GUIDE

STORMSHIELD VPN CLIENT

USER GUIDE

Date	Version	Details
May 2017	V6.4	Creation

Table of Contents

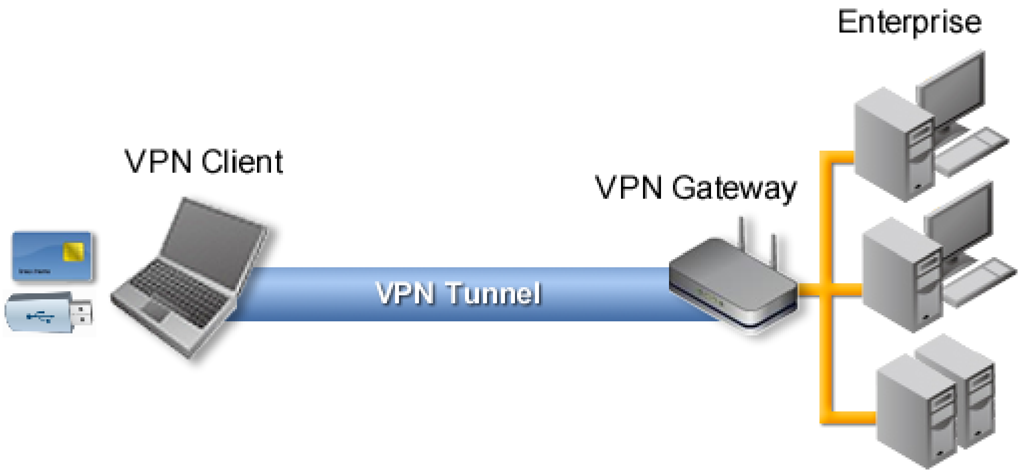
1 Presentation

The Stormshield VPN Client is based on the TheGreenBow VPN Client software and the present guide therefore derives from the official TheGreenBow User Guide.
All images in this document are for representational purposes only. They are based on the TheGreenBow VPN Client version and the actual Stomshield product may differ.

1.1 The Universal VPN Client

Stormshield VPN Client is a VPN Client software designed for any Windows workstation or laptop. It establishes a connection, and guarantees a secure communication with the information system of the company.

Stormshield VPN Client is universal and compatible with all IPsec VPN gateways on the market. It also helps to establish VPN tunnels in point-to-point connection between two machines equipped with the software.
Stormshield VPN Client implements IPsec, IKE and SSL standards to be compatible with openVPN Gateway.



1.2 Full compatibility with PKI

Stormshield VPN Client is fully integrated in all PKI (Public Key Infrastructure). He brings unparalleled flexibility in taking account of certificates and Smartcards:

- Compatibility with a wide range of Token and Smartcard (see list of qualified Tokens)
- Automatic detection of smartcard and token (PKCS11 or CSP) or storage media (file, Windows certificate store)
- Configuring Tokens "on the fly"
- Taking into account multi-format certificates (X509, PKCS12, PEM)
- Configuring multi-criteria certificates to be used (subject, key usage, etc...).

Stormshield VPN Client offers more features with additional security around the PKI management, such as the opening and closing of the tunnel upon insertion and removal of the Smartcard, or the ability to configure the PKI interface and Smartcard in the installer software, to automate deployment.

1.3 VPN security policies

Stormshield VPN Client provides a high level of security management and the consideration of VPN security policies.

The software can be configured when installed to restrict all access VPN security policies the administrator only.

The software also allows you to secure the maximum use of VPN security policies, conditioning the opening of a tunnel to the various authentication mechanisms available: X-Auth, certificates...

1.4 Stormshield VPN Client features

Stormshield VPN Client provides several specific features that made the software popular:

- Multi-tunnelling: simultaneous VPN tunnels, IKEv1, IKEv2 or SSL
- VPN Tunnel stability enhanced mechanisms
- VPN USB Mode: protection of VPN security policy on a removable media
- Secured Remote Desktop Sharing
- VPN Automations: scripts, automatic tunnel opening, etc.
- GINA Mode: VPN tunnel opening before Windows logon
- Deployment and integration facilities: customization, setup configuration, etc.

1.5 Specifications

Stormshield VPN Client provides the following features:

- Ability to support network in IPv4 and IPv6 simultaneously
- Ability to create IPsec VPN tunnel using either IKEv1 or IKEv2
- Ability to create VPN tunnel using either IPsec or SSL
- Multiple VPN tunnels with a mix of IPsec and SSL
- Point-to-point or peer-to-gateway IPsec VPN tunnel
- VPN Tunnel on all media types: Ethernet, WiFi, 3G, satellite
- Support of PKI, and gateway or user certificate management
- Taking into account Smartcards or tokens, and Windows certificate store
- User mode (limited), Director (VPN Security Policy Management) and USB (roaming)
- Open tunnel automatically and GINA mode
- X-Auth Authentication static or dynamic
- "DPD" (Dead Peer Detection) features and automatic failover the tunnel to a redundant VPN gateway
- Mechanisms for maintaining the VPN tunnel in unstable network
- IP filtering unauthorized flows (firewall feature)

For detailed specifications, see chapter "Stormshield VPN Client Specifications".

2 Installation

2.1 Installation

Installing Stormshield VPN Client is done by running the program:

Stormshield-vpn-x.xx.xxx.exe

The installation is a standard procedure that requires no user input.

Note: The performance of the system is configurable using a list of command line options, or by using an initialization file. These options are described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

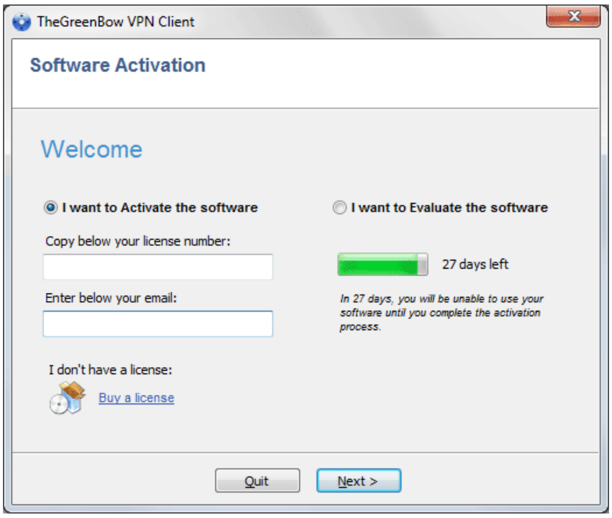
2.1.1Installation requirements

See chapter "Stormshield VPN Client specifications" for supported OS.
Installation on Windows XP, Windows Vista, Windows 7 and Windows 8 needs to be in Administrator mode the computer.
When this is not the case, a warning message notifies the user and the installation stops.

2.2 Evaluation period

At its first installation on a machine, the VPN Client is in evaluation period of 30 days. During the evaluation period, the VPN Client is fully operational: all features are available.

Each time the software is launched, the activation windows is displayed. It shows remaining number of days for evaluation.



TheGreenBow VPN Client

Software Activation

Welcome

● I want to Activate the software

Copy below your license number:

Enter below your email:

I don't have a license:

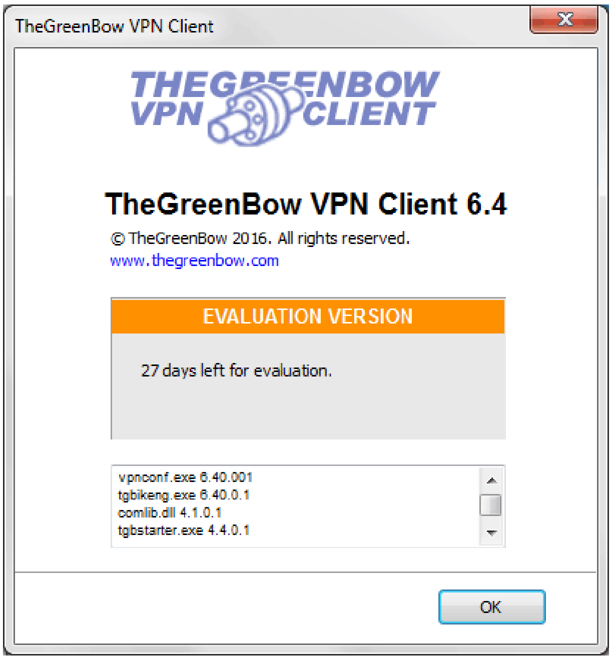
○ I want to Evaluate the software

27 days left

In 27 days, you will be unable to use your software until you complete the activation process.

For further evaluation of the software, select "I want to evaluate the software" and then click "Next>".

During the evaluation period, the "About..." window displays the remaining number of days for evaluation:



TheGreenBow VPN Client 6.4

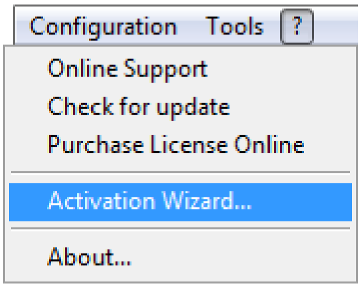
© TheGreenBow 2016. All rights reserved.
www.thegreenbow.com

EVALUATION VERSION

27 days left for evaluation.

```
vpnconf.exe 6.40.001
tgbikeng.exe 6.40.0.1
comlib.dll 4.1.0.1
tgbstarter.exe 4.4.0.1
```

During the evaluation period, it is always possible to directly access the software activation via the menu: "? > Activation Wizard..." from the Configuration Panel.



3 Activation

The VPN Client must be enabled to operate outside of the evaluation period.
The activation process is accessible either each time the software is launched or via the menu "?" > "Activation Wizard..." from the Configuration Panel.

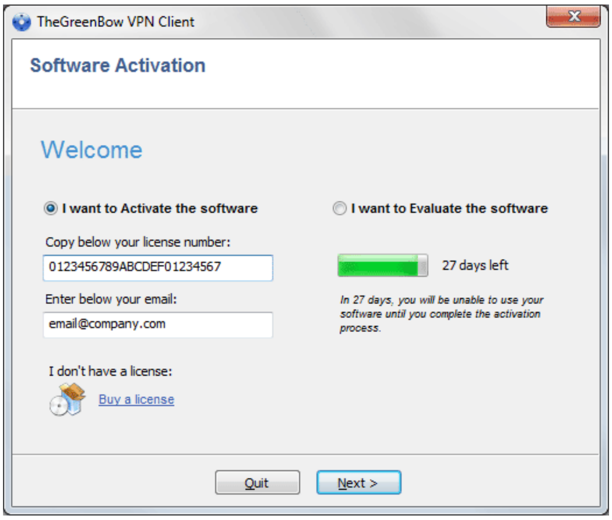
The activation process is a two-step procedure.

3.1 Step 1

Enter the license number received by email in "Copy here your license number". To get the license number, click on "Purchase license".

The license number can be copied and pasted directly from the email in the field. The license number is composed solely of characters [0 ... 9] and [A.. F], possibly grouped by 6 and separated by dashes.

Enter in the field "Enter your email address:" The email address identifying your activation. This information allows to recover in case of loss, information about your activation.



TheGreenBow VPN Client

Software Activation

Welcome

● I want to Activate the software

Copy below your license number:

0123456789ABCDEF01234567

Enter below your email:

email@company.com

I don't have a license:

Buy a license

○ I want to Evaluate the software

27 days left

In 27 days, you will be unable to use your software until you complete the activation process.

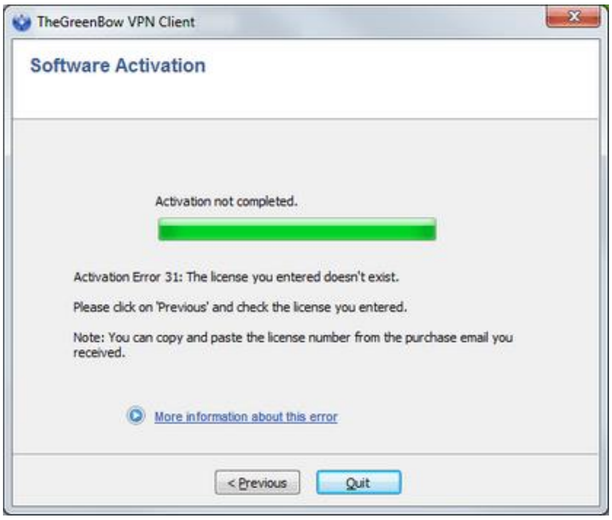
3.2 Step 2

Click "Next>", the online activation process runs automatically. When activation succeeds, click "Start" to start the software.

Note: The software activation is linked to the computer on which the software is installed. Thus, a license number which allows only one activation cannot to be reused on another computer, once activated.
Also, the activation of the license number can be reset by uninstalling the software.

3.3 Activation errors

Activating the software might fail for different reasons. Each error is indicated on the activation window. It is possible that a link provides information, or offers a way to fix the problem.



TheGreenBow VPN Client

Software Activation

Activation not completed.

Activation Error 31: The license you entered doesn't exist.

Please click on 'Previous' and check the license you entered.

Note: You can copy and paste the license number from the purchase email you received.

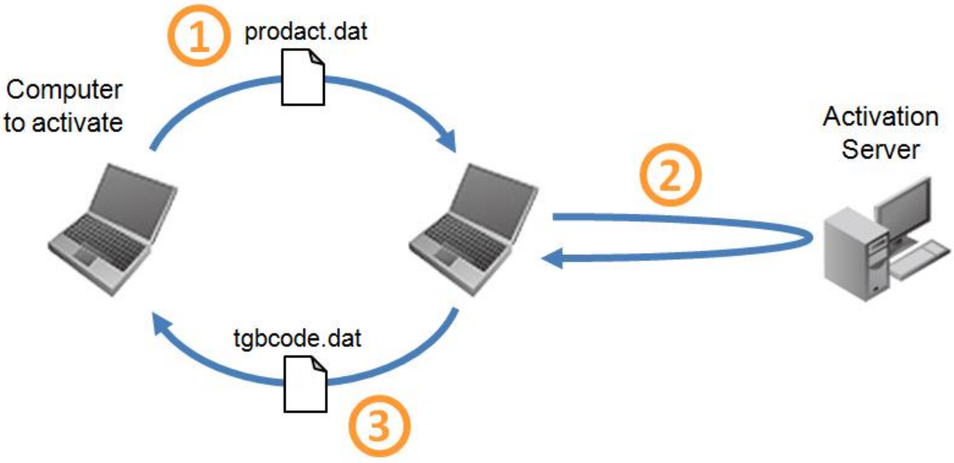
More information about this error

Activation errors that are the most common ones include:

N°	Meaning	Resolution
31	The license number is not correct	Check the license number
33	The license number is already activated on another computer	Uninstall the computer on which the license has been activated, or contact Stormshield sales team
53 54	Communication with the activation server is not possible	Check the extension is connected to the Internet Check the communication is not filtered by a firewall to a proxy. If applicable, configure the firewall to let the communication, or the proxy to redirect it correctly.

3.4 Manual activation

If you still have software activation error, it is possible to activate the software "manually" on TheGreenBow website:



① **"prodact.dat" file** On the computer to be activated, retrieve the "prodact.dat" file located in the Windows directory "My Documents". (1)

② **Activation** On a computer connected to the activation server (2), open the manual activation page (3), post prodact.dat file, and retrieve the tgbcode file automatically created by the server.

③ **"tgbcode" file** Copy this "tgbcode" file in the Windows "My Documents" of the computer to activate. Launch the software: it is activated.

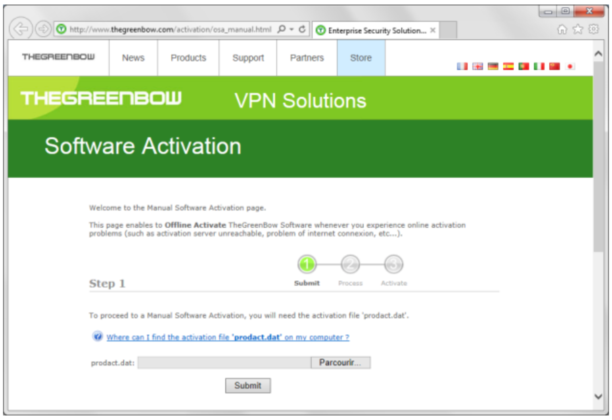
(1) The file "prodact.dat" file is a text file that contains the elements of the computer used for the activation. If this file does not exist in the "My Documents" folder, do the activation on the computer: even if it fails, it has the effect of creating this file.

(2) The activation server is TheGreenBow server available on the Internet.

(3) See detailed procedures below.

3.4.1Manual activation on the TheGreenBow server

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



http://www.thegreenbow.com/activation/osa_manual.html
Enterprise Security Solution...
THEGREENBOW
News
Products
Support
Partners
Store
THEGREENBOW
VPN Solutions

Software Activation

Welcome to the Manual Software Activation page.

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

Step 1

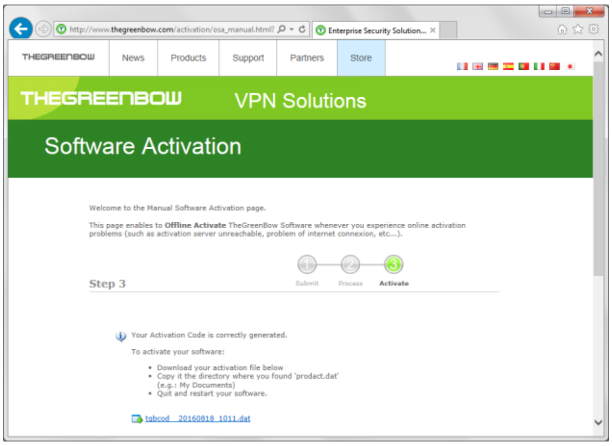
To proceed to a Manual Software Activation, you will need the activation file 'prodact.dat'.

Where can I find the activation file '**prodact.dat**' on my computer ?

prodact.dat: [Parcourir...]

[Submit]

Click the "Browse" button and open the "prodact.dat" file recovered on the computer to activate.
Click on "Submit". The activation server verifies the validity of the product.dat file information.
Click "Perform".
During download the activation server shows the file containing the activation code used to activate the computer.



http://www.thegreenbow.com/activation/osa_manual.html?
Enterprise Security Solution...
THEGREENBOW
News
Products
Support
Partners
Store
THEGREENBOW
VPN Solutions

Software Activation

Welcome to the Manual Software Activation page.

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

Step 3

Your Activation Code is correctly generated.

To activate your software:

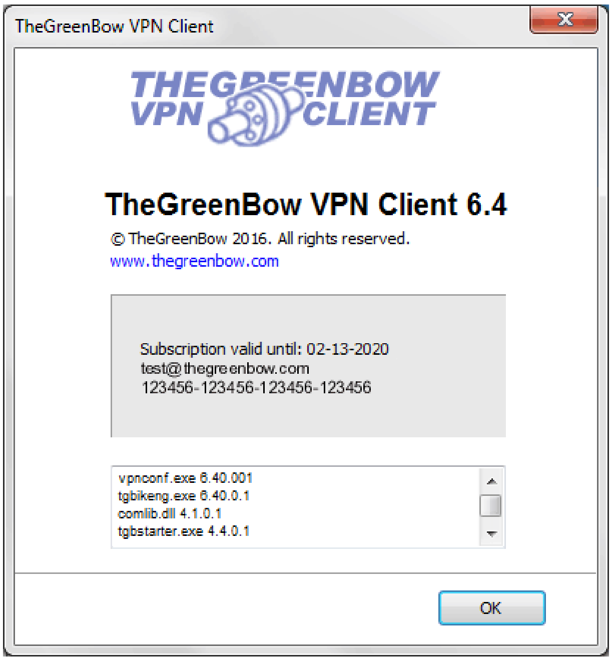
- Download your activation file below
- Copy it the directory where you found 'prodact.dat' (e.g.: My Documents)
- Quit and restart your software.

tgbcod__20160818_1011.dat

This file's name is as follow: tgbcode_[date]_[code].dat (e.g. tgbcod_20170225_1029.dat)

3.5 License and activated software

When the software is activated, the license and the email used for activation are available in the "About..." window of the software.



TheGreenBow VPN Client

TheGreenBow VPN Client 6.4

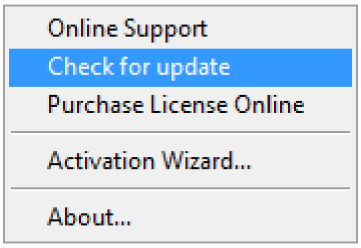
© TheGreenBow 2016. All rights reserved.
www.thegreenbow.com

Subscription valid until: 02-13-2020
test@thegreenbow.com
123456-123456-123456-123456

```
vpnconf.exe 6.40.001
tgbikeng.exe 6.40.0.1
comlib.dll 4.1.0.1
tgbstarter.exe 4.4.0.1
```

4 Software update

The software allows you to check at any time if an update is available through the menu of the Configuration Panel: "? > Check for update".



This menu opens the mystormshield.eu webpage.

4.1 How to obtain an update

The rules to obtain a software update are as follows:

During the maintenance period (1)	I can install any updates
Outside maintenance period, or without maintenance	I can install the minor updates (2)
During subscription period (3)	I can install any update

(1) The maintenance period starts on the first activation of the software.
(2) The minor releases (or maintenance updates) are identified by the last digit of the version, e.g. the "2" of "6.12".
(3) VPN Premium and VPN Certified only

Examples:
I activated the software in 6.12 release. My maintenance period has expired.
All updates from 6.13 to 6.19 releases are allowed.
Updates of 6.20 and above releases are denied.

4.2 Update of VPN security policy

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

Note: If access to the VPN security policy is locked by a password, this password is required during the update, to allow the configuration recovery.

4.3 Automation

Performing an update is configurable using a list of command line options, or by using an initialization file.

5 Uninstalling

To uninstall Stormshield VPN Client:
1/ Open the Windows Control Panel
2/ Select "Add / Remove programs"

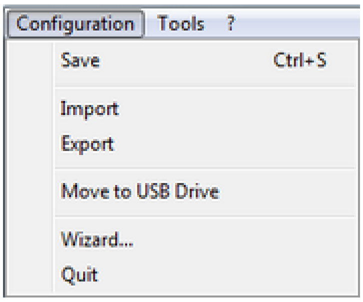
or

1/ Open Windows menu "Start"
2/ Select "Programs" > "Stormshield" > " Stormshield VPN Client" > "Network VPN Client Uninstall"

6 Quick use cases

6.1 Configuring a VPN tunnel

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



Use the wizard as described in chapter "VPN Configuration Wizard".

6.2 Setting the automatic opening of a VPN tunnel

Stormshield VPN Client allows configuring a VPN tunnel so it opens automatically.

