



STORMSHIELD



STORMSHIELD NETWORK SECURITY
STORMSHIELD NETWORK VPN CLIENT STANDARD

GUIDE

Version 6

Document last update: April 27, 2021

Reference: sns-en-vpn_client-user-guide



Table of contents

- Presentation 6
 - The universal VPN Client 6
 - Compatible with all VPN gateways 6
 - VPN on all network types 6
 - VPN IPsec and SSL 6
 - VPN compatible with all PKI 6
 - VPN integrable in any infrastructure 7
 - VPN in 25 languages 7
 - New functions 7
 - Technical characteristics 7
- Installation 9
 - Installation 9
 - Installation conditions 9
 - Evaluation period 9
- Activation 11
 - Step 1 11
 - Step 2 11
 - Activation error 11
 - Manual activation 12
 - Manual activation on the TheGreenBow activation server 13
 - License and activated software 14
- Update 15
 - Obtaining an update 15
 - Updating the VPN security policy 15
 - Automation 16
- Uninstallation 17
- Quick use 18
 - Configuring a VPN tunnel 18
 - Open a VPN tunnel automatically 18
- Configuration wizard 19
 - Step 1 19
 - Step 2 for an IKEv1 VPN tunnel 20
 - Step 2 for an IKEv2 VPN tunnel 21
 - Step 2 for SSL (OpenVPN) tunnel 21
 - Step 3 22
- User interface 24
 - User interface 24
 - Windows desktop 24
 - Start menu 24
 - Desktop 24
 - Taskbar 24
 - Icon 24
 - Menu 25



- Fade-out popup 25
- Connection panel 27
- Configuration panel 29
 - Menus 29
 - Status bar 30
 - Shortcuts 30
 - VPN tunnel tree 30
 - Use 30
 - Contextual menus 32
 - Shortcuts 34
- Import/export a VPN security policy 35
 - Importing a VPN security policy 35
 - Importing the General Settings (IKEv1 only) 36
 - Exporting a VPN security policy 36
 - Merge VPN security policies 37
 - Split a VPN security policy 37
- Configure a VPN tunnel 38
 - IPsec IKEv1, IPsec IKEv2 or SSL VPN 38
 - Edit and save the VPN configuration 38
 - Configure an IPsec IKEv1 tunnel 39
 - Phase 1: Authentication 39
 - Phase 1: Protocol 42
 - Phase 1: Gateway 44
 - Phase 1: Certificate 45
 - Phase 2: IPsec 46
 - Phase 2: Advanced 48
 - Phase 2: Automation 49
 - Phase 2: Remote sharing 49
 - IKE V1 Parameters 49
 - Configure an IPsec IKEv2 tunnel 50
 - IKE Auth: IKE SA 50
 - IKE Auth: Gateway 53
 - IKE Auth: Certificate 54
 - Child SA: Introduction 55
 - Child SA: Child SA 55
 - Child SA: Advanced 57
 - Child SA: Automation 58
 - Child SA: Remote sharing 58
 - Configure an SSL VPN tunnel 58
 - Introduction 58
 - Authentication 59
 - Security 59
 - Gateway 61
 - Establishment 63
 - Automation 64
 - Certificate 64
 - Remote sharing 64
- Redundant Gateway 65



- Automation 66
- VPN tunnel fallback 69
- IPv4 and IPv6 70
- Certificate management 71
 - Configuration 72
 - Select a certificate ("Certificate" tab) 72
 - Importing a certificate 73
 - Windows Certificate Store 75
 - CA (Certification Authority) Management 75
 - Using a VPN tunnel with a smart card certificate 76
- Remote desktop sharing 77
 - Remote desktop sharing configuration 77
- Connection panel management 78
- USB mode 80
 - VPN USB mode 80
 - Configuring USB mode 81
 - Step 1: Choosing a USB Drive 81
 - Step 2: Protecting the VPN USB security policy 82
 - Step 3: Automatically opening the tunnel 82
 - Step 4: Summary 83
 - Using the USB mode 83
- GINA mode 85
 - GINA mode 85
 - Configuring GINA mode 85
 - Using GINA mode 85
- Controlling access to the VPN policy 87
- Options 89
 - Access control 89
 - Interface display (masking) 89
 - General 89
 - Log management 90
 - PKI options 91
 - Language management 91
 - Choosing a language 91
 - Editing or creating a language 91
- Administrator logs, console and tracing 94
 - Administrator logs 94
 - Console 96
 - Tracing mode 96
 - Note for the administrator 96
- Security recommendations 98
 - Recommendations 98
 - General recommendations 98



- Operating precautions 98
- VPN Client administration 99
- VPN security policy configuration 99
- User authentication 99
- VPN gateway authentication 100
- IKE protocol 100
- GINA mode 100
- ANSSI IPsec configuration recommendations 100
- Appendices 101**
 - Shortcuts 101
 - Languages 101
 - Administrator logs 102
 - Technical characteristics of Stormshield VPN Client 103
 - License and credits 105
- Contact 109**

In the documentation, Stormshield Network VPN Client Standard is referred to in its short form: SN VPN Client Standard.

This document is not exhaustive and minor changes may have been included in this version.



Presentation

The Stormshield VPN Client is based on the TheGreenBow VPN Client software and the present guide therefore derives from the official TheGreenBowUser Guide.

All images in this document are for representational purposes only. They are based on the Stormshield VPN Client version and the actual Stormshield product may differ.

The universal VPN Client

Stormshield VPN Client is a universal VPN software for securing remote connections to a company's information system.



This User Guide is about the Windows version of Stormshield VPN Client.

Compatible with all VPN gateways

Stormshield VPN Client can create secure connections (VPN tunnels) with all VPN gateways on the market.

VPN on all network types

Stormshield VPN Client can secure and maintain communications on all network types: 3G, 4G, Wi-Fi, Ethernet, ADSL, Satellite, etc. It is designed and strengthened specifically to ensure performance on even the least reliable networks.

VPN IPsec and SSL

Stormshield VPN Client implements several VPN protocols: it can simultaneously open IPsec IKEv1 and IKEv2 VPN connections as well as SSL VPN connections. All VPN connections can be established on IPv4 or IPv6.

Since the release of version 6.6, the "tunnel fallback" function automatically switches from one protocol to the next if the one currently in use fails.

VPN compatible with all PKI

Stormshield VPN Client can use certificates issued by all PKIs. It is equipped with an extended set of parameters allowing for the characterization of certificates as well as their storage media such as token, smart card or certificate store.



VPN integrable in any infrastructure

Stormshield VPN Client is specifically designed for integration in any existing infrastructure.

On the one hand, it implements an extended set of deployment features, both for the software itself (software and updates) and the VPN configurations (VPN security policies), such as scriptable installation options, installation customization, etc.

On the other hand, it also implements a wide array of logs that can be used by any security information and event management (SIEM) system.

VPN in 25 languages

Used all over the world, Stormshield VPN Client is available in 25 languages and is equipped with an interface translation tool as a standard feature.

New functions

For a better user experience and to increase the integration and deployment of the software, Stormshield VPN Client is equipped with several new functions:

- Customizable user interface (to the point of invisibility)
- USB Mode that makes opening a tunnel subject to the insertion of a VPN USB Drive
- Comprehensive configuration of the software before deployment
- Set of options to run the software using command lines (through scripts)
- Making RDP (Remote Sharing Desktop) connections secure and automatic
- Possibility to associate scripts to the opening and closing of a tunnel
- Ways to stabilize the VPN tunnel on unstable networks
- Generation of administrator logs

Technical characteristics

Stormshield VPN Client takes into account all the characteristics required to ensure a maximum and reliable security of the connections:

- VPN tunnel on any medium: Ethernet, Wi-Fi, 3G/4G, satellite, etc.
- Automatic opening of tunnels (traffic detection, automatic, etc.)
- GINA mode (opening a tunnel before Windows logon)
- DPD and redundant gateway management (automatic switch)
- Creating VPN tunnels in point-to-point or point-to-gateway modes
- "Disable Split Tunneling" mode
- "All through the tunnel" mode
- "Tunnel fallback" function
- Nested tunnels
- IKEv1, IKEv2
- IPsec or SSL
- IPv4 or IPv6 for the tunnel and transport
- X-Auth, Mode Config/CP Mode



- Preshared Key, Certificates X509 or PKCS12
- PKCS11 or CSP tokens or smart cards management

For detailed specifications, see chapter [technical characteristics of Stormshield VPN Client](#).



Installation

Installation

The installation of Stormshield VPN Client is carried out by executing the downloadable program on the [Mystormshield](#) website:

Stormshield-vpn-x.xx.xxx.exe

Installation is a standard procedure that does not require any input from the user.

The software installation is customizable through a set of command-line options and configuration files.

Installation conditions

Stormshield VPN Client is compatible with several Windows versions. Compatible versions are listed in the [technical characteristics of Stormshield VPN Client](#).

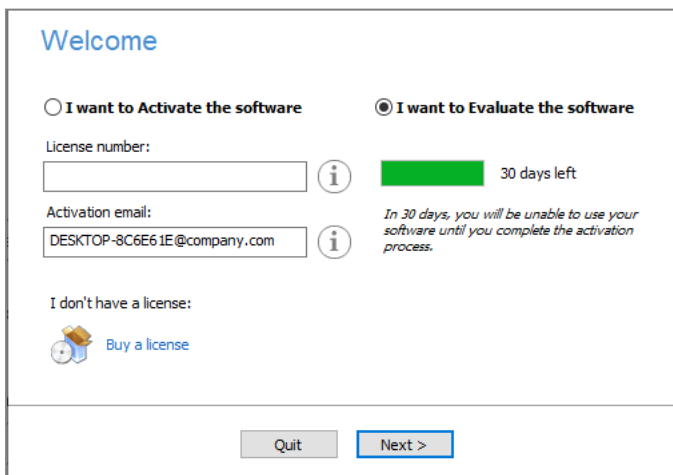
In order to install the software on Windows Vista, 7, 8 or 10, administrator rights are required. A warning will be displayed to the user if this condition is not met.

The certified version of Stormshield VPN Client will verify its own integrity. Should the program be corrupted, the software will not be executed and the user will be alerted.

Evaluation period

When installed for the first time on a workstation, the software will enter a evaluation period of 30 days. During this evaluation period, the VPN Client is fully operational and all functions are unlocked.

During the evaluation period, the activation window will be displayed every time the software is launched. This window will display the number of remaining days in the evaluation period.

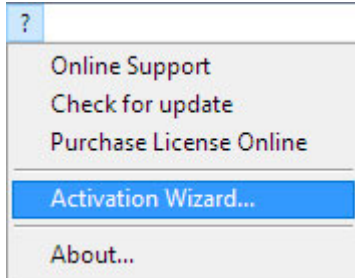


Select "I want to Evaluate the software" then "Next >" to run the software.



During the evaluation period, the "About..." window will display the number of remaining days until the end of the evaluation period.

During the evaluation period, it remains possible to access the activation window through the "? > Activation wizard" menu of the main interface (Configuration panel).





Activation

Stormshield VPN Client must be activated in order to run after the end of the evaluation period.

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

Step 1

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

In order to get the license number, click on "Buy a license".

The license number can be copy-pasted directly from the purchase confirmation email into this field.

The license number is only composed of the characters [0..9] and [A..F], sometimes in groups of 6 characters and separated by hyphens.

In the "Activation email" field, type in the email address used for identifying your activation. This information is used for recovering the activation information if lost.

Step 2

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

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

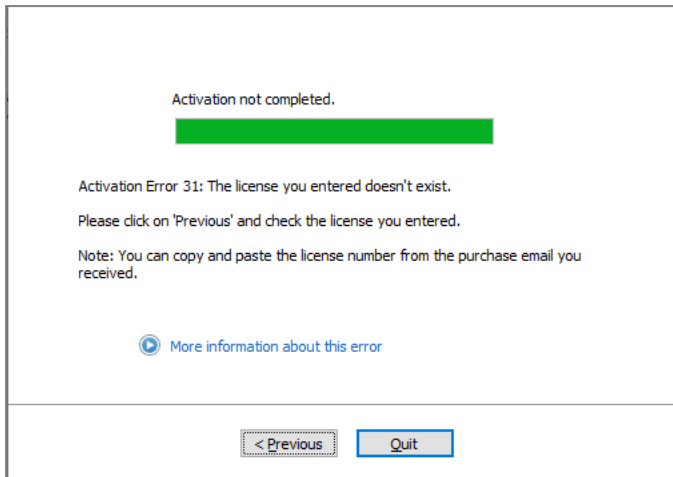
i NOTE

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

By the same token, a license number activation can be cancelled by simply uninstalling the software.

Activation error

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 suggest operations to solve the problem.



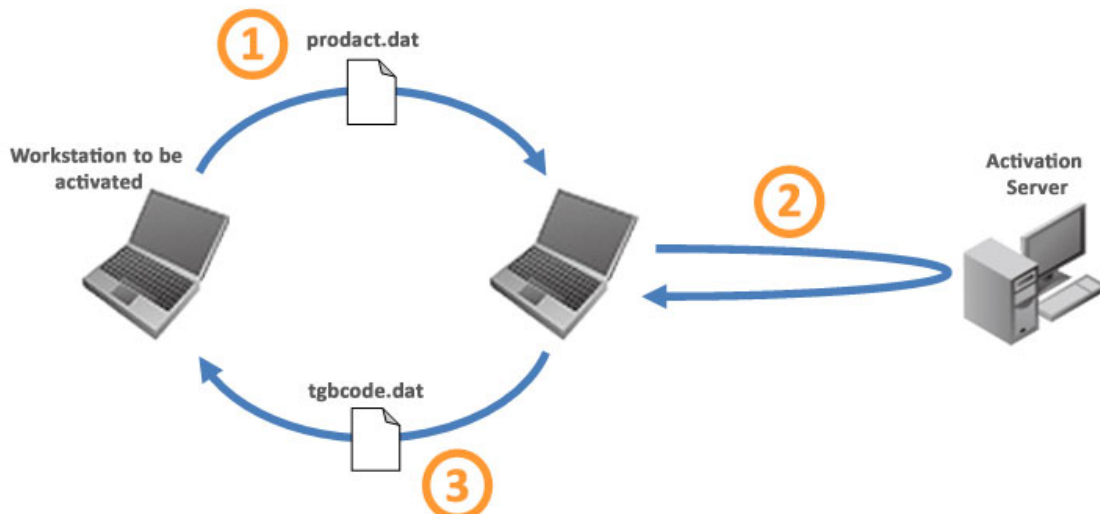
TheGreenBow lists all activation errors and [procedures for solving activation issues](#) on its website.

The most common activation errors are:

#	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.

Manual activation

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





- ① "product.dat" file Get the "product.dat" file in the "My Documents" Windows directory on the workstation that should be activated. [1]
- ② Activation On a workstation connected to the activation server [2], open the manual activation page [3] and post there the "product.dat" file. Get the tgbcode file automatically created by the server.
- ③ "tgbcode" file Copy the "tgbcode" file in the "My Documents" Windows directory on the workstation that should be activated. Launch the software; it will be activated.

[1] The "product.dat" file is a text file that contains the workstation's information used for the activation. If this file does not exist in the "My Documents" directory, activate the software on the workstation. Even if activation fails, this file will be generated.

[2] The activation server is the TheGreenBow server, which can be accessed on the internet.

[3] See the detailed procedure below.

Manual activation on the TheGreenBow activation server

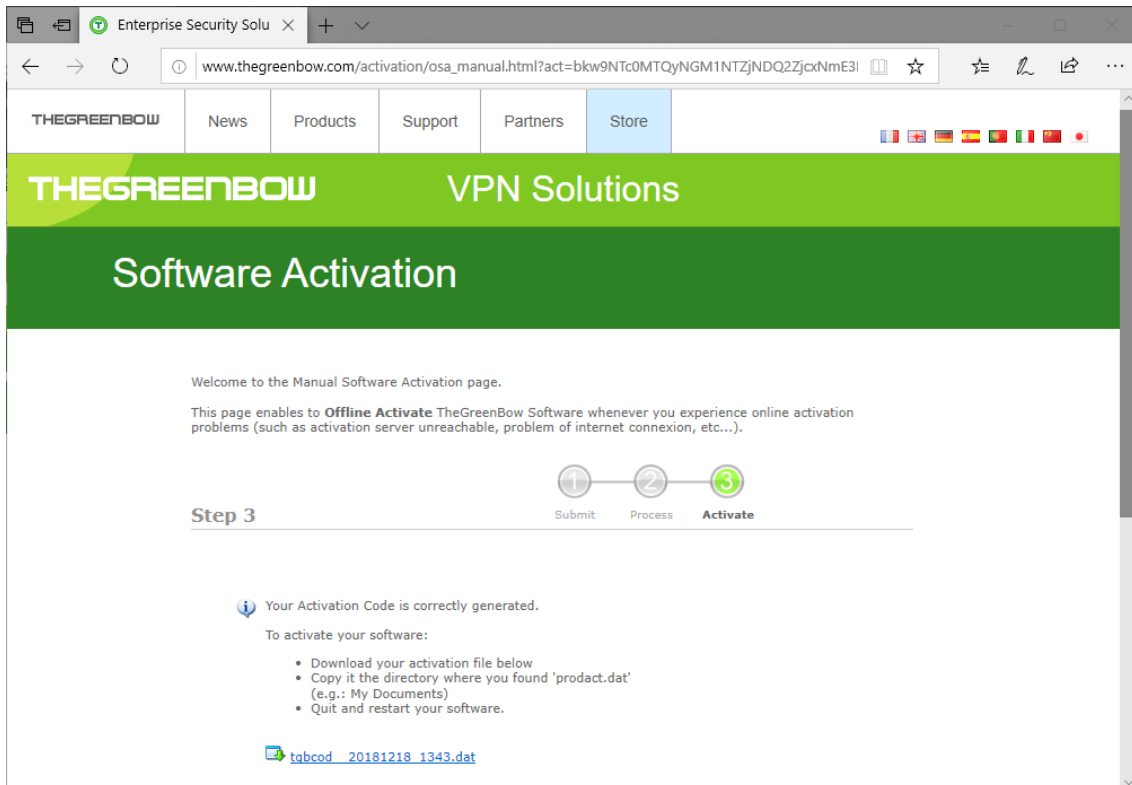
Open the following webpage: http://www.thegreenbow.com/activation/osa_manual.html

Click "Browse" and open the "product.dat" file created on the workstation that should be activated.

Click "Submit". The activation server will check the validity of the information contained in the "product.dat" file.

Click "Proceed".

The activation server will provide a link download a file that contains the activation code for the workstation that should be activated.





The name of this file has the following format: `tgbcod_[date]_[code].dat` (for example: `tgbcod_20120625_1029.dat`).

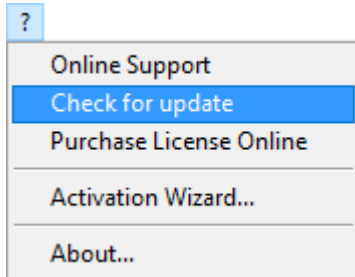
License and activated software

When the software is activated, the license and email used for activation can be verified in the "About..." window of the software.



