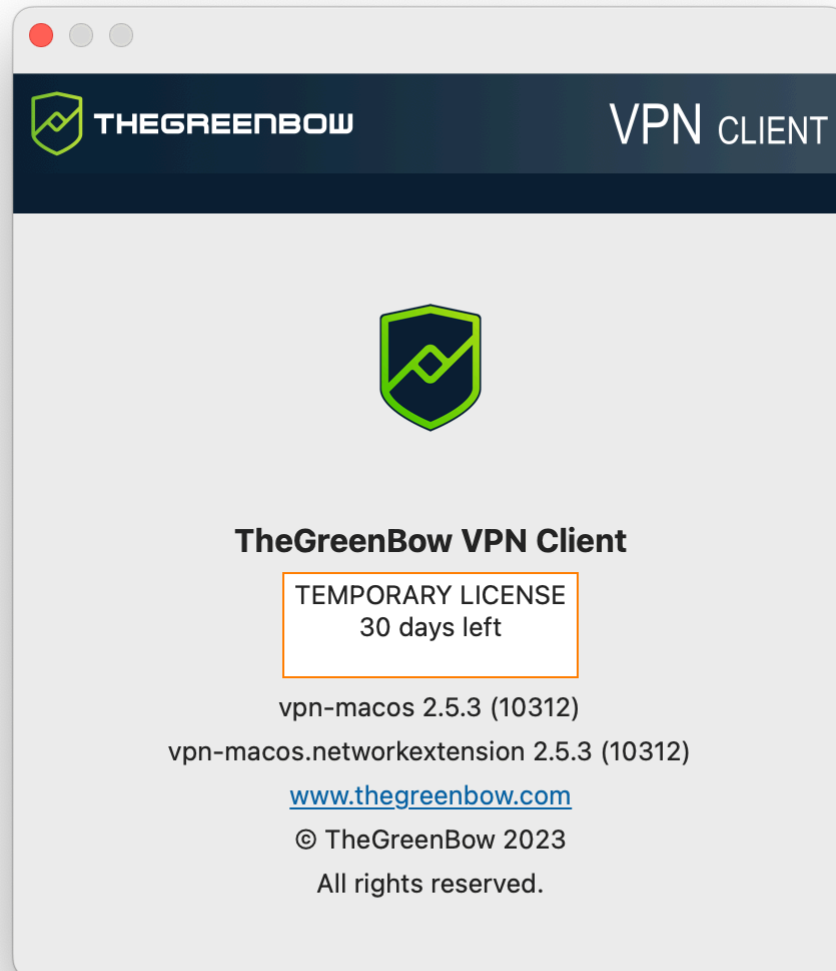
4.4.4.3 button



Open/Close tunnel	Opens the selected tunnel / Closes the open tunnel.
Export	Exports the configuration of the selected node and all its child items. If a Child SA node is selected, then the corresponding IKE Auth node is also exported.
Save	Saves all the changes you have made.

5 About window

To access the **About** window, from the **TheGreenBow VPN Client** menu, choose **About**.



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

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

6 Importing and exporting VPN configurations

6.1 Importing a VPN configuration

Use the **Configuration > Import** menu item to import a VPN configuration into the macOS VPN Client.



VPN configuration files have a `.tgb` extension.

If the VPN configuration has been saved with a password, the user will be prompted to enter it.



No check is carried out to determine whether there already is another tunnel with the same name in the VPN Client, and any duplicate names will not generate an error.

6.2 Exporting a VPN configuration

To export a VPN tunnel from the list, do one of the following:

- Select the **Configuration > Export** menu item.
- Press and hold the Control key while you click the IKEv2 or SSL item that you want to export, and then choose the **Export** option from the contextual menu
- Use the `⌘⇧H` shortcut

To export all tunnels, from the **Configuration** menu, select **Export all**.



7 Configuring a VPN tunnel

7.1 Editing and saving a VPN configuration

You can edit the VPN configuration (e.g. edit the parameters for a tunnel) and test your changes “on-the-fly” without having to save it.

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.

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

- The ⌘S keyboard shortcut
- The **Configuration** > **Save** menu item

7.2 Configuring an IPsec IKEv2 tunnel

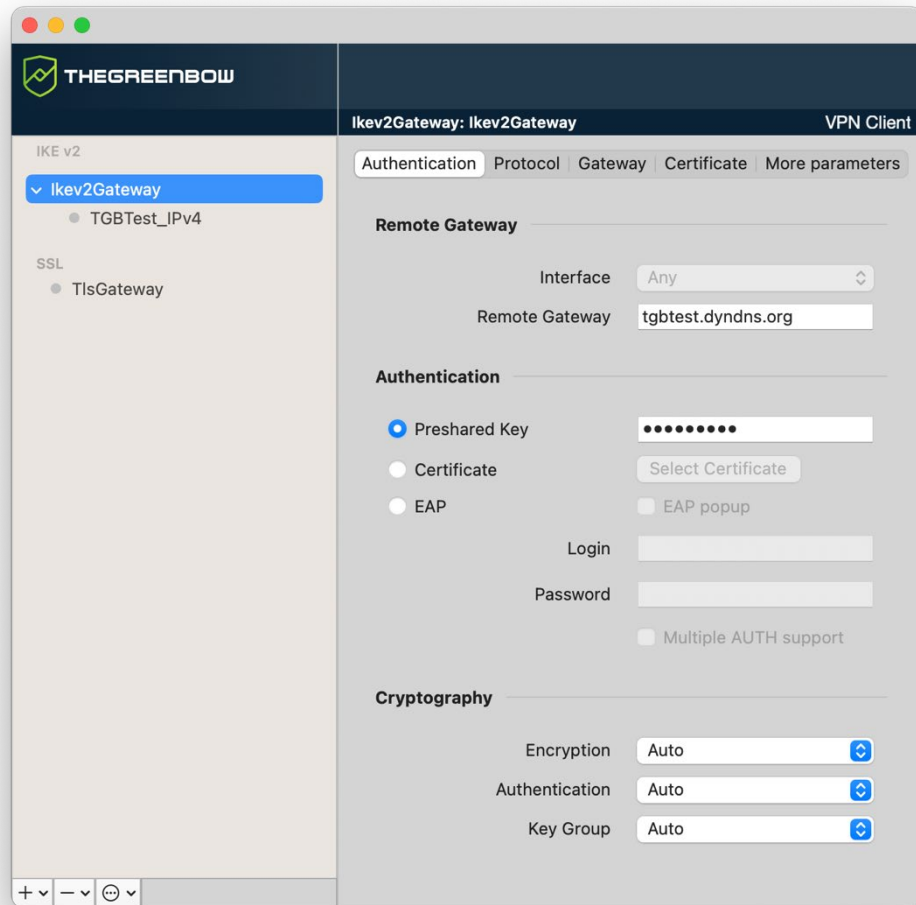
An IKE Auth VPN tunnel is the authentication phase in IKEv2.

The purpose of IKE Auth is to negotiate sets of IKE policies, authenticate peers, and configure a secure channel between peers. Within the context of IKE Auth, each end of the system must identify itself and authenticate with the other end.

To configure IKE Auth, select an IKE Auth¹ item in the VPN configuration tree on the **Configuration Panel**. The parameters can be configured in the right-hand tabs of the **Configuration Panel**.

¹ Default name: Ikev2Gateway.

7.2.1 IKE Auth: Authentication



7.2.1.1 Remote Gateway

Interface *(This feature is not currently configurable.)*

Name of the computer's network interface on which the VPN connection is established. Selecting **Automatic** enables the VPN Client to automatically choose the appropriate interface.

The **Automatic** option is used, for example, to configure a tunnel that will be deployed on other computers.

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

7.2.1.2 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 13 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 13 Security recommendations.



Refer to the dedicated chapter 11 Managing certificates.

EAP

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

When you select the EAP mode, you can choose to either 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 13 Security recommendations).

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

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

7.2.1.3 Cryptography

Encryption	Encryption algorithm negotiated during the authentication phase ¹ : Auto ² , AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Authentication	Authentication algorithm negotiated during the authentication phase ³ : Auto ⁴ , SHA2 256, SHA2 384, SHA2 512.
Key Group	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).

¹ Refer to chapter 13 Security recommendations on the choice of algorithm.

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

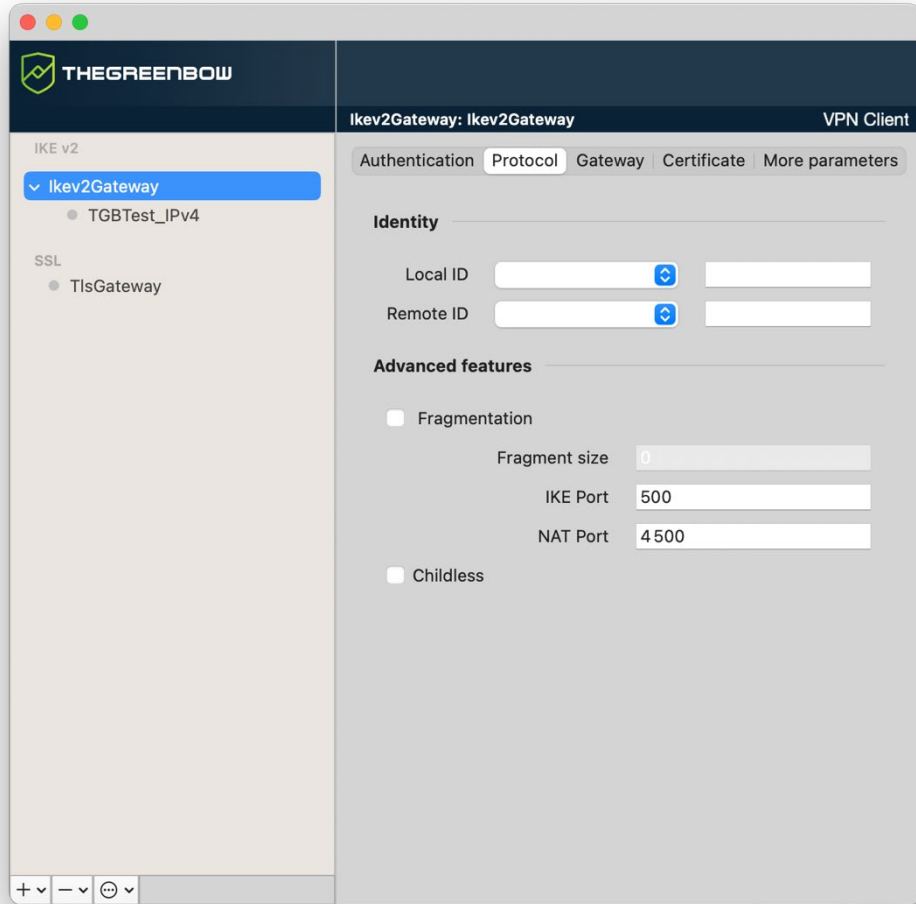
³ See note 1.