A VPN tunnel can be automatically opened:

1/ Upon detection of traffic to the remote network. See chapter "Automation"

2/ Upon opening (double-click) of a VPN security policy file (".tgb" file). See chapter "Automation"

3/ While inserting a USB drive containing the appropriate VPN security policy. See chapter "Automation"

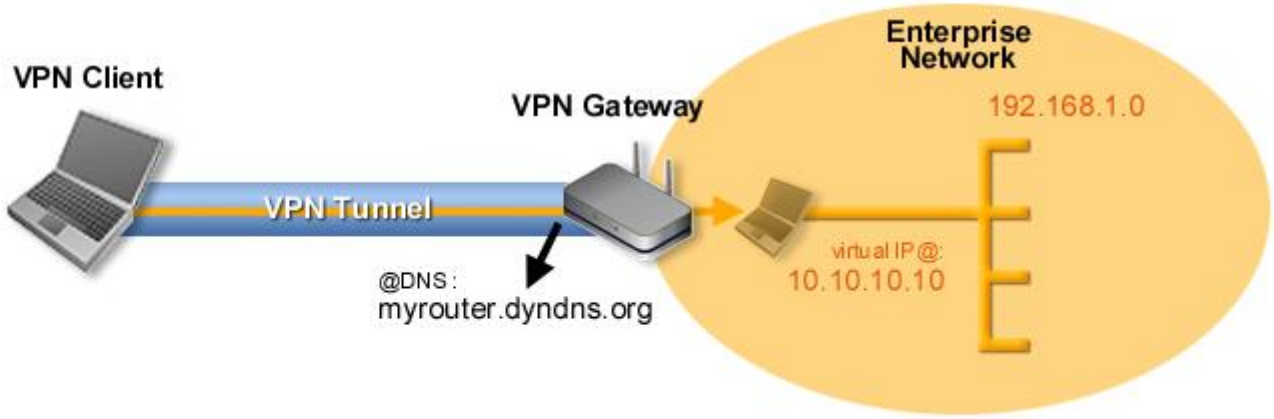
4/ While inserting a token or a smartcard containing the certificate used for the tunnel.
See chapter "Managing Certificates"

7 VPN Configuration Wizard

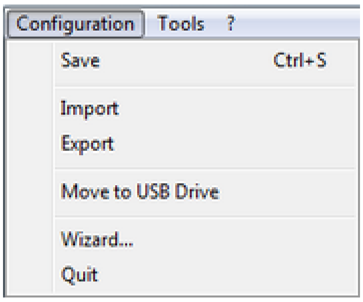
Stormshield VPN Client configuration wizard allows you to configure a VPN tunnel in 3 easy steps.

Using the Configuration Wizard is illustrated by the following example:

- The tunnel is opened between a computer and a VPN gateway with DNS address like "gateway.mydomain.com"
- The company's local network is 192.168.1.0 (it contains several machines with IP address such as 192.168.1.3, 192.168.1.4, etc...)
- Once the tunnel is open, the remote IP address in the corporate network will be: 10.10.10.10

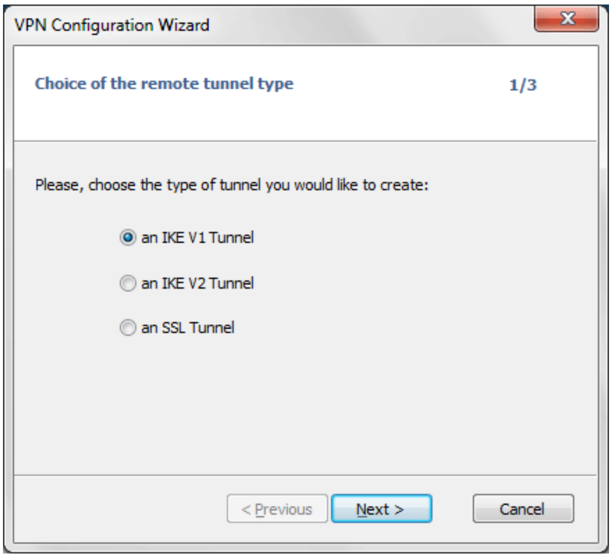


In the main interface, open the VPN Configuration Wizard: "Configuration > Wizard…".



Step 1

Choose the VPN protocol you want to use for the tunnel: IKE V1, IKE V2 or SSL.



VPN Configuration Wizard

Choice of the remote tunnel type 1/3

Please, choose the type of tunnel you would like to create:

● an IKE V1 Tunnel

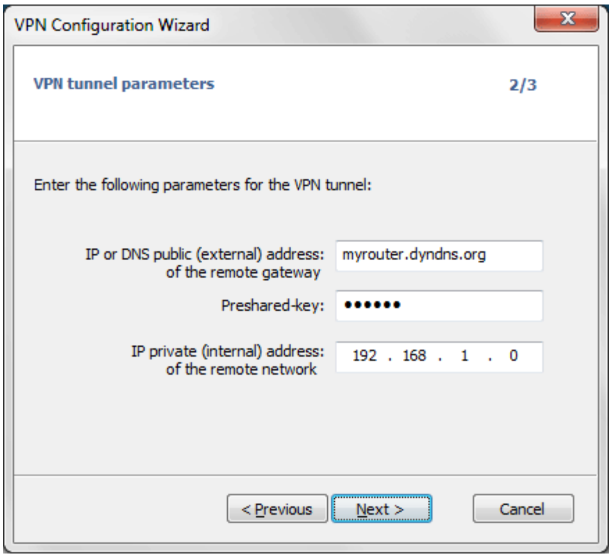
○ an IKE V2 Tunnel

○ an SSL Tunnel

Step2 with IKEv1 VPN:

Enter the following values:

- The IP or DNS address of the VPN gateway on the Internet Network side (example: myrouuter.dyndns.org)
- A preshared key which must be the same on the VPN gateway
- The IP address of the network (LAN) of the company (example: 192.168.1.0) (1)


VPN Configuration Wizard

VPN tunnel parameters 2/3

Enter the following parameters for the VPN tunnel:

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

Preshared-key: ••••••

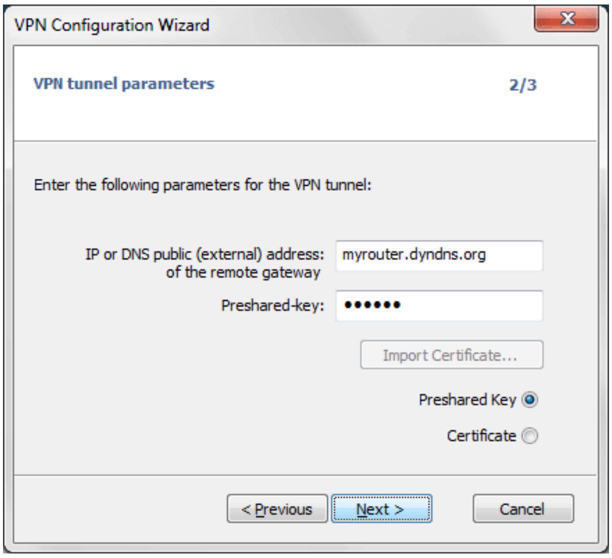
IP private (internal) address: of the remote network: 192 . 168 . 1 . 0

(1) By default, the remote network address is used with a prefix length of 24. This value can be modified later.

Step2 with IKEv2 VPN

Enter the following values:

- The IP or DNS address of the VPN gateway on the Internet Network side (example: myrouuter.dyndns.org)
- A preshared key which must be the same on the VPN gateway or
- A Certificate which must be imported via the "Import Certificate…" button (see chapter "Managing Certificates")


VPN Configuration Wizard

VPN tunnel parameters 2/3

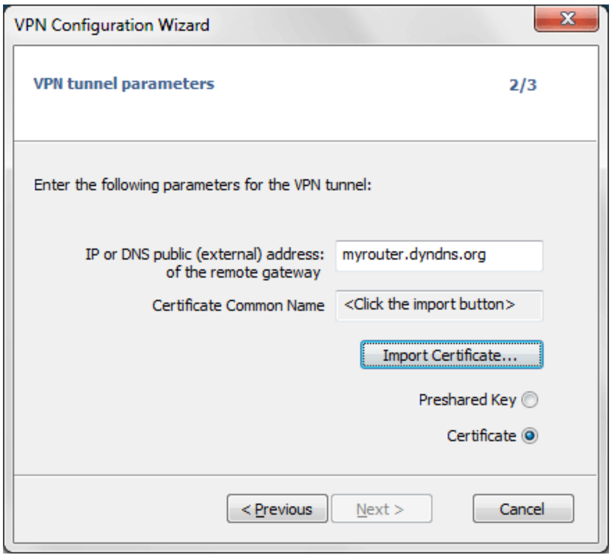
Enter the following parameters for the VPN tunnel:

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

Preshared-key: ••••••

Preshared Key ●

Certificate ○


VPN Configuration Wizard

VPN tunnel parameters 2/3

Enter the following parameters for the VPN tunnel:

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

Certificate Common Name: <Click the import button>

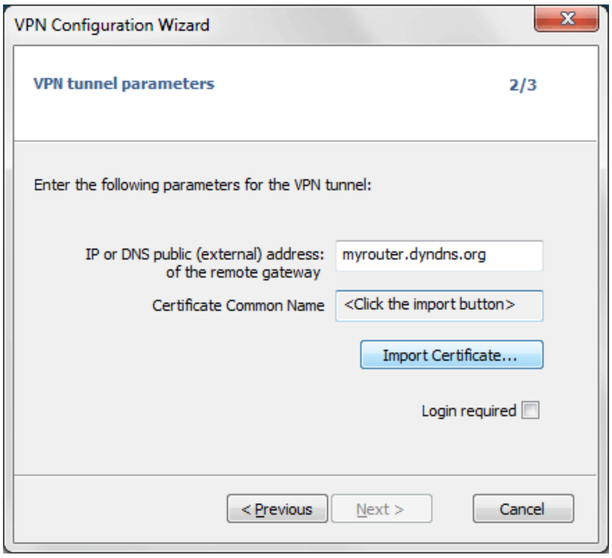
Preshared Key ○

Certificate ●

Step2 with SSL (OpenVPN) VPN

Enter the following values:

- The IP or DNS address of the VPN gateway on the Internet Network side (example: myrouuter.dyndns.org)
- A Certificate which must be imported via the "Import Certificate…" button (see chapter "Managing Certificates")



Enter the following parameters for the VPN tunnel:

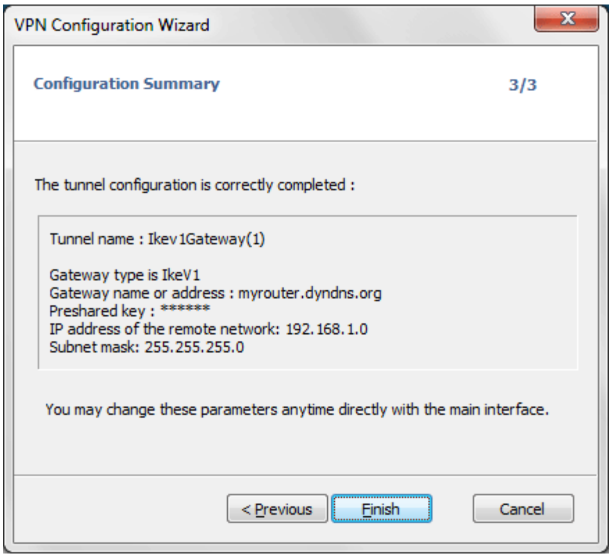
IP or DNS public (external) address: of the remote gateway myrouter.dyndns.org

Certificate Common Name <Click the import button>

Login required □

Step3

Check in the summary window that the settings are correct and click "Finish".
Example below for an IKEv1 VPN:



The tunnel configuration is correctly completed :

Tunnel name : Ikev1Gateway(1)

Gateway type is IkeV1
Gateway name or address : myrouter.dyndns.org
Preshared key : ******
IP address of the remote network: 192.168.1.0
Subnet mask: 255.255.255.0

You may change these parameters anytime directly with the main interface.

The VPN tunnel that has been configured appears in the VPN tree of the Configuration Panel.
Double-click to open the tunnel or refine the configuration using the tabs in the Configuration Panel.

8 User Interface

8.1 Overview

The VPN Client user interface allows to:
1/ configure the software itself (boot mode, language, access control, etc...)
2/ manage security policies (VPN configuration VPN tunnels, certificates management, import, export, etc.)
3/ use VPN tunnels (opening, closing, troubleshooting, etc...)

The user interface is divided into:

- The elements of the software available on the Windows Desktop (desktop icons, start menu)
- An icon in the taskbar and its associated menu
- The Connection Panel (list of VPN tunnels to open)
- The Configuration Panel

The Configuration Panel is composed of the following elements:

- A set of menus to manage the software and VPN security policies
- The VPN tunnel tree
- Configuration tabs for VPN tunnels
- A status bar

8.2 Windows Desktop

8.2.1Startup Menu

After installation, the VPN Client can be launched from the Windows Start menu.

Two links are created in the directory Stormshield / Network VPN Client start menu:
1/ Launch Network VPN Client
2/ Uninstall Network VPN Client

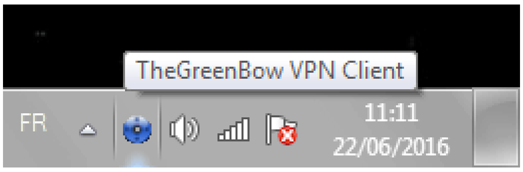
8.2.2Desktop

During the software installation, the "Network VPN Client" icon is created on the Windows desktop.
VPN Client can be launched directly by double-clicking on this icon.

8.3 Taskbar

8.3.1Icon

In current usage, Stormshield VPN Client is identified by an icon located in the taskbar.



The icon color changes if the tunnel is open:

🔵 Blue icon: no VPN tunnel is open

🟢 Green icon: at least one VPN tunnel is open

The "tooltip" the VPN Client icon indicates the status at any time of the software:

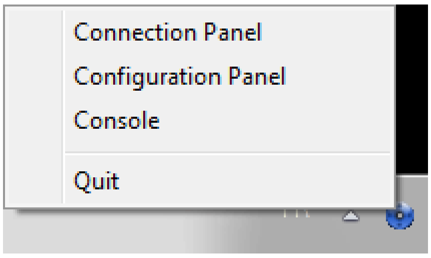
- "Tunnel <TunnelName>" if one or more tunnels are open.
- "Waiting VPN ready..." when VPN IKE is starting.
- "VPN Client" when the VPN Client is launched without tunnel opened.

Left-click on the icon opens the Connection Panel.

Right-clicking the icon displays the menu associated with the icon.

8.3.2Menu

Right click on the VPN Client icon in the taskbar displays the contextual menu associated with the icon:



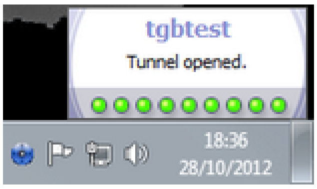
The contextual menu items are:

1/	Connection Panel:	Opens the Connection Panel
2/	Configuration Panel:	Open the Configuration Panel
3/	Console:	Opens the VPN logs window
4/	Quit:	Closes the open VPN tunnels and quit the software.

8.3.3Taskbar popup

When opening or closing a VPN tunnel, a sliding popup window appears above the icon in the VPN taskbar. This window identifies the status of the tunnel during its opening or closing, and disappears automatically, unless the mouse is over:

Tunnel open

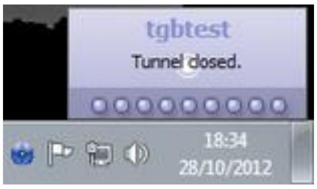


tgbtest

Tunnel opened.

18:36
28/10/2012

Tunnel close

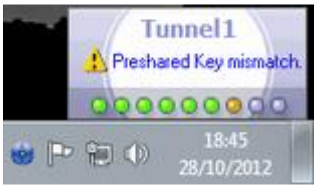


tgbtest

Tunnel closed.

18:34
28/10/2012

Problem opening of the tunnel: the window displays brief explanation of the incident, and a clickable link to more information on this incident.



Tunnel1

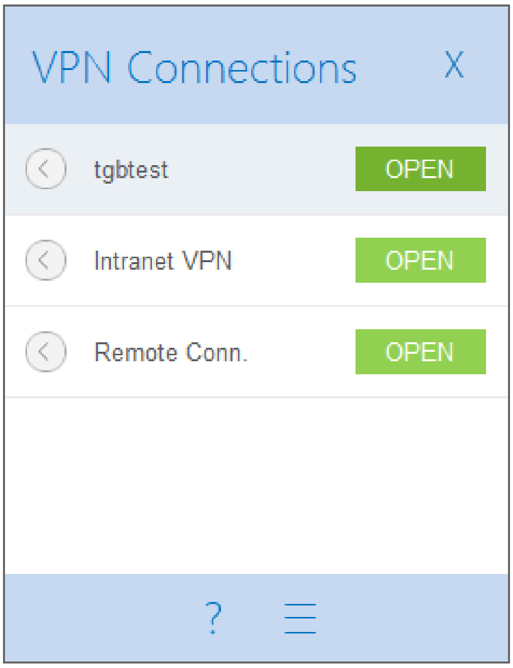
Preshared Key mismatch.

18:45
28/10/2012

Note: The display of the popup window can be disabled in the menu "Tools" > "Options" > "View" tab, option "Don't show the systray sliding popup".

9 Connection Panel

The Connection Panel enables to easily open and close the VPN Connections configured in the VPN Policy:



VPN Connections

tgbtest

Intranet VPN

Remote Conn.

New: Since version 6.4, the Connection Panel is fully configurable: It is possible to choose the VPN Connection that will appear or not in the Panel. It is also possible to rename and to sort these VPN connections.
See the chapter: "Connection Panel Management".

To open a VPN connection, click on the OPEN button of this VPN connection.
The icon on the left shows the state of the connection:

- VPN Connection closed. Click on the icon will open the Configuration Panel.
- VPN Connection being opened or closed.
- VPN connection opened. The traffic in the VPN connection is shown through the variation of the green central disk.
- VPN connection with a problem during opening or closing process. Click on the icon will open a popup window which gives detailed information about the problem.

The buttons of the Connection Panel enable to:

- ? Open the window "About…".
- ☰ Open the Configuration Panel (Note: The access to the Configuration Panel may be protected with a password. See the chapter: "Access Control")
- X Close the Connection Panel

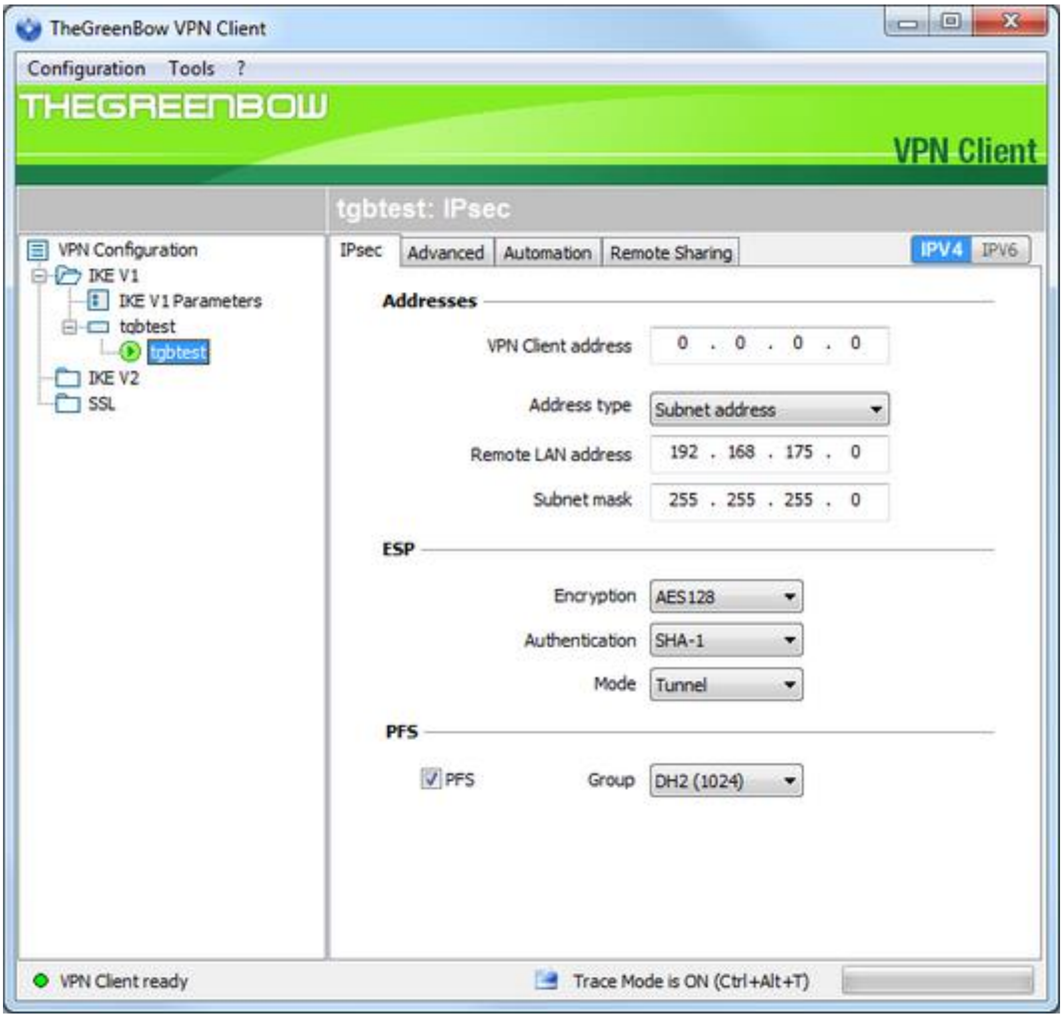
On the Connection Panel, the following shortcuts are available:

ESC (or ALT+F4)	Close the window
CTRL+ENTER	Open the Configuration Panel (main interface)
CTRL+O	Open the selected VPN Connection
CTRL+W	Close the selected VPN Connection
up/down arrows	Enable to change the selected VPN Connection

10 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 managing software and VPN security policies
- The VPN tunnel tree
- Configuration tabs for VPN tunnels
- A status bar



Addresses

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 192 . 168 . 175 . 0

Subnet mask: 255 . 255 . 255 . 0

ESP

Encryption: AES128

Authentication: SHA-1

Mode: Tunnel

PFS

☑ PFS

Group: DH2 (1024)

10.1 Menus

The Configuration Panel menus are:

- "Configuration"
  - Import: Importing a VPN security policy (VPN Configuration)
  - Export: Exporting a VPN security policy (VPN Configuration)
  - Move to USB drive: USB Mode settings and enable the USB mode
  - VPN Configuration Wizard: **C**reating a VPN security policy
  - Quit: Close the open VPN tunnels and quit the software

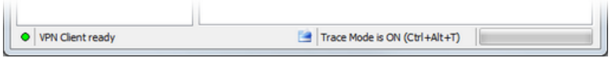
- "Tools"
  - Connection Panel
  - Console: IKE connection trace Window
  - Reset IKE: Reboot IKE
  - Options: Options to restrict the display of some features, startup mode, language management

- " ? "
  - Online Support: Access to online support

- Software update: Check the availability of an update
- Buy a license online: Access to the online shop
- Activation Wizard
- "About..." window

10.2 Status bar

The status bar at the bottom of the Configuration Panel provides more information:



VPN Client ready

Trace Mode is ON (Ctrl+Alt+T)

- The "LED" on the far left is green when all services are operational software (IKE).
- The text to the left indicates the status of the software ("VPN ready", "Save configuration", "Apply Settings", etc.)
- When enabled, tracing mode is identified in the middle of the status bar. The icon on the left blue is a clickable icon that opens the folder containing the log files generated by the mode tracing.
- The progress bar on the right of the status bar identifies the progress of the backup of Configuration.

