



User Guide

TP-LINK **SafeStream**[™] IPSec VPN Client



COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **TP-LINK®** is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2012 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

<http://www.tp-link.com>

CONTENTS

Chapter 1 Introduction	1
1.1 Linux Appliance Support	1
1.2 The VPN Client Features	1
Chapter 2 Installation	5
2.1 Software Installation	5
2.1.1 Access Rights	6
2.2 Trial Software Evaluation	7
2.3 Software Activation.....	7
2.3.1 Software Activation Wizard	7
2.3.2 Activation Troubleshooting.....	9
2.4 Software Upgrade	9
2.5 Software Uninstallation	10
Chapter 3 User Interface Overview	11
3.1 User Interface Elements.....	11
3.2 System Tray Popup Screens.....	12
3.3 Keyboard Shortcuts.....	12
3.4 Connection Panel.....	13
3.5 Configuration Panel	13
3.5.1 Main Menus	14
3.5.2 Status Bar	15
3.5.3 Windows "About"	15
3.5.4 Options	15
3.5.5 Wizards.....	23
Chapter 4 Connection Panel	24
4.1 Connection Panel basics.....	24
Chapter 5 Configuration Panel	25
5.1 VPN Configuration Overview	25

5.1.1	How to create a VPN Tunnel?.....	25
5.1.2	Multiple Authentication or IPSec Configuration Phase.....	26
5.1.3	Advanced Features.....	26
5.2	Configuration Wizard.....	27
5.2.1	Three step Configuration Wizard	27
5.2.2	Step 1 of 3: Choice of remote equipment.....	28
5.2.3	Step 2 of 3: VPN tunnel parameters	28
5.2.4	Step 3 of 3: Summary	29
5.3	Authentication or Phase 1	30
5.3.1	What is Phase 1 ?.....	30
5.3.2	Phase 1 Settings Description.....	31
5.3.3	Phase1 Advanced Settings Description	32
5.4	IPSec Configuration or Phase 2.....	36
5.4.1	What is Phase 2?.....	36
5.4.2	Phase 2 Settings Description.....	36
5.4.3	Phase2 Advanced Settings Description	38
5.4.4	Script configuration	39
5.4.5	Remote Desktop Sharing.....	40
5.5	Global Parameters	42
5.5.1	Global Settings Description.....	42
5.6	USB Mode.....	44
5.6.1	What is USB Mode?	44
5.6.2	How to enable a new USB Drive?.....	44
5.6.3	How to automatically open tunnels when an USB Drive is plugged in?	47
5.7	Configuration Management.....	49
5.7.1	Import or Export VPN Configuration via menu	49
5.7.2	Merge of VPN Configurations	50
5.7.3	Split of VPN Configuration	51

5.7.4	Embed your own VPN Configuration into VPN Client Setup.....	52
5.7.5	Demo VPN Configuration.....	53
Chapter 6 VPN Client Software Setup and Deployment		54
6.1	Embedded VPN Configuration	54
6.2	Setup options	54
6.2.1	Setup option overview	54
6.2.2	Setup option for GUI mode	55
6.2.3	Setup option for GUI mode access control	55
6.2.4	Setup option for systray menu items.....	56
6.2.5	Other Setup options.....	56
6.3	Command line.....	59
6.3.1	Command line options	59
6.3.2	Opening or closing VPN Tunnel options	59
6.3.3	Stopping IPsec VPN Client: option "/stop".....	60
6.3.4	Import or Export VPN Configuration options.....	60
Chapter 7 Configuring the VPN Client with a TP-LINK VPN Router		61
7.1	Example VPN Network Topology	61
7.2	Configuring the TP-LINK VPN Router	62
7.3	Configuring the VPN Client	66
7.3.1	Use the Configuration Wizard to Configure the VPN Client	66
7.3.2	Manually Configure the VPN Client	71
7.3.3	Establish a VPN connection.....	77
Chapter 8 Console and Logs		78
8.1	Console Windows	78

Chapter 1 Introduction

The VPN Client supports all Windows versions and allows you to establish secure connections over the Internet usually between a remote worker and the corporate Intranet. IPSec is the most secure way to connect to the enterprise as it provides strong user authentication and strong tunnel encryption with the ability to work with existing network and firewall settings. The VPN Client software and Download tool are in the Resource CD, you can click **TheGreenBow VPN Client** to install the VPN Client or click **TP-LINK VPN Client** to download the latest software.