⁴ See note 2.

⁵ See note 1.

⁶ See note 2.

7.2.2 IKE Auth: Protocol



If you use an IPsec DR gateway, you must add the dynamic parameter `nonce_size` (see section 7.2.8 Child SA: More parameters) and set its value to 16. These gateways will not accept any other nonce size.

7.2.2.1 Identity

Local ID Local ID is the identifier that the VPN Client sends to the remote VPN gateway during the authentication phase.

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

- **IPV4 Address:** an IPv4 address (type = IPV4 ADDR), e.g. 195.100.205.101
- **DNS:** a domain name (type = FQDN), e.g. gw.mydomain.net
- **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)
- **KEY ID:** a character string (type = KEY ID), e.g. 123456

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

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

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

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

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

7.2.2.2 Advanced features

Fragmentation Enables IKEv2 packet fragmentation in accordance with RFC 7383.

This function prevents IKEv2 packets from being fragmented by the IP network they're passing through.

The fragment size must generally be set to a value that is smaller by 200 bytes than the MTU of the physical interface, e.g. 1300 bytes for a typical 1500-byte MTU.

IKE Port IKE Auth (Authentication) exchanges 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.

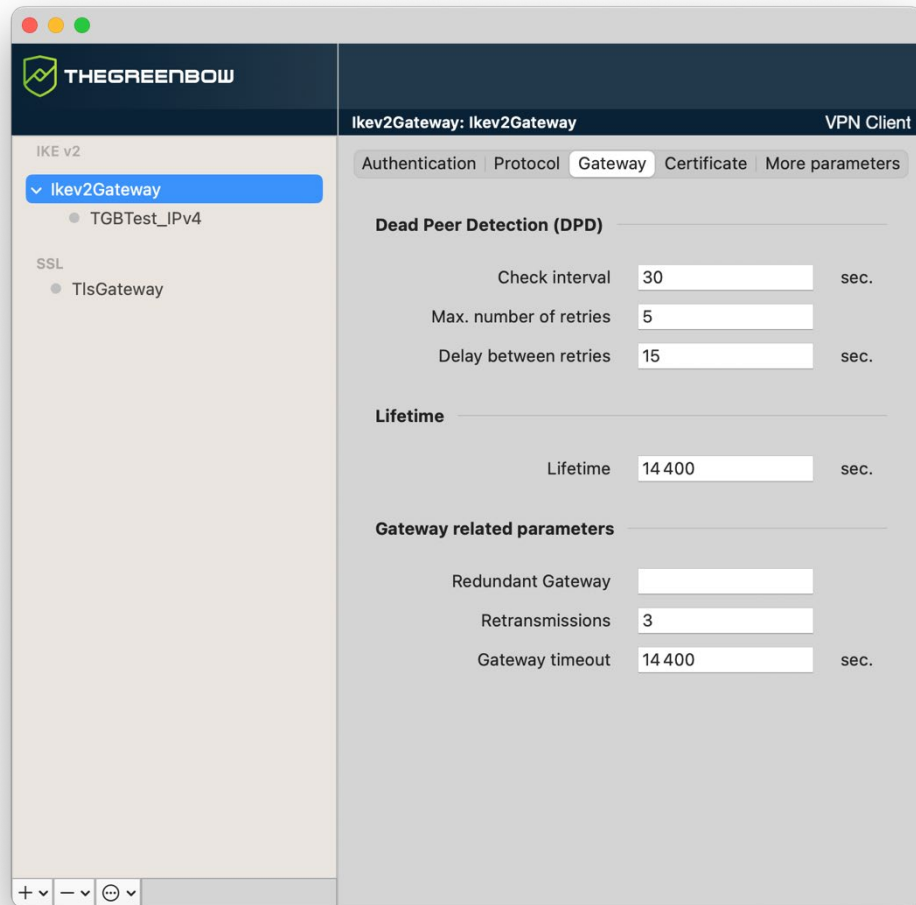
NAT Port IKE Child SA (IPsec) exchanges use the UDP protocol and port 4500 by default. NAT port configuration can bypass the networking hardware (firewalls, routers) that filter port 4500.



The remote VPN gateway must also be able to perform the IKE Child SA exchanges on a port other than 4500.

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.

7.2.3 IKE Auth: Gateway



7.2.3.1 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.



7.2.3.2 Lifetime

Lifetime Lifetime of the IKE Auth phase.
The lifetime is expressed in seconds.
The default value is 1,800 seconds (30 min).

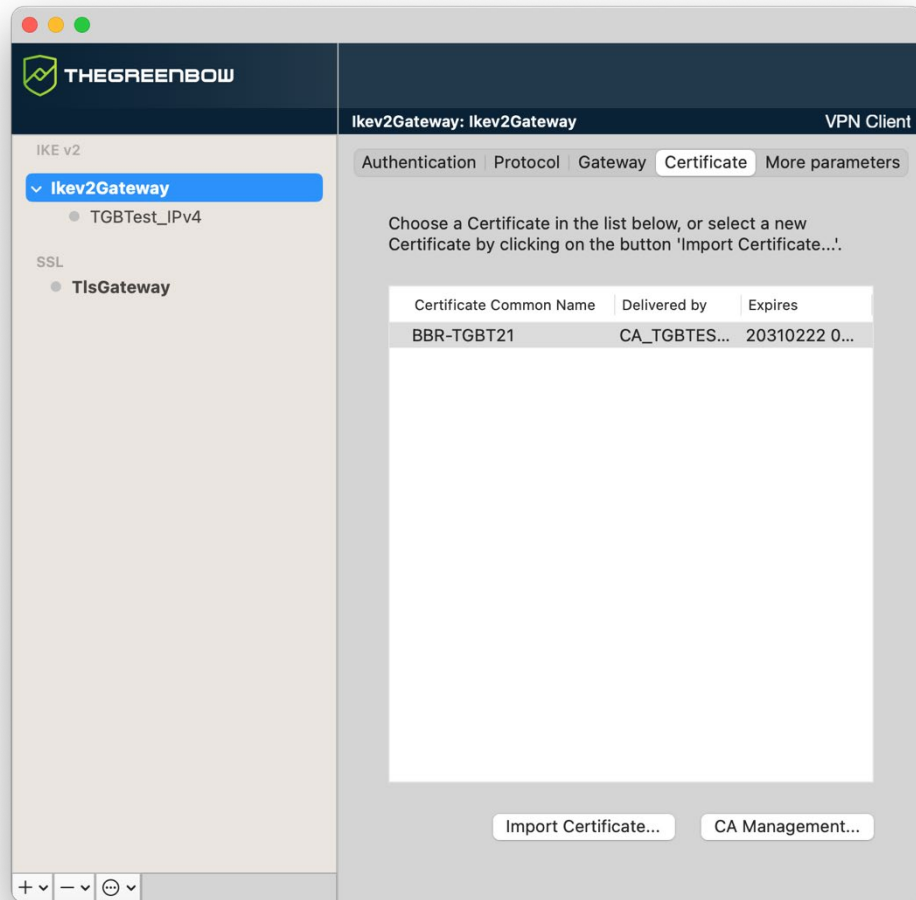
7.2.3.3 Gateway-related parameters

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.
 Refer to chapter 8 Redundant gateway.

Retransmissions Number of IKE protocol message resends before failure.

Gateway timeout Delay between two retransmissions

7.2.4 IKE Auth: Certificate

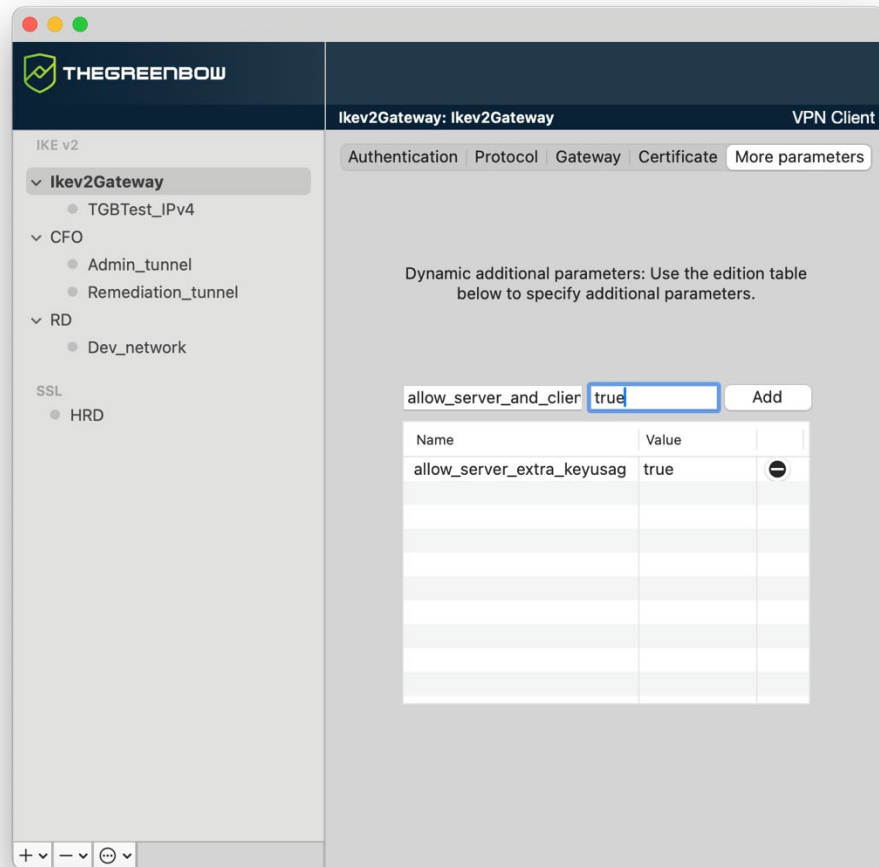


This tab is only available if the Certificate or EAP mode is selected in the **Authentication** tab.