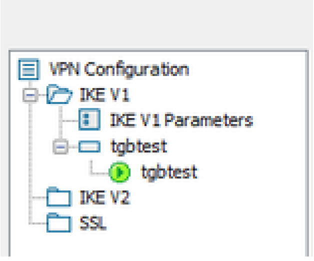
10.3 Shortcuts

CTRL+S	Save a VPN Configuration
CTRL+ENTER	Toggles to the Connection Panel
CTRL+D	Open the "Console" VPN traces
CTRL+ALT+R	Restart the IKE daemon
CTRL+ALT+T	Trace mode activation (generation of logs).

10.4 VPN Tunnel tree

10.4.1 Introduction

The left side of the Configuration Panel is the tree representation of the VPN security policies. The tree can contain an unlimited number of VPN tunnels.



There are three entries at the root level which allow you to see, edit or create either:

1. IPsec tunnel using IKEv1 with multiple Phase 1 and Phase 2. Each Phase 1 can contain several Phases 2.

2. IPsec tunnel using IKEv2 with multiple IKE Auth and Child SA connections. Each IKE Auth can contain multiple Child SA.
3. SSL tunnel with multiple TLS connections.

1. IPsec IKEv1 VPN tunnel

- Clicking on a Phase 1 opens the configuration tabs for Phase 1 ("Configure IPsec IKEv1: Authentication").
- Clicking on a Phase 2 opens the configuration tabs for Phase 2 ("Configure IPsec IKEv1: IPsec").

2. IPsec IKEv2 VPN tunnel

- Clicking on a IKE Auth opens the configuration tabs for IKE Auth ("Configure IPsec IKev2: IKE Authentication").
- Clicking on a Child SA opens the configuration tabs for Child SA ("Configure IPsec IKEv2: Child SA").

3. SSL VPN tunnel

- Clicking on a TLS opens the configuration tabs for TLS ("Configure SSL: TLS connection").

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

○ Closed tunnel. Double-click on this icon opens or closes the related VPN tunnel.
○↑ Tunnel configured to automatically open on traffic detection
⟳ Tunnel being opened
▶ Open tunnel
⚠ Incident opening or closure of the tunnel

By clicking twice (slowly) on any item, it is possible to edit and modify the name of this item.

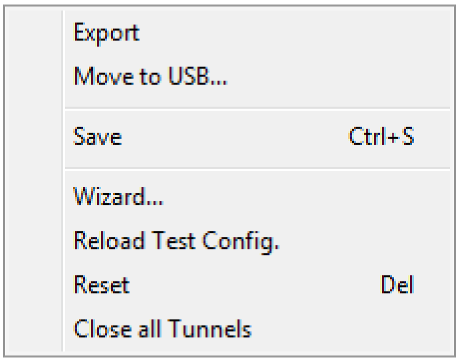
Note: Two items with the same root shall not have the same name. If the user enters a name that is already assigned, the software displays a warning.

Unsaved changes to the VPN Configuration are identified by bold font for the tunnel that changed. The tree returns to normal font when it is saved.

10.4.2 Contextual Menus

1. Configuration VPN

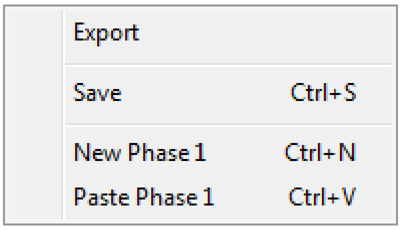
Right click on the VPN Configuration (root of the tree) displays the following context menu:



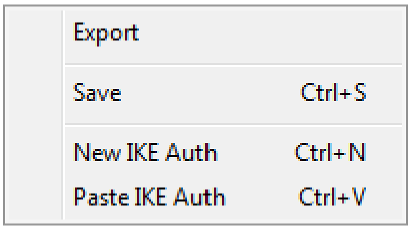
Export	Exports the entire VPN security policy.
Move to USB...	Configure a USB drive to switch to "USB Mode".
Save	Save the VPN security policy.
Wizard...	Open the VPN Configuration Wizard
Reload Test Config.	Stormshield VPN Client is installed with a default configuration that allows to test opening a VPN tunnel. This menu allows to reload it at any time.
Reset	Reset the VPN security policy, subject to confirmation by the user.
Close all tunnels	Close all open tunnels.

2. IKEv1, IKEv2, SSL

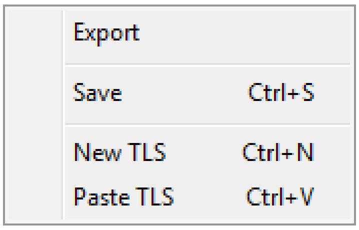
Right-click on the item IKEv1, IKEv2 or SSL displays the following contextual menu which allows to export, save, create or paste a Phase1/IKE Auth/TLS:



IKEv1 Menu



IKEv2 Menu



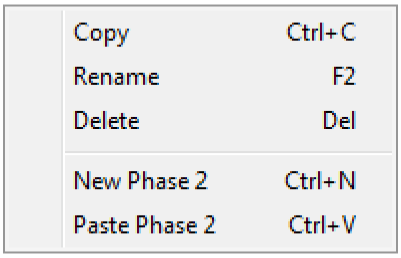
SSL Menu

Export	Export all IKEv1 / IKEv2 / SSL tunnels
Save	Save all IKEv1 / IKEv2 / SSL tunnels
New Phase 1 New IKE Auth New TLS	Create a new Phase 1 / IKE Auth / TLS, configured with default parameters
Paste Phase1 Paste IKE Auth Paste TLS	Add a Phase1 / IKE Auth / TLS previously copied in the clipboard (1)

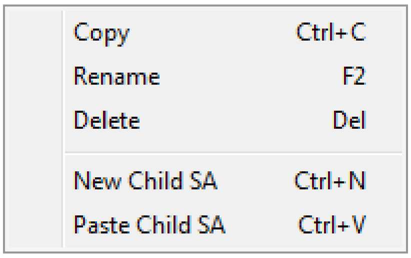
(1) This choice only appears if a Phase 1 / IKE Auth /TLS was copied in the clipboard, via the menu "Copy" of each Phase 1 / IKE Auth / TLS (see above).

3. Phase1, IKE Auth

Right-click on a Phase1 or IKE Auth item displays the following contextual menu which allows to copy, rename or delete a Phase1/IKE Auth/TLS:



Phase1 Menu



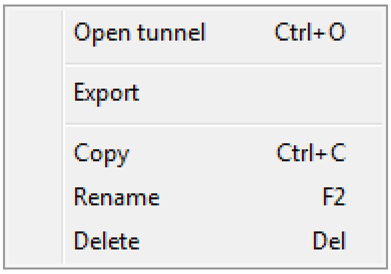
IKE Auth Menu

Copy	Copy the selected Phase1 / IKE Auth into the clipboard
Rename (1)	Rename the Phase1 / IKE Auth.
Delete (1)	Delete, after user confirmation, the Phase1 / IKE Auth, including all Phases2 / Child SA of the Phase1 / IKE Auth.
New Phase2 New Child SA	Add a new Phase 2 / ChildSA to the selected Phase1 / IKE Auth
Paste Phase2 (2) Paste Child SA	Add to the Phase1 / IKE Auth the Phase2 /Child SA previously copied into the clipboard.

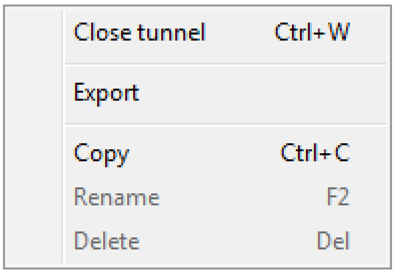
(1) This menu is disabled as long as the VPN Tunnel is opened.
(2) This choice appears when a Phase2 / ChildSA was copied into clipboard via the contextual menu of this Phase2 / Child SA (see above)

3. Phase2, ChildSA or TLS

Right-click on a Phase2 / Child SA / TLS item displays the following contextual menu:



Menu tunnel closed



Menu tunnel open

Open Tunnel	Displayed if the VPN tunnel is closed: opens the selected VPN tunnel
Close tunnel	Displayed if the VPN tunnel is opened: closes the selected VPN tunnel
Export (1)	Export the selected tunnel
Copy	Copy the selected tunnel
Rename (2)	Rename the selected tunnel

Delete (2)	Delete, after user confirmation, the selected tunel

(1) This feature allows you to export the entire tunnel (i.e. the associated Phase 2-Phase 1 or IKE Auth-Child SA or TLS) and to create a single VPN tunnel security policy fully operational (which can for example be imported and immediately functional).
(2) This menu is disabled as long as the tunnel is open.

10.4.3 Shortcuts

For the management of the tree, the following shortcuts are available:

F2	Allows to edit the name of the selected item
DEL	Delete the selected item after user confirmation If the whole configuration is selected (root of the VPN tree), allows the deletion of the whole configuration after user confirmation
CTRL+O	Open the VPN tunnel of the selected Phase2/ChildSA/TLS
CTRL+W	Close the VPN tunnel of the selected Phase2/ChildSA/TLS
CTRL+C	Copy the selected item to the "clipboard"
CTRL+V	Paste (add) the item copied in the clipboard
CTRL+N	Create a new Phase1 if the item IKEv1 is selected Create a new IKE Auth if the item IKEv2 is selected Create a new TLS if the item SSL is selected Create a new Phase 2 if a Phase 1 is selected Create a new Child SA if an IKE Auth is selected
CTRL+S	Save the VPN Security policy

11 Import, Export VPN Security Policy

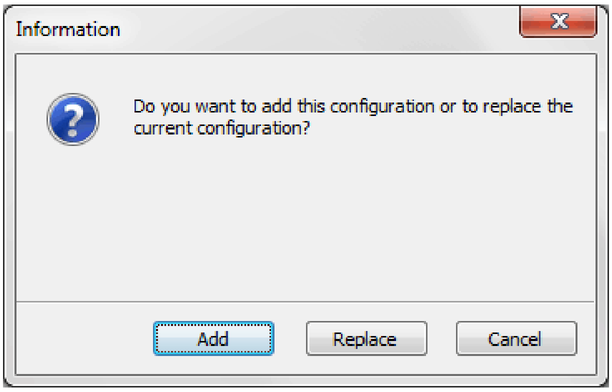
11.1 Import a VPN security policy

Stormshield VPN Client can import a VPN security policy in different ways:
- From the menu "Configuration" > "Import" in the Configuration Panel
- By drag and drop of a VPN Configuration file (file ".tgb") onto the Configuration Panel
- By double-clicking a VPN Configuration file (file ".tgb")
- By using the command line option "/import" (1)

(1) The use of command line options of the software is described in the document "Deployment Guide". All the options available for importing a VPN security policy are detailed there: "/import", "/add", "/replace" or "/importonce".

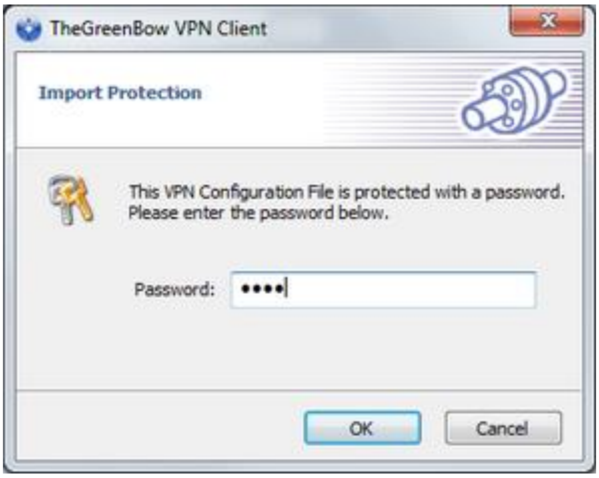
Note: The VPN configuration files have the following extension ".tgb".

To import a VPN configuration, the user shall say if he wants to add new Configuration to the current VPN Configuration, or if he wants to replace (overwrite) the current configuration with the new VPN Configuration.


Information

Do you want to add this configuration or to replace the current configuration?

If the VPN security policy has been saved with a password, it will be asked to the user.


TheGreenBow VPN Client

Import Protection

This VPN Configuration File is protected with a password. Please enter the password below.

Password: ••••

If the VPN security policy has been exported with integrity check (see chapter "Exporting a VPN Security Policy") and it has been corrupted, a message alerts the user, and the software does not import the Configuration.

Note: If VPN tunnels added have the same name as the VPN tunnel in current configuration, they are automatically renamed during import (adding an increment between brackets).

Importing Global Parameters

If during import, the user selects "Replace", or if the current configuration is empty, the Global Parameters from the imported configuration replace VPN Global Parameters from the current configuration.
If during import, the user chooses "Add", Global Parameters of the current VPN configuration are kept.

Import user choice	Current configuration is empty	Current configuration is not empty
Add	Global Parameters replaced by the new ones	Global Parameters kept
Replace	Global Parameters replaced by the new ones	Global Parameters replaced by the new ones

11.2 Exporting a VPN security policy

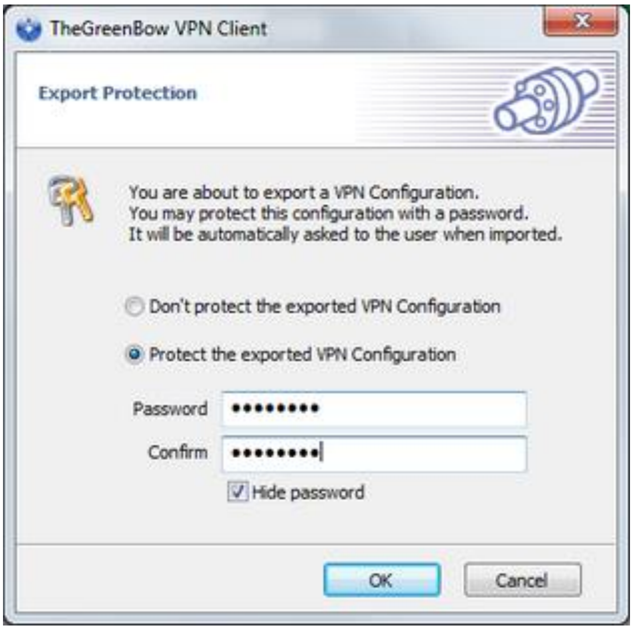
Stormshield VPN Client can export a VPN security policy in different ways:

- In the menu "Configuration" > "Export" from the Configuration Panel: The entire VPN security policy is exported.
- Via right click on the root of the tree of the Configuration Panel (menu choose "Export"): The entire VPN security policy is exported.
- Via right click on any items in the tree (then choose "Export"): the item selected and depending ones are exported (e.g. Phase 1 and all associated Phase 2, or Phase 2 and the associated Phase 1)
- By using the command line option "/export" (1)

(1) The use of command line options of the software is described in the document "Deployment Guide". All the options available for exporting a VPN security policy are detailed there: "/export" or "/exportonce".

Note: The VPN configuration files have the following extension ".tgb".

Whatever the method used, the export operation begins with the choice of protection for the exported VPN security policy: It can be exported protected (encrypted) by a password, or exported "readable" (clear). When configured, the password is required from the user at the time of import.


TheGreenBow VPN Client

Export Protection

You are about to export a VPN Configuration.
You may protect this configuration with a password.
It will be automatically asked to the user when imported.

○ Don't protect the exported VPN Configuration

● Protect the exported VPN Configuration

Password ••••••••

Confirm ••••••••

☑ Hide password

Note: whether exported encrypted or "clear", the exported configuration integrity can be protected.

When exported VPN security policy integrity is protected, and subsequently corrupted, a warning message notifies the user during import, and the software does import the configuration (see chapter "Importing a VPN security policy" above).

11.3 Merge VPN security policies

It is possible to merge multiple security policies in a single VPN, by importing all VPN configurations, and selecting "Add" for each import (see chapter "Importing a VPN security policy").

11.4 Split VPN security policies

Using different export options (e.g. export a Phase 1 with all associated Phase 2 or export a single tunnel), it is possible to split a VPN security policy in many "sub-configurations" (See chapter "Exporting a VPN security policy").

This technique can be used to deploy VPN security policies on a large pool of computers: you can derive, the VPN policies associated with each computer from a common VPN policy, before distributing to each user for import.

12 Configure a VPN tunnel

12.1 VPN SSL, IPsec IKEv1 or IPsec IKEv2

Stormshield VPN Client enables to create and to configure different types of VPN tunnel. It also allow to open different types of VPN tunnels simultaneously.

Stormshield VPN Client enables to create VPN tunnels:

- IPsec IKEv1
- IPsec IKEv2
- SSL

The way to configure a new VPN tunnel is described in the previous chapters: "Configuration Wizard" and "VPN Tree > Contextual menus".

12.2 Modify and save the VPN configuration

It is possible to modify the VPN configuration (for example modification of the parameters of a tunnel) and to test this modification "on-the-fly" without having to save it.
Any modification of the VPN Configuration is identified in the VPN Tree with bold characters.

The VPN Configuration can be saved at any time using:

- CTRL+S
- The menu "Configuration > save"

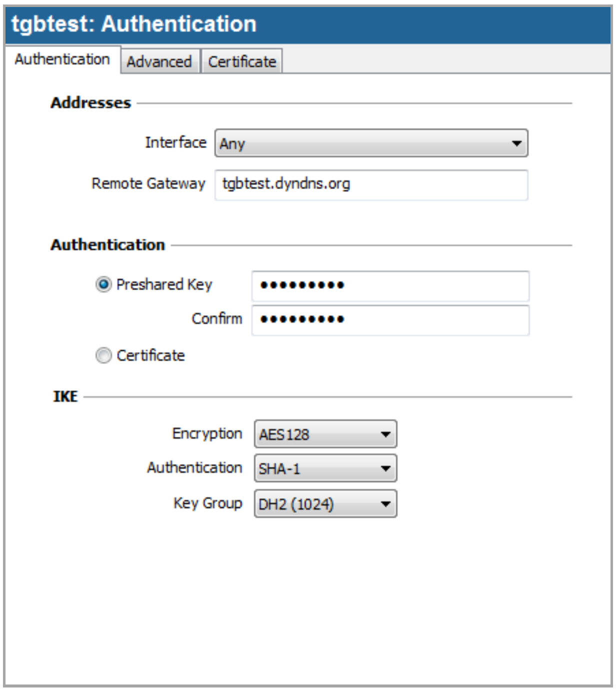
If a VPN Configuration is modified without being saved, the user is warned as he quits the application.

12.3 Configure an IPsec IKEv1 VPN tunnel

12.3.1 Phase1: Authentication

A VPN tunnel Phase 1 is the Authentication Phase in IKEv1.
Phase 1's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of Phase 1, each end system must identify and authenticate itself to the other.

To configure Phase 1, select this Phase 1 in Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.



tgbtest: Authentication

Addresses

Interface: Any

Remote Gateway: tgbtest.dyndns.org

Authentication

● Preshared Key: ••••••••••

Confirm: ••••••••••

○ Certificate

IKE

Encryption: AES128

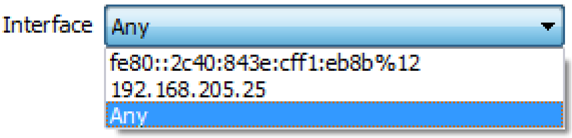
Authentication: SHA-1

Key Group: DH2 (1024)

Adresses

Interface

IP address of the network interface of the computer, through which the VPN connection is established. Select "any" to enable the VPN Client to automatically choose the interface.



Interface: Any

Choosing "Any" is useful when configuring a VPN Configuration which will be deployed on several computers.

Remote Gateway

IP address (IPv4 or IPv6) or DNS address of the remote gateway (in our example: myrouter.dyndns.org). This field is mandatory.

Authentication

Pre Shared Key	Password or key shared with the remote gateway. Note: The pre shared key is a simple way to configure a VPN tunnel. However, it provides less flexibility in the management of security than using certificates. See "Recommendations for Security".
Certificates	Use certificate for authentication of the VPN connection. Note: Using Certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...). See "Recommendations for Security".

IKE

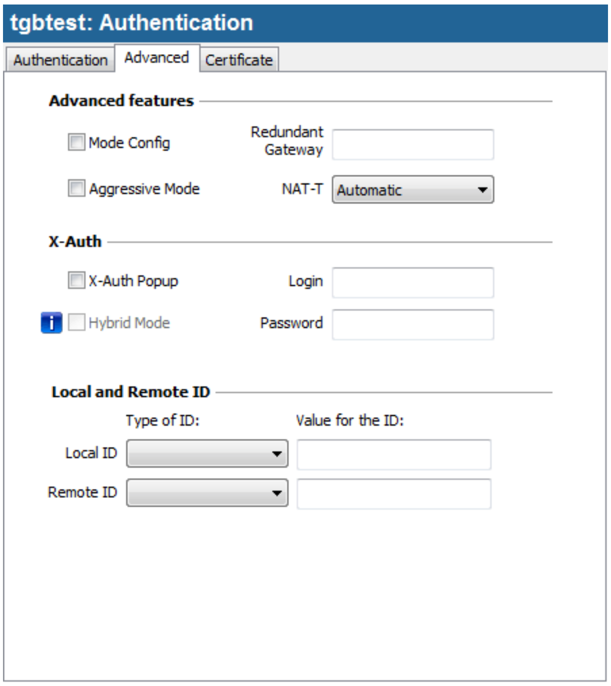
Encryption	Encryption algorithm used during Authentication phase: Auto (1), DES, 3DES, AES-128, AES-192, AES-256. See "Recommendations for Security".
Authentication	Authentication algorithm used during Authentication phase: Auto (1), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. See "Recommendations for Security".
Key Group	Diffie-Hellman key length: Auto (1), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192) See "Recommendations for Security".

(1) Auto means that the VPN Client will adapt automatically to the settings done in the gateway. When Auto is selected, the following algorithms (and their combinations) are supported:

- Encryption: 3DES, AES-128, AES-192
- Authentication: SHA-1, SHA2-256
- Key Group: DH1, DH2, DH5

If the gateway is configured with a different algorithm then Auto can't be used, and the algorithm must be explicitly specified in the VPN Client.