Update

The software also gives the possibility to check at any time whether an update is available through the main interface menu "? > Check for update".



This menu opens the [Mystormshield](#) webpage.

Obtaining an update

Getting an update follows the rules below:

During the maintenance period (1)	All updates can be installed
Outside of the maintenance period or no maintenance at all	All minor updates can be installed (2)
During subscription (3)	All updates can be installed

- (1) The maintenance period starts when the software is activated for the first time.
- (2) Minor updates (or maintenance updates) are identified by the last digit of the version number, e.g. the "2" in "6.12".
- (3) For VPN Premium or VPN Certified versions.

EXAMPLE

I activated the software in its 6.12 version. My maintenance period is expired.
All updates from versions 6.13 to 6.19 are authorized.
All updates from versions 6.20 and above will be denied.

Updating the VPN security policy

During an update, the VPN security policy (VPN configuration) is automatically backed up and restored.

NOTE

If access to the VPN security policy is protected with a password, it must be entered during update to authorize restoring the configuration.



Automation

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



Uninstallation

In order to uninstall Stormshield VPN Client:

1. Open the Windows Control panel
2. Select "Add/Uninstall programs"

Or

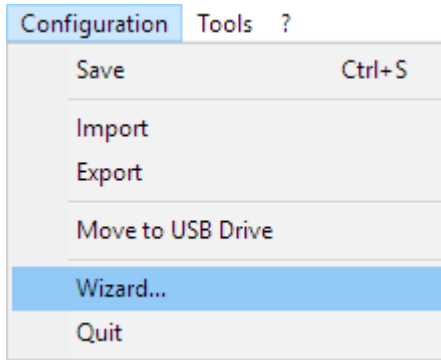
1. Open the "Start" menu on Windows
2. Select "Programs" > "Stormshield" > "Stormshield VPN Client" > "Network VPN Client Uninstall"



Quick use

Configuring a VPN tunnel

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



Use the wizard as described in the section [Configuration Wizard](#) below.

Open a VPN tunnel automatically

Stormshield VPN Client gives the possibility to open a VPN tunnel automatically by different means:

- 1/ A VPN tunnel can open automatically when traffic headed towards the remote network is detected. See Section "[Automation](#)"
- 2/ A tunnel can be opened automatically when opening (double-clicking) a VPN security policy (.tgb file). See Section "[Automation](#)"
- 3/ A tunnel can be opened automatically when inserting a USB Drive containing the relevant VPN security policy. See Section "[USB mode](#)"
- 4/ A VPN tunnel can be opened automatically when the smart card (or token) containing the certificate used for this tunnel is inserted. See Section "[Using a VPN tunnel with a smart card certificate](#)"

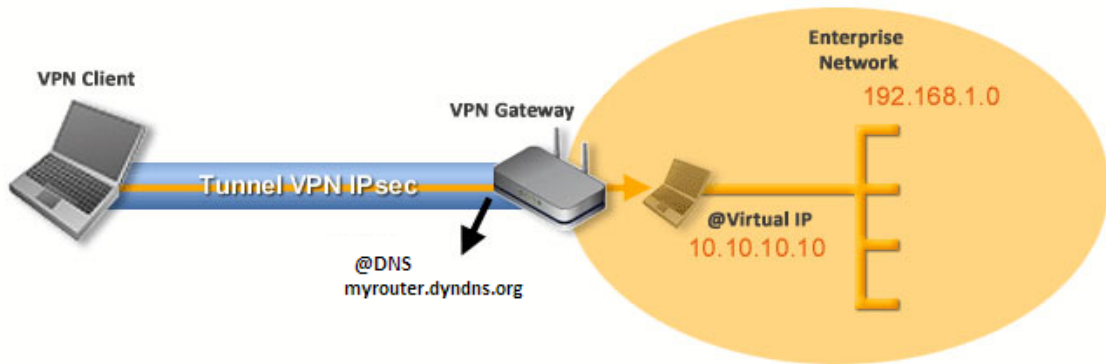


Configuration wizard

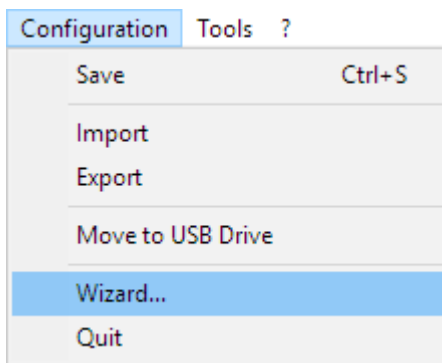
The Stormshield VPN Client configuration wizard gives the possibility to configure a VPN tunnel in 3 simple steps.

The operation of the Configuration wizard is illustrated in the example below:

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

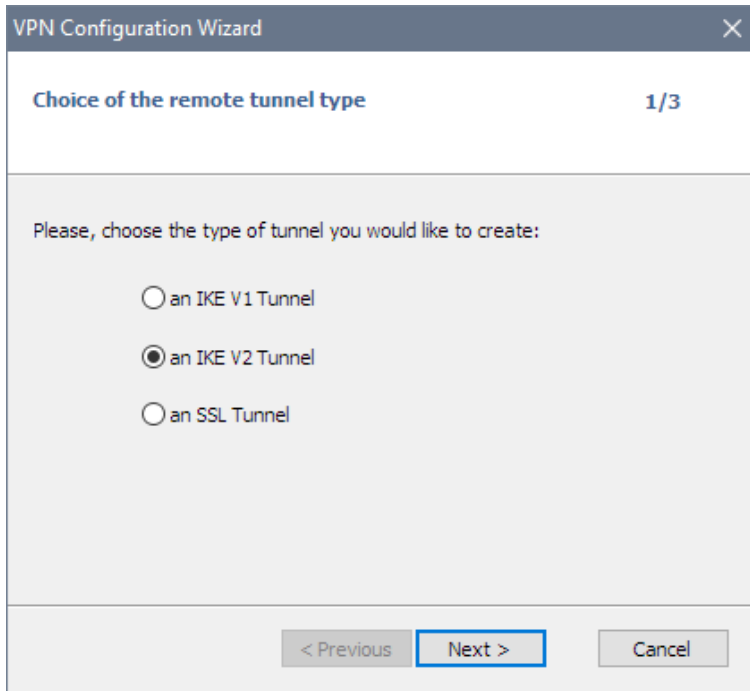


In the main interface, open the VPN configuration wizard: "Configuration > Wizard ..."



Step 1

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

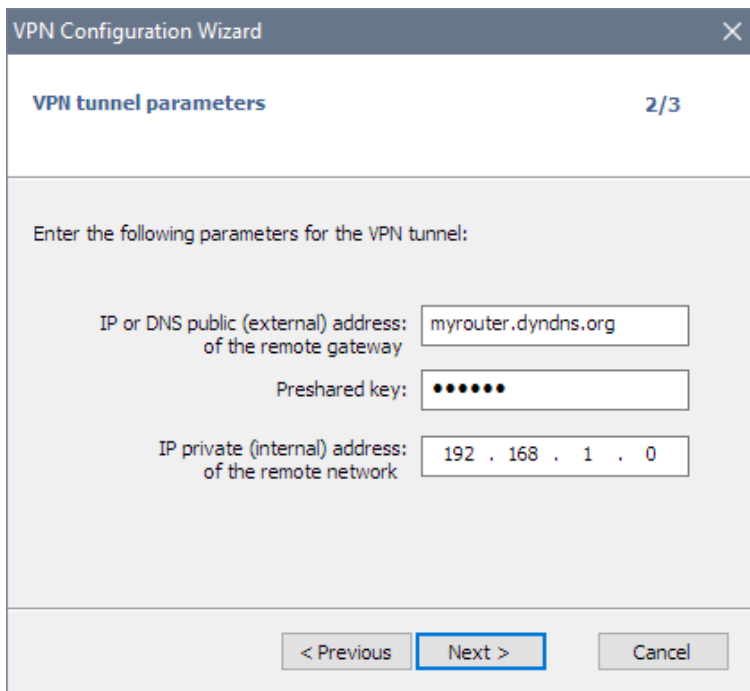


The screenshot shows the 'VPN Configuration Wizard' window at step 1/3, titled 'Choice of the remote tunnel type'. The instruction reads: 'Please, choose the type of tunnel you would like to create:'. There are three radio button options: 'an IKE V1 Tunnel', 'an IKE V2 Tunnel' (which is selected), and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

Step 2 for an IKEv1 VPN tunnel

Type in the following values:

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



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

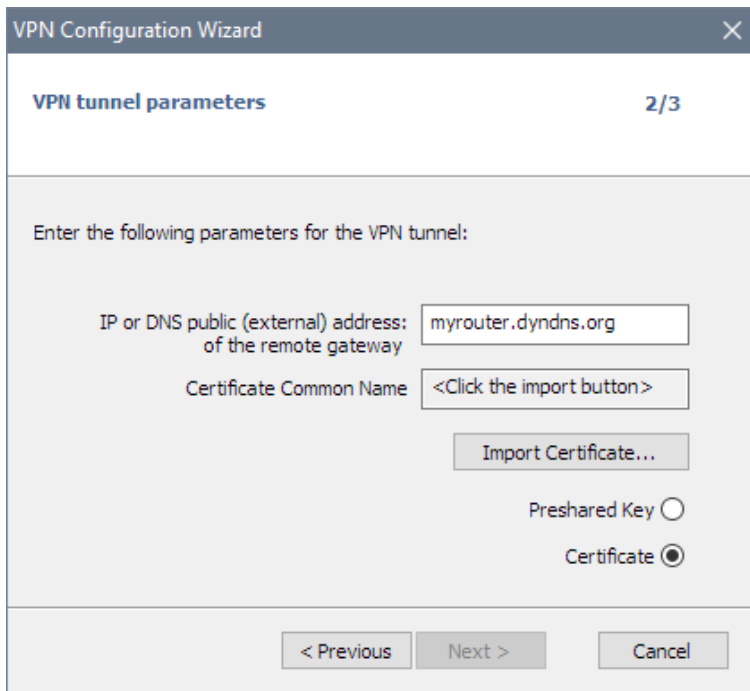


[1] The remote network’s address is used by default with a prefix length of 24. This value can be modified later.

Step 2 for an IKEv2 VPN tunnel

Type in the following values:

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



Step 2 for SSL (OpenVPN) tunnel

Type in the following values:

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



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

Step 3

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

The screenshot shows the 'VPN Configuration Wizard' window at step 3 of 3, titled 'Configuration Summary'. It states 'The tunnel configuration is correctly completed :'. A summary box contains: 'Tunnel name : Ikev2Gateway', 'Tunnel type is IKE V2', 'Gateway name or address : myrouter.dyndns.org', and 'Preshared key : *****'. Below this, it says 'You may change these parameters anytime directly with the main interface.' At the bottom, there are '< Previous', 'Finish', and 'Cancel' buttons.

The tunnel that has just been configured now appears in the tunnel tree of the main interface. Double-click the tunnel to open it or use the tabs of the main interface for further configuration. Security recommendation: When using the VPN Client in certified mode, it is recommended to configure IKEv2 tunnels with certificates. See Section "[Security recommendations](#)"





User interface

User interface

The VPN Client's user interface allows you to:

- 1/ configure the software itself (start mode, language, access controls, etc.),
- 2/ manage VPN security policies (VPN tunnel configuration, certificate management, import, export, etc.),
- 3/ use VPN tunnels (opening, closing, incident identification, etc.).

The user interface is divided as follows:

- The software items that appear on the **Windows Desktop** (desktop icons, Start menu)
- An **icon on the taskbar** and the associated menu
- The **Connection panel** (list of VPN tunnels to open)
- The **Configuration panel** (VPN security policy and software configuration)

The Configuration panel is composed of the following elements:

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

Windows desktop

Start menu

Once the installation is completed, the VPN Client can be launched from the Windows Start menu.

Links are created in the Start menu, in the directory named Stormshield / Network VPN Client.

Desktop

During the software installation, the "Network VPN Client" icon is created on the Windows desktop.

The VPN Client can be launched by double-clicking this icon.

Taskbar

Icon

Under normal operating conditions, Stormshield VPN Client is identified by an icon in the taskbar.



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



Blue icon: no VPN tunnel open



Green icon: at least one VPN tunnel is open

VPN Client's icon's "tooltip" always displays the software's status:

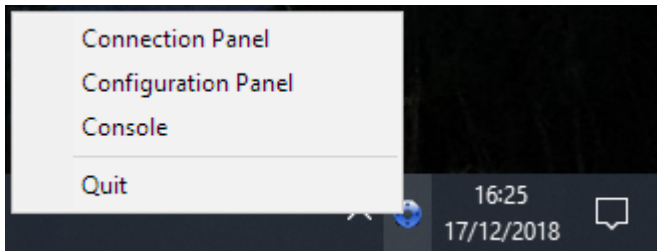
- "VPN Tunnel Opened" if one or several tunnels are open.
- "Waiting for VPN ready..." while the VPN IKE engine starts.
- "Stormshield VPN Client" when VPN Client is running, but no tunnels are open.

Left-clicking the icon will open the Connection panel.

Right-clicking the icon will open the contextual menu associated with the icon.

Menu

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



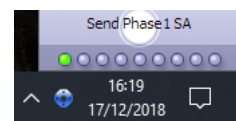
The items in the contextual menu are the following:

- 1/ Connection panel: opens the Connection panel
- 2/ Configuration panel: opens the Configuration panel
- 3/ Console: opens the VPN traces window
- 4/ Quit: Closes all open VPN tunnels and quits the software.

Fade-out popup

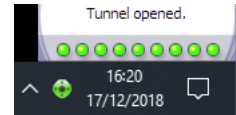
When opening or closing a VPN tunnel, a popup window appears above the VPN Client icon on the taskbar. This window will indicate the tunnel's status when it is being opened or closed and automatically fades out unless the mouse cursor is placed directly upon it:

Tunnel is being opened

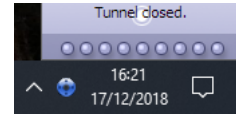




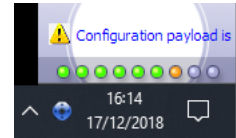
Tunnel is open



Tunnel is closed



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

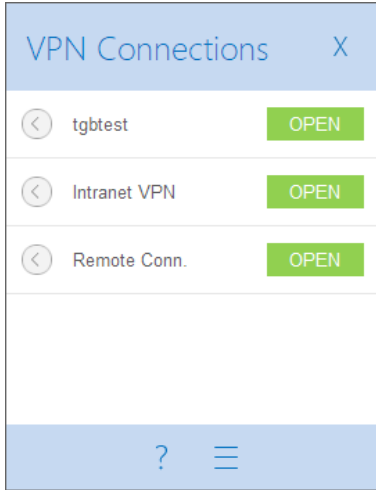


i NOTE
The fade-out window can be deactivated in the "View" tab of the "Tools > Options" menu. The option to tick is "Don't show the systray sliding popup".



Connection panel

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



New: Since the release of version 6.4, it is possible to customize the Connection panel: It is possible to select the VPN connections to be displayed. It is also possible to rename or sort these VPN connections.

See Section "[Connection panel management](#)".

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

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

- Closed connection. Clicking on this icon opens the connection configuration in the Configuration panel.
- Connection being opened or closed.
- Open connection. Traffic in the connection is illustrated by a change in the color intensity of the disk at the center.
- The connection experienced an incident during opening or closing. Clicking the alert icon will open a popup window giving detailed or additional information about the incident.

The Connection panel buttons give the possibility to:

- Open the "About..." window
- Open the Configuration panel (Note: It is possible to use a password to restrict access to the Configuration panel. See Section "[Controlling access to the VPN policy](#)")
- Close the Connection panel

The following keyboard shortcuts are available in the Connection panel:



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

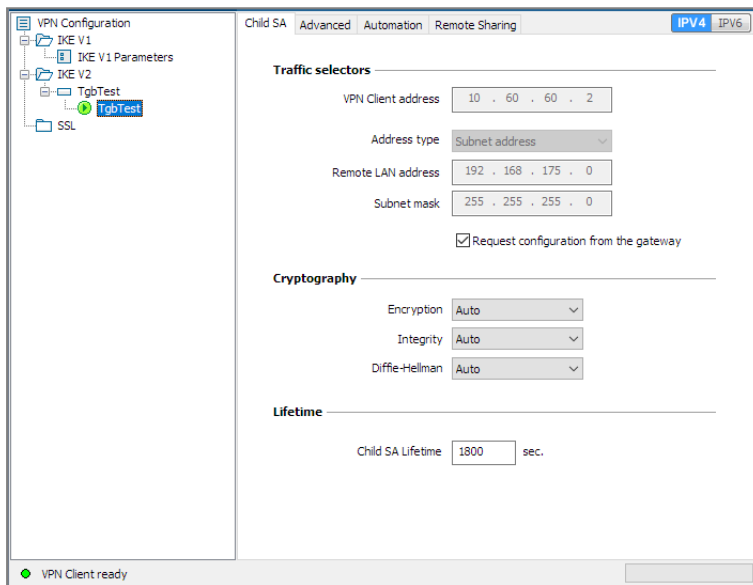


Configuration panel

The Configuration panel is the main interface of Stormshield VPN Client.

It is composed of the following elements:

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



Menus

The following menus are accessible in the Configuration panel:

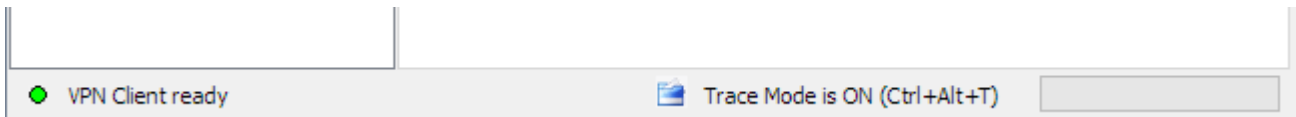
- Configuration
 - Save
 - Import: Importing a VPN security policy (VPN Configuration)
 - Export: Exporting a VPN security policy (VPN Configuration)
 - Move to a USB Drive: USB mode
 - **Wizard** : Configuration wizard
 - Quit: Close all VPN tunnels currently open and quit the software
- Tools
 - **Connection panel**
 - **Connection Panel Management**
 - Console: IKE connection traces window
 - Reset IKE: Restarts the IKE service
 - Options: Protection, display, start, language management, PKI management options
- ?



- - Online support: Access to the online support
- **Update-** : Check for update availability
- - Purchase License Online: Access to the online store
- - **Activation wizard**...
- - About...

Status bar

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



- The "LED" on the left edge is green when all the software's services are functional (IKE service)
- The text on the left displays the software status ("VPN Client ready", "Saving configuration", "Applying configuration", etc.)
- When activated, the "Trace Mode is ON" text is displayed in the middle of the status bar.

The icon  appears left of this text is a clickable icon which opens the folder containing the log files generated by the trace mode.

- The progress bar on the right of the status bar displays the progress when saving a configuration.