Refer to chapter 11 Managing certificates.

7.2.5 IKE Auth: More parameters



If required, you can configure additional dynamic parameters for the macOS VPN Client under its IKE Auth configuration.



Refer to chapter 10 Managing dynamic parameters for further details.

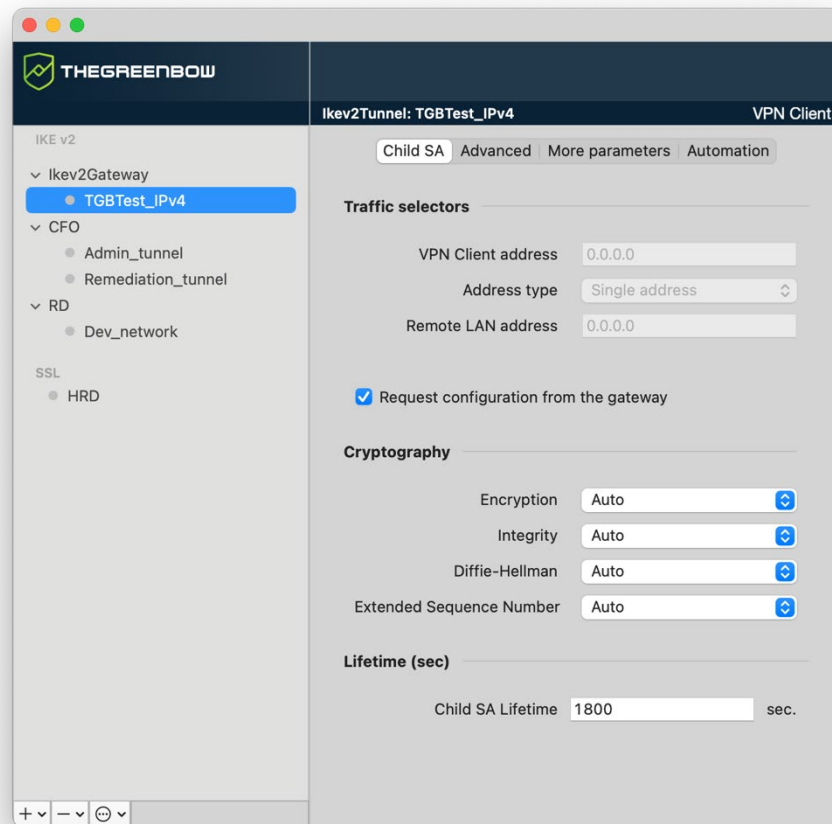
7.2.6 Child SA: Child SA

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 tree on the **Configuration Panel**. 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.



7.2.6.1 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.

Address type

The endpoint of the tunnel can be a network or a remote workstation.

 Refer to section 7.2.6.2 Configuring the address type below.

Request configuration from the gateway

This option (also called “Configuration Payload” or “Mode CP”) lets the VPN Client get all the information required for the VPN connection from the gateway: VPN Client addresses, remote network address, subnet mask, and DNS addresses.

When this option is checked, all corresponding fields are disabled (uneditable).

They are filled in dynamically as the tunnel is opened with the values sent by the VPN gateway during the Mode CP exchange.

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 returned to be compatible with IPsec DR gateways that have strictly adhered to this recommendation.
True	The list of traffic selectors (TSr) the gateway sent during initial key establishment is sent again.



Default behavior for Stormshield gateways is `True`.

`local_virtual_network_size`

The default virtual local network size is 24. To use a different size (e.g. 32), set the `local_virtual_network_size` dynamic parameter to the desired value (possible values: 1 to 32).



Refer to chapter 10 Managing dynamic parameters.

7.2.6.2 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	192.168.1.0
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	192.168.1.0
End address	255.255.255.0

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

Address type	Single address
Remote LAN address	192.168.1.0



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



“All traffic through the VPN tunnel” configuration

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



When using the “All through the tunnel” mode, the interface metric is set to 1 by default, which allows all packets to be routed through the tunnel.

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

Maximum value: 50

Moreover, the dynamic parameter `VirtualInterfaceProfile` is used to change the network profile type of the connection associated with the virtual card (only in “All traffic through the tunnel” mode).

Possible values:

0 or undefined	Public
1	Private



Refer to section 7.2.6.2 Configuring the address type and chapter 10 Managing dynamic parameters.

7.2.6.3 Cryptography

Encryption	Encryption algorithm negotiated during the IPsec phase ¹ : Auto ² , AES CBC (128, 192, 256), AES CTR (128, 192, 256), AES GCM (128, 192, 256).
Integrity	Authentication algorithm negotiated during the IPsec phase 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 that you enable the ESN mode.

7.2.6.4 Lifetime (sec)

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).
--------------------------	--

¹ Refer to chapter 13 Security recommendations on the choice of algorithm.

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

³ See note 1.

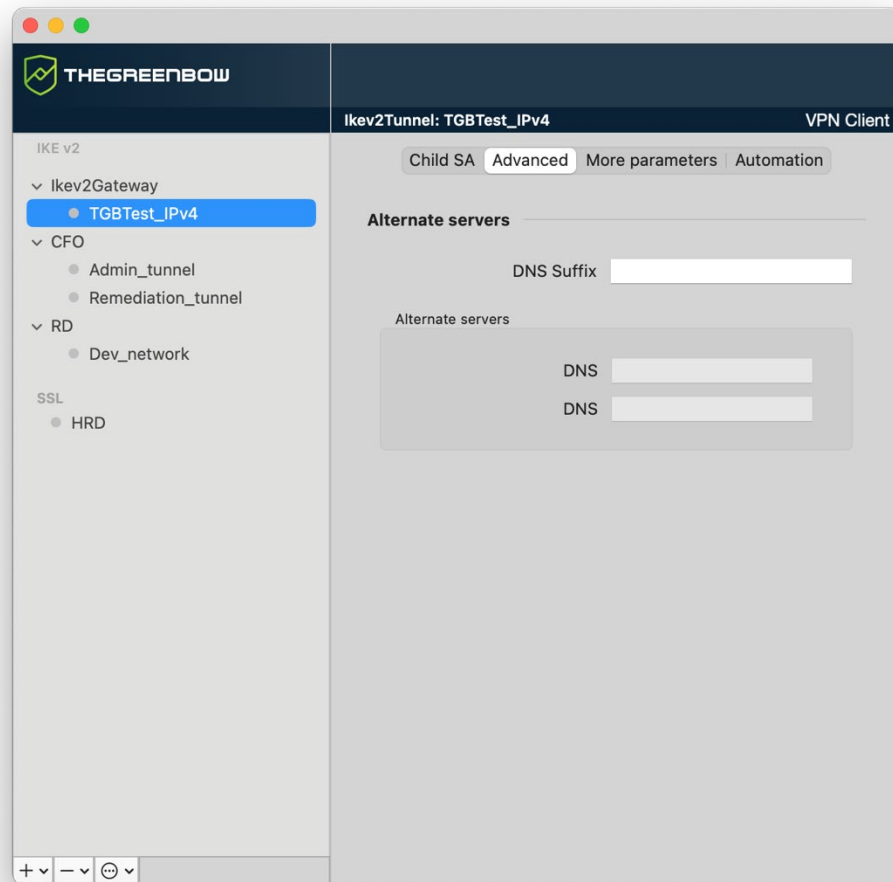
⁴ See note 2.

⁵ See note 1.

⁶ See note 2.

⁷ See note 2.

7.2.7 Child SA: Advanced



7.2.7.1 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.

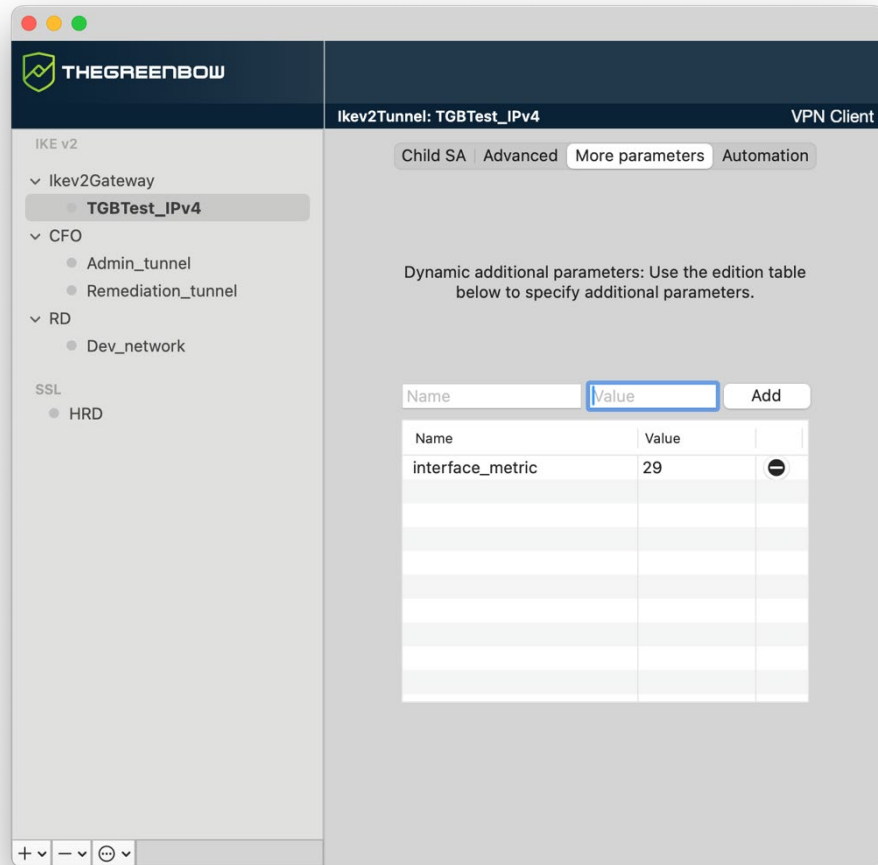
Alternate servers

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 addresses, since IPv6 is not supported in the current version of the product.



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.

7.2.8 Child SA: More parameters



If required, you can configure additional dynamic parameters for the macOS VPN Client under its Child SA configuration.



Refer to chapter 10 Managing dynamic parameters for further details.