12.3.2 Phase1: Advanced


tgbtest: Authentication

Advanced features

□ Mode Config

Redundant Gateway

□ Aggressive Mode

NAT-T: Automatic

X-Auth

□ X-Auth Popup

Login

□ Hybrid Mode

Password

Local and Remote ID

	Type of ID:	Value for the ID:
Local ID		
Remote ID		

Advanced features

Mode Config	If checked, the VPN Client will activate Config-Mode for this tunnel. Config-Mode allows to the VPN Client to fetch some VPN Configuration information from the VPN gateway. See "Mode Config" settings below.
Redundant Gateway	This allows the VPN Client to open an IPsec tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router.dyndns.com). See section "Managing Redundant Gateway" below.
Aggressive Mode	If checked, the VPN Client will used aggressive mode as negotiation mode with the remote gateway. See "Recommendations for Security" on Aggressive Mode vs. Main Mode.
NAT-T	"NAT-Traversal" Mode. The VPN Client enables to manage 3 types of NAT-T mode: Disabled: Prevents the VPN Client and the VPN gateway to start NAT-Traversal Automatic: Leaves the VPN Gateway and VPN Client negotiate the NAT-Traversal Forced: The VPN Client will force NAT-T by encapsulating IPsec packets into UDP frames to solve traversal with intermediate NAT routers.

X-Auth

X-Auth Popup	See "Managing X-Auth" section below.
Hybrid Mode	Hybrid Mode is a mode that "blends" two types of authentication: classic VPN Gateway Authentication and X-Auth Authentication for VPN Client. To activate the Mode Hybrid, it is necessary that the tunnel is associated with a certificate (see "Managing Certificates"), and the X-Auth must be set. (See "Managing X-Auth" section below).

Local and Remote ID

Local ID	"Local ID" is the identifier of the Authentication phase (Phase 1) that the VPN Client sends to the remote VPN gateway. Depending on the type selected, this identifier can be: − IP address (type = IP address), e.g. 195.100.10.101 − A domain name (type = FQDN), e.g. gw.mydomain.net − Address (type = USER FQDN), e.g. admin@mydomain.com − A string (type = KEY ID), e.g. 123456 − The subject of a certificate (type = Subject X509 (aka DER ASN1 DN)). This happens when the tunnel is associated with a user certificate. See "Managing Certificates" When this parameter is not set, the IP address of the VPN Client is used by default.
Remote ID	"Remote ID" is the identifier the VPN Client expects from the remote VPN gateway. Depending on the type selected, this identifier can be: − IP address (type = IP address), e.g. 80.2.3.4 − A domain name (type = FQDN), e.g. router.mydomain.com − Address (type = USER FQDN), e.g. admin@mydomain.com − A string (type = KEY ID), e.g. 123456 − The subject of a certificate (type = DER ASN1 DN) When this parameter is not set, the VPN Client will accept any identifier sent by the VPN Gateway without any check.

Mode Config

Mode Config, when activated, allows the VPN Client to recover some parameters from the VPN gateway configuration needed to open the VPN tunnel:

− Virtual IP address of the VPN Client
− The address of a DNS server (optional)
− The address of a WINS server (optional)

Important: the VPN gateway must support the Mode Config.

When the Mode Config is not enabled, all 3 parameters "VPN Client address", "DNS Server" and "WINS Server" can be configured manually in the VPN Client (see "Phase 2 IPsec Advanced").

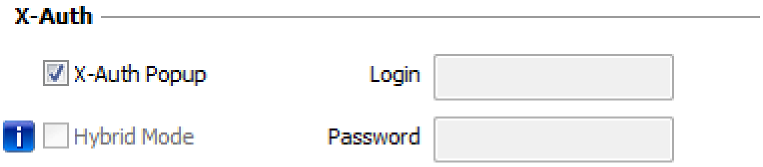
When the Mode Config is activated, all 3 parameters "VPN Client address", "DNS Server" and "WINS Server" are automatically filled during the opening of the VPN tunnel. Therefore they cannot be modified manually.

Managing X-Auth

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

X-Auth is used to force the user to enter a login and a password before the opening the VPN tunnel.

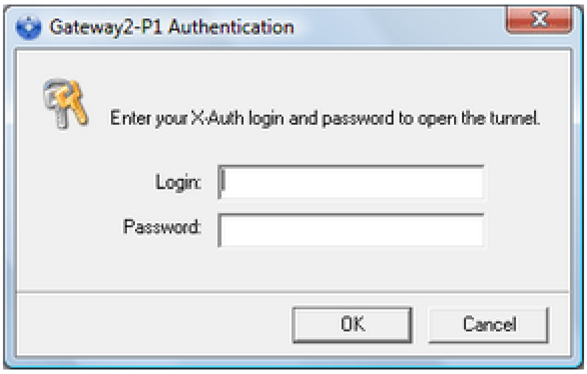
Note: This feature requires a corresponding configuration on the VPN gateway.



X-Auth

☑ X-Auth Popup　Login
□ Hybrid Mode　Password

When the "X-Auth Popup" is selected, a window will ask the login and password to authenticate the user each time a VPN tunnel open (the window requesting the login and password has the name of the tunnel to avoid confusion).



Gateway2-P1 Authentication

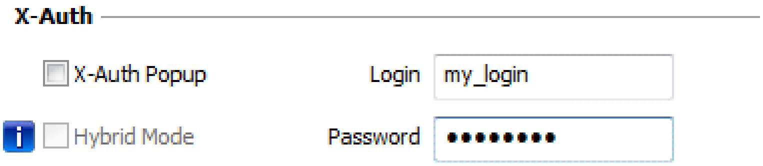
Enter your X-Auth login and password to open the tunnel.

Login:
Password:

Upon time out (configurable in "**Global Parameters**"), a warning message alerts the user to re-open the tunnel.

Upon incorrect login/password, a warning message alerts the user to re-open the tunnel.

VPN Client allows you to store the login and password in the X-Auth VPN security policy. This login and password are automatically sent to the VPN Gateway when the tunnel opens.



X-Auth

□ X-Auth Popup　Login my_login
□ Hybrid Mode　Password ••••••••

This eases the use and deployment of software. However, it is still less secure than the popup window that asks X-Auth login/password when the tunnel opens.

It is recommended to look at the chapter "Recommendations for Security".

12.3.3 Phase1: Certificate

See chapter Managing Certificates.

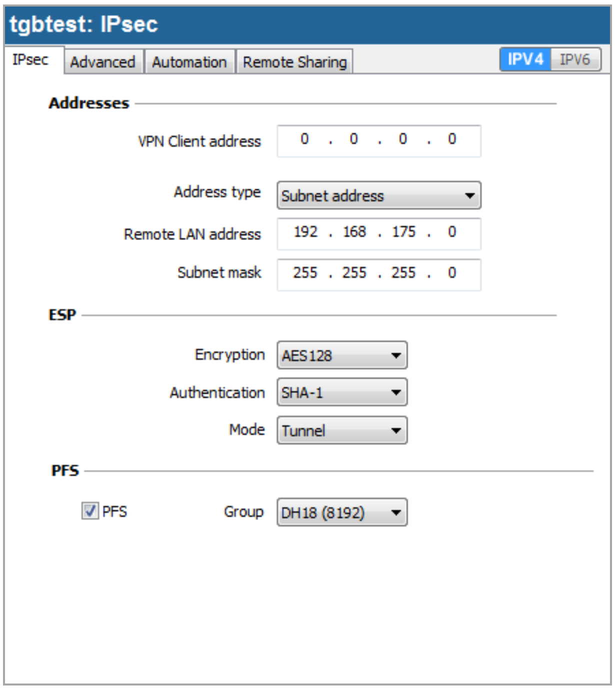
12.3.4 Phase2

The purpose of Phase 2 is to negotiate the IPsec security parameters that are applied to the traffic going through tunnels negotiated during Phase 1.

To configure a Phase 2, select this Phase 2 in the Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

After modification, the VPN tunnel is set in bold characters in the VPN tree. It is not required to save the VPN configuration: the VPN Tunnel can be tested immediately with the modified configuration.

12.3.5 Phase2: IPsec



VPN Client address: 0 . 0 . 0 . 0
Address type: Subnet address
Remote LAN address: 192 . 168 . 175 . 0
Subnet mask: 255 . 255 . 255 . 0
Encryption: AES128
Authentication: SHA-1
Mode: Tunnel
☑ PFS
Group: DH18 (8192)

Addresses

VPN Client address	This is the "virtual" IP address of the computer, as it will be seen on the remote network. Technically, it is the source IP address of IP packets carried in the IPsec tunnel. If the address is set to "0.0.0.0", the VPN Client automatically set the virtual IP address with the IP address of the physical interface of the computer. Note: If the Mode Config is enabled, this field is disabled. Indeed, it is automatically filled during the opening of the tunnel, with the value sent by the VPN gateway.
Address type	The remote endpoint may be a LAN or a single computer. See section "Address type configuration" below.

ESP

Encryption	Encryption algorithm negotiated during IPsec phase: Auto (1), DES, 3DES, AES-128, AES-192, AES-256.
Authentication	Authentication algorithm: Auto (1), MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
Mode	IPsec encapsulation mode: tunnel or transport

(1) Auto means that the VPN Client will adapt automatically to the settings done in the gateway. When Auto is selected, the following algorithms (and their combinations) are supported:

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

If the gateway is configured with a different algorithm then Auto can't be used, and the algorithm must be explicitly specified in the VPN Client.

PFS

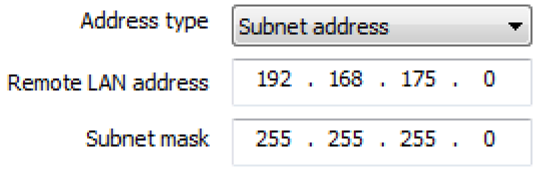
PFS - Groupe	Diffie-Hellman key length if selected: DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048) Note: IKEv1 doesn't provide an automatic mode for the DH Group. It must be explicitly configured.

IPv4 / IPv6

IPv4-IPv6	See chapter "IPv4 and IPv6".

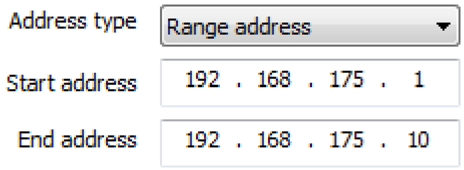
Address type configuration

If the end of the tunnel is a network, choose the "Network Address" and then set the address and mask of the remote network:



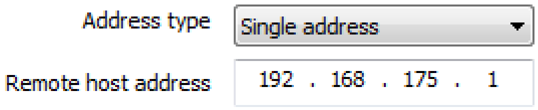
Address type	Subnet address
Remote LAN address	192 . 168 . 175 . 0
Subnet mask	255 . 255 . 255 . 0

Or choose "Range Address" and set the start address and the end address:



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

If the end of the tunnel is a computer, select "Single Address" and set the address of the remote computer:



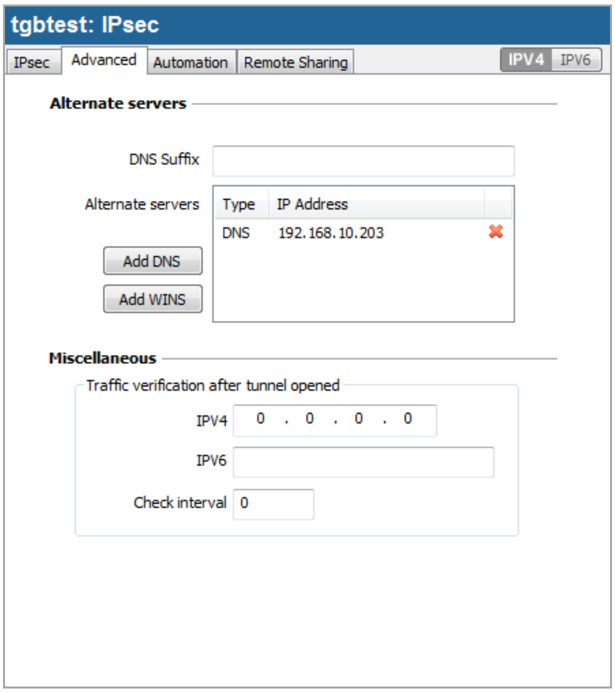
Address type	Single address
Remote host address	192 . 168 . 175 . 1

Note: The "Range Address" combined with the "Open automatically on traffic detection" allows to automatically open tunnel on traffic detection to one of the addresses in the specified address range (assuming the address range is also authorized in the configuration of the VPN gateway). "Open automatically on traffic detection" is also operational with the address type "subnet address" and "single address".

Note: If the IP address of the VPN Client is part of the IP address plan of the remote network (e.g. @IP poste = 192.168.10.2 and @remote network = 192.168.10.x), the opening of tunnel prevents the computer to contact its local network. All communications are routed within the VPN tunnel.

Configuration "all traffic through the VPN tunnel"
It is possible to configure the VPN Client to force all traffic exiting the computer passes through the VPN tunnel. To do so, select the address type "Network Address" and enter subnet mask as "0.0.0.0".

12.3.6 Phase2: Advanced



tgbtest: IPsec

Alternate servers

DNS Suffix:

Alternate servers:

Type	IP Address
DNS	192.168.10.203

Miscellaneous

Traffic verification after tunnel opened

IPV4: 0 . 0 . 0 . 0

IPV6:

Check interval: 0

Alternate servers

DNS Suffix	Domain suffix to be added to any machine, e.g. "mozart.dev.stormshield". This parameter is optional: The VPN Client will first try to translate the machine address without adding a DNS suffix. If the translation fails, the VPN Client will add the DNS suffix and try to translate the address again.
Alternate servers	Table of the IP addresses of DNS servers (2 maximum) and WINS servers (2 maximum) available on the remote network. The IP addresses to be entered will be either IPv4 or IPv6 depending on the network type selected in the "IPsec" tab. Note: If the Mode Config is enabled, these fields are disabled (they cannot be entered). They are actually automatically filled in during the opening of the tunnel, with the values sent by the VPN gateway in the Config Mode exchange.

Miscellaneous

Traffic verification after tunnel opened	It is possible to configure the VPN Client to regularly check the connection to the remote network. If the connection is lost, the VPN Client automatically closes and tries to re-open the tunnel. The IPv4/IPv6 field is the address of a machine on the remote network, which is expected to answer the "ping" sent by the VPN Client. If no answer is received, the connection is considered lost. Note: If the tunnel is configured as an IPv4 tunnel (tab "IPsec", up-right button),

	the IPv4 field must be filled in. If the tunnel is configured as an IPv6 tunnel, the IPv6 field must be filled in. "Check interval" is the period, in seconds, between two "ping" sent by the VPN Client to the IP address specified above.

12.3.7 Phase2: Automation

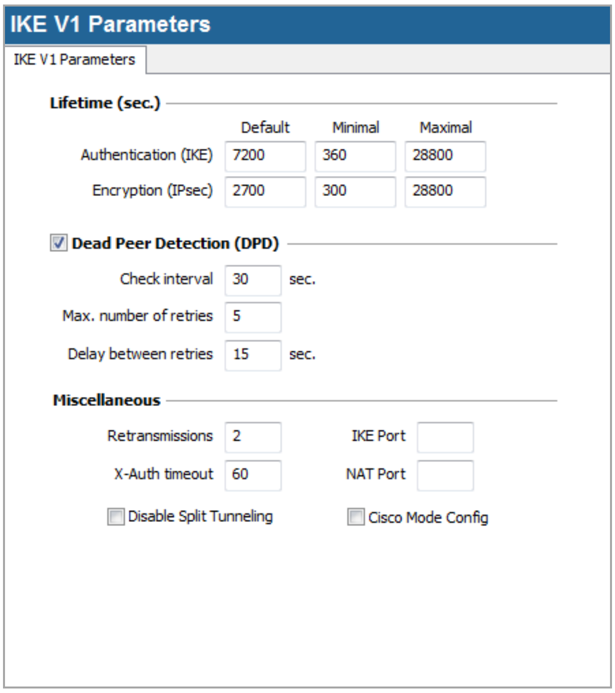
See chapter Automation

12.3.8 Phase2: Remote Sharing

See chapter Remote Desktop Sharing

12.3.9 IKEv1 Global Parameters

The IKEv1 global parameters are the parameters common to all VPN security policies using IKEv1 (all Phase 1 and Phase 2).



IKE V1 Parameters

IKE V1 Parameters

Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	7200	360	28800
Encryption (IPsec)	2700	300	28800

☑ **Dead Peer Detection (DPD)**

Check interval: 30 sec.

Max. number of retries: 5

Delay between retries: 15 sec.

Miscellaneous

Retransmissions: 2

IKE Port:

X-Auth timeout: 60

NAT Port:

□ Disable Split Tunneling

□ Cisco Mode Config

Lifetime

Lifetime (sec.)

Lifetimes are negotiated when tunnel opens, between the VPN Client and the VPN gateway.
Each peer is expected to transmit the "default" lifetime and to verify that the lifetime of the other peer is in the expected range (between minimal and maximal value). (1)

When a lifetime expires (Phase 1 for Authentication or Phase 2 for encryption) the relevant phase is renegotiated.

Lifetimes are expressed in seconds. The default values are:

	Default	Min	Max
Authentication (IKE)	7200 (2h)	360 (6min)	28800 (8h)
Encryption (IKE)	2700 (45min)	300 (5min)	28800 (8h)

(1) Lifetimes are expected to be negotiated between the VPN Client and the VPN Gateway. However, some VPN Gateways just return the default lifetime value proposed by the VPN Client. In any case, the VPN Client always applies the lifetime sent by the VPN Gateway.

Dead Peer Detection (DPD)

DPD	DPD Feature (Dead Peer Detection) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive. (1) − Audit Period: Period between 2 DPD verification messages sent. − Number of attempts: Number of consecutive unsuccessful attempts before declaring the remote gateway unreachable − Time between attempts: Interval between DPD messages when no response is received from the VPN gateway.

(1) The DPD feature is active once the tunnel open (phase 1 open). Associated with a "Redundant Gateway", the DPD allows the VPN Client to automatically switch a gateway to another on the unavailability of one or the other.

Miscellaneous

Retransmissions	Number of IKE protocol messages retransmissions before failure.
X-Auth timeout	Time to enter the X-Auth login/password
Port IKE	IKE Phase 1 exchanges (Authentication) are performed on the UDP protocol, using the default port 500. Some network devices (firewalls, routers) filter port 500. Setting of the IKE port allows to pass through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Phase 1 exchanges on a different port than 500.
Port NAT	IKE Phase 2 exchanges (IPsec) are performed on the UDP protocol, using default port 4500. Some network devices (firewalls, routers) filter port 4500. Setting of the IKE port allows to pass through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Phase 2 exchange on a different port than 4500.
Bloquer les flux non chiffrés	When this option is checked, only the traffic through the tunnel is allowed. Please check the note (1) above
Cisco Mode Config	This checkbox must be checked to ensure the compatibility with CISCO ASA gateway.

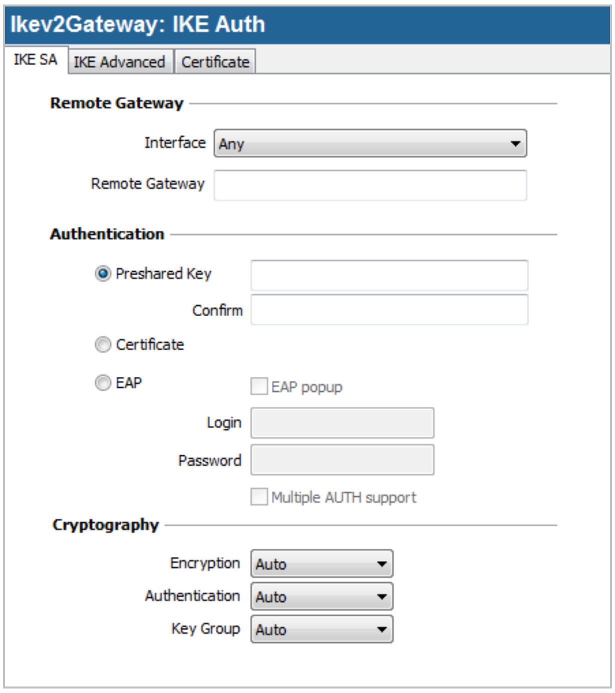
(1) The configuration option "Disable Split Tunneling" increases the security of the computer, when the VPN tunnel is opened. This feature prevents the risk of incoming traffic that could pass through the VPN tunnel. Associated with the configuration option "Force all traffic in the tunnel" (see chapter "IPsec"), this option ensures a complete sealing of the computer, as soon as the VPN tunnel is opened.

12.4 Configure an IKEv2 IPsec tunnel

A VPN tunnel IKE Auth is the Authentication Phase in IKEv2.
IKE Auth purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of IKE Auth, each end system must identify and authenticate itself to the other.

To configure IKE Auth, select this IKE Auth in Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

12.4.1 IKE Auth: IKE SA



Ikev2Gateway: IKE Auth

IKE SA | IKE Advanced | Certificate

Remote Gateway

Interface: Any

Remote Gateway:

Authentication

● Preshared Key

Confirm

○ Certificate

○ EAP □ EAP popup

Login

Password

□ Multiple AUTH support

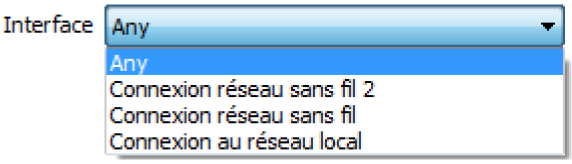
Cryptography

Encryption: Auto

Authentication: Auto

Key Group: Auto

Remote Gateway

Interface	Name of the network interface of the computer, through which VPN connection is established. Selecting "Any" enables the VPN Client to automatically choose the appropriate interface.  Interface: Any Any Connexion réseau sans fil 2 Connexion réseau sans fil Connexion au réseau local The choice "any" enables, for example, to configure a tunnel which is expected to be distributed among several computers.
Remote Gateway	IP address (IPv4 or IPv6) or DNS address of the remote gateway (in our example: myrouter.mydomain.com). This field is mandatory.

Authentication

Pre Shared Key	Password or key shared with the remote gateway. Note: The pre shared key is a simple way to configure a VPN tunnel. However, it provides less flexibility in the management of security than using certificates. See "Recommendations for Security".
Certificate	Use certificate for authentication of the VPN connection. Note: Using Certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...). See chapter "Recommendations for Security". See chapter "Managing Certificates".
EAP	EAP (i.e. Extensible Authentication Protocol) enables to authenticate the user through a login/password. When the "EAP Popup" is selected, a window will ask the login and password to authenticate the user each time a VPN tunnel opens.
Multiple Auth Support	Multiple Auth Support enables the combination of both Certificate authentication then EAP (login/password) authentication. (1)

(1) The double authentication "Certificate then EAP" is supported by the VPN Client. The double authentication "EAP then certificate" is not supported by the VPN Client.