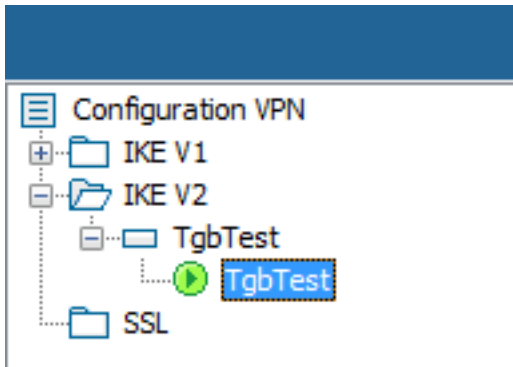
Shortcuts

CTRL+S	Save the VPN Configuration
CTRL+ENTER	Switch to the Connection panel
CTRL+D	Open the VPN traces "Console" window
CTRL+ALT+R	Restart the IKE service
CTRL+ALT+T	Activate the tracing mode (log generation)

VPN tunnel tree

Use

The left side of the Configuration panel is the tree diagram of the VPN security policy. The tree can contain an infinite number of tunnels.



Under the "VPN Configuration" root, 3 levels allow for the creation of, respectively:

- IPsec IKEv1 tunnels, characterized by a Phase 1 and a Phase 2, each Phase 1 being able to contain more than one Phase 2.
- IPsec IKEv2 tunnels, characterized by an IKE Authentication and a Child SA, each IKE Authentication being able to contain more than one Child SA.
- SSL/TLS tunnels.

Clicking on a Phase 1, Phase 2, IKE Auth, Child SA or TLS will open in the right-hand side of the Configuration panel the corresponding configuration tabs. See the following Sections:

1. IPsec IKEv1 VPN tunnel

[IKEv1 \(Phase1\): Authentication](#)

[IKEv1 \(Phase2\): IPsec](#)

2. IPsec IKEv2 VPN tunnel

[IKEv2 \(IKE Auth\): Authentication](#)

[IKEv2 \(Child SA\): IPsec](#)

3. SSL VPN tunnel

[SSL: TLS](#)

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

- Tunnel is closed
- Tunnel is configured to open automatically when traffic is detected
- Tunnel is being opened
- Tunnel is open
- Incident when opening or closing the tunnel

It is possible to edit and modify the name of any item in the tree by clicking twice in a row on it, without double-clicking.



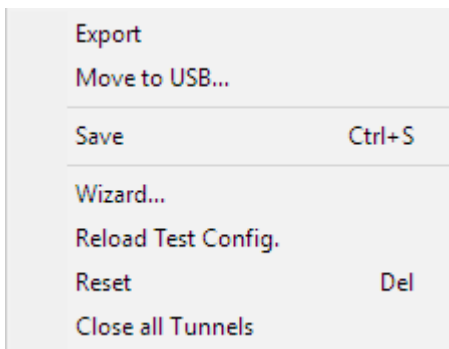
i NOTE
 Two items in the tree cannot have the same name. The software sends a message to the user if the name entered is taken.

Every unsaved change in the VPN Configuration is identified by the modified item in bold. As soon as the tree is saved, all text formatting is removed.

Contextual menus

VPN Configuration

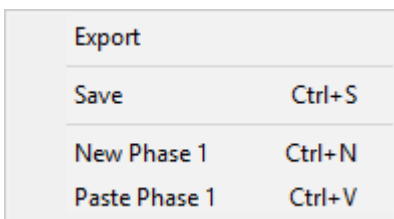
Right-clicking the VPN Configuration (the root of the tree) displays the following contextual menu:



- Export Gives the option to [export the complete VPN security policy](#).
- Move to USB Drive... Moves the VPN security policy to a USB Drive and initiate [USB mode](#)
- Save Gives the option to save the VPN security policy.
- Wizard Opens the [VPN Configuration wizard](#).
- Reload Test Config. Stormshield VPN Client is equipped with a Default configuration which gives the possibility to test-open a VPN tunnel. This menu gives the option to reload this configuration at any time.
- Reset Resets the VPN security policy after confirmation by the user.
- Close all tunnels Closes all open tunnels.

IKEv1, IKEv2, SSL

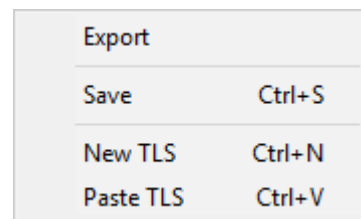
Right-clicking the IKEv1, IKEv2 or SSL items will display the following contextual menu which allows you to export, save, create or paste a Phase 1/IKE Auth/SSL:



IKEv1 menu



IKEv2 menu



SSL menu



- Export Gives the possibility to export all IKEv1 tunnels (resp. all IKEv2 tunnels).
- Save Gives the possibility to save all IKEv1 tunnels (resp. all IKEv2 tunnels).
- New Phase 1 Gives the possibility to create a new Phase 1/IKE Auth/TLS. The parameters of this new Phase 1/IKE Auth/TLS will be default values.
- New IKE Auth
- New TLS
- Paste Phase 1 Adds a previously copied Phase 1/IKE Auth/TLS to the clipboard.
- Paste IKE Auth
- Paste TLS

[1] This choice will appear when a Phase 1/IKE Auth/TLS has been copied to the clipboard through the contextual menu associated to this Phase 1/IKE Auth/TLS (see below).

Phase 1 or IKE Auth

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

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

IKEv1 menu

IKEv2 menu

- Copy Copies the selected Phase 1 or IKE Auth to the clipboard.
- Rename Gives the possibility to rename the Phase 1/IKE Auth.
[1]
- Delete [1] Gives the possibility to delete the selected Phase 1 or IKE Auth after confirmation by the user, including every corresponding Phase 2 (resp. Child SA).
- New Phase 2 Adds a new Phase 2/Child SA to the selected Phase 1/IKE Auth.
- New Child SA
- Paste Phase 2 Adds the Phase 2/Child SA copied to the clipboard to the selected Phase 1/IKE Auth.
[2]
- Paste Child SA

[1] This menu is deactivated as long as one of the tunnels of the relevant Phase 1/IKE Auth is open.

[2] This choice will appear when a Phase 2/Child SA has been copied to the clipboard through the contextual menu associated to this Phase 2/Child SA (see below).



Phase 2, Child SA or TLS

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

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

Tunnel closed menu

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

Tunnel open menu

Open tunnel Displayed if the VPN tunnel is closed and opens the selected tunnel (Phase 2, Child SA or TLS).

Close tunnel Displayed if the VPN tunnel is open and closes the selected tunnel (Phase 2, Child SA or TLS).

Export (1) Gives the possibility to export the selected Phase 2/Child SA/TLS.

Copy Gives the possibility to copy the selected Phase 2/Child SA/TLS.

Rename (2) Gives the possibility to rename the selected Phase 2/Child SA/TLS.

Delete (2) Gives the possibility to delete, after confirmation by the user, the selected Phase 2/Child SA/TLS.

(1) This function allows the user to export the entire tunnel, i.e. both the Phase 2 and the corresponding Phase 1 (resp. Child SA and IKE Auth, or TLS) and to create a fully operational, single-tunnel VPN security policy as a result (which becomes immediately functional when imported).

(2) This menu is deactivated while the tunnel is open.

Shortcuts

The following shortcuts are available for tree management:

F2 Edit the name of the selected Phase.

DEL Delete a selected phase, if any, after confirmation by the user.
If the Configuration itself is selected (root of the tree), a full reset of the configuration will be proposed.

CTRL+O Open the corresponding VPN tunnel, if a Phase 2/Child SA/TLS is selected.

CTRL+W Close the corresponding VPN tunnel, if a Phase 2/Child SA/TLS is selected.

CTRL+C Copy the selected Phase to the clipboard.

CTRL+V Paste (add) the Phase copied to the clipboard.

CTRL+N If the VPN Configuration is selected, create a new Phase 1/IKE Auth. If a Phase 1/IKE Auth is selected, create a Phase 2/Child SA/TLS.

CTRL+S Save the VPN security policy.



Import/export a VPN security policy

Importing a VPN security policy

Stormshield VPN Client gives the possibility to import a VPN security policy in various ways:

- Through the "Configuration > Import" menu of the Configuration panel (main interface).
- By dragging and dropping a VPN Configuration file (".tgb" file) into the Configuration panel (main interface).
- By double-clicking on a VPN Configuration file (".tgb" file). [1]
- Through command lines, using the "/import" option. [2]

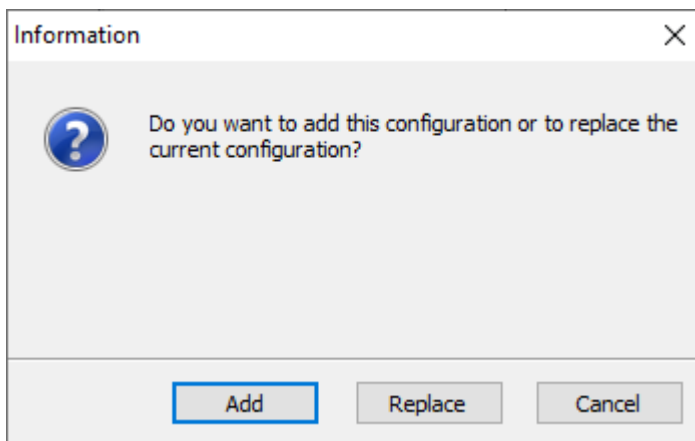
[1] The "double-click on a configuration file to import a configuration" function is not available in the TheGreenBow VPN Certified version.

[2] The use of command-line options within the software is covered in the "Deployment Guide". In particular, it details all the options available for importing a VPN security policy: "/import", "/add", "/replace" or "/importance".

i NOTE

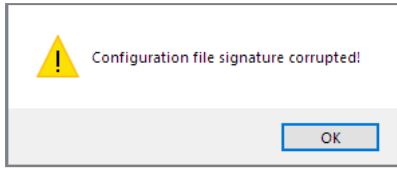
The imported VPN configuration files' extension is, by default, ".tgb".

When importing a VPN Configuration, the user is asked whether to add the new VPN Configuration to the current one or replace (overwrite) the current Configuration with the new one:



If the imported VPN security policy is exported with a password protection (see "[Exporting a VPN security policy](#)" below), the user will have to provide the password.

If the VPN security policy is exported with an integrity control (see "[Exporting a VPN security policy](#)" below) and it has been corrupted, a warning will be displayed to the user and the software will not import the Configuration.



i NOTE
 If some of the VPN tunnels added have the same name as the current configurations, they are automatically renamed during import (an incrementing number will be added between brackets).

Importing the General Settings (IKEv1 only)

When importing, the user chooses "Replace" or if the current Configuration is empty, the General settings of the imported VPN Configuration replaces the General settings of the current configuration.

When importing, the user chooses "Add", the General settings of the current VPN configuration are preserved.

The user's choice for the import	Current Configuration empty	Current Configuration not empty
Add	General settings replaced by the new ones	General settings preserved
Replace	General settings replaced by new ones	General settings replaced by new ones

Exporting a VPN security policy

Stormshield VPN Client gives the possibility to export a VPN security policy in various ways:

- 1/ "Configuration > Export" menu: The entire VPN security policy is exported.
- 2/ Contextual menu associated with the VPN tree root > Export: The entire VPN security policy is exported.
- 3/ Contextual menu associated with a Phase 1 (IKEv1) or an IKE Auth (IKEv2) > Export: The entire Phase 1/IKE Auth (including all Phase 2/Child SA contained within) is exported.
- 4/ Contextual menu associated with a Phase 2 (IKEv1) or a Child SA (IKEv2) > Export: The Phase 2/Child SA is exported along with the Phase 1/IKE Auth with which it is associated.
- 5/ Contextual menu associated with a TLS > Export: The TLS is exported.
- 6/ Through command lines, using the "/export" option [1]

[1] The use of command-line options within the software is covered in the "Deployment Guide" [tgbvpn_ug_deployment_en.pdf]. In particular, it details all the options available for exporting a VPN security policy: "/export" or "/exportonce".

i NOTE
 The exported VPN configuration files' extension is, by default, ".tgb".



Whatever method is used, the export will start with the choice of the protection for the exported VPN security policy: It can be exported protected (encrypted) with or without a password. If configured, the password is requested from the user when importing.

i NOTE

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

Protecting the integrity of a VPN security policy when it is exported is a function that can be activated by a registry key.

It is recommended to always export VPN security policies with a password protection (encrypted).

If an exported VPN security policy is integrity-protected, but is corrupted subsequently, a warning will be displayed to the user during the import and the software will not import the configuration (see Section "[Importing a VPN security policy](#)" above).

Merge VPN security policies

It is possible to merge several VPN security policies by importing all VPN Configurations and choosing "Add" each time (see Section "[Importing a VPN security policy](#)" above).

Split a VPN security policy

By using the various export options offered (export a Phase 1/IKE Auth/TLS with all corresponding Phase 2/Child SA/TLS or export a single tunnel), a VPN security policy can be split in as many "Sub-Configurations" as desired. (See "[Exporting a VPN security policy](#)" above).

This method can be used to deploy the VPN security policies of a given set of workstations: derive from a common VPN security policy the VPN policies associated to every single workstation before sending them to every user for import.



Configure a VPN tunnel

IPsec IKEv1, IPsec IKEv2 or SSL VPN

It is possible to use Stormshield VPN Client for creating and configuring several types of VPN tunnels.

It is also possible to open them simultaneously.

Stormshield VPN Client can be used for configuring the following types of tunnels:

- IPsec IKEv1
- IPsec IKEv2
- SSL

The procedure to create a new VPN tunnel is described in the previous Sections: "Configuration wizard" and "VPN tunnel tree > Contextual menu".

Security recommendation: When using and operating TheGreenBow VPN Certified, it is recommended to configure the IKEv2 tunnels with certificates. See "[Security recommendations](#)"

Edit and save the VPN configuration

Stormshield VPN Client allows you to modify the VPN tunnels and test these modifications "on-the-fly" without saving the configuration.

Every unsaved change in the VPN Configuration is identified in the tree by the modified item in bold.

The configuration can be saved at any time:

- By using CTRL+S
- In the "Configuration > Save" menu

If a configuration has been modified and the user tries to quit the software without saving, an alert will be displayed.



Configure an IPsec IKEv1 tunnel

Phase 1: Authentication

Authentication | Protocol | Gateway | Certificate

Remote Gateway

Interface: Any

Remote Gateway: tgbtest.dyndns.org

Authentication

Preshared Key

Confirm

Certificate

X-Auth

Enabled X-Auth Popup

Login: Once

Password: Hybrid Mode

Cryptography

Encryption: AES 128

Authentication: SHA-1

Key Group: DH2 (1024)

Addresses

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

Interface: Any

192.168.205.52

Any

It is recommended to choose this option if the configured tunnel is intended to be deployed on a different workstation.

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

Authentication

Preshared key Password or key shared by the remote gateway.

Note: 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. See "[Security recommendations](#)"



Certificate Use of certificates for VPN connection authentication.

Note: Using certificates strengthens the security in terms of the management of VPN connections (mutual authentication, verification of the validity periods, cancellation, etc.) See "[Security recommendations](#)"

See dedicated Section: "[Certificate management](#)"

X-Auth

See Section "X-Auth management" below.

IKE

- Encryption Encryption algorithm negotiated during the Authentication phase [1]:
Auto [2], DES, 3DES, AES-128, AES-192, AES-256.
- Authentication Authentication algorithm negotiated during the Authentication phase [1]:
Auto [2], MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
- Key group Diffie-Hellman key length [1]:
Auto [2], DH1 [768], DH2 [1024], DH5 [1536], DH14 [2048], DH15 [3072], DH16 [4096], DH17 [6144], DH18 [8192]

- [1] See "[Security recommendations](#)" for the choice of the algorithm.
- [2] Auto means that the VPN Client will be automatically adjusted to the gateway parameters.

When "Auto" is selected, the following algorithms (and the combinations thereof) are compatible:


- Encryption: DES, 3DES, AES-128, AES-192, AES-256
- Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512
- Key group: DH1, DH2, DH5, DH14, DH15, DH16, DH17, DH18

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

X-Auth management

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

The X-Auth function is used for setting up the requirement of entering a login name and password for opening a VPN tunnel.

 NOTE
A similar configuration needs to be established on the VPN gateway.

X-Auth

Enabled
 X-Auth Popup

Login
 Once

Password
 Hybrid Mode



If the "X-Auth Popup" box is ticked, a popup window asking for the user's login and authentication password will appear each time a VPN tunnel is opened (the login and password window will have the same name as the tunnel in order to avoid confusion).




This window has a timeout limit (which can be set in the [IKE V1 Parameters](#)) which, when reached, will display an alert message to the user asking him to re-open the tunnel.

The VPN Client can store the X-Auth login and password in the VPN security policy. If so, this login and password will be sent automatically to the VPN gateway when opening the tunnel.

X-Auth

Enabled X-Auth Popup

Login: Once

Password:  Hybrid Mode

This option makes the use and deployment of the software much easier. However, it is considered a less secure option than the dynamic display of an X-Auth login/password window.

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

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

In order to activate Hybrid mode, the tunnel must be associated with a certificate (see [Certificate management](#)) and the X-Auth function must be configured.




X-Auth

Enabled X-Auth Popup

Login

Password

Once

Hybrid Mode 

It is recommended to refer to the Section "[Security recommendations](#)" in order to properly assess whether this option should be used.

Phase 1: Protocol

Authentication | Protocol | Gateway | Certificate

Identity

Local ID

Remote ID

Advanced features

Fragmentation Fragment size

IKE Port Enable NATT offset

NAT Port

Mode Config

Aggressive Mode NAT-T

Identity

Local ID "Local ID" is the identity that the VPN Client is sending to the remote VPN gateway during the Authentication phase (Phase 1).

Depending on the type selected, this identity can be:

- an IP address (type=IP address), e.g. 195.100.205.101
- a domain name (type=FQDN), e.g. gw.mydomain.net
- an email address (type=USER FQDN), e.g. support@thegreenbow.com
- a character string (type=KEY ID), e.g. 123456
- the subject of a certificate (type=X509 subject (aka DER ASN1 DN)). This is the case when the tunnel is associated with a user certificate (see [Certificate management](#))

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



Remote ID "Remote ID" is the identity VPN Client is expecting to receive from the VPN gateway.

- Depending on the type selected, this identity can be:
- an IP address (type=IP address), e.g. 80.2.3.4
 - a domain name (type=FQDN), e.g. router.mydomain.com
 - an email address (type=USER FQDN), e.g. admin@mydomain.com
 - a character string (type=KEY ID), e.g. 123456
 - the subject of a certificate (type=DER ASN1 DN).

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



Security advisory: See chapter "Security recommendations" for the Remote ID management when the VPN Client is configured to check the VPN Gateway Certificate.