7.2.9 Child SA: Automation

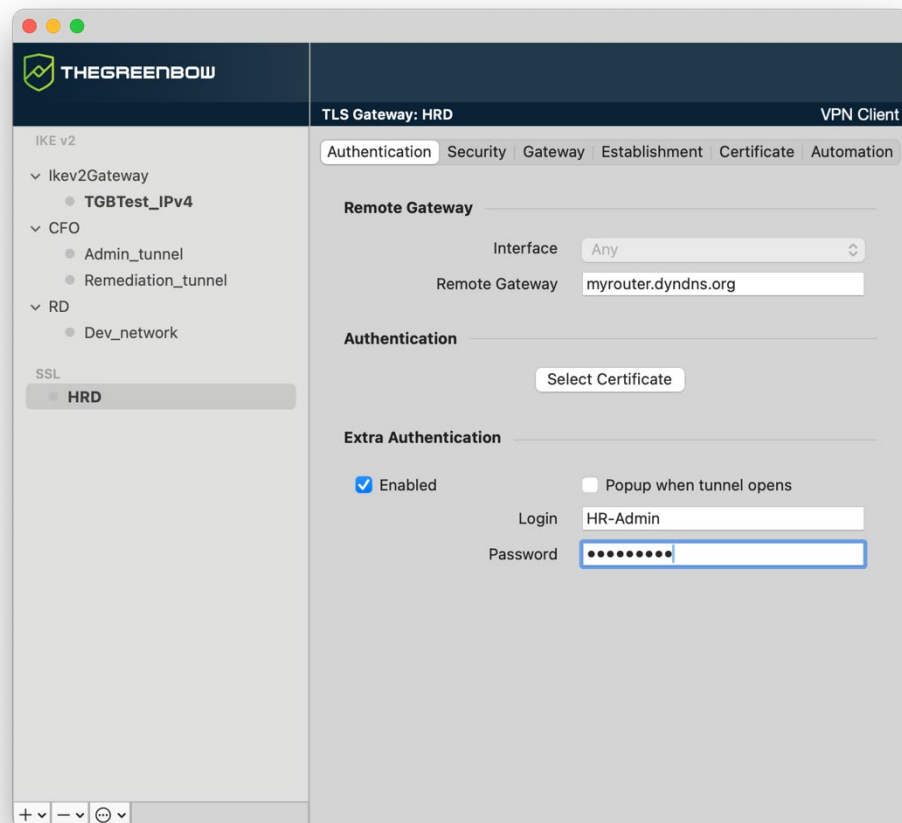
Refer to chapter 9 Automation.

7.3 Configuring an SSL/OpenVPN tunnel

The macOS VPN Client can be used to open SSL VPN tunnels.

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

7.3.1 SSL: Authentication





7.3.1.1 Remote Gateway

Interface (This option is currently not editable.)
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.

When the network interface has several IP addresses, you can specify the address using the dynamic parameter `local_subnet` (see chapter 10 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 address (IPv4, since IPv6 is not currently supported) or DNS address of the remote VPN gateway.
This field is required.

7.3.1.2 Authentication

Select Certificate Choose a certificate for VPN connection authentication.
 Refer to the dedicated chapter 11 Managing certificates.

7.3.1.3 Extra Authentication

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

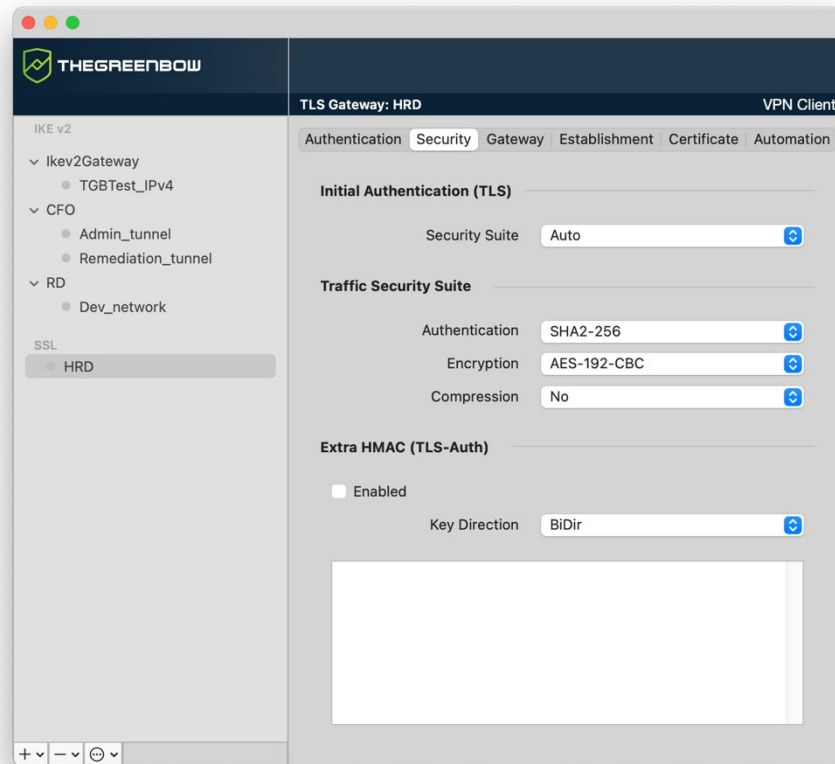
Enabled Enables or disables the increased security level.

Popup when tunnel opens When this box 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.

Login The username registered with the VPN gateway.

Password The matching password for the specified login name.

7.3.2 SSL: Security



7.3.2.1 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.
- **Low:** Only weak cryptography suites are sent to the gateway. In the current version, these are suites that use 64 or 56-bit encryption algorithms.
- **Normal:** Only “medium” cryptography suites are sent to the gateway. In the current version, these are suites that use 128-bit encryption algorithms.
- **High:** Only strong cryptography suites are sent to the gateway. In the current version, these are suites that use 128-bit or higher encryption algorithms.

For further information, refer to the following page:
<https://www.openssl.org/docs/man1.1.1/man1/ciphers.html>

7.3.2.2 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, LZO, No, LZ4.

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

² *ibid*

³ *ibid*

7.3.2.3 Extra HMAC (TLS-Auth)

Enabled 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").

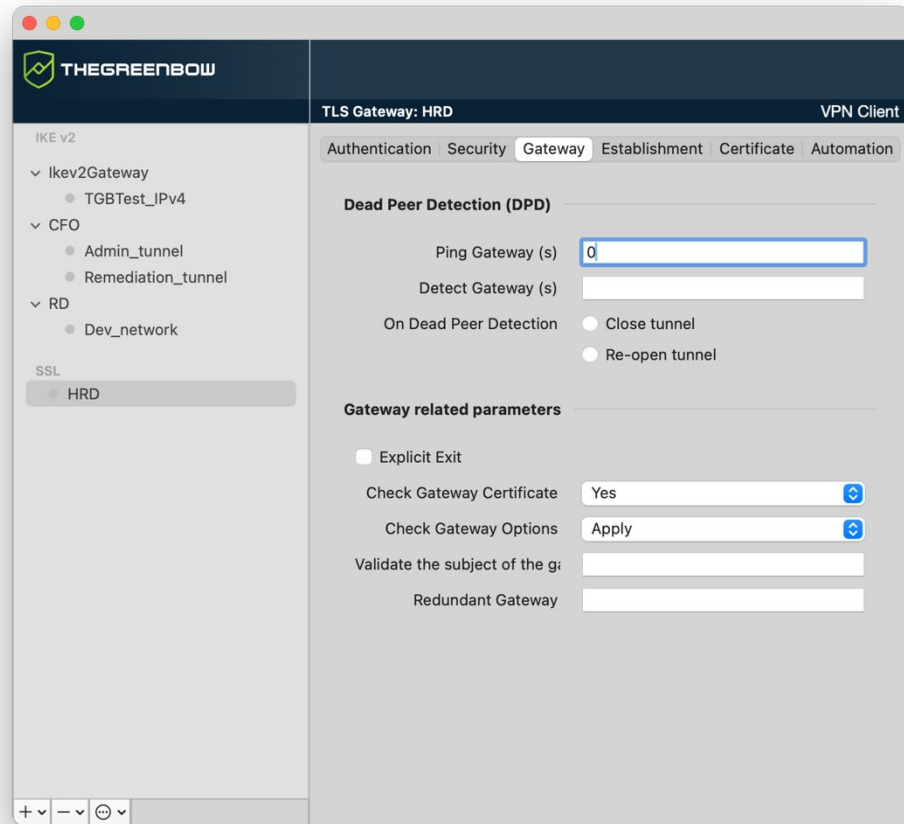
If this option is enabled, a key must be entered in the field below the checked box. The same key must also be entered on the gateway. It consists of a string of hexadecimal characters, in the following format:

```
-----BEGIN Static key-----  
362722d4fbff4075853fbe6991689c36  
b371f99aa7df0852ec70352122aee7be  
...  
515354236503e382937d1b59618e5a4a  
cb488b5dd8ce9733055a3bdc17fb3d2d  
-----END Static key-----
```

Key Direction When the Extra HMAC option is enabled, choose the key direction from this drop-down list:

- **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.