This Guide is intended for Network Engineer and Network Administrator.

1.1 Linux Appliance Support

The VPN Client supports several versions of Linux IPSec VPN such as StrongS/WAN and FreeS/WAN. The VPN Client is compatible with most of the IPSec routers/appliances based on those Linux implementations.

1.2 The VPN Client Features

Feature	Specifications
Windows versions	<ul style="list-style-type: none">• Windows 2000 32-bit• Windows XP 32-bit• Windows Server 2003 32-bit• Windows Server 2008 32/64-bit• Windows Vista 32/64-bit• Windows 7 32/64-bit
Languages	Arabic, Chinese (simplified), Dutch, English, Finnish, French, German, Greek, Hindi, Italian, Japanese, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, and Turkish
Connection modes	<ul style="list-style-type: none">• Operates in a peer-to-peer VPN as well as point-to-multiple mode without a gateway or server. All connection types such as dial-up, DSL, cable, GSM/GPRS, and Wi-Fi are supported.• Allows IP range networking.• Runs in a Remote Desktop (RDP) connection session.

Tunneling protocols	<ul style="list-style-type: none"> • Full Internet Key Exchange (IKE) support: the IKE implementation is based on the OpenBSD 3.1 implementation (ISAKMPD). This provides the best compatibility with existing IPSec routers and gateways. • Full IPSec support: <ul style="list-style-type: none"> • Main mode and aggressive mode • MD5 and SHA-1 hash algorithms • Change IKE port
NAT Traversal	<ul style="list-style-type: none"> • NAT Traversal Draft 1 (enhanced), Draft 2 and 3 (full implementation), including: <ul style="list-style-type: none"> • - NAT OA support • - NAT keepalive • - NAT T aggressive mode • Forced NAT-Traversal mode.
Encryption	<p>Provides the following encryption algorithms:</p> <ul style="list-style-type: none"> • 3DES, DES and AES 128/192/256bits encryption • Support of Group 1, 2, and 5 (that is, 768, 1024, and 1536)
User authentication	<p>Supports the following user authentication methods:</p> <ul style="list-style-type: none"> • Preshared keying and X509 certificates support. Compatible with most of the currently available IPSec gateways. • Extended authentication (AUTH) • Flexible certificates: PEM, PKCS#12 certificates can be directly imported from the user interface. Ability to configure one certificate per tunnel. • Hybrid authentication method

	<p>Certificate storage capabilities:</p> <ul style="list-style-type: none"> • USB token and smart card support • Windows certificate store support • VPN configuration file
	<p>Remote login:</p> <ul style="list-style-type: none"> • Vista Credential Providers support (also known as GINA on Windows 2000 and Windows XP) to enable Windows logon via a VPN tunnel or choose to logon on a local machine.
Dead Peer Detection	<p>Dead Peer Detection (DPD) is an IKE extension (RFC3706) for detecting a dead IKE peer.</p>
Redundant Gateway	<p>The Redundant Gateway feature provides a highly reliable secure connection to a corporate network. The Redundant Gateway feature allows the VPN Client to open an IPSec tunnel with an alternate gateway if the primary gateway is down or not responding.</p>
Mode Config	<p>Mode Config is an IKE extension that enables the VPN gateway to provide LAN configuration to the remote user's machine (that is, the VPN Client). With Mode Config, you can access all servers on the remote network by using their network name (for example, //myserver/marketing/budget) instead of their IP address.</p>
USB dDrive	<p>You can save VPN configurations and security elements (certificates, preshared key, and so on) to a USB drive to remove security information (for example, user authentication) from the computer. You can automatically open and close tunnels when plugging in or removing the USB drive. You can attach a VPN Configuration to a specific computer or to a specific USB drive.</p>