Cryptography

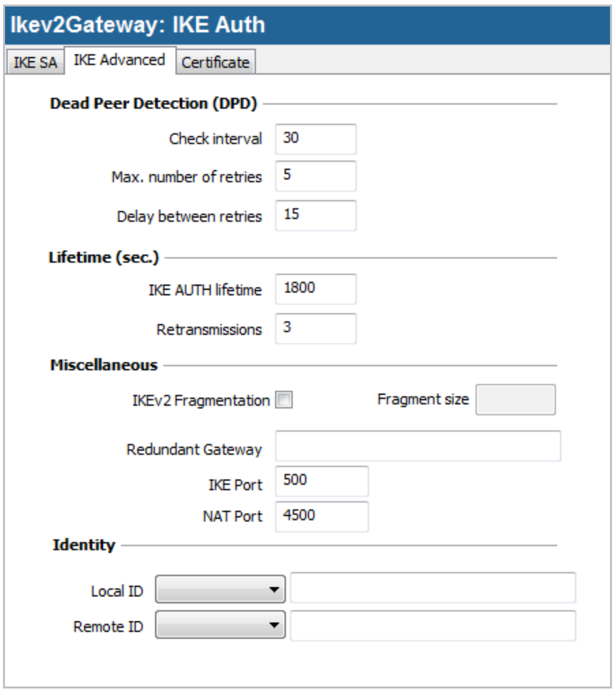
Encryption	Encryption algorithm used during Authentication phase: Auto (1), DES, 3DES, AES-128, AES-192, AES-256
Authentication	Authentication algorithm used during Authentication phase: Auto (1), MD5, SHA-1 and SHA2-256, SHA2-384, SHA2-512.
Key Group	Diffie-Hellman key length: Auto (1), DH1 (768), DH2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

(1) Auto means the VPN Client automatically adapts to the VPN gateway parameters. When "Auto" is selected, the following algorithms (with their various combinations) are supported:

- Encryption: 3DES, AES-128, AES-192
- Authentication: SHA-1, SHA2-256
- Key group: DH1, DH2, DH5

If the VPN gateway is configured with another algorithm, then the "Auto" mode cannot be used. The algorithm must be explicitly defined.

12.4.2 IKE Auth: IKE Advanced



Dead Peer Detection (DPD)

Check interval: 30

Max. number of retries: 5

Delay between retries: 15

Lifetime (sec.)

IKE AUTH lifetime: 1800

Retransmissions: 3

Miscellaneous

IKEv2 Fragmentation ☐ Fragment size

Redundant Gateway

IKE Port: 500

NAT Port: 4500

Identity

Local ID

Remote ID

Dead Peer Detection (DPD)

Check interval	DPD Feature (Dead Peer Detection) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive. (1) Check interval: Period between 2 DPD verification messages.
Max. number of retries	Number of consecutive unsuccessful attempts before declaring the remote gateway unreachable.
Delay between retries	Interval between DPD messages when no response is received from the VPN gateway.

(1) The DPD feature is active once the tunnel open (phase 1 open). Associated with a "**Redundant Gateway**", the DPD allows the VPN Client to automatically switch a gateway to another on the unavailability of one or the other.

Lifetime (sec)

IKE AUTH lifetime	Lifetimes of IKE Authentication phase. Expressed in seconds. Lifetimes are not negotiated during IKEv2 exchanges
Retransmissions	Number of IKE protocol messages retransmissions before failure

Miscellaneous

IKEv2 Fragmentation	Enables the fragmentation of IKEv2 packets, in accordance to the RFC 7383.

	This function avoids IKEv2 packets are fragmented by the IP network. Thus, the value "Fragment size" must be less or equal to the IP network fragment size (typically 1500).
Redundant gateway	This allows the VPN Client to open an IPsec tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router2.dyndns.com). See section "Managing Redundant Gateway" below.
Port IKE	IKE Auth phase exchanges (Authentication) are performed on the UDP protocol, using the default port 500. Some network devices (firewalls, routers) filter port 500. Setting of the IKE port allows to pass through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Auth Phase exchanges on a different port than 500.
Port NAT	Child SA phase exchanges (IPsec) are performed on the UDP protocol, using default port 4500. Some network devices (firewalls, routers) filter port 4500. Setting of the NAT port allows to pass through these filtering devices. Note: The remote VPN gateway must also be capable of performing the Child SA phase exchange on a different port than 4500.

Identity

Local ID	"Local ID" is the identifier of the authentication phase (IEK Auth), sent by the VPN Client to the VPN Gateway. Depending on the selected type, the identifier can be: − IP address (type = IP address), e.g. 195.100.10.101. Either IPv4 or IPv6 addresses are supported. − A domain name (type = FQDN), e.g. gw.mydomain.net − Address (type = USER FQDN), e.g. admin@mydomain.com − A string (type = KEY ID), e.g. 123456 − The subject of a certificate (type = Subject X509 (aka DER ASN1 DN)). This happens when the tunnel is associated with a user certificate. See "Managing Certificates" If this parameter is not set, the IP address of the VPN Client is used by default.
Remote ID	"Remote ID" is the identifier the VPN Client expects from the VPN gateway. Depending on the type selected, this identifier can be: − IP address (type = IP address), e.g. 80.2.3.4. Either IPv4 or IPv6 addresses are supported. − A domain name (type = FQDN), e.g. routeur.mydomain.com − Address (type = USER FQDN), e.g. admin@mydomain.com − A string (type = KEY ID), e.g. 123456 − The subject of a certificate (type = DER ASN1 DN)

	When this parameter is not set, the VPN Client will accept any identifier sent by the VPN Gateway without any check.

12.4.3 IKE Auth: Certificate

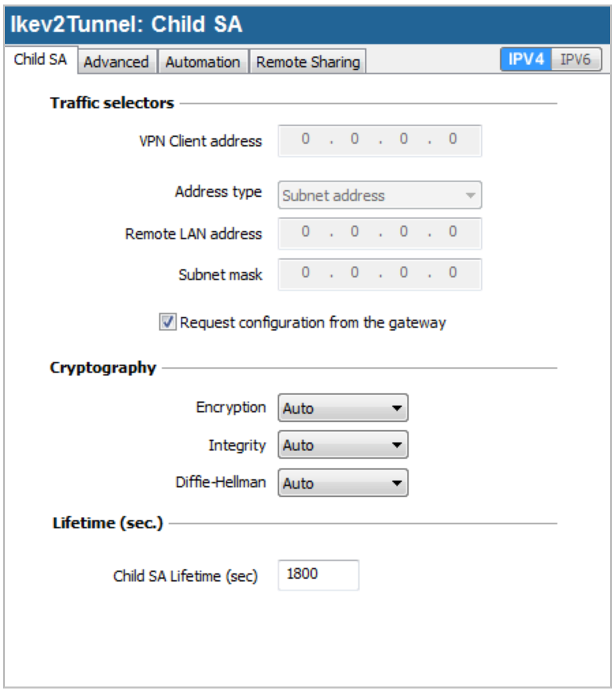
See chapter: Managing Certificates

12.4.4 Child SA

The purpose of Child SA is to negotiate the IPsec security parameters that are applied to the traffic going through tunnels negotiated during IKE Auth.

To configure a Child SA, select this Child SA in the Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

12.4.5 Child SA: Child SA



Ikev2Tunnel: Child SA

Traffic selectors

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption: Auto

Integrity: Auto

Diffie-Hellman: Auto

Lifetime (sec.)

Child SA Lifetime (sec): 1800

Traffic selectors

VPN Client address	This is the "virtual" IP address of the computer, as it will be seen on the remote network. Technically, it is the source IP address of IP packets carried in the IPsec tunnel.
Address type	The remote endpoint may be a LAN or a single computer. See section "Address type configuration" below

Request configuration from the gateway	When this option is selected (also known as "Configuration Payload" or "CP"), all information (VPN Client address, Remote LAN address, Subnet mask and DNS addresses) are sent by the VPN gateway. Each field is disabled. It is filled in dynamically during the opening of the tunnel as soon as the values are received from the VPN gateway.

Cryptography

Encryption	Encryption algorithm negotiated during IPsec phase: Auto (1), DES, 3DES, AES-128, AES-192, AES-256. Cf. "Recommendations for security"
Integrity	Authentication algorithm negotiated during IPsec phase: Auto (1), MD5, SHA-1 et SHA2-256, SHA2-384, SHA2-512. Cf. "Recommendations for security"
Diffie-Hellman	Diffie-Hellman key length: Auto (1), DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048), DH15 (3072), DH16 (4096), DH17 (6144), DH18 (8192), No Diffie-Hellman Cf. "Recommendations for security"

(1) Auto means that the VPN Client will adapt automatically to the settings done in the gateway. When Auto is selected, the following algorithms (and their combinations) are supported:

- Encryption: 3DES, AES-128, AES-192
- Authentication: SHA-1, SHA2-256
- Diffie-Hellman: DH1, DH2, DH5

If the gateway is configured with a different algorithm then Auto can't be used, and the algorithm must be explicitly specified in the VPN Client.

Lifetime

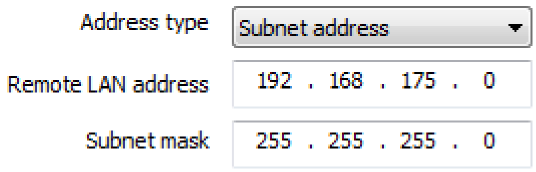
Child SA lifetime	Child SA time in seconds before re-negotiation. Note: Unlike IKEv1, the lifetimes are not negotiated in IKEv2, between the VPN Client and the VPN Gateway. The Lifetimes used for the tunnel are the lifetimes set in the VPN Client configuration.

IPv4 / IPv6

IPv4 / IPv6	See chapter "IPv4 and IPv6"

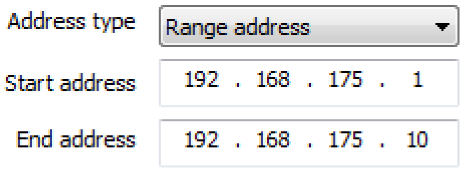
Address type configuration

If the end of the tunnel is a network, choose the "Network Address" and then set the address and mask of the remote network:



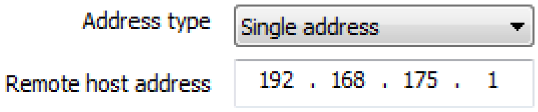
Address type: Subnet address
Remote LAN address: 192 . 168 . 175 . 0
Subnet mask: 255 . 255 . 255 . 0

Or choose "Range Address" and set the start address and the end address:



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

If the end of the tunnel is a computer, select "Single Address" and set the address of the remote computer:



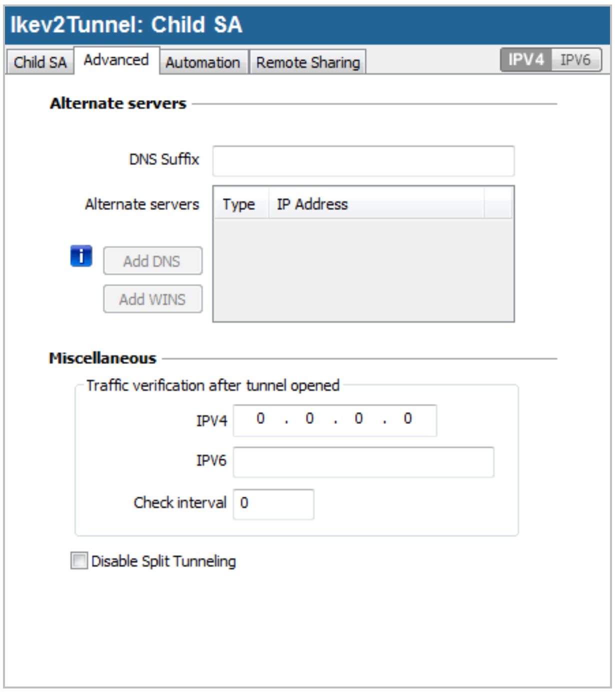
Address type: Single address
Remote host address: 192 . 168 . 175 . 1

Note: The "Range Address" combined with the "Open automatically on traffic detection" allows to automatically open tunnel on traffic detection to one of the addresses in the specified address range (assuming the address range is also authorized in the configuration of the VPN gateway). "Open automatically on traffic detection" is also operational with the address type "subnet address" and "single address".

Note: If the IP address of the VPN Client is part of the IP address plan of the remote network (e.g. @IP computer = 192.168.10.2 and @remote network = 192.168.10.x), the opening of tunnel prevents the computer to contact its local network. All communications are routed within the VPN tunnel.

Configuration "all traffic through the VPN tunnel"
It is possible to configure the VPN Client to force all traffic exiting the computer passes through the VPN tunnel.
To do so, select the address type "Network Address" and enter subnet mask as "0.0.0.0".

12.4.6 Child SA: Advanced



Ikev2Tunnel: Child SA

Alternate servers

DNS Suffix

Alternate servers

Type	IP Address

Miscellaneous

Traffic verification after tunnel opened

IPV4 0 . 0 . 0 . 0

IPV6

Check interval 0

□ Disable Split Tunneling

Alternate servers

DNS Suffix	Domain suffix to be added to any machine, e.g. "mozart.dev.stormshield". This parameter is optional: The VPN Client will first try to translate the machine address without adding a DNS suffix. If the translation fails, the VPN Client will add the DNS suffix and try to translate the address again.
Alternate servers	Table of the IP addresses of DNS servers (2 maximum) and WINS servers (2 maximum) available on the remote network. The IP addresses to be entered will be either IPv4 or IPv6 depending on the network type selected in the "Child SA" tab. Note: If the CP Mode is enabled (see "Request configuration from the gateway" in the "Child SA" tab), these fields are disabled (they cannot be entered). They are actually automatically filled in during the opening of the tunnel, with the values sent by the VPN gateway in the CP Mode exchange.

Miscellaneous

Traffic verification after tunnel opened	It is possible to configure the VPN Client to regularly check the connection to the remote network. If the connection is lost, the VPN Client automatically closes and tries to re-open the tunnel. The IPv4/IPv6 field is the address of a machine on the remote network, which is expected to answer the "ping" sent by the VPN Client. If no answer is received, the connection is considered lost.

	Note: If the tunnel is configured as an IPv4 tunnel (tab "IPsec", up-right button), the IPv4 field must be filled in. If the tunnel is configured as an IPv6 tunnel, the IPv6 field must be filled in. "Check interval" is the period, in seconds, between two "ping" sent by the VPN Client to the IP address specified above.
Disable split tunneling	When this option is checked, only the traffic in the tunnel is authorized. See note (1) below.

(1) The configuration option "Disable Split Tunneling" increases the security of the computer, when the VPN tunnel is opened. In particular, this feature prevents the risk of incoming traffic that could pass through the VPN tunnel. Associated with the configuration "Force all traffic in the tunnel" (see chapter "IPsec"), this option ensures complete sealing of the computer, when the VPN tunnel is opened

12.4.7 Child SA: Automation

See chapter Automation

12.4.8 Child SA: Remote Sharing

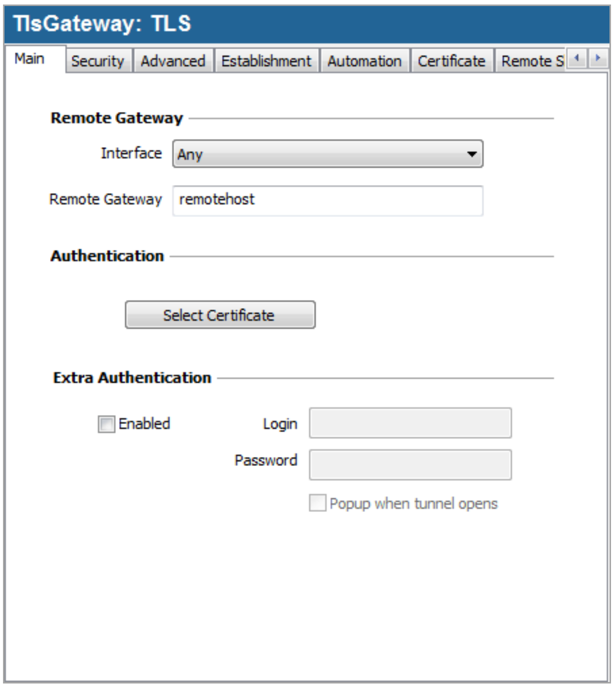
See chapter Remote Desktop Sharing

12.5 Configure a SSL VPN tunnel

12.5.1 Introduction

Since version 6, Stormshield VPN Client enables to open SSL VPN Tunnels.
Stormshield SSL VPN Tunnels are compatible with OpenVPN configurations. So, Stormshield VPN Client enables to open SSL tunnels with each SSL VPN Gateway implementing OpenVPN protocol.

12.5.2 Main



Remote Gateway

Interface: Any

Remote Gateway: remotehost

Authentication

Extra Authentication

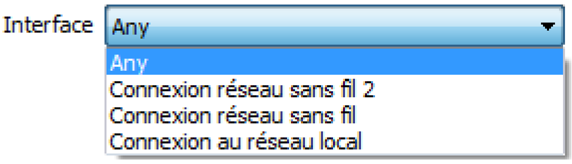
□ Enabled

Login:

Password:

□ Popup when tunnel opens

Remote Gateway

Interface	Name of the network interface of the computer, through which VPN connection is established. Selecting "Any" enables the VPN Client to automatically choose the appropriate interface.  Interface: Any Any Connexion réseau sans fil 2 Connexion réseau sans fil Connexion au réseau local The choice "any" enables, for example, to configure a tunnel which is expected to be distributed among several computers.
Remote Gateway	IP address (IPv4 or IPv6) or DNS address of the remote gateway (in our example: myrouter.mydomain.com). This field is mandatory.

Authentication

Select Certificate

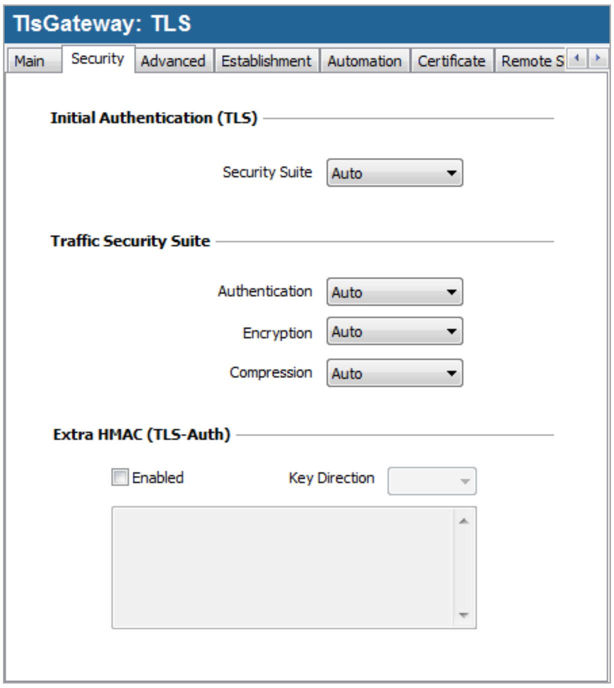
Selection of the Certificate for the VPN connection authentication.
See chapter "Managing Certificate"

Extra Authentication

Extra authentication

The Extra Authentication enables to authenticate the user through a login/password. When the "Popup when tunnel opens" is selected, a window will ask the login and password to authenticate the user each time a VPN tunnel opens.

12.5.3 Security


TlsGateway: TLS

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

It is used in the SSL handshake phase to authenticate both parties. It can be set to Auto (1), Low, Normal, High. Each items of this dropdown menu is a pre-selection of algorithms as follow:

- Auto: All cipher suites except the null ciphers are proposed to the gateway. The gateway then decides the best security suite.
- Low: Only 'low' encryption cipher suites are proposed to the gateway; currently, those using 64 or 56 bit encryption algorithms.
- Normal: Only 'medium' encryption cipher suites are proposed to the gateway; currently, some of those using 128 bit encryption.
- High: Only 'high' encryption cipher suites are proposed to the gateway; currently, those with key lengths larger than 128 bits, and some cipher suites

	with 128-bit keys. Reference for more information: https://www.openssl.org/docs/apps/ciphers.html

Traffic Security Suite

Authentication	Authentication algorithm negotiated for the traffic: Auto (1), MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512. Note: If the option "Extra HMAC" is activated (see below), the authentication algorithm cannot be "Auto". It must be explicitly configured, and must be identical to the algorithm configured in the VPN Gateway.
Encryption	Encryption algorithm of the traffic: Auto (1), BF-CBC-128, AES128-CBC, AES192-CBC, AES256-CBC.
Compression	Traffic compression: Auto (1), Yes: enabled, No: disabled.

(1) Auto means that the VPN Client will adapt automatically to the settings of the gateway.

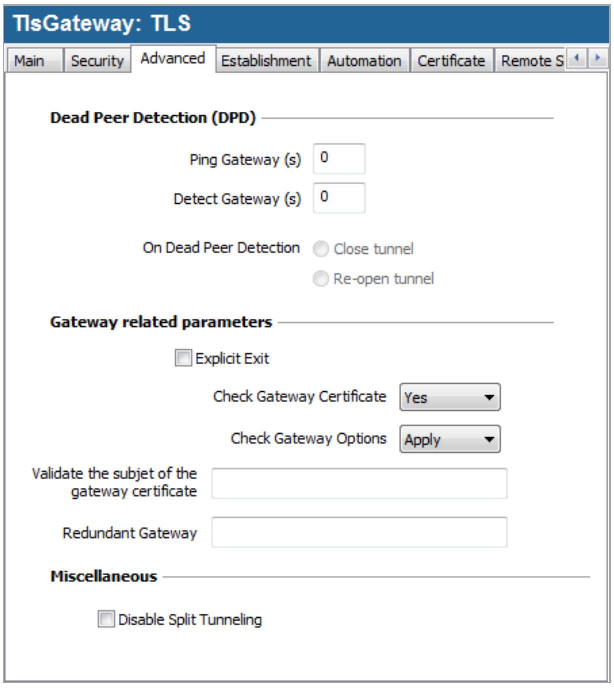
Extra HMAC (TLS-Auth)

<table>
<tr><td>Extra HMAC</td><td>This option adds an authentication level to packets exchanged between the client and the gateway. To be used on the client, the VPN Gateway has also to be configured with this option (on the gateway, the option is often called "TLS-Auth").