7.3.3 SSL: Gateway




7.3.3.1 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

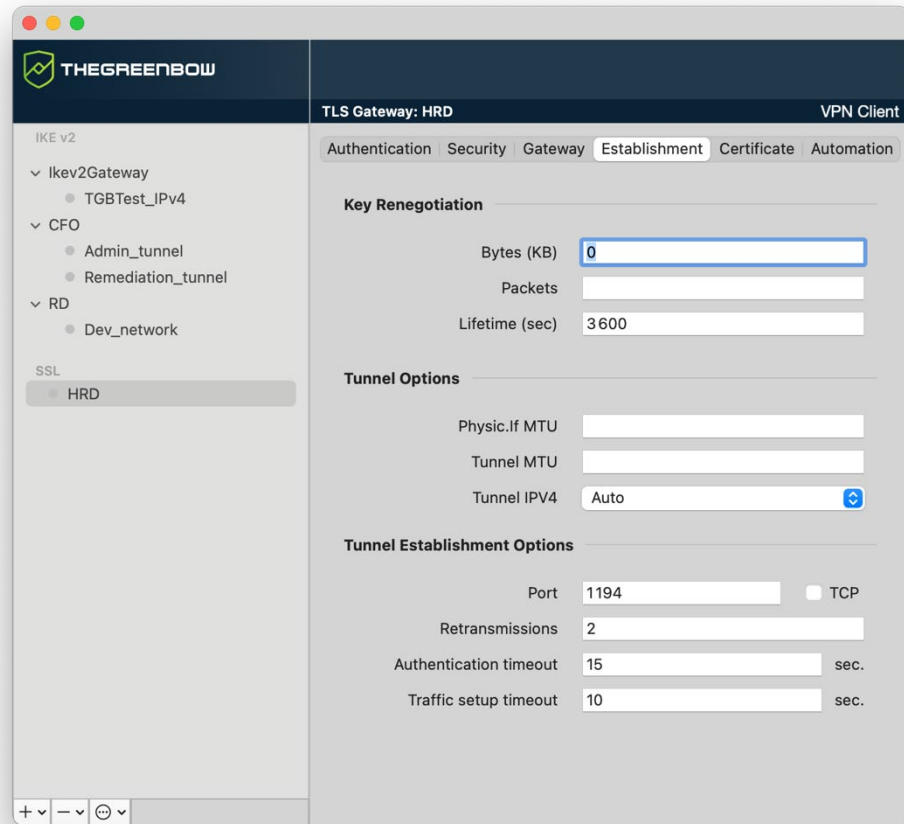
Ping Gateway (s)	Period, expressed in seconds, between two pings sent by the VPN Client to the gateway. Sending this ping enables the gateway to determine whether the VPN Client is still active.
Detect Gateway (s)	Time, expressed in seconds, after which the gateway is considered down if no ping has been 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.

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

7.3.3.2 Gateway-related parameters

Explicit Exit	<p>This parameter configures the VPN Client to send a specific VPN tunnel closing frame to the gateway when closing the tunnel.</p> <p>If this option is not selected, the gateway will use DPD to close the tunnel at its end, which is less effective.</p>
Check Gateway Certificate	<p>Specifies the control level applied to the gateway certificate.</p> <p>In the current version, two levels are available:</p> <ul style="list-style-type: none">• Yes (the certificate's validity is checked)• No (the certificate's validity is not checked) <p>The Lite option is reserved for future use. In this version, it is equivalent to the Yes option.</p>
Check Gateway Options	<p>Used to determine the level of consistency between the VPN tunnel and gateway parameters (encryption algorithms, compression, etc.).</p> <ul style="list-style-type: none">• Yes: Consistency is checked for all VPN parameters. The VPN tunnel will not open if any parameter is different.• No: Consistency is not checked before opening the tunnel. The VPN tunnel will try to open, even though no traffic may pass through because certain parameters are not consistent.• Lite: Consistency between the VPN Client and the gateway is only checked for essential parameters.• Apply: Gateway parameters will be applied.
Validate the subject of the gateway certificate	<p>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.</p>
Redundant gateway	<p>Defines the address of a spare VPN gateway that the VPN Client will switch to when the initial gateway is unavailable or unreachable.</p> <p>The address of the redundant VPN gateway can be either an IP or a DNS address.</p> <p> Refer to chapter 8 Redundant gateway.</p>

7.3.4 SSL: Establishment



7.3.4.1 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.

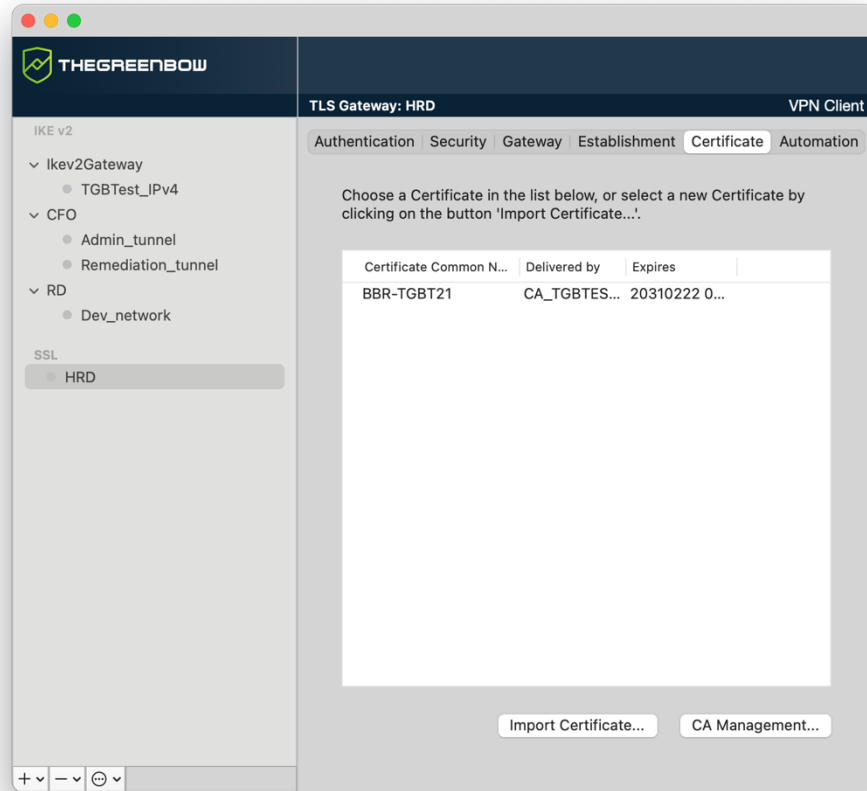
7.3.4.2 Tunnel Options

Physic.If MTU	<p>Maximum size of OpenVPN packets.</p> <p>Used to set a packet size so that OpenVPN frames are not fragmented at the network level.</p> <p>The default value for MTU is 0, meaning that the software will use the MTU value of the physical interface.</p>
Tunnel MTU	<p>Virtual interface MTU.</p> <p>When values have been entered, we recommend setting a lower value for the tunnel MTU than that of the physical interface MTU.</p> <p>The default value for MTU is 0, meaning that the software will use the physical interface's MTU value.</p>
Tunnel IPV4	<p>Defines the VPN Client's behavior when it receives an IPv4 configuration from the gateway:</p> <ul style="list-style-type: none">• Auto: Accepts the information sent by the gateway• Yes: Checks whether the information sent by the gateway matches the configured behavior. If this is not the case, a warning message is displayed on the console and the tunnel is not established.• No: Ignores it.

7.3.4.3 Tunnel Establishment Options

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

7.3.5 SSL: Certificate



 Refer to chapter 11 Managing certificates.

7.3.6 SSL: Automation

 Refer to chapter 9 Automation.

8 Redundant gateway

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

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

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

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

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

The same algorithm applies to the redundant gateway:

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



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



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



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 (refer to chapter 10 Managing dynamic parameters).



9 Automation

The macOS VPN Client allows you to execute scripts at different stages while opening a VPN tunnel.

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).

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.

The command lines can be as follows:

- Calling a “batch” file, e.g. `~/vpn/batch/script.sh`
- Running a program, e.g. `~/vpn/scripts/openTextEdit.sh` (see description below)
- Opening a web page, e.g. `https://my.site`
- etc.



The VPN Client only supports shell scripts with an `sh` extension or Z shell scripts with `zsh` extension.

To create a script that will open the TextEdit app, proceed as follows:

1. Create a script file named `openTextEdit.sh`, for instance.
2. Insert the following lines in the script file:

```
#!/bin/bash
open -a TextEdit
```

3. Run the following command to make the script file executable:

```
chmod a+x openTextEdit.sh
```

The TextEdit app will open before or after the tunnel opens, depending on the selected opening stage.

There are many possible applications, such as the following:

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

10 Managing dynamic parameters

If required, you can configure additional dynamic parameters for the macOS VPN Client under its IKE Auth (see section 7.2.5 IKE Auth: More parameters) and Child SA (see section 7.2.8 Child SA: More parameters) configuration.

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

Parameter	Usage	Scope
<code>local_subnet</code>	Specify IP address of network interface (see 7.3.1.1)	IKE Auth and TLS
<code>nonce_size</code>	Specify nonce size for IPsec DR gateways (see 7.2.2)	IKE Auth
<code>user_cert_dnpattern</code>	Select a certificate based on its subject (see 11.2.2.1)	IKE Auth and TLS
<code>user_cert_keyusage</code>	Select a certificate based on its "key usage" field (see 11.2.2.2)	IKE Auth and TLS
<code>check_pki</code>	Specify gateway certificate verification method (see Error! Reference source not found.)	IKE Auth and TLS
<code>VirtualInterfaceProfile</code>	Change the profile type of the connection to which the virtual card belongs (see 7.2.6.2)	Child SA and TLS
<code>interface_metric</code>	Apply a metric to the virtual interface (see 7.2.6.2)	Child SA and TLS
<code>local_virtual_network_size</code>	Specify virtual local network size (see 7.2.6.1)	Child SA
<code>allow_server_extra_keyusage</code>	Validate the certificate even if it does not comply with the constraints on the Key Usage extension (see 11.5)	IKE Auth and TLS
<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 11.5.3)	IKE Auth and TLS
<code>sha2_in_cert_req</code>	Use the SHA-2 hash algorithm in the certificate request payload (see 11.6.3)	IKE Auth
<code>Method14_RSASSA_PKCS1</code>	Use other certificate authentication methods (see 15.1.3)	IKE Auth
<code>use_method_214</code>	Use method 214 or method 14 for Brainpool user certificate authentication (see 15.1.3)	IKE Auth
<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 7.2.6.1)	Child SA

Parameter	Usage	Scope
<code>redundant_retry</code>	Define the maximum number of attempts to switch from the main gateway to the redundant gateway (see 8)	IKE Auth and 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.



11 Managing certificates

11.1 Introduction

The macOS VPN Client includes a selection of interfacing functions with various types of certificates, issued by any PKI and stored in files.

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

- Support for X.509 certificate formats: PKCS#12, PEM, PFX
- Management of certificates on user's side (the VPN Client's side), such as VPN gateway certificates, including validity dates, certificate chains, root certificates, and CRL management
- Certificate authority management
- Validation of client and gateway certificates: mutual authentication with identical or different certificate authorities (import specific CAs)

The certificates to be used are configured and specified on the **Certificate** tab of the tunnel concerned: IKE Auth (IKEv2) or TLS (SSL).