Advanced functions

Fragmentation/Fragment size	This function enables IKE fragmentation, which prevents packets from being fragmented (and potentially blocked) by the IP network they're passing through. It is generally necessary to set a fragment size smaller than the MTU of the physical interface, e.g. 1400 octets for a typical MTU of 1500.
IKE port	IKE Phase 1 (Authentication) exchanges use the UDP protocol and port 500 by default. IKE port configuration can bypass the network elements (Firewall, routers) that filter port 500. Note: The remote VPN gateway must also be able to perform the IKE Phase 1 exchanges on a port other than 500.
NAT port	IKE Phase 2 (IPsec) exchanges use the UDP protocol and port 4500 by default. NAT port configuration can bypass the network elements (Firewall, routers) that filter port 4500. Note: The remote VPN gateway must be able to perform IKE Phase 2 exchanges on a different port than 4500.
Enable NATT offset	When the IKE port is different from 500, it may be necessary to check this option for the gateway to accept the connection.
Mode Config	Once activated, Mode Config grants the VPN Client the possibility to get the configuration information necessary for opening the VPN tunnel from the VPN gateway. See paragraph below: Mode Config management.
Aggressive mode	VPN Client uses the Aggressive mode to connect to the VPN gateway. See Section "Security recommendations" for more details regarding the use of Aggressive mode vs. Main mode.
NAT-T	"NAT-Traversal" mode. The VPN Client can handle 3 types of NAT-T modes: <ul style="list-style-type: none"> Disabled Prevents the VPN Client and the VPN gateway to switch to NAT-Traversal mode. Automatic Leaves the VPN Client and the VPN gateway negotiate the NAT-Traversal mode. Forced The VPN Client will force NAT-T mode by systematically encapsulating IPsec packets into UDP frames. This will solve NAT-Traversal issues using intermediate routers.



Mode Config management

Once activated, Mode Config grants the VPN Client the possibility to get the configuration information necessary for opening the VPN tunnel from the VPN gateway:

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

! IMPORTANT

Mode Config will be operational only if supported by the VPN gateway.

When Mode Config is disabled, the 3 items "VPN Client address", "DNS server" and "WINS server" can be configured manually in the VPN Client (see "[Phase 2: Advanced](#)").

In the same time, when Mode Config is enabled, the Phase 2 fields: "VPN Client address", "DNS server" and "WINS server" will be automatically filled in when opening the VPN tunnel. The corresponding fields will be disabled and cannot be modified.

Phase 1: Gateway

The screenshot shows the 'Gateway' configuration tab in the VPN Client interface. It contains the following sections and fields:

- Dead Peer Detection (DPD)**
 - Check interval: 30 sec.
 - Max. number of retries: 3
 - Delay between retries: 15 sec.
- Lifetime**
 - Lifetime: 2700 sec.
- Gateway related parameters**
 - Redundant Gateway: (empty text box)
 - Retransmissions: 3

Dead Peer Detection (DPD)

Dead Peer Detection The DPD (Dead Peer Detection) function enables the VPN Client to detect whether the VPN gateway has been disabled or has become inactive. [1]

- Check interval: Time interval between two DPD check messages, expressed in seconds.
- Max. number of retries: Number of consecutive unsuccessful attempts before concluding that the VPN gateway is inactive.
- Delay between retries: Time between two DPD messages when the VPN gateway is not answering, expressed in seconds.



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

Lifetime

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

[1] Lifetimes are negotiated between the VPN Client and the VPN Gateway. However, some gateways simply return the default value of the lifetime proposed by the VPN Client. Whatever the method used, the lifetime value sent by the VPN gateway will always be the one applied by the VPN Client.

Gateway related parameters

Redundant Gateway	Defines the address of an alternate VPN gateway that the VPN Client will switch to when the initial gateway is down or inactive. The redundant VPN gateway's address can be either an IP or DNS address. See Section " Redundant Gateway ".
Retransmissions	Number of IKE protocol message resends when the gateway is not answering. After all these resends, the tunnel is declared a failure.

Phase 1: Certificate

See Section [Certificate management](#).

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

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

If modified, a tunnel will appear in bold in the VPN tree. A configuration does not have to be saved to be taken into account; the tunnel can be tested with the modified configuration immediately.



Phase 2: IPsec

IPsec Advanced Automation Remote Sharing IPV4 IPV6

Addresses

VPN Client address

Address type Subnet address

Remote LAN address

Subnet mask

ESP

Encryption AES256

Authentication SHA-512

Mode Tunnel

PFS

PFS Group DH18 (8192)

Lifetime

IPsec Lifetime sec.

Addresses

VPN Client address "Virtual" IP address of the workstation, the way it will be "seen" on the remote network.
 From a technical standpoint, it is the source IP address of the IP packets going through the IPsec tunnel.

When the field is set to "0.0.0.0" the software will use the workstation's physical IP address automatically for the virtual IP address provided to the gateway.

Note: When **Mode Config** is activated, this field will be disabled and uneditable. It is automatically filled in when the tunnel is opened with the value sent by the VPN gateway during the Mode Config exchange.

Address type The endpoint of the tunnel can be a network or a remote workstation. See paragraph below for the address type configuration.

Encryption Encryption algorithm negotiated during the IPsec phase [1]:
 Auto [2], DES, 3DES, AES-128, AES-192, AES-256.

Authentication Authentication algorithm negotiated during the IPsec phase [1]:
 Auto [2], MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.

Mode IPsec encapsulation mode: Tunnel or transport [1]

[1] See "[Security recommendations](#)" for the choice of the algorithm.



[2] Auto means that the VPN Client will be automatically adjusted to the gateway parameters. When "Auto" is selected, the following algorithms (and the combinations thereof) are compatible:

- Encryption: DES, 3DES, AES-128, AES-192
- Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512

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

PFS

PFS	Can be enabled or disabled: Diffie-Hellman key length: DH1 {768}, DH2 {1024}, DH5 {1536}, DH14 {2048}), DH15 {3072}, DH16 {4096}, DH17 {6144}, DH18 {8192}
	Note: IKEv1 does not have an automatic mode for the DH group. It must be indicated beforehand. See " Security recommendations " for the choice of the algorithm.

Lifetime

Lifetime	Lifetimes are negotiated when the tunnel is established. [1] When the lifetime is reached, Phase 2 will be renegotiated. The default value for the lifetime of Phase 2 is 1800 sec. {30 min.}
-----------------	---

[1] Lifetimes are negotiated between the VPN Client and the VPN Gateway. However, some gateways simply return the default value of the lifetime proposed by the VPN Client. Whatever the method used, the lifetime value sent by the VPN gateway will always be the one applied by the VPN Client.

IPv4 / IPv6

IPv4-IPv6 See Section "[IPv4 and IPv6](#)".

Address type configuration

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

Address type

Remote LAN address

Subnet mask

Alternatively, select "Range address" and type in the Start and End addresses:

Address type

Start address

End address

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

Address type

Remote host address

**i NOTE**

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

i NOTE

If the IP address of the VPN Client workstation is included in the address range for a remote network (e.g. @workstation IP=192.168.10.2 and @remote network=192.168.10.x), then opening a tunnel will prevent communication between the workstation and the local network. All communications will be 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. In order to do this, select the "Subnet address" address type and type in "0.0.0.0" as the Remote LAN address and Subnet mask.

Phase 2: Advanced

IPsec Advanced Automation Remote Sharing IPV4 IPV6

Alternate servers

DNS Suffix: dev.corporate

Type	IP Address	
DNS	192.168.175.50	✘
WINS	192.168.175.50	✘

Add DNS Add WINS

Tunnel traffic check

Period and IP Address of the remote host to ping:

IPv4 Address: 0 . 0 . 0 . 0

Check interval: 0 sec.

Other servers

DNS Suffix Domain extension added to each machine's name, for example: "mozart.dev.corporate". This is an optional parameter: When specified, the VPN Client will try to translate the machine's address without adding the DNS extension. If, however, the translation fails, the DNS extension will be added and the Client will try to translate the address again.



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

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

Tunnel traffic check

IP address The VPN Client can be configured so that connectivity to the remote network is checked frequently. If the connection is lost, the VPN Client will automatically close and re-attempt to open the tunnel.

The IPv4/IPv6 field is the address of a machine within the remote network which should reply to "pings" sent by VPN Client. If a "ping" goes unanswered, the connection is considered lost.

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

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

Phase 2: Automation

See Section Automation

Phase 2: Remote sharing

See Section Remote desktop sharing

IKE V1 Parameters

The IKE V1 Parameters are shared by all IKEv1 tunnels (every Phase 1 and every Phase 2).

The screenshot shows a configuration window titled "IKE V1 Parameters" with a "Miscellaneous" tab selected. The window contains the following fields and options:

- Retransmissions: Input field with the value "2".
- X-Auth timeout: Input field with the value "60".
- IKE Port: Empty input field.
- NAT Port: Empty input field.
- Disable Split Tunneling
- Cisco Mode Config

Miscellaneous

Retransmissions Number of IKE protocol message resends before failure.

X-Auth timeout Time allowed for X-Auth login/password input

IKE Port This field enables the configuration of the IKE port for all IKEv1 tunnels. Note: IKE ports customizable in each tunnel have the priority for this parameter.



NAT Port	This field enables the configuration of the NAT port for all IKEv1 tunnels. Note: NAT ports customizable in each tunnel have the priority for this parameter.
Disable Split Tunneling	When this option is selected, only the traffic going through the tunnel is authorized. See note [1] below.
Cisco Mode Config	This box must be ticked to ensure compatibility with Cisco ASA-type gateways (Premium and Certified versions only)

[1] The "Disable Split Tunneling" configuration option increases the "leakproofness" of the workstation, provided that the VPN tunnel is open. In particular, this function eliminates the risk of incoming data flows not going through the VPN tunnel.

Combined with the "All traffic through the VPN tunnel" Configuration (see Section [Phase 2: IPsec](#)), this option guarantees the complete leakproofness of the workstation provided the VPN tunnel is open.

Configure an IPsec IKEv2 tunnel

IKE Auth: IKE SA

The screenshot shows a configuration window for an IKEv2 tunnel. It has three tabs: 'Authentication', 'Protocol', and 'Gateway'. The 'Authentication' tab is active. The 'Remote Gateway' section includes an 'Interface' dropdown set to 'Any' and a 'Remote Gateway' text field containing 'tgbtest.dyndns.org'. The 'Authentication' section has three radio buttons: 'Preshared Key' (selected), 'Certificate', and 'EAP'. Under 'Preshared Key', there are two password fields, 'Preshared Key' and 'Confirm', both filled with dots. Under 'EAP', there is a checkbox for 'EAP popup' (unchecked), a 'Login' text field, a 'Password' text field, and a checkbox for 'Multiple AUTH support' (unchecked). The 'Cryptography' section has three dropdown menus: 'Encryption' (set to 'Auto'), 'Authentication' (set to 'Auto'), and 'Key Group' (set to 'Auto').



Addresses

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

Interface 

It is recommended to choose this option if, for example, the configured tunnel is intended to be deployed on a different workstation.

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

Authentication

Preshared key Password or key shared by the remote gateway.

Note: 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. See "[Security recommendations](#)"

Certificate Use of certificates for VPN connection authentication.

Note: Using certificates strengthens the security in terms of the VPN connections management (mutual authentication, verification of the validity periods, cancellation, etc.) See "[Security recommendations](#)"

See dedicated Section: "[Certificate management](#)"

EAP The EAP (Extensible Authentication Protocol) mode checks the identity of the user using a login and password. When the EAP mode is selected, a popup window will ask the user's login and password each time the tunnel is open.

When the EAP mode is selected, it is possible to choose between a prompt for the EAP login and password each time the tunnel is opened (through the "EAP popup" box) or have them memorized in the VPN Configuration by filling them in the Login and Password fields.

The latter is not recommended when using the software in certified mode. See "[Security recommendations](#)"

Multiple AUTH Support Enables the combination of certificate and EAP authentications. {1}

- {1} The VPN Client is compatible with the "Certificate then EAP" double authentication.
The VPN Client is not compatible with the "EAP then Certificate" double authentication.

Cryptography

Encryption Encryption algorithm negotiated during the Authentication phase {1}:
Auto {2}, DES, 3DES, AES-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256).



Authentication	Authentication algorithm negotiated during the Authentication phase [1]: Auto [2], MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
Key Group	Diffie-Hellman key length [1]: Auto [2], DH1 {768}, DH2 {1024}, DH5 {1536}, DH14 {2048}, DH15 {3072}, DH16 {4096}, DH17 {6144}, DH18 {8192}, DH19 {ECP256}, DH20 {ECP384}, DH21 {ECP521}, No Diffie-Hellman.

[1] See "[Security recommendations](#)" for the choice of the algorithm.

[2] Auto means that the VPN Client will be automatically adjusted to the gateway parameters. When "Auto" is selected, the following algorithms (and the combinations thereof) are compatible:

- Encryption: DES, 3DES, AES-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256)
- Authentication: MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512
- Key group: DH1, DH2, DH5, DH14, DH15, DH16, DH17, DH18, DH19, DH20, DH21

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

The screenshot shows a configuration window with tabs for Authentication, Protocol, Gateway, and Certificate. The Identity section includes dropdown menus for Local ID and Remote ID, each followed by a text input field. The Advanced features section includes a checkbox for Fragmentation, a text input for Fragment size, a text input for IKE Port (set to 500), a text input for NAT Port (set to 4500), and a checkbox for Enable NATT offset.

Identity

Local ID

"Local ID" is the identity that the VPN Client sends to the remote VPN gateway during the Authentication phase.

Depending on the type selected, this identity can be:

- an IP address (type=IP address), e.g. 195.100.205.101
- a domain name (type=FQDN), e.g. gw.mydomain.net
- an email address (type=USER FQDN), e.g. support@thegreenbow.com
- a character string (type=KEY ID), e.g. 123456
- the subject of a certificate (type=X509 subject [aka DER ASN1 DN]), when the tunnel is associated to a user certificate [see [Certificate management](#)]

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



Remote ID "Remote ID" is the identity VPN Client is expecting to receive from the VPN gateway.

Depending on the type selected, this identity can be:

- an IP address (type=IP address), e.g. 80.2.3.4
- a domain name (type=FQDN), e.g. router.mydomain.com
- an email address (type=USER FQDN), e.g. admin@mydomain.com
- a character string (type=KEY ID), e.g. 123456
- the subject of a certificate (type=DER ASN1 DN)

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



Security advisory: See chapter "[Security recommendations](#)" for the Remote ID management when the VPN Client is configured to check the VPN Gateway Certificate.

Advanced features

Fragmentation	Enables IKEv2 packets fragmentation in accordance with RFC 7383. This function prevents IKEv2 packets from being fragmented by the IP network they're passing through. Because of this, the value in the "Fragment size" field must be equal to or smaller than the size of the network's fragments (typically 1500). E.g. 900 or 1000 or 1100.
IKE Port	IKE Auth (Authentication) exchanges use the UDP protocol and port 500 by default. IKE port configuration can bypass the network elements (Firewall, routers) that filter port 500. Note: 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 network elements (Firewall, routers) that filter port 4500. Note: The remote VPN gateway must also be able to perform the IKE Child SA exchanges on a port other than 4500.
Enable NATT offset	When the IKE port is different from 500, it may be necessary to check this option for the gateway to accept the connection.

IKE Auth: Gateway



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

Dead Peer Detection (DPD)

- Checking interval** The DPD (Dead Peer Detection) function enables VPN Client to detect whether the VPN gateway is down or inactive. [1]
The checking period is the time interval between the dispatch of two DPD check messages, expressed in seconds.
- Max. number of retries** Number of consecutive unsuccessful attempts before concluding that the VPN gateway is unavailable.
- Delay between retries** Time between two DPD messages when the VPN gateway is not answering, expressed in seconds.

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

Lifetime

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

Gateway related parameters

- Redundant Gateway** Defines the address of an alternate VPN gateway that the VPN Client will switch to when the initial VPN gateway is down or inactive.
The redundant VPN gateway's address can be either an IP or DNS address.
See Section "[Redundant gateway](#)".
- Retransmissions** Number of IKE protocol message resends before failure.
- Gateway timeout** Delay between two resends

IKE Auth: Certificate

See Section [Certificate management](#)



Child SA: Introduction

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

In order to configure the Child SA parameters, select it from the Configuration panel tree. Parameters can be configured in the right-hand tabs of the Configuration panel.

If modified, a tunnel will appear in bold in the VPN tree. A configuration does not have to be saved to be taken into account; the tunnel can be tested with the modified configuration immediately.

Child SA: Child SA

Traffic selectors

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

Cryptography

- Encryption** Encryption algorithm negotiated during the IPsec phase (1): Auto (2), DES, 3DES, AES-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256).



- Integrity Authentication algorithm negotiated during the IPSec phase [1]:
Auto [2], MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
- Diffie-Hellman Diffie-Hellman key length [1]:
Auto [2], DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192), DH19 (ECP256), DH20 (ECP384), DH21 (ECP521), No Diffie-Hellman.

[1] See "[Security recommendations](#)" for the choice of the algorithm.

[2] Auto means that VPN Client will automatically be adjusted to the gateway parameters. When "Auto" is selected, the following algorithms (and the combinations thereof) are compatible:

- Encryption: DES, 3DES, AES-CBC (128, 192, 256), AES-CTR (128, 192, 256), AES-GCM (128, 192, 256)
- Authentication: MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512
- Key group : DH1, DH2, DH5, DH14, DH15, DH16, DH17, DH18, DH19, DH20, DH21

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

Lifetime

Child SA Time interval, expressed in seconds, between two renegotiations.

Lifetime

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

IPv4 / IPv6

IPv4 / IPv6 See Section "[IPv4 and IPv6](#)".

Address type configuration

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

Address type

Remote LAN address

Subnet mask

Alternatively, select "Range Address" and type in the Start and End addresses:

Address type

Start address

End address

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

Address type

Remote host address

i NOTE
 The function "[Automatically open this tunnel on traffic detection](#)" gives the possibility to automatically open a tunnel towards one of the specified addresses in the address range when



traffic is detected (provided that this address range is authorized in the VPN gateway configuration).

i NOTE
If the IP address of the VPN Client workstation is included in the address range for a remote network (e.g. @workstation IP=192.168.10.2 and @remote network=192.168.10.x), then opening a tunnel will prevent communication between the workstation and the local network. All communications will be 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. In order to do this, select the "Subnet address" address type and type in "0.0.0.0" as the Remote LAN address and Subnet mask.

Child SA: Advanced

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

Alternate servers

DNS Suffix

Alternate servers

Type	IP Address
------	------------

i Add DNS
Add WINS

Tunnel traffic check

Period and IP Address of the remote host to ping:

IPV4 Address

Check interval sec.

Miscellaneous

Disable Split Tunneling

Alternate servers

DNS Suffix Domain extension added to each machine's name, for example: "mozart.dev.corporate". This is an optional parameter: When specified, the VPN Client will try to translate the machine's address without adding the DNS extension. If, however, the translation fails, the DNS extension 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. IP addresses will be either IPv4 or IPv6 depending on the network type configured in the "Child SA" tab.

Note: When CP mode is activated (see the "Request configuration from the gateway" parameter in the "Child SA" tab), these fields will be greyed out (uneditable). They are automatically filled in when the tunnel is opened with the values sent by the VPN gateway during the CP mode exchange.