Selecting this option enables to enter a key in the text area below the checkbox. The key must be the same as the one configured in the VPN gateway. The key is a strong of hexadecimal characters with the following format:

<pre>
-----BEGIN Static key-----
362722d4fbff4075853fbe6991689c36
b371f99aa7df0852ec70352122aee7be
...
515354236503e382937d1b59618e5a4a
cb488b5dd8ce9733055a3bdc17fb3d2d
-----END Static key-----
</pre>
The "Key direction" must then be selected:
- BiDir: The key is used both ways (default mode)
- Client: The key direction of the gateway must be "server"
- Server: The key direction of the gateway must be "client"</td></tr>
</table>

12.5.4 Advanced



Dead Peer Detection (DPD)

Ping Gateway (s) 0

Detect Gateway (s) 0

On Dead Peer Detection ○ Close tunnel ○ Re-open tunnel

Gateway related parameters

□ Explicit Exit

Check Gateway Certificate: Yes

Check Gateway Options: Apply

Validate the subject of the gateway certificate:

Redundant Gateway:

Miscellaneous

□ Disable Split Tunneling

Dead Peer Detection (DPD)

DPD Feature (Dead Peer Detection) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive, and reversely to allow the gateway to detect the client is no longer alive. (1)

Ping gateway	Time in seconds between pings sent to the gateway. This is used by the gateway to know if the client is still there.
Detect Gateway	Timeout in seconds before considering the gateway dead because no ping was received from the gateway.
On Dead Peer Detection	Once the gateway has been detected to be dead (i.e. at the end of the timeout entered in "Detect gateway"), you can decide to close the VPN tunnel, or keep trying to re-open the VPN tunnel.

(1) The DPD feature is active once the tunnel open (phase 1 open). Associated with a "Redundant Gateway", the DPD allows the VPN Client to automatically switch a gateway to another on the unavailability of one or the other.

Gateway related parameters

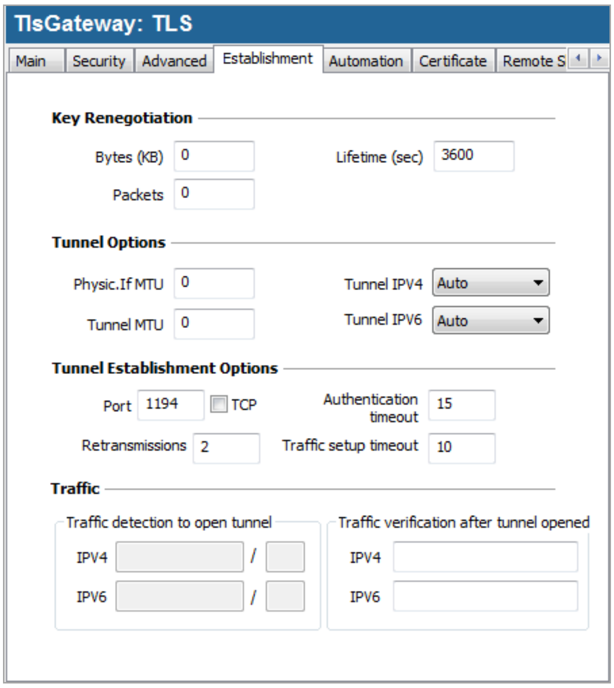
Explicit exit	This parameter enables the VPN Client to send a specific "closing" packet to the gateway when the tunnel is closed. If this option is not checked, the VPN gateway will use the DPD function to close the tunnel, which is less efficient.
Check Gateway Certificate	Defines the level of control executed on the certificate received from the gateway. Two levels are available:

	- Yes: full control of the certificate validity - No: no control of the certificate validity "Lite" is reserved for future use and has the same behaviour as "yes".
Check Gateway Options	Defines the level of control on coherency of settings (e.g. encryption algorithm, compression,..) between the VPN Client and the gateway: - Yes: the VPN tunnel cannot open if at least one setting differs from the gateway - No: no control on settings is done before opening VPN tunnel The settings must be identical for the VPN tunnel to open - Lite: some controls are done to check that there is coherency of settings with the gateway - Apply: the VPN Client will apply the settings sent by the gateway
Validate the subject of the gateway certificate	If this field is filled in, the VPN Client check if the subject of the certificate received from the gateway is identical.
Redundant gateway	This allows the VPN Client to open a tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router.dyndns.com). See section "Managing Redundant Gateway" below

Miscellaneous

Disable split tunneling	When this option is checked, only the traffic in the tunnel is authorized. It increases the security of the computer, when the VPN tunnel is opened. In particular, this feature prevents the risk of incoming traffic that could pass through the VPN tunnel.

12.5.5 Establishment



Key Renegotiation

Bytes (KB) 0 Lifetime (sec) 3600

Packets 0

Tunnel Options

Physic.If MTU 0 Tunnel IPV4 Auto

Tunnel MTU 0 Tunnel IPV6 Auto

Tunnel Establishment Options

Port 1194 □ TCP Authentication timeout 15

Retransmissions 2 Traffic setup timeout 10

Traffic

Traffic detection to open tunnel: IPV4 / ; IPV6 /

Traffic verification after tunnel opened: IPV4 ; IPV6

Key Renegotiation

Bytes, Packets, Lifetime	Keys can be renegotiated when different criteria expire: - Traffic quantity, expressed in KB - Packet quantity, expressed in number of packets - Lifetime, expressed in second Several criteria can be configured. Keys are negotiated when the first criteria expires.

Tunnel options

Physic. If MTU	Maximum size of the OpenVPN packets. This parameter enables to specify a packet size which avoids the OpenVPN frames to be fragmented at the network level. By default, the MTU is specified to 0. It means the VPN Client will use the MTU of the physical interface.
Tunnel MTU	Maximum packet size on the virtual network interface (expressed in bytes). It is recommended to configure a Tunnel MTU value less than the physical interface MTU. The default value for the MTU is 0. In this configuration, the VPN Client uses the value of the physical interface minus a fixed delta.
Tunnel IPv4	Specifies the behaviour of the VPN Client when it receives an IPv4 configuration from the VPN gateway: - Auto: Accepts the configuration sent by the gateway

	- Yes: Check the configuration sent by the gateway versus the VPN configuration. If it doesn't match, a warning is displayed and the tunnel doesn't open - No: Ignore the configuration sent by the gateway Note: Please check the choices "Tunnel IPv4" and "Tunnel IPv6" are not both set to "No".
Tunnel IPv6	Specifies the behaviour of the VPN Client when it receives an IPv6 configuration from the VPN gateway: - Auto: Accepts the configuration sent by the gateway - Yes: Check the configuration sent by the gateway versus the VPN configuration. If it doesn't match, a warning is displayed and the tunnel doesn't open - No: Ignore the configuration sent by the gateway Note: Please check the choices "Tunnel IPv4" and "Tunnel IPv6" are not both set to "No".

Tunnel Establishment Options

Port / TCP	Port number used for the tunnel establishment. The default value is 1194. By default, the tunnel uses UDP. The "TCP" option enables to transport the tunnel over TCP.
Authentication timeout	Timeout of the authentication phase establishment (TLS handshake). When this timeout expires, the VPN Client considers the authentication phase won't open, the tunnel is closed.
Retransmissions	Number of retransmissions of a protocol message. If no answer is received after the number of retransmissions, the tunnel is closed.
Traffic setup timeout	Timeout after which, if all establishment steps are not completed, the tunnel is closed.

Traffic

Traffic detection to open tunnel	The remote network characteristics are not configured in OpenVPN. They are automatically received from the gateway during the tunnel opening. But the "open tunnel on traffic detection" function requires these network characteristics to work. So they have to be explicitly configured: the two fields IPv4 and IPv6 are used to specify the subnet which will activate the traffic detection function. It is not mandatory to fill in both fields. The IP field is a subnet 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 used, i-e: the network 192.168.1.x Note: These parameters concern the traffic detection function. To activate the

	function, the option "Automatically open tunnel on traffic detection" must be checked. See chapter "Automation"
Traffic verification after tunnel opened	When these fields are set, the VPN Client sends "ping" to the specified IP addresses once the tunnel is opened. The state of the connection (the "ping" are answered or not) is displayed in the Console. It is not mandatory to fill in both fields. Note: The VPN Client doesn't take any specific action if no answer to the ping is received.

12.5.6 Automation

See chapter Automation

12.5.7 Certificate

See chapter Managing Certificates

12.5.8 Remote Sharing

See chapter Remote Desktop Sharing

13 Redundant Gateway

Stormshield VPN Client allows managing a redundant VPN gateway.

The use of a redundant gateway can be coupled with the implementation of DPD. Thus, when the VPN Client detects, through the DPD, the original gateway is unavailable, it automatically switches to the redundant gateway.

Note: It is possible to configure the same gateway for the main gateway and the redundant gateway in order to benefit from the automatic re-open function with only one gateway.

The redundant gateway algorithm is the following:

- The VPN Client contacts the original Gateway to open the VPN tunnel.
- If no tunnel can be opened after N retries (number of retries for the DPD function)
    - The VPN Client contacts the redundant gateway.

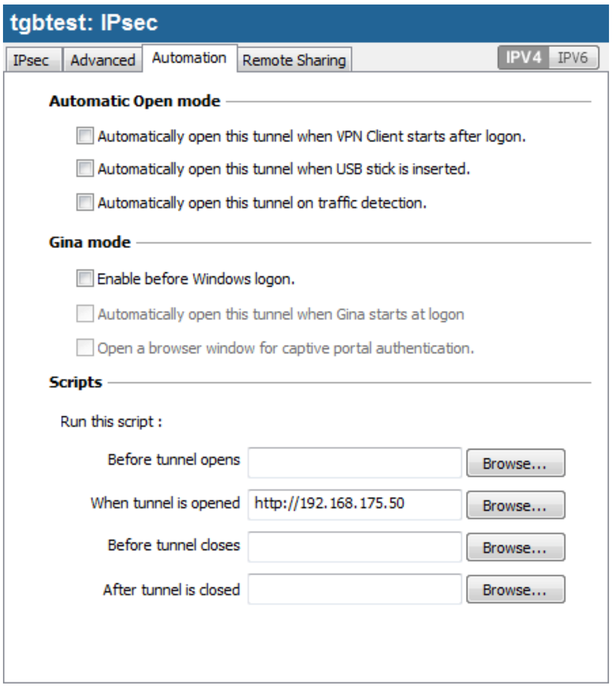
The same algorithm applies to the Redundant Gateway: If the redundant gateway is unavailable, the VPN Client attempts to open the VPN tunnel with the original Gateway.

Note: The VPN Client does not try to contact the redundant gateway if the original Gateway is available and there are troubles opening of the tunnel.

14 Automation

Stormshield enables to associate automation with VPN tunnels: automatic opening upon various criteria, batches or scripts running on different steps during tunnel opening or closing, etc.

The automation configuration is possible for all type of VPN tunnel via the "Automation" tab of the tunnel (Phase2 (IKEv1), Child SA (IKEv2) or TLS (SSL)).



Automatic Open mode

□ Automatically open this tunnel when VPN Client starts after logon.
□ Automatically open this tunnel when USB stick is inserted.
□ Automatically open this tunnel on traffic detection.

Gina mode

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

Scripts

Run this script :

Before tunnel opens
When tunnel is opened: http://192.168.175.50
Before tunnel closes
After tunnel is closed

Automatic Open mode

When VPN Client starts after logon	The tunnel opens automatically when the VPN Client starts (1)
When USB stick is inserted	The tunnel is part of a configuration on USB (see "USB mode"), and it is opened automatically USB drive is plugged in (2)
On traffic detection	The tunnel opens automatically on traffic detection to an IP address belonging to the remote network (see "How to configure the address of the remote network").

(1) This option allows you to configure to open a tunnel automatically when double-click on the file ".tgb": Select the option "Automatically open this tunnel when the VPN Client starts," save and export the configuration file "tunnel_auto.tgb" leave the VPN Client. By double-clicking on the file "tunnel_auto.tgb" VPN Client starts and the tunnel opens automatically.

(2) By extension, this option is also used to configure a tunnel to open automatically when a Smartcard or a token containing the certificate used by the VPN tunnel is plugged in.

GINA Mode

Enable before Windows logon	By checking this option, the tunnel appears in the VPN Gina and can be opened before Windows logon (see chapter "GINA Mode")
Automatically open when GINA starts	By checking this option, the VPN tunnel automatically opens before Windows Logon. This option is enabled if the option "Enable before Windows logon" is checked.
Open a browser window for captive portal authentication	Using WiFi network sometimes requires a local authentication on a dedicated portal. For users of the GINA Mode, the VPN Client implements a new browsing window which automatically enables the user to authenticate on the WiFi captive portal before the tunnel opens.

Scripts

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

The command line can be:
- a call to a "batch" file, e.g. "`C:\vpn\batch\script.bat`"
- the execution of a program, e.g. "`C:\Windows\notepad.exe`"
- opening a web page, e.g. "`http://192.168.175.50`"
- etc.

There are many possible applications for this function:
- Creating a semaphore file when the tunnel is open, so that a third-party application can detect when the tunnel is opened
- Automatic opening an intranet server, once the tunnel opens
- Cleaning or checking a configuration before the opening of the tunnel
- Check the computer (anti-virus updated, correct versioning of application, etc.) before the opening of the tunnel
- Automatic cleaning (deleting files) of a work area on the computer before closing the tunnel
- Application counting openings, closings and duration of VPN tunnel sessions
- Changing the network configuration, once the tunnel opened and restoration of the initial network configuration after closing the tunnel
- etc.

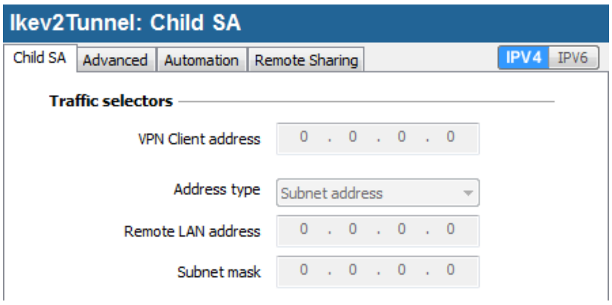
Note: Scripts are not available for tunnel in GINA Mode. For a tunnel in GINA Mode, the script fields are disabled.

15 IPv4 and IPv6

Stormshield VPN Client supports both IPv4 and IPv6 protocols, either for the local (LAN) or for the remote (WAN) network. The VPN Client enables to combine IPv4 and IPv6 to establish, for example, a secured IPv4 VPN connection in a tunnel over IPv6 communication.

The IPv4 or IPv6 configuration is available through the button in the upper-right corner of the tab "IPsec" for IKEv1 Phase2 or the tab "Child SA" for IKEv2 Child SA.

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



Ikev2Tunnel: Child SA

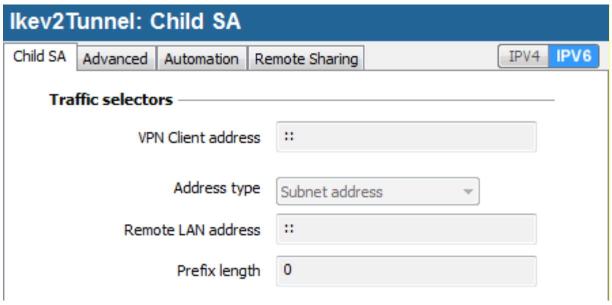
Traffic selectors

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0



Ikev2Tunnel: Child SA

Traffic selectors

VPN Client address: ::

Address type: Subnet address

Remote LAN address: ::

Prefix length: 0

Note: Choosing IPv4 or IPv6 impacts parameters of other tabs of the tunnel. So, the choice is displayed, disabled, at the upper-right corner of each tab.

For SSL tunnels, the IP type detection is automatic. No configuration is required. Moreover, an SSL tunnel is able to support IPv4 and IPv6 traffic simultaneously in a single tunnel: it is not required to configure two separate tunnels.

16 Managing Certificates

Stormshield VPN Client is fully integrated with most PKI solution in the market.

The software implements a set of features for different certificates storage (files, Windows Certificate Store, Smartcard and Token).

Stormshield VPN Client supports X509 certificates.
Stormshield VPN Client uses the certificate files formats, PKCS12, PEM.
Stormshield VPN Client supports the following storage devices: Windows Certificate Store (CSP), Smartcard or Token (PKCS11 CSP).
The VPN Client supports user certificates (VPN Client side) as well as the VPN Gateway certificates.

Note: Stormshield VPN Client cannot create certificates. However, the VPN Client can manage certificates created by third-party software, and stored on a Smartcard, token or in the Windows Certificate Store. VPN Client can also import certificates in the VPN security policy.

Stormshield VPN Client also enables to refine Smartcard, Token and Certificate management through a set of "PKI options". Example: automatic smartcard reader recognizing, certificate filters, etc.
See chapter "PKI Options" below.

16.1 Configuration

16.1.1 Select a Certificate ("Certificate" tab)

VPN Client allows you to assign a user certificate to a VPN tunnel.
There can be only one certificate per tunnel, but each tunnel can have its own certificate.

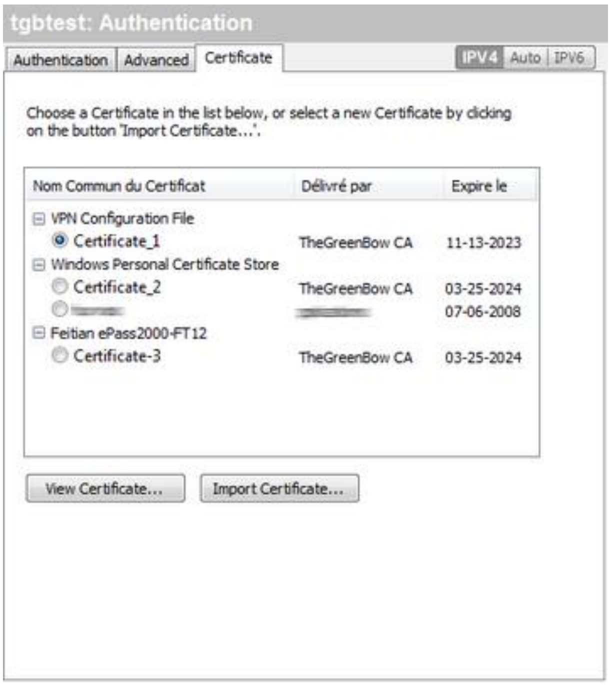
VPN Client allows you to select a certificate stored:

- In the VPN Configuration file (see "Import Certificate")
- In the Windows certificate store (see "Windows Certificate Store")
- On a Smartcard or a token (see "Configure a Smartcard or Token")

The "Certificate" tab will list all relevant media available on the computer, which contain certificates. If a media does not have a certificate, it is not displayed in the list (e.g. if the VPN Configuration file contains no certificate, it does not appear in the list).

By clicking one of the media, the list of certificates it contains is displayed.

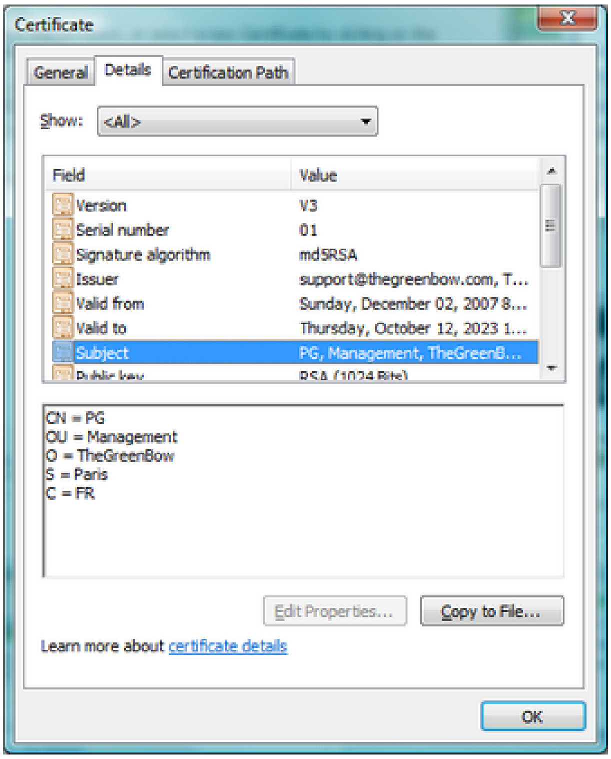
Click on the desired certificate to assign to the VPN tunnel.



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

Nom Commun du Certificat	Délivré par	Expire le
⊟ VPN Configuration File		
● Certificate_1	TheGreenBow CA	11-13-2023
⊟ Windows Personal Certificate Store		
○ Certificate_2	TheGreenBow CA	03-25-2024
○ [redacted]	[redacted]	07-06-2008
⊟ Feitian ePass2000-FT12		
○ Certificate-3	TheGreenBow CA	03-25-2024

Once the certificate is selected, the button "View Certificate" allows to view the details of the certificate.



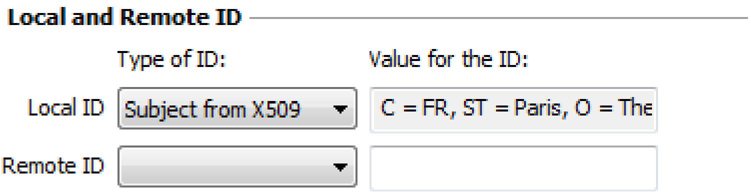
Show: <All>

Field	Value
Version	V3
Serial number	01
Signature algorithm	md5RSA
Issuer	support@thegreenbow.com, T...
Valid from	Sunday, December 02, 2007 8...
Valid to	Thursday, October 12, 2023 1...
Subject	PG, Management, TheGreenB...
Public key	RSA (1024 Bits)

CN = PG
OU = Management
O = TheGreenBow
S = Paris
C = FR

Learn more about certificate details

Note: Once the certificate is selected, the Phase 1 type of Local ID will automatically switch to "Subject X509" (aka DER ASN1 DN), and the certificate subject is used as the default value of this "Local ID".



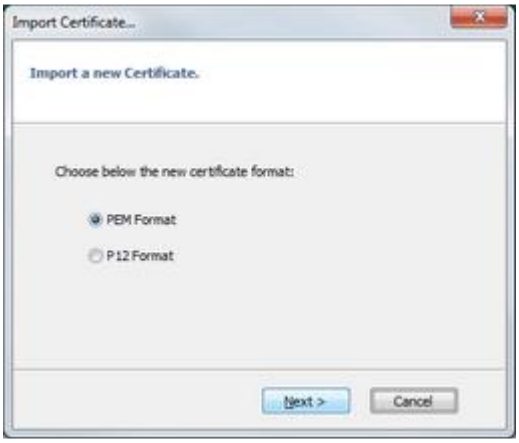
	Type of ID:	Value for the ID:
Local ID	Subject from X509	C = FR, ST = Paris, O = The
Remote ID		

16.2 Import a certificate

Stormshield VPN Client can import certificates in the VPN security policy with PEM or PKCS12 format. The advantage of this solution, less secure than using the Windows certificate store or a Smartcard, is to enable the easy and fast deployment of certificates.