The following certificate types are supported:

- RSASSA-PKCS1-v1.5 with SHA-2 (only if the corresponding dynamic parameter has been configured, see section 15.1.3 Certificate authentication methods)
- RSASSA-PSS with SHA-2 (only if the corresponding dynamic parameter has been configured, see section 15.1.3 Certificate authentication methods)
- ECDSA "secp256r1" with SHA-2 (256 bits)
- ECDSA "BrainpoolP256r1" with SHA-2 (256 bits)



To find out more about the authentication methods and cryptography used in the macOS VPN Client, refer to section 15.1 Basic cryptography concepts in the appendix.

11.2 User certificate

11.2.1 Overview

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

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

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

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

11.2.2 Dynamic parameters for automatic certificate selection

As of version 2.5 of the macOS VPN Client, two dynamic parameters now replace the corresponding MSI properties. They are defined within the IKE_AUTH authentication payload and apply to a given tunnel, whereas the MSI properties apply to all tunnels.

11.2.2.1 `user_cert_dnpattern`

The dynamic parameter `user_cert_dnpattern` is used to specify the certificate to be used. When it is defined, the macOS VPN Client searches for the certificate whose subject contains the `[text]` pattern on the token, smart card or in the Windows certificate store.

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

11.2.2.2 `user_cert_keyusage`

The dynamic parameter `user_cert_keyusage` is used to select a certificate based on its “key usage” field.

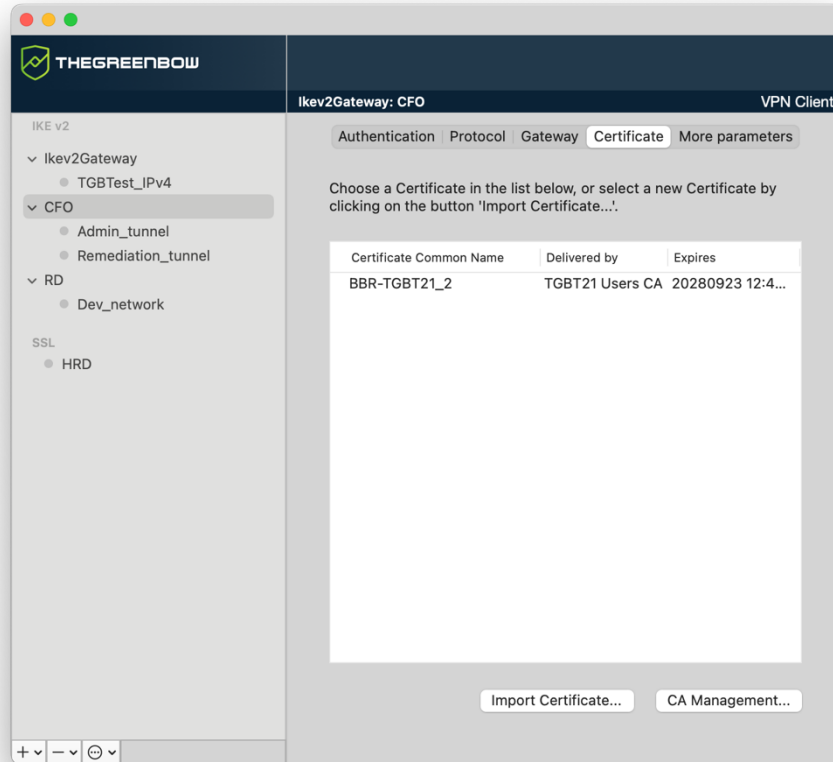
0 or undefined	Certificate is not selected based on “key usage” field.
1	Certificate is selected based on “key usage” field whose attribute <code>digitalSignature=1</code> .
2	Certificate is selected based on “key usage” field whose attributes <code>digitalSignature=1</code> and <code>keyEncipherment=1</code> .

11.3 Selecting a certificate (Certificate tab)

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

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

The **Certificate** tab shows the certificate currently used in the tunnel's configuration.



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.



As of version 2.4 of the macOS 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.



11.4 Importing a certificate

The macOS VPN Client can import certificates in PKCS#12 and PEM format to the VPN configuration.

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.

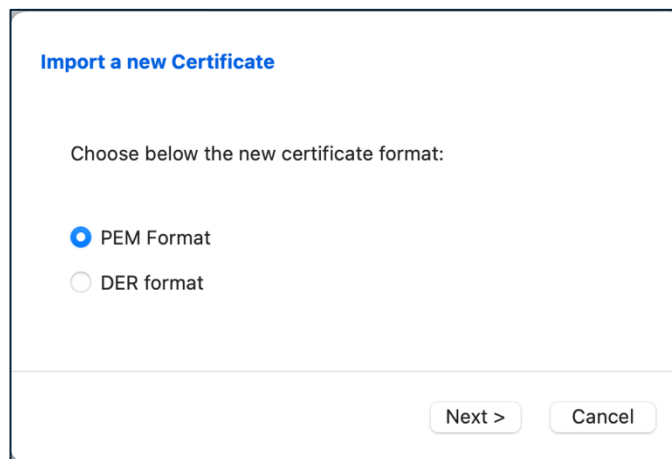
Nevertheless, the disadvantage of transporting certificates in a VPN configuration is that each configuration then becomes user-specific. We therefore do not recommend this solution for a substantial deployment.



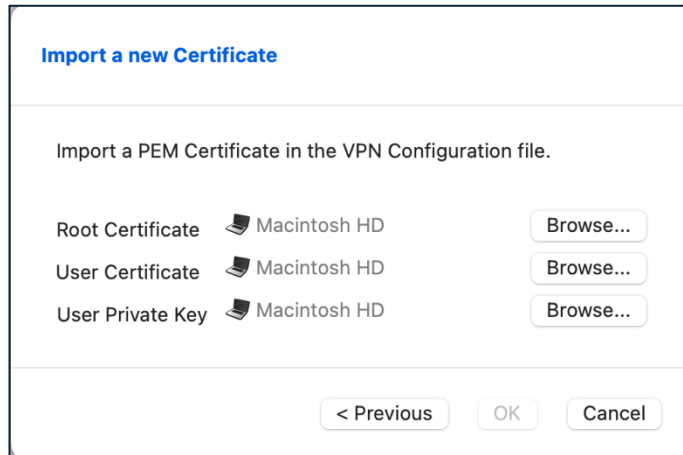
Whenever you import a certificate into a VPN configuration, we strongly recommend that you protect the configuration file with a password when you export it (see section 6.2 Exporting a VPN configuration) so that the certificate does not become visible in clear text.

11.4.1 Importing a PEM/PFX certificate

1. On the **Certificate** tab, click **Import Certificate....**



2. Choose the **PEM Format**, and then click **Next >**.



3. Click **Browse** to select the **Root Certificate**, the **User Certificats** and 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.

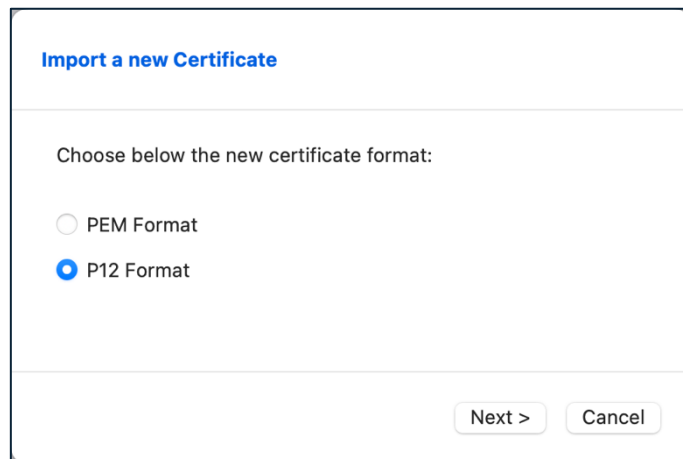
Save the VPN configuration. The certificate will be saved in the VPN configuration.



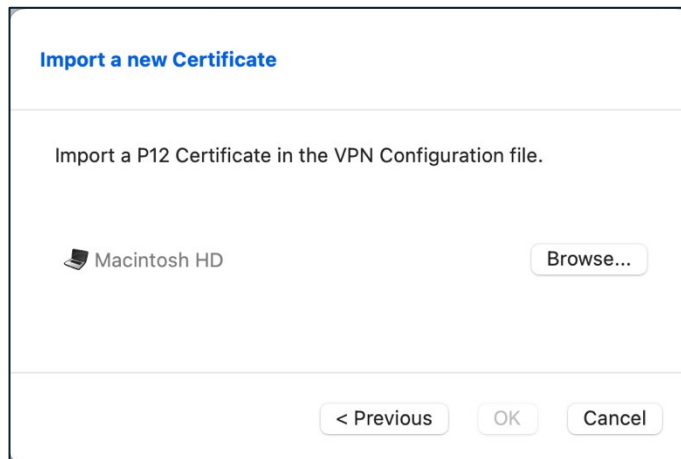
The file containing the private key may not be encrypted.

11.4.2 Importing a PKCS#12 certificate

1. On the **Certificate** tab, click **Import Certificate....**



2. Choose the **P12 Format**, and then click **Next >**.



3. Click **Browse** to select the PKCS#12 certificate to import.
4. If it is password-protected, enter the password and then 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.



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

11.5 VPN gateway certificate



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



See sections 7.2.3 IKE Auth: Gateway and 7.3.3 SSL: Gateway.

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.

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)

11.5.1 Specify gateway certificate verification method

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, certification chain, signature and CRL of each certificate in the certification 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. It must never be disabled in a production environment or in any context involving sensitive security requirements.

11.5.2 Constraints on the Key Usage extension

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

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

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`.

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

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

11.5.3 Constraints on the Extended Key Usage extension

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

- Be present
- Be marked as non-critical, and
- Only contain the value `id-kp-serverAuth`

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`.

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

- `id-kp-ServerAuth + id-kp-ClientAuth`

11.6 Managing certificate authorities

11.6.1 Overview

The macOS VPN Client systematically authenticates the client and gateway certificates based on the certificate authorities (CAs) available in the VPN configuration. You must therefore import the CA certificates into the VPN Client.

If the macOS 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.