Tunnel traffic check

IP Address The VPN Client can be configured so that connectivity to the remote network is checked frequently. If the connection is lost, the VPN Client will automatically close and re-attempt to open the tunnel.

The IPv4/IPv6 field is the address of a machine within the remote network which should reply to "pings" sent by VPN Client. If a "ping" goes unanswered, the connection is considered lost.

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

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

Others

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

[1] The "Disable Split Tunneling" configuration option increases the "leakproofness" of the workstation, provided that the VPN tunnel is open. In particular, this function eliminates the risk of incoming data flows not going through the VPN tunnel.

Combined with the "All traffic through the VPN tunnel" Configuration (see Section [IPSec](#)), this option guarantees the complete leakproofness of the workstation, provided that the VPN tunnel is open.

This mode is recommended for the "VPN Certified" version.

Child SA: Automation

See Section "[Automation](#)"

Child SA: Remote sharing

See Section "[Remote desktop sharing](#)"

Configure an SSL VPN tunnel

Introduction

Versions 6 and later of Stormshield VPN Client can be used for opening SSL VPN tunnels.

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



Authentication

Remote Gateway

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

It is recommended to choose this option if, for example, the configured tunnel is intended to be deployed on a different workstation.

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

Authentication

Select Certificate Choice of the certificate for VPN connection authentication.
See dedicated Section: "[Certificate management](#)"

Extra Authentication

Extra authentication This option increases the security level by asking the user to type in a login and password whenever a tunnel is opened.

The login and password can be entered in a static manner or, if the "Popup when tunnel opens" box is ticked, requested dynamically from the user whenever a tunnel is opened.

Security



Authentication Security Gateway Establishment Automation Certificate Remote Sharing

Initial Authentication (TLS)

Security Suite Auto

Traffic Security Suite

Authentication Auto

Encryption Auto

Compression Auto

Extra HMAC (TLS-Auth)

Enabled Key Direction

Initial Authentication (TLS)

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

- Auto all Cryptography suites (except null) are presented to the gateway, which will use the best fit.
- Low only weak Cryptography suites are presented to the gateway. In the current version, these are suites using 64- or 56-bit encryption algorithms.
- Normal only "medium" Cryptography suites are presented to the gateway. In the current version, these are suites using 128-bit encryption algorithms
- High only strong Cryptography suites are presented to the gateway. In the current version, these are suites using 128-bit or higher encryption algorithms.

For more information: <https://www.openssl.org/docs/apps/ciphers.html>

Traffic Security Suite

Authentication Authentication algorithm negotiated for traffic:
Automatic [1], MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512.

Note: If the "Extra HMAC" option is activated (see below), the authentication algorithm cannot be set to "Auto". It will have to be explicitly configured and identical to the one chosen at the gateway endpoint.

Encryption Traffic encryption algorithm:
Automatic [1], BF-CBC-128, AES128-CBC, AES192-CBC, AES256-CBC.

Compression Traffic compression: Automatic [1], enabled [yes] or disabled [no].

[1] In Automatic mode, the VPN Client will automatically adapt to the gateway's parameters.



Extra HMAC (TLS-Auth)

Extra HMAC This option adds an authentication layer to the packets exchanged between the VPN Client and the VPN gateway. For this option to be fully operational, it must also be configured for the gateway (on gateways, this option is often referred to as "TLS-Auth").

If this option is activated, a key must be typed in the field below the ticked box. The same key must also be typed in 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" must also be defined:

- BiDir The specified key is used both ways (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

Gateway

Dead Peer Detection (DPD)

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

Ping Gateway Period, expressed in seconds, between two "pings" sent by the VPN Client to the gateway. By this, the VPN Client confirms to the gateway that it is still active.

Detect Gateway Time, expressed in seconds, after which the gateway is considered down if no "ping" has been received.



On Dead Peer Detection When the gateway is detected as down (i.e. after the "Detect Gateway" time is up), the tunnel can be closed or the VPN Client may try and reopen it.

[1] The DPD function is activated 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.

Gateway related parameters

Explicit exit	This parameter configures the VPN Client to send the gateway a specific VPN tunnel closing frame when the tunnel is closed. If this option is not selected, the gateway will use DPD to close the tunnel on the gateway's endpoint, which is less effective.
Check Gateway Certificate	Determines the control level of the gateway's certificate. In the current version, two levels are available: <ul style="list-style-type: none">• - Yes (the validity of the certificate is verified)• - No (the validity of the certificate is not verified) The "Lite" choice is reserved for later usage and, in the current version, is equivalent to "yes".
Check Gateway Options	Gives the possibility to determine the coherence level between the VPN tunnel and gateway parameters (encryption algorithms, compression, etc.). <ul style="list-style-type: none">• - Yes: Coherence is verified for all VPN parameters. The VPN tunnel won't open if a parameter is different.• - Lite: The coherence between the VPN Client and the gateway is only verified for essential parameters.• - Apply: Gateway parameters will be applied.• - No: Coherence isn't verified before opening the tunnel. The VPN tunnel will try to open, even though no traffic may pass if some parameters aren't coherent.
Validate the subject of the gateway certificate	If this field is filled in, the VPN Client will check that the subject of the certificate received from the gateway is, indeed, the one specified.
Redundant Gateway	Defines the address of an alternate VPN gateway that the VPN Client will switch to when the initial gateway is down or inactive. The redundant VPN gateway's address can be either an IP or DNS address. See Section " Redundant gateway ".

Others

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



Establishment

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

Key Renegotiation

Bytes, Packets, Lifetime

Keys can be renegotiated when any of 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 criteria is set, keys will be renegotiated when the first of these expires.

Tunnel Options

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

Tunnel MTU Virtual interface MTU. When the values are set, it is recommended that the tunnel MTU's value be lower than the one of the physical interface MTU. The default value for MTU is 0, meaning that the software will use the MTU value of the physical interface minus a fixed delta value.

Tunnel IPv4 Defines the VPN Client's behavior when receiving an IPv4 configuration from the gateway:

- Automatic: Accepts the information sent by the gateway
- Yes: Checks whether the information sent by the gateway matches the configured behavior. If not, a warning message is displayed on the console and the tunnel is not established.
- No: Ignore

Note: Please check that "IPv4 tunnel" and "IPv6 tunnel" aren't both set to "No".



Tunnel IPv6 Defines the VPN Client's behavior when receiving an IPv6 configuration from the gateway:

- - Automatic: Accepts the information sent by the gateway
- - Yes: Checks whether the information sent by the gateway matches the configured behavior. If not, a warning message is displayed on the console and the tunnel is not established.
- - No: Ignore

Note: Please check that "IPv4 tunnel" and "IPv6 tunnel" aren't both set to "No".

Tunnel Establishment Options

Port/TCP	Port number used for establishing the tunnel. The default port value is 1194. The tunnel will use UDP by default. The "TCP" option transfers the tunnel to TCP.
Authentication Timeout	Time allowed for establishing the authentication phase, at the end of which it will be assumed that the tunnel won't open. When this timeout is reached, the tunnel is closed.
Retransmissions	Number of protocol message retries. If no answer is received before this number is reached, the tunnel is closed.
Traffic setup timeout	Tunnel establishment phase: time after which the tunnel is closed if any of the steps hasn't been completed.

Traffic

Traffic detection to open the tunnel With OpenVPN, the remote network's details are not configured (they are automatically obtained during the tunnel opening exchange with the gateway). In order to implement traffic detection with OpenVPN, it becomes necessary to explicitly state the remote network's details. That is the purpose of the IPv4 and IPv6 fields.

Filling in both fields is not necessary.

The IP field is a sub-network address, configured as an IP address and a prefix length. Example: IP=192.168.1.0 / 24: the first 24 bits of the IP address are taken into account, i.e. the network: 192.168.1.x

Note: These parameters are associated with the traffic detection function. The box "Automatically open this tunnel on traffic detection" in the "**Automation**" tab must be ticked for the IPv4 and IPv6 fields to be active.

Tunnel traffic check If these fields are filled in, VPN Client will try to send a "ping" to these addresses after opening the VPN tunnel. The connection status (reply to pings or no reply to pings) will be displayed in the console.

Filling in both fields is not necessary.

Note: No particular steps are taken if the "ping" goes unanswered.

Automation

See Section [Automation](#)

Certificate

See Section [Management of Certificates](#).

Remote sharing

See Section [Remote desktop sharing](#)



Redundant Gateway

Stormshield VPN Client can be used for managing a redundant VPN gateway.

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

If the DPD is lost and a redundant gateway has been configured, the tunnel will automatically try to re-open. It is possible to configure the redundant gateway identical with the main one, in order to benefit from the automatic reopening mode without having to use two gateways.

The algorithm for taking the redundant gateway into account 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 is applied to the redundant gateway:

- If the redundant gateway isn't responding,

 - the VPN Client will try to open the VPN tunnel with the initial gateway.

i NOTE

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.



Automation

Stormshield VPN Client can perform automatic operations for each VPN tunnel, such as switching to a tunnel fallback, opening the tunnel automatically if certain criteria are met, running batches or scripts at various points when opening or closing a tunnel, etc.

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

For each tunnel type, configuring these automatic operations is done via the "Automation" tab of the tunnel: Phase 2 (IKEv1), Child SA (IKEv2) or TLS (SSL).

Tunnel fallback

See Section [VPN tunnel fallback "VPN tunnel fallback"](#)

Automatic opening mode

- When the VPN Client starts The tunnel will automatically open when the VPN Client is launched [1]
- When a USB Drive is inserted The tunnel is included in a USB Drive configuration (see Section "[USB mode](#)") and will automatically open when this USB Drive is inserted [2]
- When traffic is detected The tunnel will automatically open when traffic is detected that is heading towards an IP address on the remote network.



[1] This option gives the possibility to open a tunnel automatically by double-clicking on the ".tgb" file in which it is included: Choose the option "Automatically open this tunnel when VPN Client starts after logon", export the configuration in a file called "tunnel_auto.tgb", quit the VPN Client. By double-clicking the "tunnel_auto.tgb" file, the VPN Client starts and the tunnel opens automatically.

NOTE

The automatic opening of a tunnel by double-clicking the ".tgb" file which contains it is a function that is not available on TheGreenBow VPN Certified.

[2] This option is also used to characterize a VPN tunnel that should open automatically when a smart card or token containing the certificate used by the VPN tunnel is inserted.

GINA mode

Enable before Windows logon	This option indicates that the VPN connection can be opened before the Windows logon: It appears in the GINA connections window (see Section " GINA mode " below)
Open automatically when GINA starts at logon	When this option is ticked, the tunnel will automatically open before the Windows logon. This option is enabled if the option "Enable before Windows logon" is selected.
Open a browser window for captive portal authentication	When using Wi-Fi networks, it is sometimes necessary to perform a local authentication on a dedicated portal. For GINA mode users, the VPN Client will implement a new browsing window which opens automatically before the tunnel is opened and allows the user to authenticate itself on the captive Wi-Fi portal.



Security advisory: for security reason, this function is no longer available from release 6.62. [Contact us](#) if this feature is required for your use of the VPN Client.

Scripts

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

The command lines can be:

- Calling a "batch" file, e.g. "C:\vpn\batch\script.bat"
- Executing a program, e.g. "C:\Windows\notepad.exe"
- Opening a webpage, e.g. "http://192.168.175.50"
- etc.

Several applications are possible:

- Creating a semaphore file when the tunnel is opened so that a third-party application can detect the moment the tunnel is opened,
- The automatic opening of one of the intranet servers of the company once the tunnel is opened,
- Cleaning or checking a configuration before opening the tunnel,



- Checking the workstation (antivirus is up-to-date, correct versions of the applications, etc.) before opening the tunnel,
- Automatic cleaning (file deletion) of a workspace on the workstation before closing the tunnel,
- Application for counting openings, closings, and durations of VPN tunnels,
- Changing the network configuration, once the tunnel is opened, then restoring the initial network configuration once the tunnel is closed,
- etc.

i NOTE

Scripts cannot be configured for a tunnel configured in GINA mode. Editable fields are deactivated.

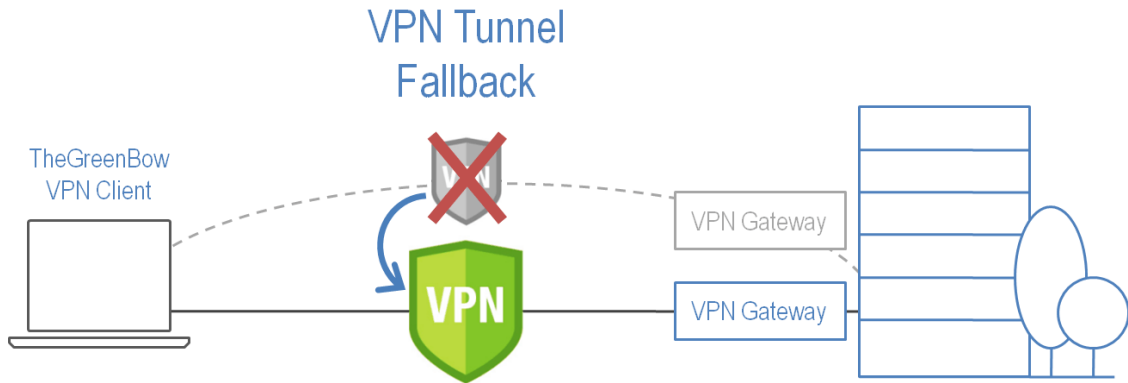


VPN tunnel fallback

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

VPN tunnel

Automatic fallback



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

Tunnel fallback

Tunnel to switch to

Message to display

Fallback retries

Allow the user to refuse the fallback.

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



IPv4 and IPv6

Stormshield VPN Client is compatible with IPv4 and IPv6 protocols, both for communicating with the gateway and with the remote network. The VPN Client gives the possibility to combine the use of IPv4 and IPv6, for example for opening an IPv4 secure connection in a VPN tunnel transported on IPv6.

The choice between IPv4 and IPv6 is made according to the IP address if it is digital, otherwise according to the DNS resolution. For the latter, the resolution of the gateway name will provide an IPv4 or IPv6 IP address, or both. If both are provided, the IPv4 address is selected by default.

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

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

The image shows two screenshots of the Stormshield VPN Client configuration interface for a Child SA. The top screenshot shows the IPv4 configuration tab selected, with the following fields: VPN Client address (0 . 0 . 0 . 0), Address type (Subnet address), Remote LAN address (0 . 0 . 0 . 0), and Subnet mask (0 . 0 . 0 . 0). The bottom screenshot shows the IPv6 configuration tab selected, with the following fields: VPN Client address (::), Address type (Subnet address), Remote LAN address (::), and Prefix length (0).

i NOTE

Choosing IPv4 or IPv6 has an impact on the settings of the other configuration tabs of the tunnel. Therefore, for these other tabs, the IPv4/IPv6 selection button still appears on the top-right corner but is disabled.

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



Certificate management



Stormshield VPN Client is the VPN connection software for which the innovations in terms of PKI integration are the most advanced on the market. Stormshield VPN Client is compatible with every PKI on the market in a flexible, evolutive, vastly customizable manner, with many automatic operations available.

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

Stormshield VPN Client specifically implements the following functions and features:

- Interface with the various means of storing certificates: token, smart card, certificate store, file, VPN security policy, USB Drive
- Characterization of the means of storing certificates to be used: automatic selection between several competing means
- PKCS11 and CSP access to tokens and smart cards
- Management of PKCS12, X509, PEM and PFX type certificates
- Configuration of certificates to be used according to multiple criteria: subject, key usage, etc.
- Management of certificates on the user's side (the VPN Client's side) such as VPN gateway certificates, including validity dates, certificate chains, root certificates and CRL management
- Validation of client and gateway certificates: mutual authentication with identical or different certification authorities (importation of specific CAs)
- Use of private PKCS1 and PKCS8 keys
- Possible pre-configuration of all PKI parameters for an automatic integration during installation

Stormshield VPN Client is equipped with additional security features for PKI management, such as automatically opening or closing a tunnel upon insertion or removal of the smart card, or the possibility to configure the PKI and smart card interface in the software setup file in order to make the deployment more automatic.

The configuration and characterization of the certificates to be used is done in three steps:

1/ The "Certificate" tab of the relevant tunnel: Phase 1 (IKEv1) or IKE Auth (IKEv2) or TLS (SSL).



2/ The "PKI Options" tab of the "Tools > Options" window in the Configuration panel

3/ An optional initial configuration file: vpnconf.ini

Configuration

Select a certificate ("Certificate" tab)

The 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.

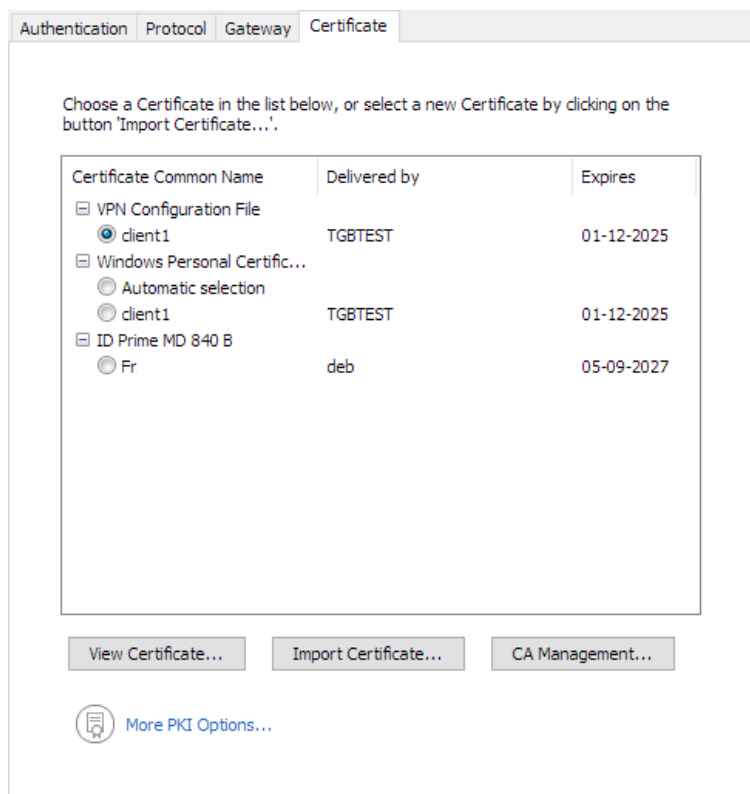
The VPN Client gives the possibility to choose a certificate stored:

- In the VPN Configuration file (see below "[Importing a certificate](#)")
- In the Windows Certificate Store (see below "[Windows Certificate Store](#)")
- On a smart card or token (see below "[Configuring a smart card or token](#)")

The "Certificate" tab for the relevant tunnel lists all accessible storage units that contain certificates. If a unit does not contain any certificates, it will simply not appear in the list (e.g. if the VPN Configuration file does not contain any certificates, it will not appear in the list).