Import a PEM certificate

1/ In the "Certificate" tab of either a Phase 1 (IKEv1), IKE auth (IKEv2) or SSL, click on "Import a Certificate..."
2/ Select "PEM Format"
3/ Select ("Browse") root certificates, user and private key to import
Note: The file with the private key must not be encrypted.
4/ Validate



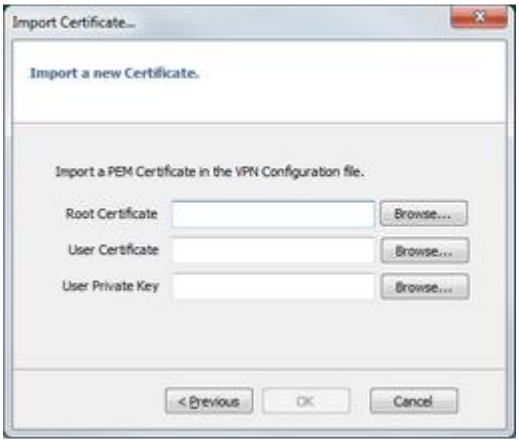
Import Certificate...

Import a new Certificate.

Choose below the new certificate format:

● PEM Format

○ P12 Format



Import Certificate...

Import a new Certificate.

Import a PEM Certificate in the VPN Configuration file.

Root Certificate

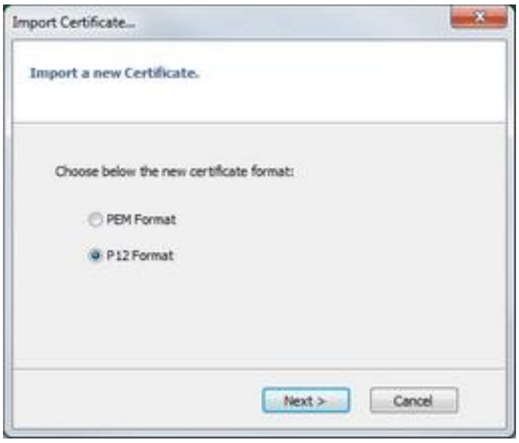
User Certificate

User Private Key

The certificate appears and is selected from the list of certificates on the "Certificate" tab.
Save the VPN security policy: The certificate is stored in the VPN security policy.

Import a PKCS12 certificate

1/ In the "Certificate" tab of either a Phase 1 (IKEv1), IKE auth (IKEv2) or SSL, click on "Import a Certificate..."
2/ Select "Format P12"
3/ Browse to import the PKCS12 certificate
4/ If it is protected by a password, enter the password and validate



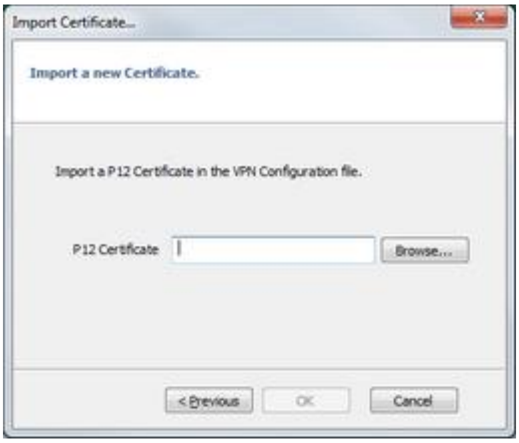
Import Certificate...

Import a new Certificate.

Choose below the new certificate format:

○ PEM Format

● P12 Format



Import Certificate...

Import a new Certificate.

Import a P12 Certificate in the VPN Configuration file.

P12 Certificate

The certificate appears and is selected from the list of certificates on the "Certificate" tab.
Save the VPN security policy: The certificate is stored in the VPN security policy.

16.3 Using the Windows Certificate Store

For a certificate of Windows Certificate Store to be identified by the VPN Client, it must meet the following specifications:

- The certificate must be certified by a certification authority (excluding the self-signed certificates)
- The certificate must be located in the Certificates store "Personal" (It represents the personal identity of the user who wants to open a VPN tunnel to the corporate network).

Note: To manage certificates in the Windows Certificate Store, Microsoft offers a standard management tool "certmgr.msc." To run this tool, go to the Windows menu "Start," then in the "Search programs and files", enter "certmgr.msc."

16.4 Define a Smartcard or a Token ("Options PKI")

Stormshield VPN Client offers many possibilities to define the Certificate to be used, the smartcard o the token to be used: automation to retrieve a token to be used, various criteria to select one certificate among several certificates, deployment options for tokens or smartcard readers, etc.

This function is only available for Premium and Certified VPN Client version.

This function is described in the document: "Token and Smartcard User Guide" available on the web page: http://www.thegreenbow.com/vpn_token.html.

16.5 Use a VPN Tunnel with a Certificate from a Smartcard

When a VPN tunnel is configured to use a certificate stored on Smartcard or token, a PIN code to access to the Smartcard is required to the user when tunnel opens.

If the Smartcard is not inserted, or if the token is not available, the tunnel does not open.
If the PIN code entered is incorrect, the VPN Client notifies the user that has 3 consecutive attempts before locking out the Smartcard.

The VPN Client implements a mechanism for automatically detecting the insertion of a Smartcard.
Thus, the tunnels associated with the certificate contained on the Smartcard are opened automatically upon inserting the Smartcard. Conversely, removal of the Smartcard automatically closes all associated tunnels.
This functionality is achieved by checking the option "Open tunnel automatically when the USB drive is inserted" (see chapter "Automation").

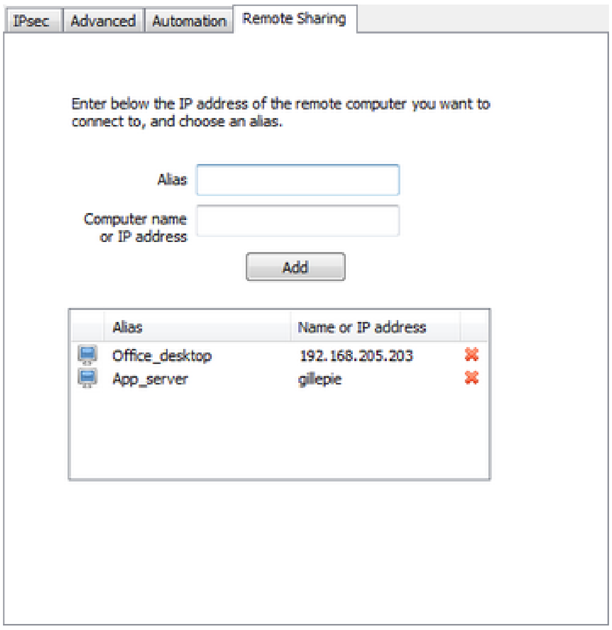
17 Remote Desktop Sharing

Stormshield VPN Client allows to configure the "Remote Desktop" logon in the VPN tunnel with one click only: With one click, the VPN tunnel opens to the remote network, and the RDP (Windows Remote Desktop Protocol) session is automatically opened on the remote computer.

17.1 Configuring the Remote Desktop Sharing

1/ Select the VPN tunnel in which the "Remote Desktop" session will be opened.
2/ Select the "Remote Sharing" tab.
3/ Enter an alias for the connection (this name is used to identify the connection in the different software menus), and enter either the IP address or the name of the machine of the remote computer.

4/ Click on "Add": The Remote Desktop Sharing session is added to the list of sessions.



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

Alias

Computer name or IP address

	Alias	Name or IP address	
	Office_desktop	192.168.205.203	✖
	App_server	gillepie	✖

Connection configuration management

It is possible to give an explicit connection title to this new "Remote Desktop" connection, via the window "Connection Panel management". See chapter "Connection Panel Management".

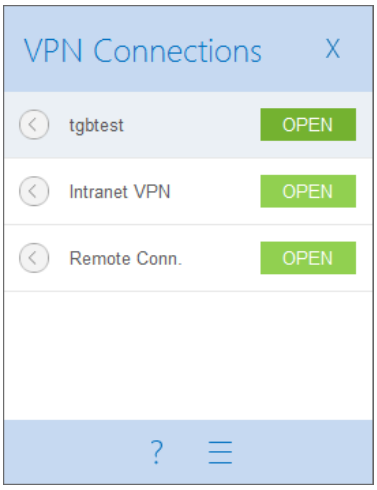
17.2 Using the Remote Desktop Sharing

1/ Right click on the icon in the taskbar: the menu is displayed

2/ Click on the "Connect to Remote Desktop" in the menu in the taskbar: the VPN tunnel opens and the desktop sharing session opens.

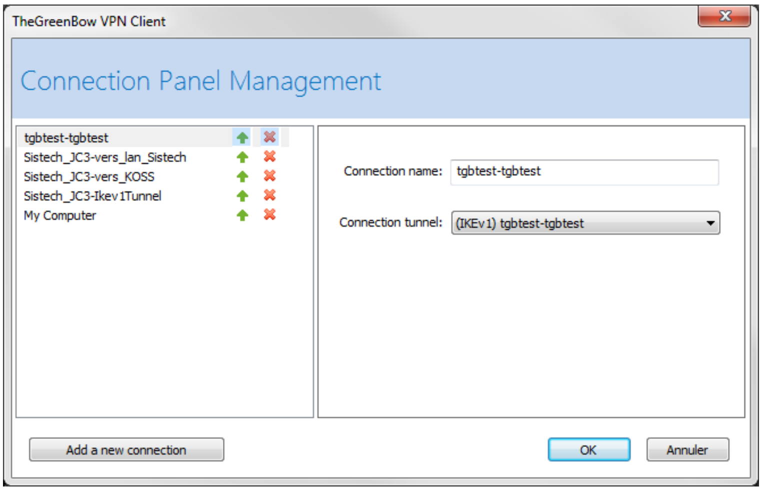
18 Connection Panel Management

From version 6.4, the connection panel of the VPN Client is fully configurable.



A VPN Connection is either a VPN tunnel or a "Remote Desktop" connection (i-e: a VPN tunnel with a Remote Desktop Sharing connection configured).

A new window which can be open from the main interface menu "Tools > Connection Panel Management" enables the VPN connection management in the Connection Panel: creating, renaming, sorting, etc.



tgbtest-tgbtest
Sistech_JC3-vers_lan_Sistech
Sistech_JC3-vers_KOSS
Sistech_JC3-Ikev1Tunnel
My Computer

Connection name: tgbtest-tgbtest

Connection tunnel: (IKEv1) tgbtest-tgbtest

The new Connection Panel Management windows enables to:

- Choose which connection will appear in the Connection Panel
- Create and sort the VPN Connections
- Rename the VPN Connections

The left part shows the list of VPN Connections as it is displayed in the connection Panel.
The right part indicates the parameters of each connection: its name, the associated tunnel and the optional RDP (remote sharing) connection.

In order to create a new connection, click on the button "Add a new connection", choose a name and the relevant tunnel. If a Remote Sharing connection is configured for the selected VPN tunnel, it is possible to choose it in the list box automatically displayed below. Once they are validated, the modifications automatically appear in the Connection panel.

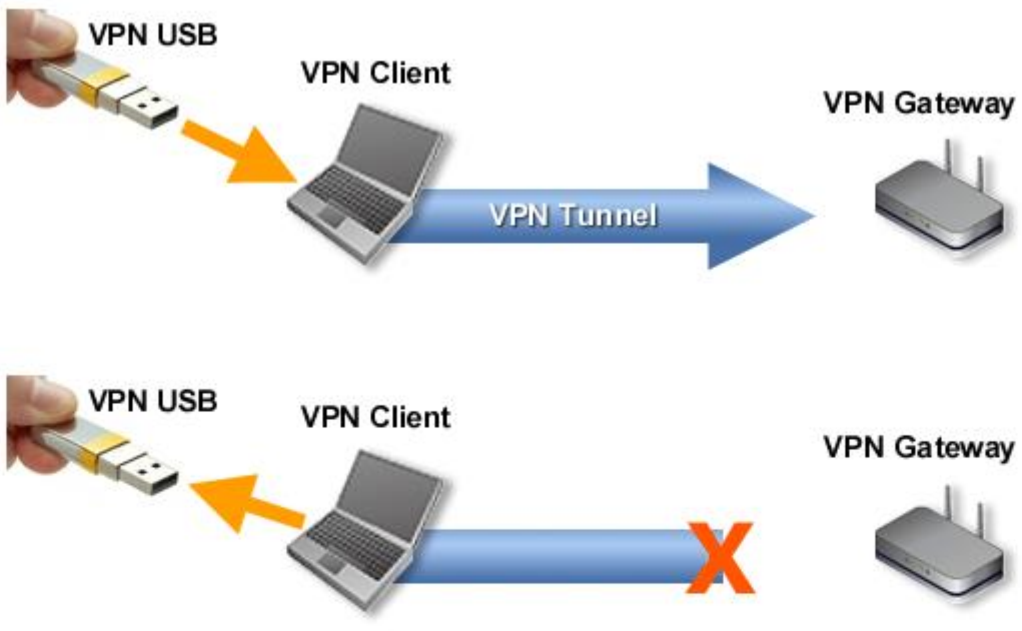
19 USB Mode

19.1 The VPN USB Mode

Stormshield VPN Client provides the ability to protect the VPN security policy (VPN Configuration, pre-shared key, certificate) on a USB drive.

The advantages of this mode are:

1/ The security policy is no longer stored on the computer but on a removable media (VPN Configuration stored is encrypted and protected with password)
2/ The VPN Client automatically detects USB drive containing a VPN Configuration. It will automatically load the configuration, and automatically opens the configured tunnel.
3/ When the USB drive is removed, the tunnel is automatically closed (and previous VPN Configuration restored)



In this document, the USB drive containing the VPN security policy is called "USB VPN Drive".

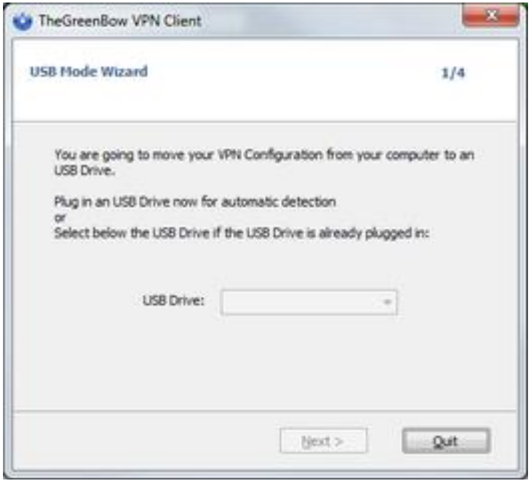
19.2 USB Mode settings

The USB mode can be configured via the setup wizard accessible via the Configuration Panel menu "Configuration" > "Move to USB drive".

Step 1: Select the USB drive

Select the USB Drive to be used to protect the VPN security policy.
If a USB Drive is already plugged in, it is automatically shown in the list of USB drives available.
Otherwise, simply plug in the USB drive.

USB drive not plugged in

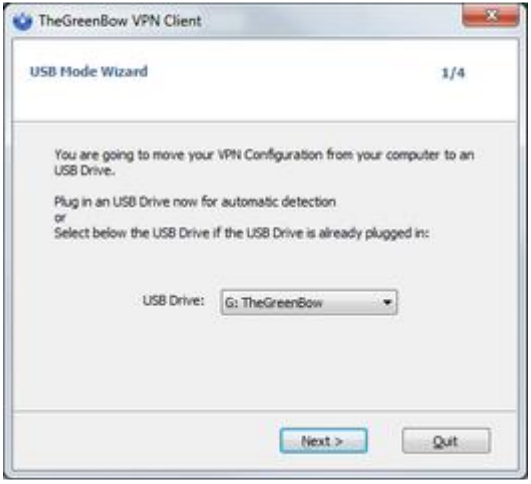


You are going to move your VPN Configuration from your computer to an USB Drive.

Plug in an USB Drive now for automatic detection
or
Select below the USB Drive if the USB Drive is already plugged in:

USB Drive:

USB drive plugged in



You are going to move your VPN Configuration from your computer to an USB Drive.

Plug in an USB Drive now for automatic detection
or
Select below the USB Drive if the USB Drive is already plugged in:

USB Drive: G: TheGreenBow

Note: The USB mode allows the protection of a single VPN Configuration on a USB drive. If a VPN Configuration is already present on the USB drive plugged in, a warning message is displayed.

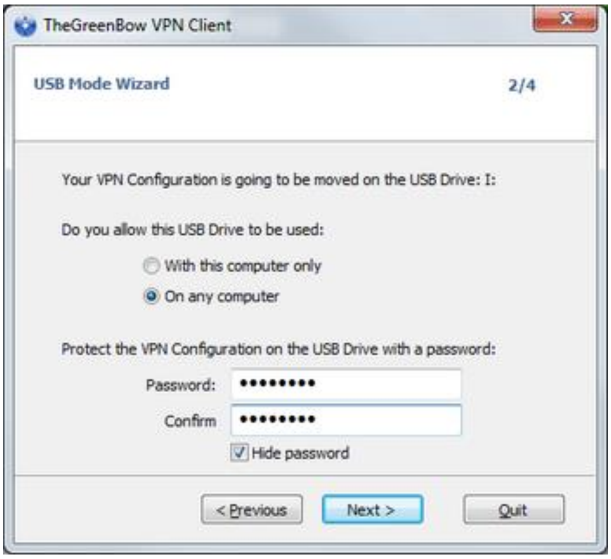
Note: When a USB drive plugged in is empty and it is the only one plugged in on the computer, the wizard automatically moves to step 2.

Step 2: Protection of the USB VPN security policy

Two protections are available:

1/ Association with the current computer:
The USB VPN policy can be uniquely associated to the current computer. In this case, the USB VPN can only be used on that computer. Otherwise (the USB is not associated with a particular computer), USB VPN can be used on any computer with a VPN Client.

2/ Password protection:
The USB VPN security policy can be protected by password. In this case, the password is required each time you plug in the VPN USB drive.



TheGreenBow VPN Client

USB Mode Wizard 2/4

Your VPN Configuration is going to be moved on the USB Drive: I:

Do you allow this USB Drive to be used:

○ With this computer only

● On any computer

Protect the VPN Configuration on the USB Drive with a password:

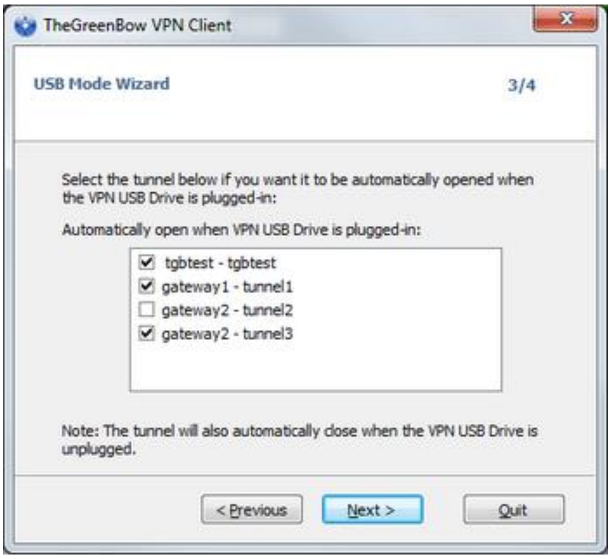
Password: ••••••••

Confirm ••••••••

☑ Hide password

Step 3: Open tunnel automatically

The wizard allows you to configure tunnels that will automatically open each time you insert the USB VPN.



TheGreenBow VPN Client

USB Mode Wizard 3/4

Select the tunnel below if you want it to be automatically opened when the VPN USB Drive is plugged-in:

Automatically open when VPN USB Drive is plugged-in:

☑ tgbtest - tgbtest
☑ gateway1 - tunnel1
□ gateway2 - tunnel2
☑ gateway2 - tunnel3

Note: The tunnel will also automatically close when the VPN USB Drive is unplugged.

Step 4: Summary

The summary is used to validate the correct setting of the USB VPN.

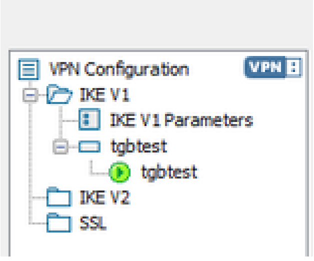
After validation of this last step, the VPN security policy is transferred to the USB.
It remains active as long as the USB is plugged in. Extraction of the USB VPN, VPN Client returns an empty VPN Configuration.

19.3 Use the USB Mode

When Stormshield VPN Client is launched, with a VPN security policy loaded or not, plug in the USB VPN. A popup window will ask to activate the USB mode.

After validation, the USB VPN policy is automatically loaded and, if applicable, tunnel(s) automatically open. The USB mode is identified in the Configuration Panel by a "USB Mode" icon at the top right of the tree.

Configuration Panel



Upon USB VPN drive removal the tunnel(s) are closed, and the previous VPN policy is restored.

Note: The VPN Client takes into account only one USB VPN at a time. Other USB VPN drives are not taken into account as long as the first one is plugged in.

Note: The import feature is disabled in USB mode.

In USB mode, the USB VPN security policy can be changed. Changes to the VPN policy is saved on the USB VPN.

Note: The VPN Client does not provide a direct option to change the password and association to the computer. To change them, use the following procedure:
1/ Plug in the USB VPN drive
2/ Export VPN Configuration
3/ Remove the USB VPN drive
4/ Import VPN Configuration exported in step 2
5/ Restart the Wizard USB mode with this configuration and the new desired settings.

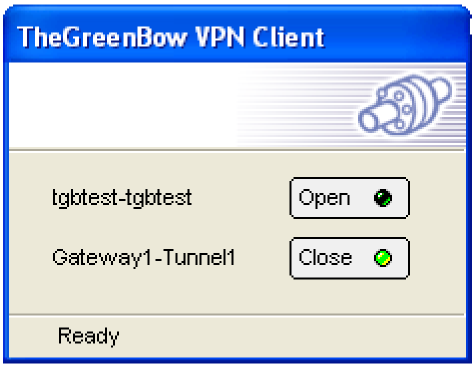
20 GINA Mode

20.1 GINA Mode

The GINA Mode enables to open VPN Connection before Windows Logon.

This function allows for example to open a secured connection to an access rights server, in order to retrieve the access rights of the user, before the Windows session opens.

When a GINA VPN tunnel is configured, it appears in a window similar to the Connection Panel, displayed on the Logon Windows screen. This window allows to manually open the VPN tunnel.



TheGreenBow VPN Client

tgbtest-tgbtest Open ●

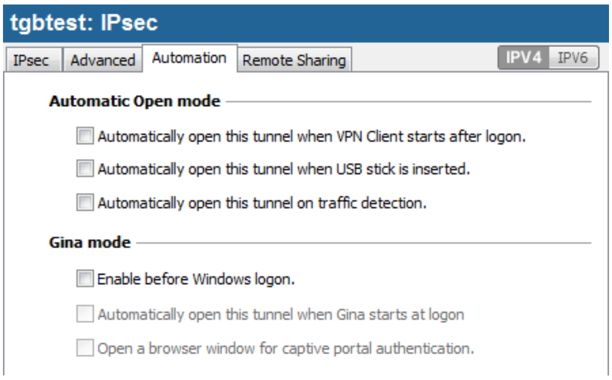
Gateway1-Tunnel1 Close ●

Ready

Like the Connection Panel, this window allows to manually open the VPN Connection.
A VPN Connection may also be open automatically before the Windows Logon.
For users a WiFi networks, an automatic browsing window opens before the tunnel opens, to enable an authentication on the WiFi captive portal.