The following intermediate CA types are supported:

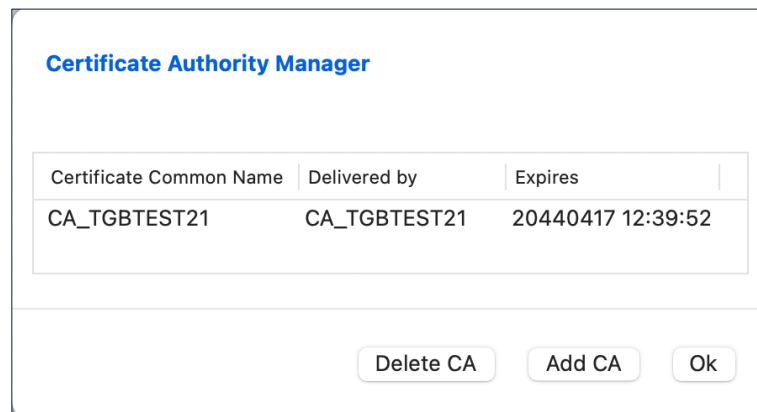
- RSASSA-PKCS1-v1.5 with SHA-2
- RSASSA-PSS with SHA-2
- ECDSA “secp256r1” with SHA-2
- ECDSA “BrainpoolP256r1” with SHA-2

The following root CA types are supported:

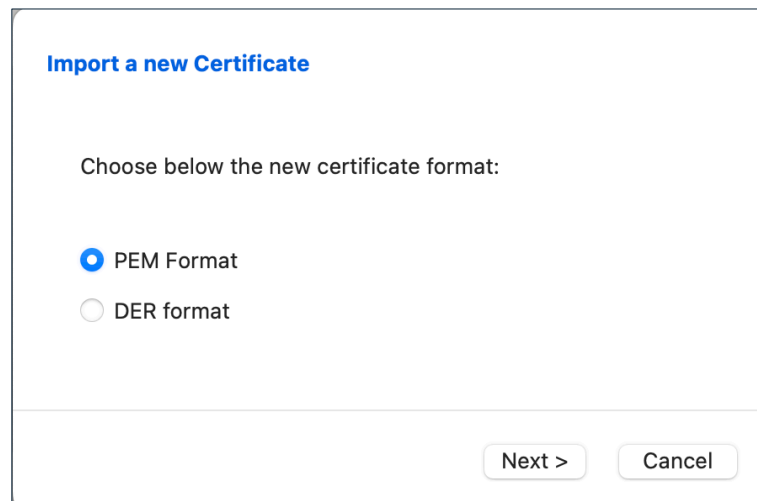
- RSASSA-PKCS1-v1.5 with SHA-2
- RSASSA-PSS with SHA-2
- ECDSA “secp256r1” with SHA-2
- ECDSA “BrainpoolP256r1” with SHA-2

11.6.2 Importing a certificate authority

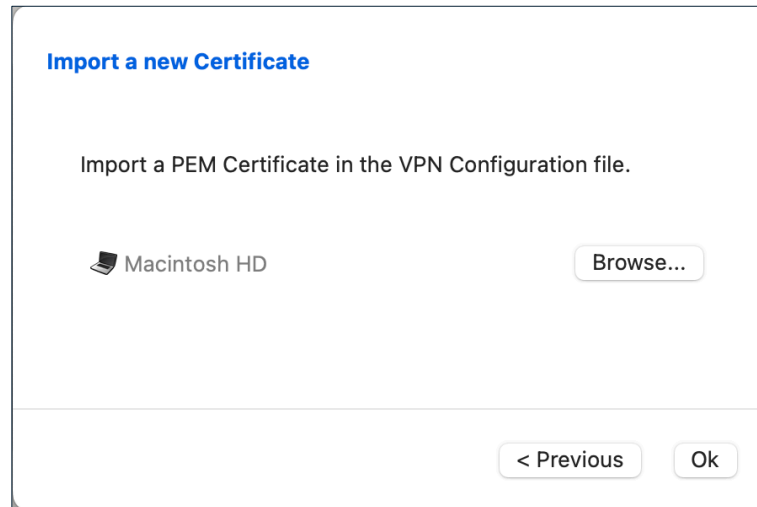
5. On the **Certificate** tab, click **CA Management**, the **Certificate Authority Manager** dialog box is displayed.



6. Click **Add CA**. The **Import a new Certificate** dialog box is displayed.



7. Choose the desired CA certificate type (PEM or DER), then click **Next >**.



8. Click **Browse** and then select the CA to import.

11.6.3 IPsec DR mode

To be able to use the macOS 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.

To achieve this, you must add the dynamic parameter `sha2_in_cert_req` set to the value `true` (see section 7.2.8 Child SA: More parameters).



To find out how to configure the macOS 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.

12 Logs

The macOS VPN Client comes equipped with three types of logs:

1. The macOS **Console**, which provides information on the various steps performed when opening and closing tunnels
2. The trace mode, which provides detailed information
3. System logs, which record general events, such as tunnels opened or closed

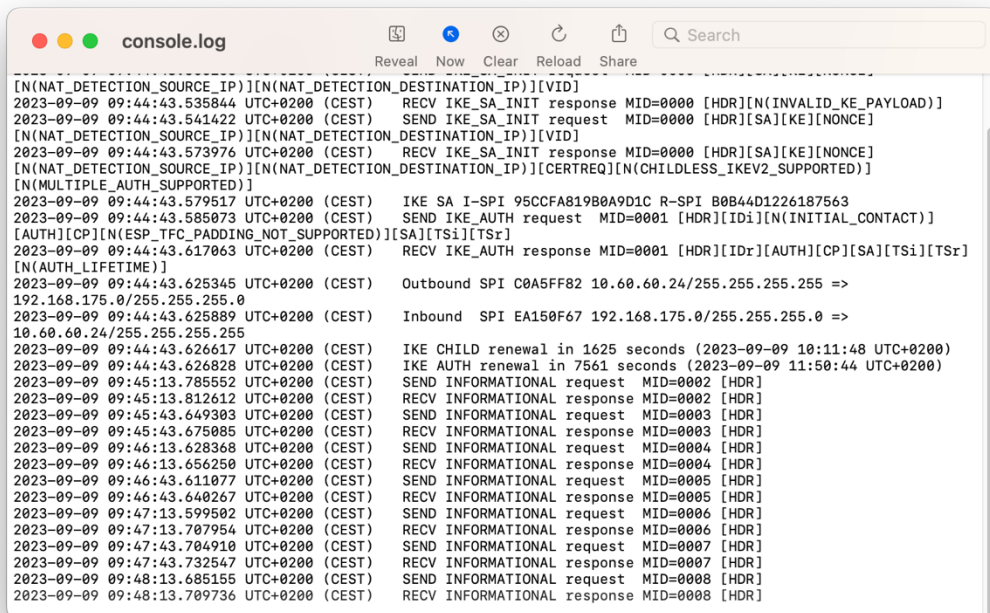
This facility is intended to help network administrators diagnose a problem when opening tunnels, or the TheGreenBow support team to identify software incidents.

12.1 Console

You can display the Console in either of the following ways:

- In the **Configuration Panel** (main interface), from the **View** menu, choose **Console**
- Use the **⌘D** shortcut when the **Configuration Panel** is open

This will open the `console.log` file in the native macOS **Console**.

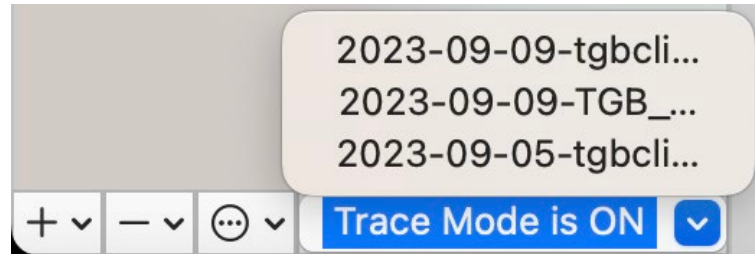


```

-----
[N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][VID]
2023-09-09 09:44:43.535844 UTC+0200 (CEST)  RECV IKE_SA_INIT response MID=0000 [HDR][N(INVALID_KEY_PAYLOAD)]
2023-09-09 09:44:43.541422 UTC+0200 (CEST)  SEND IKE_SA_INIT request  MID=0000 [HDR][SA][KE][NONCE]
[N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][VID]
2023-09-09 09:44:43.573976 UTC+0200 (CEST)  RECV IKE_SA_INIT response MID=0000 [HDR][SA][KE][NONCE]
[N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][CERTREQ][N(CHILDLESS_IKEV2_SUPPORTED)]
[N(MULTIPLE_AUTH_SUPPORTED)]
2023-09-09 09:44:43.579517 UTC+0200 (CEST)  IKE SA I-SPI 95CCFA819B0A9D1C R-SPI B0B44D1226187563
2023-09-09 09:44:43.585073 UTC+0200 (CEST)  SEND IKE_AUTH request  MID=0001 [HDR][IDi][N(INITIAL_CONTACT)]
[AUTH][CP][N(ESP_TFC_PADDING_NOT_SUPPORTED)][SA][TSi][TSr]
2023-09-09 09:44:43.617063 UTC+0200 (CEST)  RECV IKE_AUTH response MID=0001 [HDR][IDr][AUTH][CP][SA][TSi][TSr]
[N(AUTH_LIFETIME)]
2023-09-09 09:44:43.625345 UTC+0200 (CEST)  Outbound SPI C0A5FF82 10.60.60.24/255.255.255.255 =>
192.168.175.0/255.255.255.0
2023-09-09 09:44:43.625889 UTC+0200 (CEST)  Inbound  SPI EA150F67 192.168.175.0/255.255.255.0 =>
10.60.60.24/255.255.255.255
2023-09-09 09:44:43.626617 UTC+0200 (CEST)  IKE CHILD renewal in 1625 seconds (2023-09-09 10:11:48 UTC+0200)
2023-09-09 09:44:43.626828 UTC+0200 (CEST)  IKE AUTH renewal in 7561 seconds (2023-09-09 11:50:44 UTC+0200)
2023-09-09 09:45:13.785552 UTC+0200 (CEST)  SEND INFORMATIONAL request  MID=0002 [HDR]
2023-09-09 09:45:13.812612 UTC+0200 (CEST)  RECV INFORMATIONAL response MID=0002 [HDR]
2023-09-09 09:45:43.649303 UTC+0200 (CEST)  SEND INFORMATIONAL request  MID=0003 [HDR]
2023-09-09 09:45:43.675085 UTC+0200 (CEST)  RECV INFORMATIONAL response MID=0003 [HDR]
2023-09-09 09:46:13.628368 UTC+0200 (CEST)  SEND INFORMATIONAL request  MID=0004 [HDR]
2023-09-09 09:46:13.656250 UTC+0200 (CEST)  RECV INFORMATIONAL response MID=0004 [HDR]
2023-09-09 09:46:43.611077 UTC+0200 (CEST)  SEND INFORMATIONAL request  MID=0005 [HDR]
2023-09-09 09:46:43.640267 UTC+0200 (CEST)  RECV INFORMATIONAL response MID=0005 [HDR]
2023-09-09 09:47:13.599502 UTC+0200 (CEST)  SEND INFORMATIONAL request  MID=0006 [HDR]
2023-09-09 09:47:13.707954 UTC+0200 (CEST)  RECV INFORMATIONAL response MID=0006 [HDR]
2023-09-09 09:47:43.704910 UTC+0200 (CEST)  SEND INFORMATIONAL request  MID=0007 [HDR]
2023-09-09 09:47:43.732547 UTC+0200 (CEST)  RECV INFORMATIONAL response MID=0007 [HDR]
2023-09-09 09:48:13.685155 UTC+0200 (CEST)  SEND INFORMATIONAL request  MID=0008 [HDR]
2023-09-09 09:48:13.709736 UTC+0200 (CEST)  RECV INFORMATIONAL response MID=0008 [HDR]
    
```