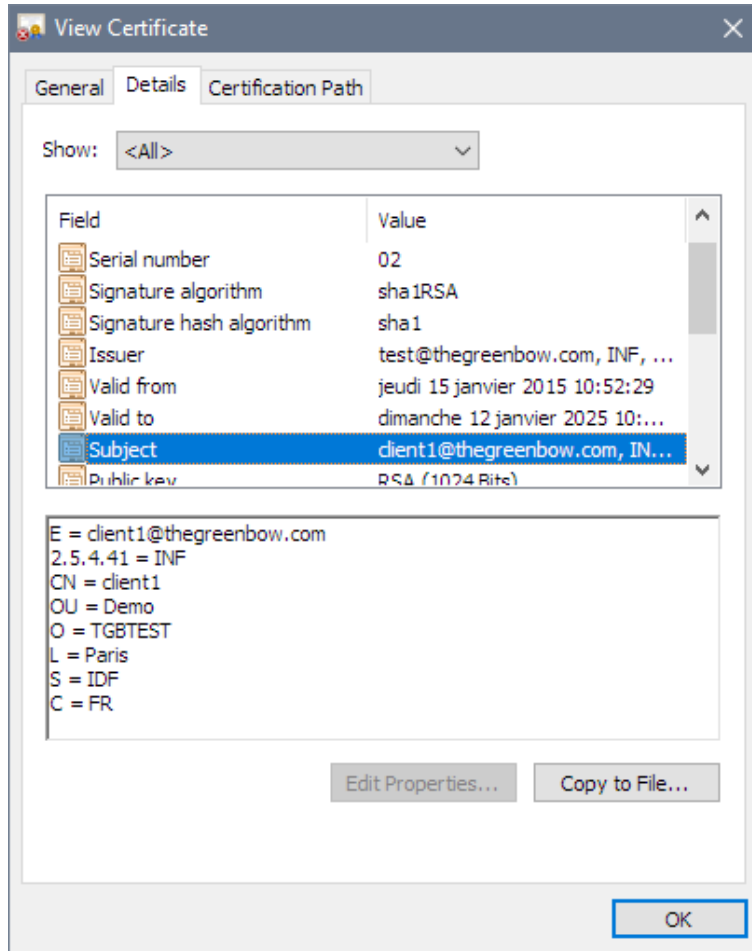
Clicking the desired unit displays the list of stored certificates.

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





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



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

Identity _____

Local ID

Remote ID

Importing a certificate

Stormshield VPN Client can import PEM or PKCS12 type certificates in the VPN security policy. This solution is less secure than using the Windows Certificate Store or a smart card, but makes transporting certificates easier.

Importing a PEM type certificate



- 1/ In a phase 1's Certificate tab, click "Import Certificate..."
 - 2/ Choose "PEM type"
 - 3/ Select ("Browse") the root and user certificates and the user private key to import
- Note: The file containing the private key should not be encrypted.
- 4/ Confirm

The certificate appears and is selected in the certificate list displayed in the "Certificate" tab.
Saving the VPN policy: The certificate will be saved in the VPN security policy.

Importing a PKCS12 type certificate

- 1/ In a phase 1's Certificate tab, click "Import Certificate..."
- 2/ Choose "P12 type"
- 3/ Select ("Browse") the PKCS12 certificate to import
- 4/ If it is password-protected, type in the password and confirm

The certificate appears and is selected in the certificate list displayed in the "Certificate" tab.
Saving the VPN policy: The certificate will be saved in the VPN security policy.



Windows Certificate Store

In order to be identified by the VPN Client, certificates from the Windows Certificate Store must meet the following criteria:

- The Certificate must be certified by a certification authority (which excludes self-signed certificates)
- The Certificate must be located in the "Personal" Certificate Store (it represents the personal identity of the user who wants to open a VPN tunnel towards his company network).

i NOTE

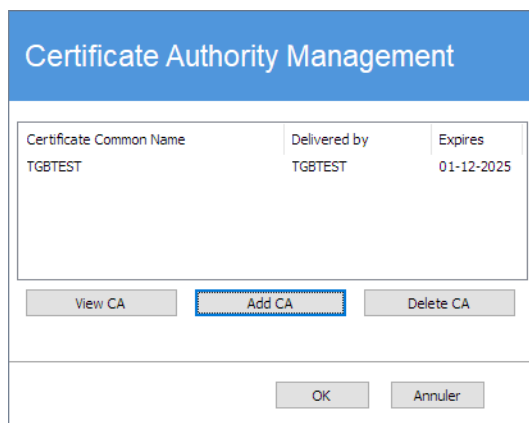
In order to manage the certificates in the Windows Certificate Store, Microsoft offers in the standard version the management tool "certmgr.msc". To use this tool, go to the Windows "Start" menu then type "certmgr.msc" in the "Search for programs or files" field.

CA (Certification Authority) Management

If Stormshield VPN Client is configured to check the Client and gateway certificates, importing the Certification Authorities (CAs) may be required in addition to the already used certificates.

This is the case every time the software fails to find the gateway certificate's CA locally, i.e. in the following situations:

- 1/ The gateway certificate's CA is different from the Client's, and this gateway CA is not present/accessible on the workstation (typically, it is not found in the Windows certificate store)
- 2/ The gateway certificate's CA is the same as the client's, but the client's CA is stored on a token or smart card. In such cases, the software cannot access it.
- 3/ EAP mode is selected (this mode doesn't require a client certificate), and the gateway certificate's CA is not present/accessible on the workstation.



- 1/ In the "CA Management" window, click on "Add CA"
- 2/ Choose the desired CA certificate type (PEM or DER)
- 3/ Select ("Browse") the CA to be imported



Using a VPN tunnel with a smart card certificate

When a VPN tunnel is configured to use a certificate stored on a smart card or token, the PIN code for this smart card will be required from the user each time a tunnel is opened.

If the smart card isn't inserted or the token can't be accessed, the tunnel won't open.

If the certificate found doesn't meet the configured criteria (see "PKI options" above), the tunnel won't open.

If the PIN code entered is wrong, VPN Client will warn the user about having 3 consecutive attempts before the smart card is blocked.

VPN Client is equipped with a mechanism for automatically detecting the insertion of a smart card.

This means that the tunnels associated with the certificate stored on a smart card will be established automatically when this smart card is inserted. By the same token, pulling out the smart card will close all corresponding tunnels.

To activate this function, tick: "Automatically open this tunnel when a USB stick is inserted" (see Section [Automation](#))



Remote desktop sharing

Usually, opening a "Remote desktop" session on a Windows computer through internet requires the establishment of a secure connection as well as the input of the connection parameters (the remote computer's address, etc.).

Stormshield VPN Client can be used for simplifying and automatically securing the opening of a "Remote desktop" session: With a single click, the VPN connection with the remote workstation is established and the RDP (Remote Desktop Protocol) session automatically opens on this remote workstation.



Remote desktop sharing configuration

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

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

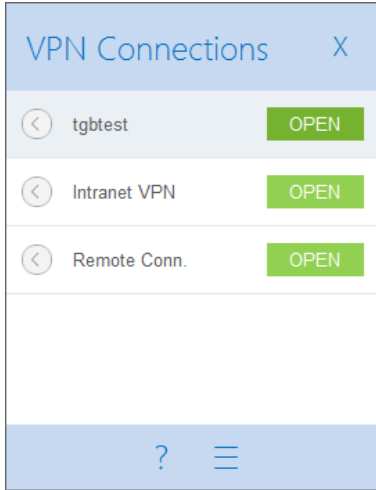
Alias	Name or IP address
Corporate_desktop	192.168.175.50

In order to open this RDP connection in a single click, it is recommended to use the "**Connection panel management**" function to have it specifically displayed in the connection panel.



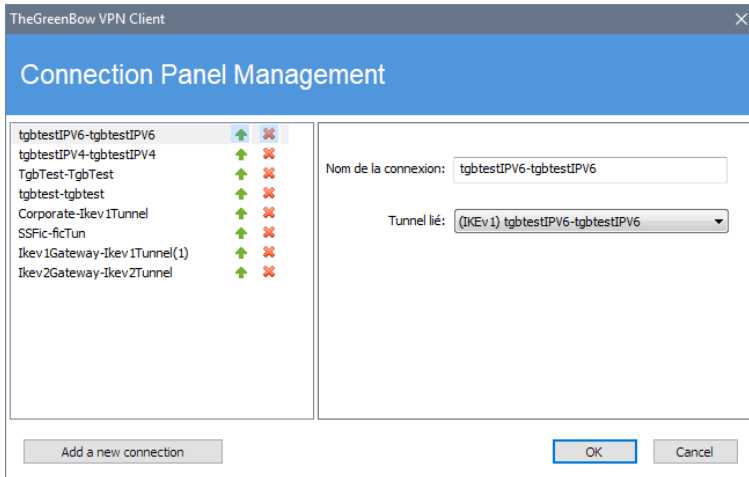
Connection panel management

In version 6.4 and later of the VPN Client, the Connection panel is entirely customizable.



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

A new window, available through the "Tools > Connection Panel Management" menu, allows for the management of VPN connections in the Connection panel, including creation, naming and sorting.



The new configuration window of the Connection panel gives the possibility to:

- Choose the VPN connections that appear in the Connection panel
- Create and sort VPN connections
- Rename VPN connections

The left side of the window displays the list of connections as they appear in the Connection panel, while the right side displays the connection's parameters: name, corresponding VPN tunnel and RDP [remote sharing] configured connection, if any.



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

i NOTE FOR THE ADMINISTRATOR

The connection panel configuration is saved in the VPN Configuration file. Therefore, it can be exported into .tgb files, which are useful for deploying an identical connection panel across all workstations.

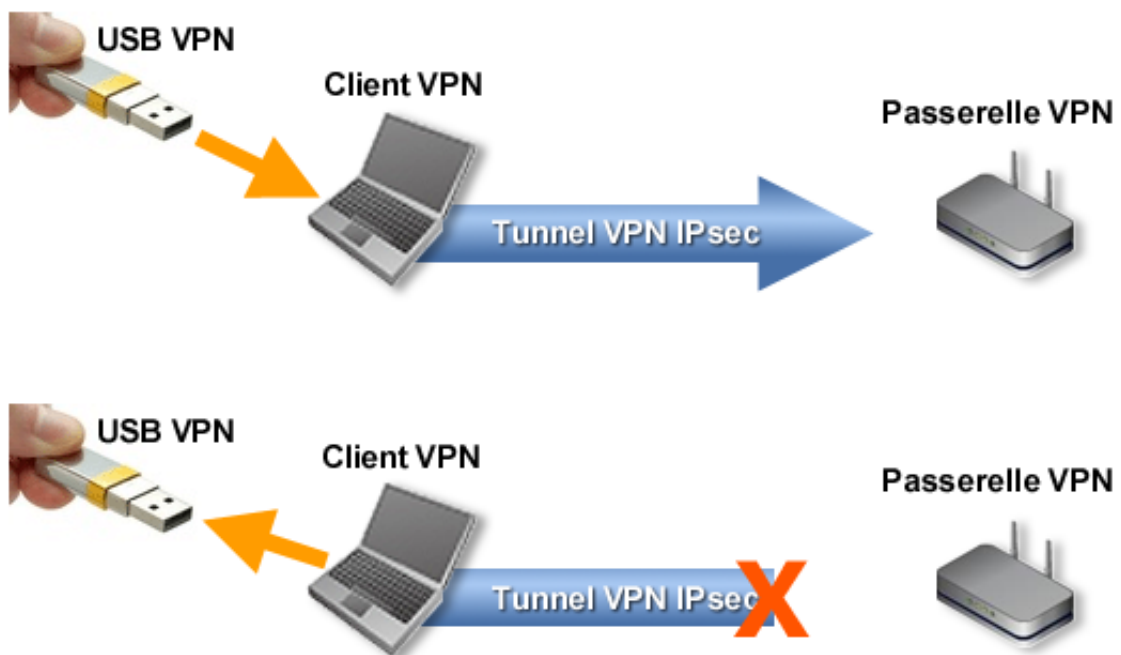


USB mode

VPN USB mode

Stormshield VPN Client is equipped with a unique VPN connection management mode known as the VPN USB mode.

In this mode, the VPN security policy is memorized securely on a removable storage device (USB Drive). The workstation from which the VPN connection is opened is clear of all VPN security elements. The VPN connection is established automatically as soon as the USB Drive is inserted and closed when the USB Drive is removed.



In the VPN USB mode:

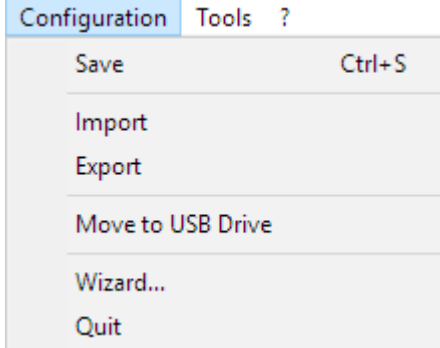
- No security elements are memorized on the workstation from which the VPN connection is opened as the workstation is clear of any VPN security policy.
- The security elements are transported securely on the removable storage device (USB Drive).
- The removable storage device can be a standard USB Drive.
- The security elements are memorized on the USB Drive and protected with a password.
- The VPN connection automatically opens when the USB Drive is inserted.
- The VPN connection automatically closes when the USB Drive is removed.

The USB Drive containing the VPN security policy will hereinafter be referred to as "VPN USB Drive".



Configuring USB mode

VPN USB mode configuration is done through the configuration wizard available in the "Configuration > Move to USB Drive" menu of the Configuration panel.



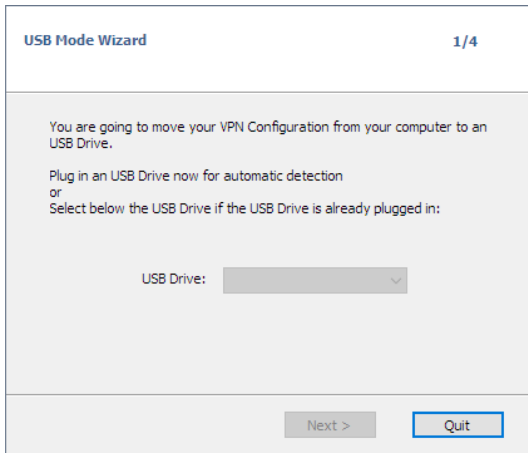
Step 1: Choosing a USB Drive

Step 1 gives the possibility to choose the removable device (USB Drive) to use for protecting the VPN security policy.

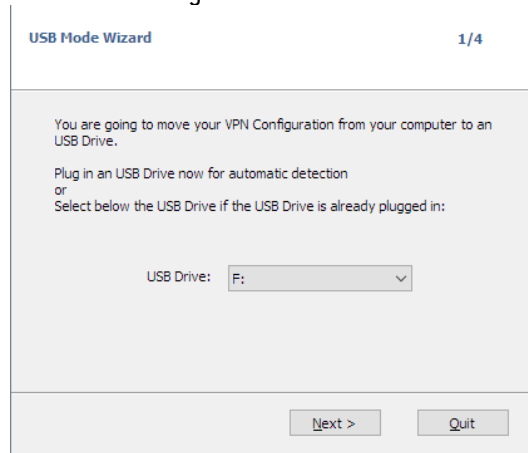
If a key is already inserted, it is automatically displayed in the list of available USB Drives.

Otherwise simply insert the chosen USB Drive during this step. It will be detected automatically upon insertion.

No USB Drive inserted

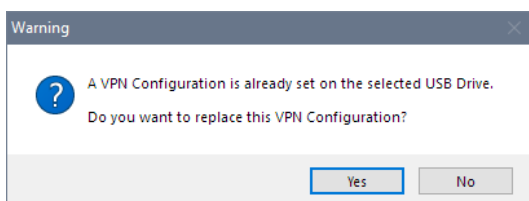


USB Drive already inserted



i NOTE

The USB mode only permits the protection of a single VPN Configuration on a USB Drive. If a VPN Configuration already exists on the inserted USB Drive, the following warning will be displayed:





i NOTE
If an empty USB Drive is inserted and it is the only key inserted into the workstation, the wizard will automatically move on to step 2.

Step 2: Protecting the VPN USB security policy

Two protections are available:

1/ Pairing with the user's workstation:

The VPN USB policy can be uniquely paired to the workstation from which it originates.

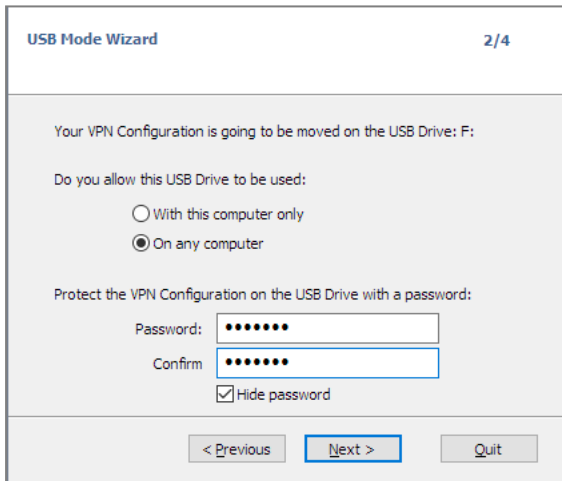
In this case, the VPN USB Drive can be used on this workstation only.

On the other hand, if the USB Drive is not paired with a specific workstation, the VPN USB Drive can be used on any workstation equipped with the VPN Client.

2/ Password protection:

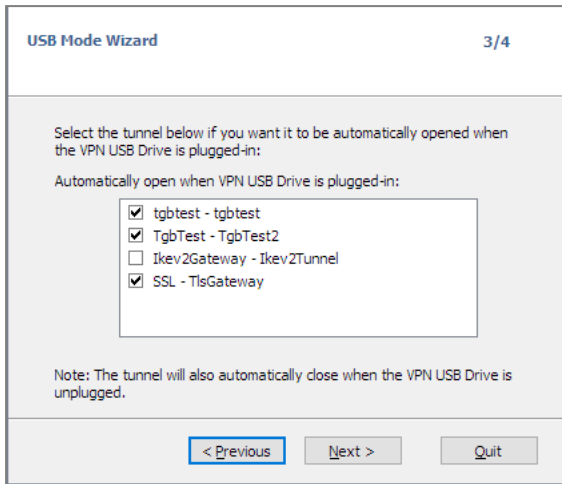
The VPN USB security policy can be protected with a password.

If so, the password will be required every time the VPN USB Drive is inserted.



Step 3: Automatically opening the tunnel

The wizard gives the possibility to configure the VPN connections that will be opened automatically every time the VPN USB Drive is inserted.



Step 4: Summary

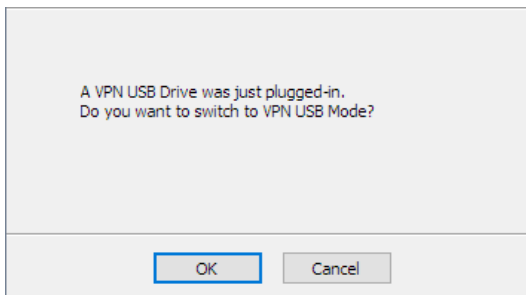
The summary gives you the opportunity to check whether the VPN USB Drive is properly configured.