20.2 Configuring the GINA Mode

The GINA Mode can be configured in the tab "Automation" of each VPN tunnel. See chapter "Automation".



tgbtest: IPsec

IPsec | Advanced | Automation | Remote Sharing | IPV4 | IPV6

Automatic Open mode

□ Automatically open this tunnel when VPN Client starts after logon.

□ Automatically open this tunnel when USB stick is inserted.

□ Automatically open this tunnel on traffic detection.

Gina mode

□ Enable before Windows logon.

□ Automatically open this tunnel when Gina starts at logon

□ Open a browser window for captive portal authentication.

20.3 Using the GINA Mode

When the VPN tunnel is configured in GINA mode, the window of the GINA tunnels opening is displayed on the Windows logon screen. The VPN tunnel is automatically opened if configured to do so.

VPN Tunnel in GINA mode can perfectly implement an X-Auth Authentication (the user must then enter his login / password), or a certificate authentication (the user must then enter the PIN access code to the Smartcard).

Warning: If two tunnels are configured in GINA Mode, and one of them opens automatically, it is possible that both tunnels are opened automatically.

Note: In order to get the "Automatically open on traffic detection" option operational, after opening of a Windows session, the "Enable before the Windows logon" option should not be checked.

Limitation: Scripts and USB Mode are not available for VPN tunnels in GINA mode.

Security considerations:

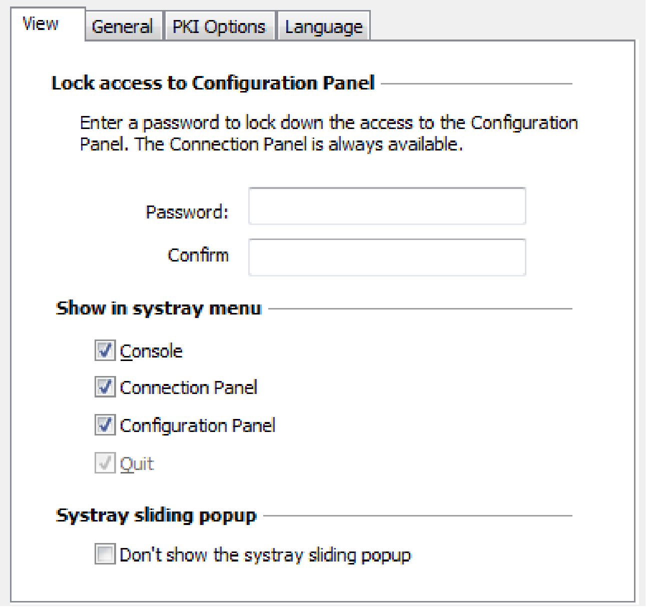
A tunnel configured in GINA Mode can be opened before the Windows logon, therefore by any user of the computer. It is strongly recommended that you configure an authentication, strong whenever possible, for a tunnel in Gina Mode, e.g. an X-Auth Authentication, or preferably a certificate authentication, if possible on removable media.

21 Access control to the VPN security policy

Any access to the VPN security policy (reading, change, application, import, export) can be protected by a password. This protection also applies to transactions done via the command line.

To ensure the integrity and confidentiality of VPN security policy, it is recommended to implement this protection.

The protection of the VPN security policy is configured via "Tools" > "Options" > "View" tab.



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

Once a password is configured, opening the Configuration Panel or accessing the VPN security policy (import substitution, addition) is always conditioned by entering this password:

- when the user clicks on the icon in the taskbar
- when the user selects the Configuration Panel menu in the icon menu in the taskbar
- when the user clicks on the [+] button of the Connection Panel
- when importing a new VPN security policy via the command line
- during a software update.

By combining this option with other options to limit the display of software, the administrator can configure the software in almost invisible and non-editable mode.

To remove the protection via password, empty both "Password" and "Confirm" fields, then confirm.

Note for the IT Manager: The protection of the VPN security policy can also be configured via the set up command line.

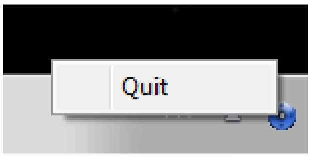
22 Options

22.1 Access Control

See chapter "Access control to the VPN Security Policy".

22.2 Hide menus

The options on the "View" tab of the "Options" window also allow to hide all software interfaces, by removing from the taskbar menu the "Console", "Configuration Panel" and "Connection Panel" items. The menu in the taskbar is then reduced to the single list of available VPN tunnels.



Note for the IT Manager: When deploying software, all these options can be preconfigured during the installation of Stormshield VPN Client software.

The "Quit" item from the taskbar menu cannot be removed via software. However, it may be removed using the installation options.

22.3 General

22.3.1 Start mode

When the "Start the VPN Client after Windows logon" option is checked, the VPN Client starts automatically when Windows starts, after the Windows Logon.

If the option is unchecked, the user must manually start the VPN Client, either by double-clicking on the desktop icon, or by selecting the start menu of the software in the Windows "Start" menu. See chapter "Windows Desktop".

22.3.2 Disabling the disconnection detection

In its generic behaviour the VPN Client closes the VPN tunnel (on its side), when it finds a problem communicating with the remote VPN gateway.

In unreliable local networks, prone to frequent micro-disconnections, this feature can have drawbacks (which can go up to unable to open a VPN tunnel).

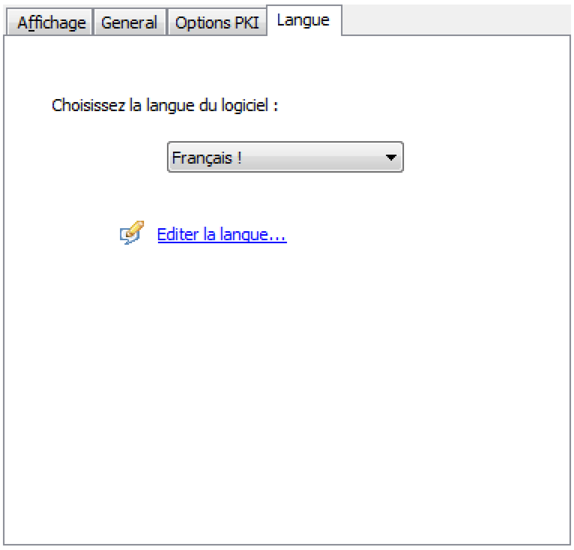
By checking the "Disable disconnection detection" box, the VPN Client avoids closing tunnels when a disconnection is detected. This ensures excellent stability of the VPN tunnel, including unreliable local networks, typically wireless networks like WiFi, 3G, 4G, or satellite.

22.4 Managing languages

22.4.1 Choosing a language

Stormshield VPN Client can be run in multiple languages.
It is possible to change the language while the software is running.

To select another language, open the "Tools" > "Options" menu and select the "Language" tab.
Choose the desired language from the proposed drop-down list:

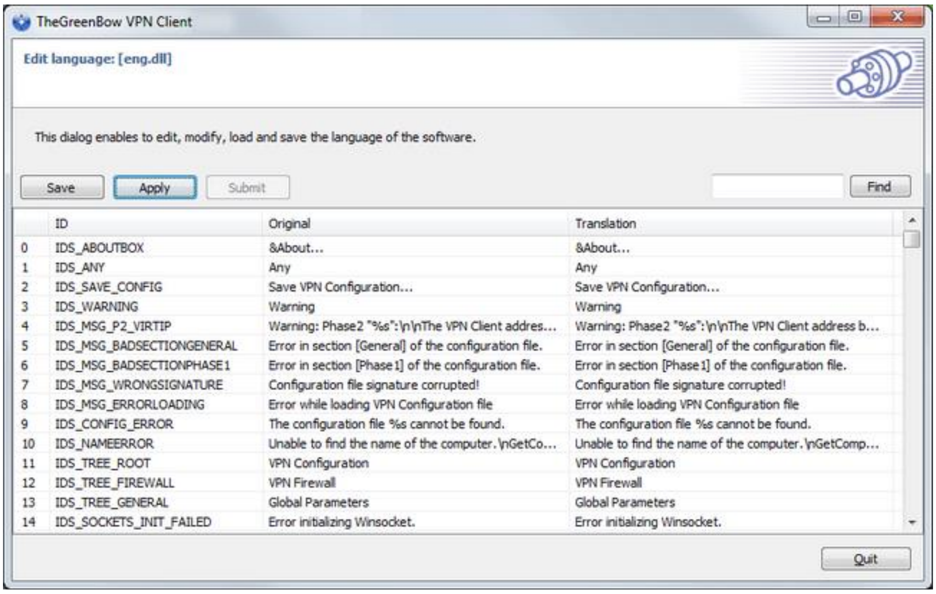


Choisissez la langue du logiciel : Français !

The list of languages available in the standard software is provided in the appendix to the chapter "List of available languages".

22.4.2 Modifying or creating a language

Stormshield VPN Client also allows to create a new translation or to make changes to the language that is being used, then to test these changes dynamically via an integrated translation tool.
In the "Language" tab, click on the "Edit language..." link; the translation window is displayed:



Edit language: [eng.dll]

This dialog enables to edit, modify, load and save the language of the software.

	ID	Original	Translation
0	IDS_ABOUTBOX	&About...	&About...
1	IDS_ANY	Any	Any
2	IDS_SAVE_CONFIG	Save VPN Configuration...	Save VPN Configuration...
3	IDS_WARNING	Warning	Warning
4	IDS_MSG_P2_VIRTIP	Warning: Phase2 "%s":\n\nThe VPN Client addres...	Warning: Phase2 "%s":\n\nThe VPN Client address b...
5	IDS_MSG_BADSECTIONGENERAL	Error in section [General] of the configuration file.	Error in section [General] of the configuration file.
6	IDS_MSG_BADSECTIONPHASE1	Error in section [Phase1] of the configuration file.	Error in section [Phase1] of the configuration file.
7	IDS_MSG_WRONGSIGNATURE	Configuration file signature corrupted!	Configuration file signature corrupted!
8	IDS_MSG_ERRORLOADING	Error while loading VPN Configuration file	Error while loading VPN Configuration file
9	IDS_CONFIG_ERROR	The configuration file %s cannot be found.	The configuration file %s cannot be found.
10	IDS_NAMEERROR	Unable to find the name of the computer.\nGetCo...	Unable to find the name of the computer.\nGetComp...
11	IDS_TREE_ROOT	VPN Configuration	VPN Configuration
12	IDS_TREE_FIREWALL	VPN Firewall	VPN Firewall
13	IDS_TREE_GENERAL	Global Parameters	Global Parameters
14	IDS_SOCKETS_INIT_FAILED	Error initializing Winsocket.	Error initializing Winsocket.

The translation window is divided into four columns which indicate respectively the number of the string, its ID, its translation in the original language, and its translation into the selected language.

The translation window allows to:

1/ translate each string by clicking on the corresponding line

2/ search for a given string in any column of the table ("Search" input field, then use the "F3" key to run through all occurrences of the searched string)

3/ save the changes
Any language modified or created is saved in a "lng" file

4/ immediately apply a change to the software: this feature allows to validate in real time whether any string is pertinent or properly displayed ("Apply" button)

5/ send a new translation ("Send" button).

The name of the language file that is being edited is recalled in the header of the translation window.

<u>Additional notes</u>:
Characters or following sequences of characters should not be changed during the translation:

"%s"	will be replaced by the software with a string
"%d"	will be replaced by the software with a number
"\n"	indicates a carriage return
"&"	indicates that the next character should be underlined
"%m-%d-%Y"	indicates a date format (here the format U.S.: month-day-year) modify this field only if knowledge of the format in the translated language.

Note: "IDS_SC_P11_3" string must be used without modification.

23 Console and Trace Mode

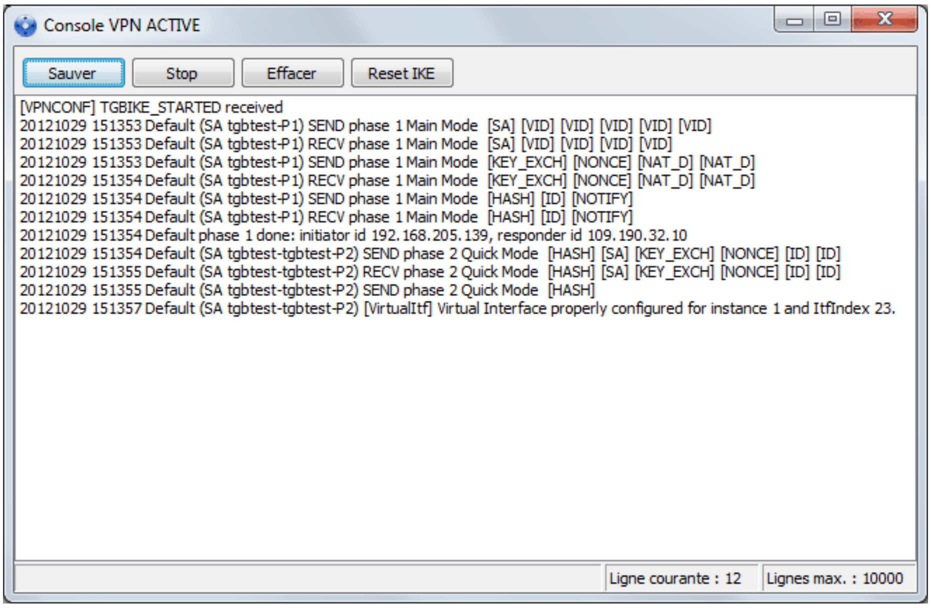
Stormshield VPN Client offers two tools that generate logs:
1/ The "Console" provides information and steps to open and close the tunnels (IKE messages for most of them)
2/ The "Trace Mode" asks each software component to produce its activity’s log.

Both tools are designed to help the network administrator to diagnose a problem during tunnels opening, or Stormshield support team in identifying software’s incidents.

23.1 Console

Console can be displayed as follows:

- Menu "Tools" > "Console" in the Configuration Panel
- Ctrl+D shortcut when the Configuration Panel is open
- In the software menu in the taskbar, select "Console"



```
[VPNCONF] TGBIKE_STARTED received
20121029 151353 Default (SA tgbtest-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID] [VID]
20121029 151353 Default (SA tgbtest-P1) RECV phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID]
20121029 151353 Default (SA tgbtest-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20121029 151354 Default (SA tgbtest-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20121029 151354 Default (SA tgbtest-P1) SEND phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20121029 151354 Default (SA tgbtest-P1) RECV phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20121029 151354 Default phase 1 done: initiator id 192.168.205.139, responder id 109.190.32.10
20121029 151354 Default (SA tgbtest-tgbtest-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20121029 151355 Default (SA tgbtest-tgbtest-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20121029 151355 Default (SA tgbtest-tgbtest-P2) SEND phase 2 Quick Mode  [HASH]
20121029 151357 Default (SA tgbtest-tgbtest-P2) [VirtualItf] Virtual Interface properly configured for instance 1 and ItfIndex 23.
```

The Console features include:

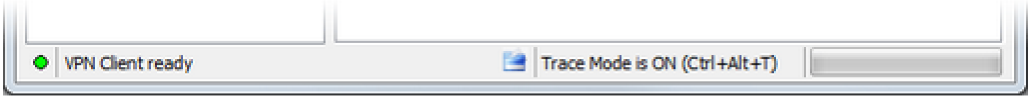
- Save: Save in a file all traces displayed in the window
- Start / Stop: Start / stop the capture of recording
- Delete: Delete the content of the window
- Reset IKE: Restart the IKE service.

23.2 Trace Mode

Trace Mode is activated by the shortcut: Ctrl+Alt+T

Switching to Trace Mode does not require to restart the software.

When Trace Mode is enabled, each component of Stormshield VPN Client generates logs of its activity. The generated logs are stored in a folder accessible by clicking the blue "Folder" icon in the status bar in the Configuration Panel.



● VPN Client ready

Trace Mode is ON (Ctrl+Alt+T)

Note: Activating logs is only possible from the main interface which can be restricted to the sole administrator with a password.
Even if the logs don't contain sensitive information, it is recommended to disable logs when they are not used anymore. It is also recommended to delete logs once they are used.

24 Recommendations for Security

24.1 General recommendations

To ensure an appropriate level of security, conditions to implement and use must be met as follows:

- The system administrator and security administrator, respectively responsible for the installation of software and the definition of VPN security policies, are considered trusted persons.
- The software user is a person trained in its use. In particular, he/she shall not disclose the information used for authentication to the encryption system.
- The VPN gateway to which the VPN Client connects allows to track the VPN activity and to show malfunctions or violations of security policies if they occur.
- The user's workstation is healthy and properly administered. It has an up-to-date anti-virus, and is protected by a firewall.
- The bi-keys and certificates used to open the VPN tunnel are generated by a trusted certification authority.

24.2 VPN Client administration

It is strongly recommended to protect access to the VPN security policy by a password and limit the visibility of the software to the end user, as detailed in chapter "**Access control to the VPN security policy**".

It is also recommended to set this protection at the time of installation, via the installation.

It is recommended to ensure that users are using the VPN Client in a "user" environment and try, as much as possible, to limit the use of the operating system with administrator rights.

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

24.3 Configuring VPN security policy

Use Authentication

The features of user authentication proposed by the VPN Client are described below, from the weakest to the strongest.

In particular, please note that authentication via pre-shared key is easy to implement, however it allows any user with access to the computer to open a tunnel without authentication check.

User authentication type	Strength
Pre Shared Key	weak
Static X-auth	🟧
Dynamic X-Auth	🟨
Certificate stored in the VPN security policy	🟩

Certificate in the Windows Certificate Store	
Certificate on Smartcard or Token	strong

IKE V1 Protocol

It is recommended to set the "Main Mode" rather than "Aggressive Mode". See chapter "**Authentication Advanced**".

Gina Mode

It is recommended to add a strong authentication to any tunnel in Gina Mode.

25 Annexes

25.1 Shortcuts

Connection Panel

- ESC	Close the window
- CTRL+ENTER	Open the Configuration Panel (Main interface)
- Arrows	The up and down arrows enable to select a VPN Connection
- CTRL+O	Open the selected VPN Connection
- CTRL+W	Close the selected VPN Connection

VPN Tree (Configuration Panel):

- F2	Edit the name of the selected Phase
- DEL	Delete the selected Phase, after user confirmation. If the whole configuration is selected (root item of the VPN tree), the whole configuration is deleted after user confirmation.
- CTRL+O	Open the tunnel associated to the selected item
- CTRL+W	Close the tunnel associated to the selected item
- CTRL+C	Copy in the clipboard the selected phase
- CTRL+V	Paste (add) the phase copied in the clipboard
- CTRL+N	Create a new phase (new Phase1 if IKEv1 is selected, new IKE Auth if IKEv2 is selected, etc.)
- CTRL+S	Save the VPN Security policy.

Configuration Panel

- CTRL+ENTER	Switch to the Connection Panel
- CTRL+D	Open the "Console" window
- CTRL+ALT+R	Restart the IKE daemon
- CTRL+ALT+T	Activate the trace mode (creation of logs)
- CTRL+S	Save the VPN security policy

25.2 Languages

Code	Language	Code ISO 639-2
1033 (default)	English	EN
1036	Français	FR
1034	Español	ES
2070	Português	PT
1031	Deutsch	DE
1043	Nederlands	NL
1040	Italiano	IT
2052	简化字	ZH
1060	Slovenscina	SL
1055	Türkçe	TR
1045	Polski	PL
1032	ελληνικά	EL
1049	Русский	RU
1041	日本語	JA
1035	Suomi	FI
2074	српски језик	SR
1054	ภาษาไทย	TH
1025	عرب ي	AR
1081	हिन्दी	HI
1030	Danske	DK
1029	Český	CZ
1038	Magyar nyelv	HU
1044	Bokmål	NO
1065	ف ار سی	FA
1042	한국어	KO

25.3 Stormshield VPN Client specifications

General

Windows Versions	Windows 2000 32bit Windows XP 32bit SP3 (Client VPN Certified 2013) 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

Utilization

Invisible mode	Automatic opening of the tunnel upon traffic detection Access control to the VPN security policy Possible interfaces mask
USB mode	No more VPN security policy on the computer Opening of the tunnel when inserting a configured VPN USB key Automatic closing of the tunnel when extracting the configured VPN USB key
Gina	Opening of a tunnel before Windows logon Credential providers on Windows Vista, Windows 7 and further
Scripts	Running scripts configurable upon opening and closing of the VPN tunnel
Remote Desktop Sharing	Opening of 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 computers equipped with VPN Client) Peer-to-Gateway
Media	Ethernet, Dial up, DSL, Cable, GSM/GPRS, WiFi Wireless LAN : 3G, 4G, satellite
Tunneling Protocol	IKE based on OpenBSD 3.1 (ISAKMPD) Diffie-Hellmann DH Group 1 to 18 Full IPsec support using IKv1 and IKEv2 Full SSL/TLS support

Tunnel mode	Main mode and Aggressive mode
Config mode	Network settings automatically retrieved from the VPN gateway

Cryptography

Encryption	Symmetric: DES, 3DES, AES 128/192/256bit Asymmetric: RSA Diffie-Hellmann: 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	Admin: Securing access to VPN security policies User: − X-Auth static or dynamic (request at each tunnel's opening) − Hybrid Authentication − Pre-shared key − EAP
PKI	− Certificates: support format X509, PKCS12, PEM − Multi-support: Windows certificate store, Smartcard, Token − Certificates criteria: expiration, revocation, CRL, subject, key usage − Ability to select the Token / Smartcard interface (see list of qualified Tokens / Smartcard) − Automatic detection of Token / Smartcard − Access to Token / Smartcard in PKCS11 or CSP − Verification of "Client" and "Gateway" certificates

Miscellaneous

NAT / NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 and RFC 3947, IP address emulation, includes support for: NAT_OA, NAT keepalive, NAT-T aggressive mode, NAT-T forced mode, automatic or off
DPD	RFC3706. Detection of non-active IKE end points.
Redundant Gateway	Management of a redundant gateway, automatically selected upon detection of DPD (inactive gateway)
Firewall	Filtering incoming / outgoing IP addresses and TCP / UDP ports

Administration

Deployment	Options to deploy VPN policies (command line options for the set up, configurable initialization files...) Silent installation
VPN policies management	Options to import and export VPN policies Securing imports / exports by password, encryption and integrity monitoring
Automation	Open, close and monitor a tunnel from the command line (batch and scripts), startup and shutdown of software by batch file

Log and trace	IKE / IPsec logs console and trace mode activated
Live update	Checking for updates from the software
License and activation	Modularity of licenses (standard, temporary, limited duration), software activation (WAN, LAN), and deployment options (deployment of enabled software, silent activation...)

25.4 Credits and Licenses

Credits and licences 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 rouines 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.]
 */
```

STORMSHIELD

documentation@stormshield.eu