12.2 Trace mode

Trace mode can be enabled or disabled using the $\mathbb{H}\uparrow T$ key combination. A new button will be shown below the list of VPN tunnels. This button allows you to view the list of detailed logs that are available.



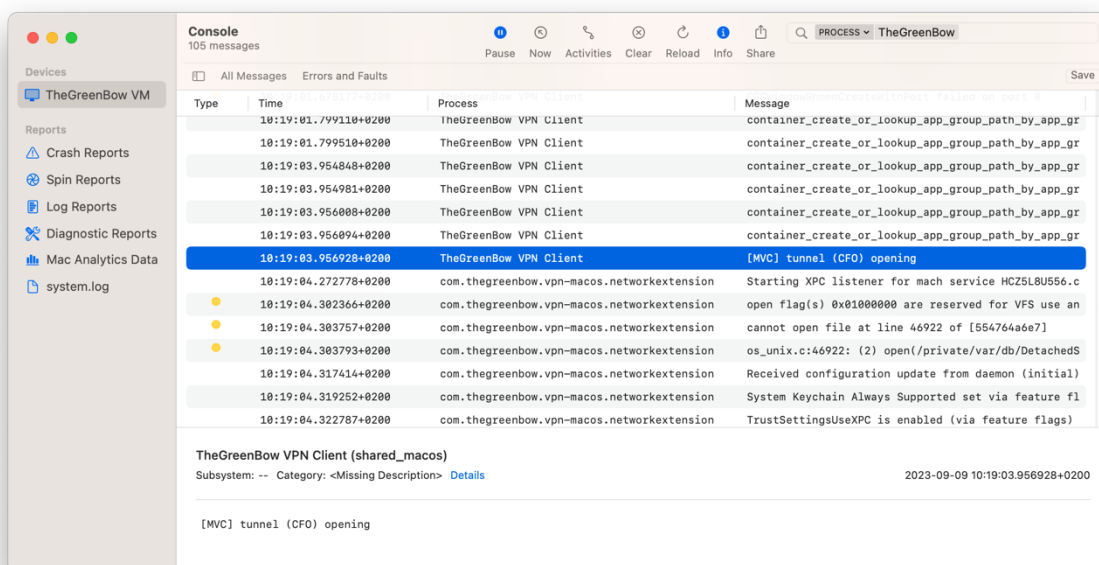
Once you select a detailed log, it will be displayed in the macOS Console application.

12.3 System logs

System logs are displayed by default when you open the macOS Console.

Be sure to select the generic **Console** window and not one of the specific ones (e.g. the one you opened to display the `console.log` file as described in section 12.1 Console or in section 12.2 Trace mode above).

In the macOS **Console** application, you can filter messages from the VPN process `TheGreenBow VPN` using the following terms: `Process: TheGreenBow VPN Client` or `Process: com.thegreenbow.vpn-macos.networkextension`.



13 Security recommendations

13.1 Assumptions

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

13.1.1 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.

13.1.2 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.

13.1.3 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).

13.2 User workstation

The machine on which the macOS 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)

13.3 VPN configuration

13.3.1 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 7.2.1.2 Authentication).
- Do not import any certificates to the VPN configuration (function described in section 11.4 Importing a certificate).
- Do not export the VPN configuration without encrypting it, i.e. not password-protected (function described in section 6.2 Exporting a VPN configuration).

13.3.2 User authentication

The user authentication functions available in the macOS 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	Strong

13.3.3 VPN gateway authentication

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 the dynamic parameter `allow_server_and_client_auth`).

13.3.4 Protocol

We recommend that you only configure IPsec/IKEv2 tunnels (and no SSL/OpenVPN tunnels).

13.3.5 ANSSI recommendations

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

14 Contact

14.1 Information

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

14.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

14.3 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/>.



15 Appendixes

15.1 Basic cryptography concepts

15.1.1 SHA, RSA, and ECDSA 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 or ECDSA: Elliptic Curve 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 macOS 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”.

15.1.2 Certificate format

As of version 2.4 of the macOS 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

15.1.2.1 Gateway certificate

Key Usage extension part

- Must be present
- Must be marked as critical, and
- Must only contain the values `digitalSignature` and/or `keyEncipherment`



If this is not the case, refer to the dynamic parameter `allow_server_extra_keyusage` described in section 11.5.2 Constraints on the Key Usage extension.

Extended Key Usage extension part

- Must be present present
- Must be marked as non-critical, and
- Must only contain the value `id-kp-serverAuth`



If this is not the case, refer to the dynamic parameter `allow_server_and_client_auth` described in section 11.5.3 Constraints on the Extended Key Usage extension.

15.1.2.2 Example of a certificate log

The extensions are included in a certificate log (file named `tg bikeng.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
```

15.1.2.3 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.

15.1.3 Certificate authentication methods

The macOS 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 and RSASSA-PKCS1-v1_5 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 7.2.8 Child SA: More parameters).

In the event that the gateway does not support method 14 with an RSASSA-PKCS1-v1_5 signature, you can configure the VPN Client to use method 1 with an RSA and SHA-2 digital signature, by adding the dynamic parameter `Method1_PKCS1v15_Scheme` with a value set to `04` (SHA-256), `05` (SHA-384), or `06` (SHA-512) (see section 7.2.8 Child SA: More parameters). The VPN Client will reject any other value entered.

The authentication method used for ECDSA certificates (elliptical curves) depends on the elliptical curve used in the certificate: ECDSA with SHA-256 on the P-256 curve, ECDSA with SHA-384 on the P-384 curve, ECDSA with SHA-512 on the P-521 curve or ECDSA with SHA-256 on the BrainpoolP256r1 curve.

When the VPN Client needs to create a signature for a Brainpool user certificate, authentication method 14 is used by default, which is appropriate for a gateway that is not running in IPsec DR mode. If this type of certificate

is to be used with a gateway running in IPsec DR mode, the dynamic parameter `use_method_214` must be added and set to the value `true` (see chapter 10 Managing dynamic parameters). The digital fingerprint algorithm `NID_sha256`, `NID_sha384`, or `NID_sha512` is used to sign depending on the size of the key.



SHA-1 algorithm cannot be used in digital signatures.



The macOS VPN Client will reject RSA certificates with a key size of less than 2048 bits.



The macOS VPN Client will reject ECDSA certificates with a key size of less than 256 bits.

15.2 macOS VPN Client technical data

15.2.1 Main functions

- Configure and establish IPsec/IKEv2 VPN connections
- Manage authentication using EAP or a certificate
- Manage the Configuration Payload (CP) mode
- Implement Dead Peer Detection (DPD) and manage a redundant gateway
- Comprehensive and intuitive configuration interface
- Configure and establish SSL/OpenVPN connections

15.2.2 Languages

French, English, Arabic, Czech, Danish, German, Greek, Spanish, Finnish, Hungarian, Hindi, Italian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Romanian, Slovenian, Bosnian, Thai, Turkish, Chinese, Farsi.

15.2.3 Compatible OSes

The minimum operating system required for the macOS VPN Client is macOS 10.15.

15.2.4 Cryptography and authentication

Encryption, Key group, Hashing (IKEv2)	<p>Symmetric: AES CBC, GCM, CTR 128/192/256-bit</p> <p>Diffie-Hellmann: 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)</p> <p>Hashing: SHA-2 (256/384/512 bits)</p>
TLS security suites (OpenVPN)	<p>TLS 1.2—Medium</p> <p>TLS 1.2—High</p> <p>TLS 1.3:</p> <ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256
Encryption, Hashing (OpenVPN)	<p>Symmetric: AES-128-CBC, AES-192-CBC, AES-256-CBC</p> <p>Hashing: SHA-2 (224/256/384/512 bits)</p>
Authentication	<ul style="list-style-type: none"> • Preshared key • EAP-MSCHAPv2 • X.509 certificates • Multiple Auth
Certificate authentication methods	<ul style="list-style-type: none"> • Method 1: RSA Digital Signature with SHA-2 [RFC 7296] • Method 9: ECDSA “secp256r1” with SHA-2 (256 bits) on the P-256 curve [RFC 4754] • Method 10: ECDSA “secp384r1” with SHA-2 (384 bits) on the P-384 curve [RFC 4754] • Method 11: ECDSA “secp521r1” with SHA-2 (512 bits) on the P-521 curve [RFC 4754] • Method 14: Digital Signature RSASSA-PSS and RSASSA-PKCS1-v1_5 with SHA-2 (256/384/512 bits) [RFC 7427] • Method 214: ECDSA “BrainpoolP256r1” with SHA-2 (256 bits) on the BrainpoolP256r1 curve (only available with gateways that support this method)
PKI	<ul style="list-style-type: none"> • Support for certificates in X.509 format • Importing PKCS#12, PEM/PFX certificates • Complete check of the “user” and “gateway” certificate chain

Secure your connections
in all circumstances

28, rue Caumartin
75009 Paris - France
sales@thegreenbow.com

www.thegreenbow.com