Upon the validation of this final step, the workstation's VPN security policy is transferred onto the USB Drive.

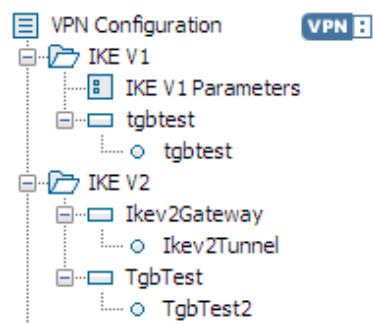
It remains active as long as the USB Drive is inserted. Upon removal of the VPN USB Drive, the VPN Client will revert to an empty VPN Configuration.

Using the USB mode

After launching Stormshield VPN Client with or without a loaded VPN security policy, insert the VPN USB Drive. The following information window is automatically displayed:



Upon validation, the VPN USB policy is loaded automatically and, if any, the corresponding tunnel(s) is/are opened automatically. USB mode is identified in the Configuration panel by a "VPN USB mode" icon in the top-right corner of the tree:





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

i NOTE

The VPN Client can only consider one VPN USB Drive at a time. As long as a VPN USB Drive is inserted, no other inserted VPN USB Drives are taken into account

i NOTE

The import function is deactivated in VPN USB mode.

The VPN USB security policy can be edited in VPN USB mode. The changes made to the VPN policy are saved on the VPN USB Drive.

i NOTE

The VPN Client has no function that would allow the direct changing of a password or the pairing with a workstation. In order to change those parameters, follow these steps:

1. Insert the VPN USB Drive
2. Export the VPN Configuration
3. Remove the VPN USB Drive
4. Import the VPN Configuration exported during step 2
5. Reload the USB mode wizard with this configuration and the new parameters.



GINA mode

GINA mode

GINA mode gives the possibility to open VPN connections before the Windows logon.

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

When a tunnel is configured in "GINA mode", a tunnel opening window similar to the Connection panel is displayed on the Windows logon screen. It lets you open the VPN tunnel manually.



Much like the VPN Connection panel, this window gives the possibility to manually open a tunnel.

A VPN tunnel can also be opened automatically before the Windows logon.

Lastly, for Wi-Fi connection users requiring an authentication on a dedicated portal, the VPN Client implements an automatic browsing window that can be used for authentication on this captive Wi-Fi portal.

Configuring GINA mode

The configuration of a VPN connection in GINA mode is done in the "Automation" tab of the relevant tunnel. See Section "[Automations](#)"

Gina mode

- Enable before Windows logon.
- Automatically open this tunnel when Gina starts at logon
- Open a browser window for captive portal authentication.

Using GINA mode

When the VPN tunnel is configured in "GINA mode", the GINA tunnels' opening window is displayed on the Windows logon screen. The tunnel will open automatically if configured so.

A GINA-mode VPN tunnel can perfectly implement an X-Auth authentication (the user must enter his login and password) or a certificate-based authentication (the user must enter the PIN access code to the smart card).

! WARNING

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

**i NOTE**

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

i LIMITATION

Scripts, Mode Config and USB mode are not available for GINA mode VPN tunnels.

Similarly, a VPN tunnel configured using a certificate memorized in the Windows Certificate Store won't work in GINA mode. The reason for this is that the GINA mode is run before a Windows user is identified (prior to opening any session). Therefore, the software cannot identify the user store to use in the Windows Certificate Store.

Security recommendation

A tunnel configured in GINA mode can be opened before Windows logon, i.e. by any user of the workstation. It is therefore strongly recommended to set up an authentication method, if possible a strong one, for a GINA-mode tunnel, e.g. an X-Auth authentication or preferentially a certificate-based authentication, on a removable device if possible. See Section [Configuring Phase 1: Authentication](#).



Security advisory: the option of opening a browser window for captive portal authentication may lead to a vulnerability (Cf. vulnerability [2018_7300](#)). It is strongly recommended to set this option only when it is strictly required.



Controlling access to the VPN policy

Any access to the VPN security policy (read, edit, apply, import, export) can be protected with a password. This protection also extends to command-line operations.

It is recommended to use this protection in order to guarantee the integrity and confidentiality of the VPN security policy.

In the version TheGreenBow VPN Certified, this protection is systematically activated: when it is not configured by the administrator, the password is set by default to "admin".

The VPN security policy's protection can be configured through the "Tools > Options" menu of the "View" tab.

View General Logs Management PKI Options Language

Lock access to Configuration Panel

Enter a password to lock down the access to the Configuration Panel. The Connection Panel is always available.

Password:

Confirm:

From the moment a password has been configured, opening the Configuration panel and accessing the VPN security policy (import, replace, add) will always be subjected to typing in the password:

- When the user clicks the icon on the taskbar
- When the user selects the "Configuration Panel" menu in the taskbar icon's menu
- When the user clicks the "Configuration Panel" button in the Connection panel
- When importing a new VPN security policy using command lines
- When updating the software

VPN Configuration

Please enter the password required to access the VPN Configuration Management.

Password:

OK Cancel

By combining this option with other display-limiting options of the software, the administrator can configure the software to be almost invisible and non-editable. See the corresponding section on display options.

In order to cancel password protection, empty both the "Password" and "Confirm" fields and confirm. This possibility is not available in TheGreenBow VPN Certified. In this version, the password is systematically configured. Emptying the two fields "Password" and "Confirm" set the password back to "admin".



i NOTE FOR THE ADMINISTRATOR

The protection of the VPN security policy can also be configured with command lines during installation.



Options

Access control

See Section "[Controlling access to the VPN security policy](#)".

Interface display (masking)

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

The popup window appearing when opening or closing a tunnel can also be hidden (taskbar popup).

View General Logs Management PKI Options Language

Lock access to Configuration Panel _____

Enter a password to lock down the access to the Configuration Panel. The Connection Panel is always available.

Password:

Confirm:

Show in systray menu _____

Console

Connection Panel

Configuration Panel

Quit

Systray sliding popup _____

Don't show the systray sliding popup

i NOTE FOR THE ADMINISTRATOR

When deploying the software, all these options can be preconfigured during Stormshield VPN Client's installation.

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

General



The screenshot shows the 'General' tab of the Stormshield VPN Client configuration window. It features two sections: 'VPN Client start mode' and 'Miscellaneous'. In the 'VPN Client start mode' section, the checkbox 'Start VPN Client after Windows Logon.' is checked. In the 'Miscellaneous' section, the checkbox 'Disable detection of network interface disconnection.' is unchecked, 'Show connection popup' is checked, and 'Show more parameters' is unchecked. The window has tabs for 'View', 'General', 'Logs Management', 'PKI Options', and 'Language'.

VPN Client start mode

If the option "Start VPN Client after Windows Logon" is ticked, the VPN Client will launch automatically at the start of the user session.

If the option isn't ticked, the user must launch the VPN Client manually, either by double-clicking on the desktop icon or by selecting the software's launch menu in the Windows "Start" menu.

See Section "[Windows desktop](#)".

Disabling detection of network interface disconnection

The normal behavior of the VPN Client is to close its endpoint of the VPN tunnel as soon as a communication problem with the remote VPN gateway is encountered.

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

By ticking the "Disabling detection of network interface disconnection" box, the VPN Client won't close tunnels as soon as a disconnection is experienced. This can guarantee a very high stability for the VPN tunnel, including on unreliable physical networks, typically wireless networks such as Wi-Fi, 3G, 4G or satellite.

Show connection popup

A connection window will automatically pop up each time a VPN connection is established.

This feature can be disabled by unticking the "Show connection popup" box.

Log management

See Section [Administrator logs](#) "Administrator logs".



PKI options

See Section [Presentation "Presentation"](#)

Language management

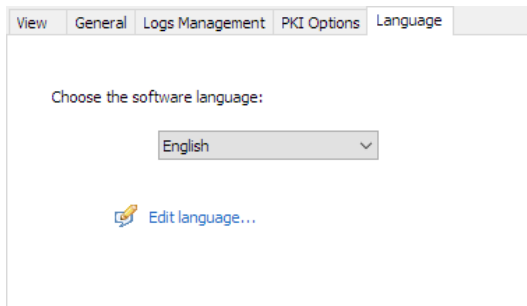
Choosing a language

Stormshield VPN Client can run in several languages.

It is possible to change languages while running the software.

In order to choose a different language, open the "Tools > Options" menu and select the "Language" tab.

Choose the preferred language in the drop-down menu:

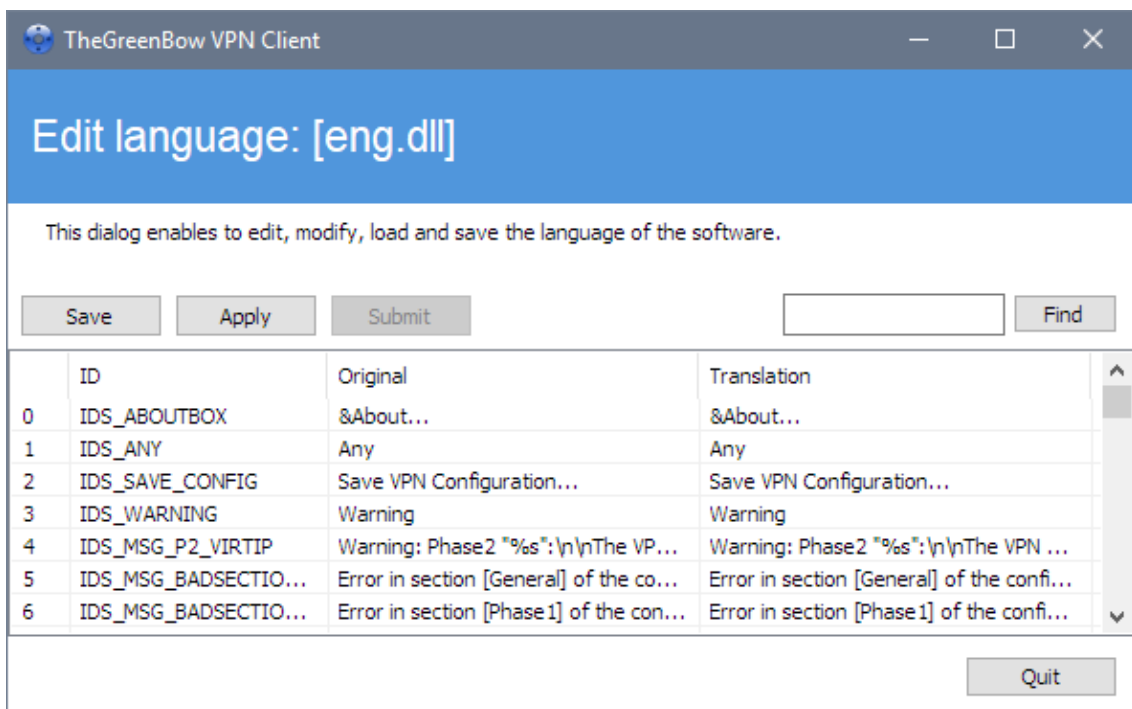


The list of available languages in the standard version of the software is presented as an appendix to the Section "[List of available languages](#)".

Editing or creating a language

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

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



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

Using the translation window, it is possible to:

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

Every edited or created language is saved in an ".lng" file

- 3/ Immediately apply changes to the software: this function lets you assess the relevance of a character string and its proper display in real time ("Apply" button)
- 4/ Send a new translation to TheGreenBow ("Submit" button)

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

i NOTE

The characters or character strings below shouldn't be modified during translation:

- "%s": the software will replace it by a character string
- "%d": the software will replace it by a digit
- "\n": indicates a carriage return
- "&": indicates that the following character should be underlined
- "%m-%d-%Y": indicates a date format (here US-style: month-day-year).



Only edit this field if confident in the format used in the translated language.

The "IDS_SC_P11_3" string must be left as is.



Administrator logs, console and tracing

Stormshield VPN Client comes equipped with three types of logs:

- The "administrator" logs are specifically designed for software activity and operation reports.
- The "Console" gives detailed information on the tunnels as well as the related opening and closing steps. It is mostly made of the IKE messages and gives high-level information about the establishment of the VPN tunnel. It is intended for use by the administrator for identifying possible VPN connection incidents.
- "Tracing" mode makes every component of the software write an activity log about its inner workings. This mode is intended for use by TheGreenBow support in order to diagnose software issues.

Administrator logs

Stormshield VPN Client can collect "administrator"-type logs: tunnel opening, expired certificate, connection duration, wrong login/password, changes to the VPN configuration, import or export of this configuration, etc. "Administrator" logs give a first-level analysis of the problems encountered.

Collected logs can be either and/or simultaneously:

- Stored in a local file
- Recorded in the Windows Event Log
- Sent in the syslog format to a Syslog server

The configuration of administrator logs is made in the "Tools > Options..." window under the "Logs management" tab.

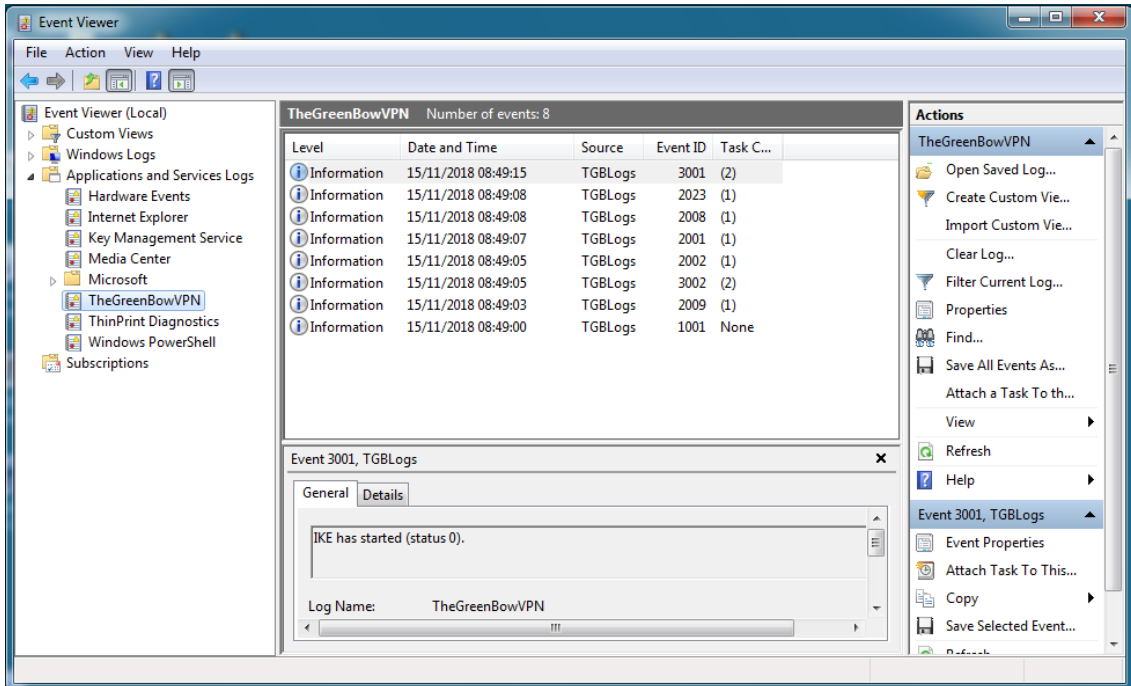
The screenshot shows the 'Logs Management' tab in the Stormshield VPN Client configuration window. The 'Syslog destination' section is expanded, showing the following options:

- Local log file
- Syslog server
 - IP or DNS Address:
 - Syslog UDP Port:
- Windows Event Viewer

**i NOTE**

The path for accessing Stormshield VPN Client's logs in the Windows Event Viewer is the following:

Event Viewer > Applications and Services Logs > TheGreenBowVPN

**i NOTE**

Administrator logs are listed in Appendix [Administrator logs](#)

i NOTE

The syslog flow can either be sent through the VPN tunnel or not, depending on the VPN Client's configuration.

i NOTE

Recording logs in the Windows Event Log or sending them to a syslog server are features available in the Premium and Certified versions only.

i NOTE

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

This directory can be read in all modes, but can only be written in Administrator mode.



Console

The Console can be accessed with the following methods:

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

The screenshot shows a window titled "VPN Console ACTIVE" with a toolbar containing "Save", "Stop", "Clear", and "Reset IKE" buttons. The main area displays a log of IKE negotiations. The status bar at the bottom right shows "Current line: 10" and "Max. lines: 10000".

```
TheGreenBow VPN Client Certified 6.50.010
20181226 15:23:57:976 TIKEV2_TgbTest SEND IKE_SA_INIT [HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20181226 15:23:58:031 TIKEV2_TgbTest RECV IKE_SA_INIT [HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][CERT]
20181226 15:23:58:031 TIKEV2_TgbTest IKE SA I-SPI 59B0601AAE2A2E63 R-SPI D0356589943EE12E
20181226 15:23:58:031 TIKEV2_TgbTest SEND IKE_AUTH [HDR][ID][AUTH][CP][SA][Tspi][Tsr][N(INITIAL_CONTACT)][N(ESP_TFC_PADDING_NOT_SUPPORTED)]
20181226 15:23:58:086 TIKEV2_TgbTest RECV IKE_AUTH [HDR][IDr][AUTHr][CP][SA][Tsr][Tspi][N(AUTH_LIFETIME)]
20181226 15:23:58:086 TIKEV2_TgbTest Outbound SPI C37807B0 10.60.60.2/255.255.255.255 => 192.168.175.0/255.255.255.0
20181226 15:23:58:086 TIKEV2_TgbTest Inbound SPI 4F7CD0EA 192.168.175.0/255.255.255.0 => 10.60.60.2/255.255.255.255
20181226 15:23:58:086 TIKEV2_TgbTest IKE CHILD renewal in 1688 seconds (15:52:06)
20181226 15:23:58:086 TIKEV2_TgbTest IKE AUTH renewal in 1708 seconds (15:52:26)
20181226 15:23:58:121 TIKEV2_TgbTest [VirtualIf] Virtual Interface properly configured for instance 1 and IfIndex 22.
```

The Console has the following functions:

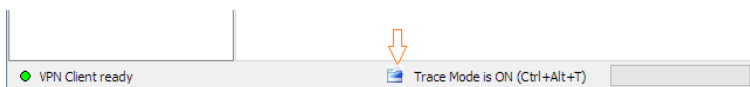
- Save: Saves all the traces displayed in the window into a file
- Start/Stop: Start/stop console log
- Clear: Erases the contents of the window
- Reset IKE: Restarts the IKE service

Tracing mode

Tracing mode is enabled using the shortcut: CTRL+ALT+T

Enabling tracing mode does not require a software restart.

When tracing mode is enabled, every component of Stormshield VPN Client generates activity logs. The logs produced are stored in a folder accessible by clicking the blue "folder" icon located in the status bar of the Configuration panel (main interface).



Note for the administrator

Activating logs can only be done through the Configuration panel, the access to which can be restricted to the administrator only.



Even though logs do not contain any sensitive information, it is recommended that, if activated by the administrator, said administrator ensures that they are deactivated and, if possible, deleted them when quitting the software.

Tracing logs are kept for 10 days. The software automatically deletes files older than this.

i NOTE

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



Security recommendations

Recommendations

The following recommendations are addressed to the software's Administrator.

General recommendations

In order to maintain a proper security level, the operating conditions and usages listed below must be followed:

- The system administrator and the security administrator, tasked respectively with installing the software and defining the VPN security policies, are considered trustworthy.
- The user of the software is a person who has proper qualifications. Specifically, said person must not reveal the information used to confirm his/her identity to the encryption system.
- The VPN gateway that the VPN Client connects to can trace the VPN activity and lead back, if necessary, to the causes of malfunctions or policy security violations.
- The user's workstation is clean and properly administered. It is equipped with an up-to-date antivirus software and is protected with a firewall.
- Bi-keys and certificates used to open the VPN tunnel are generated by a trustworthy certification authority.

Operating precautions

The machine used for the installation and running of Stormshield VPN Client software must be clean and properly administered. In particular:

- 1/ It must be equipped with an antivirus software with a regularly updated database,
- 2/ It must be protected by a firewall that controls (segregates or filters) the inbound and outbound communications of the workstation that do not already go through the VPN Client,
- 3/ Its operating system is up-to-date when it comes to the different security patches,
- 4/ Its configuration means that it is protected against local attacks (memory analysis, patch or binary corruption).

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

[Computer health guide](#) (Guide d'hygiène informatique, document in French)

[Configuration guide](#) (Guide de configuration, document in French)

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

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

When installing on Windows 7, the following Microsoft guide can also be checked for information:

[Common Criteria Security Target, Windows 7 and Windows Server 2008 R2](#)



VPN Client administration

It is strongly recommended to protect access to the VPN security policy with a password and to restrict the software's visibility to the end user as detailed in Section "[Controlling access to the VPN policy](#)".

It is also recommended that this protection be defined during installation, using the options presented in the "Deployment Guide" (tgbvpn_ug_deployment_en.pdf).

It is recommended to monitor the users of the VPN Client in a "user" environment and to restrict the use of the operating system with administrator rights as much as possible.

It is recommended to keep the "Start VPN Client after Windows Logon" mode (after Windows logon), which is the default installation mode.

Finally, it should be noted that Stormshield VPN Client will apply the same VPN configuration (security policy) to all the users of a multiple-users workstation. As a consequence, it is recommended to run the software on a dedicated workstation (for instance by keeping an administrator account and a user account, as previously mentioned).

VPN security policy configuration

Sensitive information within the VPN security policy

It is recommended that no sensitive data should be stored in the VPN configuration file.

Because of this, it is recommended not to use the following features of the software:

- 1/ Do not store the EAP login/password in the configuration (function described in Section "[IKE Auth: IKE SA](#)", paragraph "Authentication")
- 2/ Do not import any certificates in the configuration (function described in Section "[Importing a certificate](#)") and preferably use certificates stored on removable devices (tokens) or in the Windows Certificate Store.
- 3/ Do not use the "Preshared key" mode (function described in Section "[IKE Auth: IKE SA](#)") and preferably use the "Certificate" mode with certificates stored on removable devices (tokens) or on the Windows Certificate Store.
- 4/ Do not export the VPN security policy without encryption, i.e. not protected by a password (function described in Section "[Exporting a VPN security policy](#)")

User authentication

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

Specifically, it should be noted that Preshared key authentication, despite being easy to implement, grants any user of the workstation the possibility to establish a VPN tunnel without the authentication being cross-checked.

Type of user authentication	Strength
Preshared key	weak
Static X-Auth	
Dynamic X-Auth	
Certificate stored within the VPN security policy	
Certificate in the Windows Certificate Store	
Certificate on a smart card or token	strong



VPN gateway authentication

It is recommended to check the VPN gateway certificate as described in Section 3.2 "PKI options" of the document called "Management of PKI, certificates, tokens and smart cards" [tgbvpn Ug pki smartcard en].



In this configuration, to avoid any exploit of the vulnerability [2018_7293](#), it is mandatory to fill the Remote ID of the relevant VPN Tunnel with the subject of the VPN Gateway Certificate.

IKE protocol

The TheGreenBow VPN Certified software certification only applies to the IKEv2 protocol. It is recommended to configure IKEv2 tunnels exclusively.

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

It is recommended to configure the VPN tunnel using the "All traffic through the tunnel" mode and to activate the "Disable Split Tunneling" (split tunneling) mode.

See Section [Child SA: Child SA "Child SA: Child SA"](#) and [Child SA: Advanced "Child SA: Advanced"](#).

GINA mode

It is recommended to choose a strong authentication method for all tunnels in GINA mode.

Cypher algorithms and key lengths

When using TheGreenBow VPN Certified, and in order to comply with provisions contained in Appendix B-1 of RGS 2.0, the use of the following algorithms is recommended:

IKEv2	Encryption	AES128 minimum, AES192 or AES256
	Authentication	SHA2 256 minimum or SHA2 384 or SHA2 512
	Key group	DH15 (3072) minimum or DH16 (4096), DH17 (6144), DH18 (8192)
ESP	Encryption	AES128 minimum, AES192 or AES256
	Integrity	SHA2 256 minimum or SHA2 384 or SHA2 512
	Diffie-Hellman	DH15 (3072) minimum or DH16 (4096), DH17 (6144), DH18 (8192)

ANSSI IPSec configuration recommendations

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



Appendices

Shortcuts

Connection panel

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

Configuration panel tree:

- F2 Edit the name of the selected Phase.
- DEL Delete a selected phase, if any, after confirmation by the user.
If the Configuration itself is selected (root of the tree), a full reset of the configuration will be proposed.
- CTRL+O Opens the corresponding VPN tunnel if a Phase 2 is selected.
- CTRL+W Closes the corresponding VPN tunnel if a Phase 2 is selected.
- CTRL+C Copy the selected Phase to the clipboard.
- CTRL+V Paste (add) the Phase copied to the clipboard.
- CTRL+N If the VPN Configuration is selected, creates a new Phase 1. If a Phase 1 is selected, creates a Phase 2.
- CTRL+S Save the VPN security policy.

Configuration panel

- CTRL+ENTER Switches to the Connection panel.
- CTRL+D Open the VPN traces "Console" window
- CTRL+ALT+R Restart the IKE service
- CTRL+ALT+T Activate the tracing mode (log generation)
- CTRL+S Save the VPN security policy.

Languages

Code	Language	Name in English	Code ISO 639-2
1033 (default)	English	English	EN
1036	Français	French	FR
1034	Español	Spanish	ES
2070	Português	Portuguese	PT
1031	Deutsch	German	DE
1043	Nederlands	Dutch	NL
1040	Italiano	Italian	IT



2052	简化字	Simplified Chinese	ZH
1060	Slovenscina	Slovenian	SL
1055	Türkçe	Turkish	TR
1045	Polski	Polish	PL
1032	ελληνικά	Greek	EL
1049	Русский	Russian	RU
1041	日本語	Japanese	JA
1035	Suomi	Finnish	FI
2074	српски језик	Serbian	SR
1054	ภาษาไทย	Thai	TH
1025	عربي	Arabic	AR
1081	हिन्दी	Hindi	HI
1030	Danske	Danish	DK
1029	Český	Czech	CZ
1038	Magyar nyelv	Hungarian	HU
1044	Bokmål	Norwegian (Bokmål)	NO
1065	فارسی	Farsi	FA
1042	한국어	Korean	KO

Administrator logs

ID Log define	ID Log value	Severity	Log string
LOGID_STARTERINIT	1001	Notice	Starter service is started.
LOGID_VPNCONFSTARTING	2001	Notice	GUI is starting.
LOGID_VPNCONFSTOPPED	2002	Notice	GUI has closed.
LOGID_PWDSET	2004	Info	Admin password has been changed.
LOGID_PWDCHECK	2005	Error/Info	Admin password has been verified (status %d).
LOGID_PWDRESET	2006	Warning	Admin password has been reset.
LOGID_TGBIKESTARTED	3001	Notice	IKE has started (status %d).
LOGID_TGBIKESTOPPED	3002	Notice	IKE has stopped.
LOGID_TUNNELOPEN	3004	Info	Tunnel %s is asked to open.
LOGID_VPNCONFCRASHED	2003	Notice	GUI crashed (state %d).
LOGID_TGBIKECRASHED	3003	Notice	IKE crashed (state %d).
LOGID_STARTERSTOP	1002	Notice	Starter service is stopped.
LOGID_RESETIKE	2007	Warning	IKE is asked to reset.
LOGID_VPNCONFSTARTED	2008	Notice	GUI has started from user %s.
LOGID_VPNCONFSTOPPING	2009	Notice	GUI is stopping from user %s.
LOGID_VPNCONFLOADERROR	2010	Error	Configuration couldn't load (reason: %s).
LOGID_VPNCONFOPEN TUNNEL	2011	Info	GUI opens tunnel (source: %s).
LOGID_VPNCONFCLOSE TUNNEL	2012	Info	GUI closes tunnel (source: %s).
LOGID_VPNCONFSAVE	2013	Notice	New configuration is saved.
LOGID_VPNCONFIMPORT	2014	Info	%s has been imported.
LOGID_VPNCONFIMPORTERR	2015	Error	%s could not be imported (status %d).
LOGID_VPNCONFEXPORT	2016	Info	%s has been exported.
LOGID_TOKENINSERT	2017	Info	Token %s has been inserted.
LOGID_TOKENEXTRACT	2018	Info	Token %s has been extracted.
LOGID_USBININSERT	2019	Info	USB Drive has been inserted



LOGID_USBEXTRACT	2020	Info	USB Drive has been extracted
LOGID_INSTALLATION	2021	Info	VPN running for the 1st time.
LOGID_UPDATE	2022	Info	VPN software has been updated to version %s.
LOGID_VERSION	2023	Info	VPN Version is %s.
LOGID_GINASTARTED	4001	Notice	Gina has started.
LOGID_GINASTOPPING	4002	Notice	Gina is stopping.
LOGID_GINAOPENTUNNEL	4003	Info	GINA opens tunnel [source: %s].
LOGID_GINACLOSETUNNEL	4004	Info	GINA closes tunnel [source: %s].
LOGID_TUNNELAUTH_OK	3005	Info	Tunnel authentication Ok [%s].
LOGID_TUNNELTRAFFIC_OK	3006	Info	Tunnel ??? Ok
LOGID_TUNNELAUTH_NOK	3007	Error	Tunnel authentication failed [reason %d].
LOGID_TUNNELTRAFFIC_NOK	3008	Error	Tunnel ??? Failed [reason %d].
LOGID_AUTHREKEYING	3009	Info	Tunnel %s initiated rekey [source %d].
LOGID_AUTHREKEYED	3010	Info	Tunnel %s rekeyed.
LOGID_TUNNELREKEYING	3011	Info	Tunnel %s initiated rekey [source %d].
LOGID_TUNNELREKEYED	3012	Info	Tunnel %s rekeyed.
LOGID_PINCODE	3013	Notice/Error	Pincode is entered [status %d].
LOGID_DRIVERNOK	3014	Critical	Driver could not be loaded [status %d].
LOGID_IKEEXT_STOP	1003	Warning	IKEEXT service is stopped.
LOGID_IKEEXT_RESTART	1004	Notice	IKEEXT service is restarted.
LOGID_IKEEXT_ERROR	1005	Critical	IKEEXT could not be stopped [status %d].
SYSTEMLOGID_VIRTIFOK	3015	Info	Virtual interface created successfully [instance %d].
SYSTEMLOGID_VIRTIFNOK	3016	Error	Virtual interface couldn't not be created [error %d].
LOGID_TUNNELCLOSED	3017	Notice	%s tunnel successfully closed [%d min].
LOGID_TUNNELCLOSED_ERR	3018	Error	%s tunnel closed unexpectedly [%d].
LOGID_CERTERROR	3019	Error	Error %d when handling certificate %s.
LOGID_TUNNELDATA_UL	3020	Info	%d bytes sent inside the tunnel.
LOGID_TUNNELDATA_DL	3021	Info	%d bytes received inside the tunnel.

Technical characteristics of Stormshield VPN Client

General

Windows version Windows Server 2008 32/64bit
Windows Server 2012 R2 64bit
Windows Vista 32/64bit
Windows 7 32/64bit
Windows 8 32/64bit
Windows 10 32/64bit

Languages Arabic, Chinese (simplified), Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, Turkish

Operating mode

Invisible mode Automatically opening the tunnel when traffic is detected
Controlling access to the VPN security policies
Possibility to hide part or all of the interfaces

USB mode No VPN security policies on the workstation anymore
Opening the tunnel when a VPN-configured USB Drive is inserted
Automatically closing the tunnel when a VPN-configured USB Drive is extracted



Gina	Opening a tunnel before Windows logon using: Gina/XP Credential providers for Windows Vista, Windows 7 and above
Scripts	Running configurable scripts when opening or closing a VPN tunnel
Remote Desktop Sharing	Opening a remote computer (remote desktop) with a single click through the VPN tunnel
Connection/Tunnel	
Connection mode	Peer-to-peer (point-to-point between two workstations equipped with VPN Client) Peer-to-Gateway
Media	Ethernet, Dial up, DSL, Cable, GSM/GPRS, Wi-Fi Wireless LAN: 3G, 4G, satellite
Tunneling Protocol	IPSec: complete support IKEv1 or IKEv2 (IKE based on OpenBSD 3.1 [ISAKMPD]) SSL: complete support Diffie-Hellman DH group 1 to 18
Tunnel mode	Main mode and Aggressive mode
Mode Config	Obtaining automatically the network parameters from the VPN gateway
Cypher	
Encryption	Symmetric: DES, 3DES, AES 128/192/256bit Asymmetric: RSA Diffie-Hellman: DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) Hash: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512
Authentication	Administrator: Protecting access to the VPN security policies User: <ul style="list-style-type: none">- Static or dynamic X-Auth (prompt for each tunnel opening)- Hybrid Authentication- Preshared key- EAP (MSCHAP-V2)- Multiple Auth
PKI	<ul style="list-style-type: none">- Support for X509-, PKCS12- and PEM-type certificates- Multi-support: Windows Certificate Store, smart card, token- Certificate criteria: validity date, cancellation, CRL, subject, key usage- Possibility to characterize the token/smart card interface (See the list of certified tokens and smart cards)- Automatically detecting a token/smart card- Accessing the PKCS11 or CSP tokens/smart cards- "Client" and "Gateway" certificate check
Misc	
NAT/NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 and RFC 3947, IP address emulation, includes support for: NAT_OA, NAT keepalive, NAT-T aggressive mode, NAT-T in forced, automatic or disabled mode
DPD	RFC3706. Detection of inactive IKE endpoints.
Redundant Gateway	Redundant gateway management, automatically selected when DPD is triggered (inactive gateway)
Administrative	
Deployment	Options for the deployment of VPN policies (installation wizard command-line options, configurable installation files, etc.) Silent installation



VPN policy management	Import and export options for VPN policies Securing import/export using passwords, encryption and integrity control
Automatic operations	Possibility to open, close and monitor a tunnel through command lines (batch and scripts) Possibility to launch and quit the software using batchs
Log and traces	IKE/IPSec and SSL log console and possibility to enable tracing mode Administrator log: local file, Windows Event Log, syslog server.
Live update	Check for available updates using the software
License and activation	Flexibility when it comes to licenses (standard, temporary, limited duration, subscription), software activation (WAN, LAN) and deployment options (deployment of the activated softwares, silent activation, etc.)

License and credits

Credits and license references

/*

- * Copyright (c) 1998, 1999 Niels Provos. All rights reserved.
- * Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>. All rights reserved.
- * Copyright (c) 1998, 1999, 2000, 2001 Niklas Hallqvist. All rights reserved.
- * Copyright (c) 1999, 2000, 2001, 2002, 2004 Håkan Olsson. All rights reserved.
- * Copyright (c) 1999, 2000, 2001 Angelos D. Keromytis. All rights reserved.

*

- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
- * 1. Redistributions of source code must retain the above copyright
- * notice, this list of conditions and the following disclaimer.
- * 2. Redistributions in binary form must reproduce the above copyright
- * notice, this list of conditions and the following disclaimer in the
- * documentation and/or other materials provided with the distribution.

*

- * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR
- * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
- * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
- * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
- * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
- * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
- * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
- * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
- * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
- * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

*/



```
/* =====  
* Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.  
*  
* Redistribution and use in source and binary forms, with or without  
* modification, are permitted provided that the following conditions  
* are met:  
*  
* 1. Redistributions of source code must retain the above copyright  
* notice, this list of conditions and the following disclaimer.  
*  
* 2. Redistributions in binary form must reproduce the above copyright  
* notice, this list of conditions and the following disclaimer in  
* the documentation and/or other materials provided with the  
* distribution.  
*  
* 3. All advertising materials mentioning features or use of this  
* software must display the following acknowledgment:  
* "This product includes software developed by the OpenSSL Project  
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"  
*  
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to  
* endorse or promote products derived from this software without  
* prior written permission. For written permission, please contact  
* openssl-core@openssl.org.  
*  
* 5. Products derived from this software may not be called "OpenSSL"  
* nor may "OpenSSL" appear in their names without prior written  
* permission of the OpenSSL Project.  
*  
* 6. Redistributions of any form whatsoever must retain the following  
* acknowledgment:  
* "This product includes software developed by the OpenSSL Project  
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"  
*  
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY  
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR  
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
```



* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* [eay@cryptsoft.com]. This product includes software written by Tim
* Hudson [tjh@cryptsoft.com].
*
*/

Original SSLeay License

/* Copyright [C] 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson [tjh@cryptsoft.com].
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation [online or textual] provided with the package.



- *
 - * Redistribution and use in source and binary forms, with or without
 - * modification, are permitted provided that the following conditions
 - * are met:
 - * 1. Redistributions of source code must retain the copyright
 - * notice, this list of conditions and the following disclaimer.
 - * 2. Redistributions in binary form must reproduce the above copyright
 - * notice, this list of conditions and the following disclaimer in the
 - * documentation and/or other materials provided with the distribution.
 - * 3. All advertising materials mentioning features or use of this software
 - * must display the following acknowledgement:
 - * "This product includes cryptographic software written by
 - * Eric Young (eay@cryptsoft.com)"
 - * The word 'cryptographic' can be left out if the routines from the library
 - * being used are not cryptographic related :-).
 - * 4. If you include any Windows specific code (or a derivative thereof) from
 - * the apps directory (application code) you must include an acknowledgement:
 - * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 - * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
 - * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 - * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 - * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 - * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 - * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 - * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 - * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 - * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 - * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 - * SUCH DAMAGE.
- *
 - * The licence and distribution terms for any publically available version or
 - * derivative of this code cannot be changed. i.e. this code cannot simply be
 - * copied and put under another distribution licence
 - * [including the GNU Public Licence.]
- */



Contact

To contact our Technical Assistance Center (TAC) Stormshield:

- <https://mystormshield.eu/>

All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under **Technical support > Report an incident / Follow up on an incident**.

- +33 (0) 9 69 329 129

In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on <https://mystormshield.eu>.



STORMSHIELD

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2023. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.