Smart card and USB token	The VPN Client can read certificates from smart cards to make full use of existing corporate ID or employee cards that carry digital credentials. You can easily import smart card ATR codes to enable new smart card and USB token models that are not yet in the software.
Log console	All phase messages are logged for testing or staging purposes.
Flexible user interface	<ul style="list-style-type: none"> • Silent install and invisible graphical interface allow network administrators to deploy solutions while preventing user misuse of configurations. • Small Connection Panel screen and VPN Configuration Panel screen can be available to end-users separately with access control. • Drag and drop VPN configurations into the VPN Client. • Keyboard shortcuts to easily navigate the VPN Client.
Scripts	Scripts or applications can be launched automatically on events (for example, before and after a tunnel opens, or before and after a tunnel is closed).
Configuration management	<ul style="list-style-type: none"> • User interface and command-line interface (CLI) • Password protected VPN configuration file. • Specific VPN configuration file can be provided within the setup • Embedded demo VPN configuration to test and debug with online servers • Ability to prevent software upgrade or uninstallation if protected by password
Live update	Ability to check for online updates

Chapter 2 Installation

This chapter describes installation of the VPN Client and related processes.

2.1 Software Installation

The VPN Client installation does not require specific information. After completing the installation, you will be asked to reboot your computer.

After you have rebooted and logged in, the Activation Wizard screen displays.

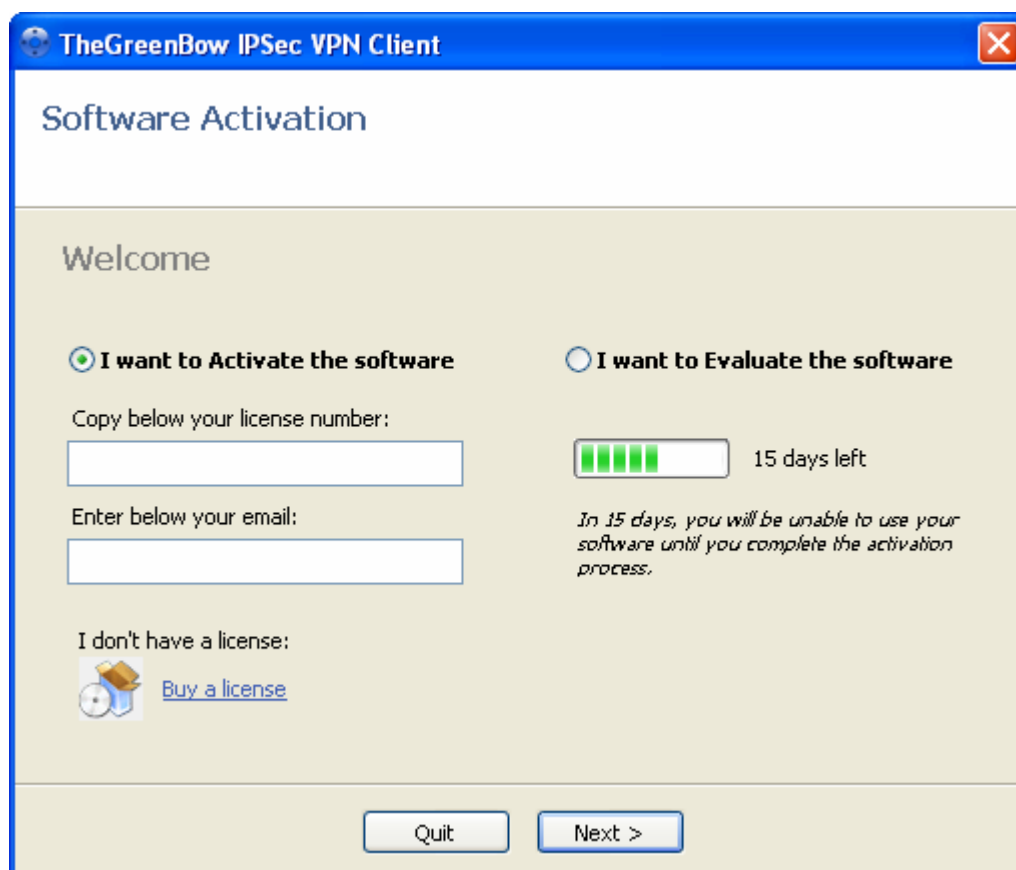


Figure 2-1

The four buttons at the bottom of the screen have the following functions:

Quit:	Closes the window and software.
I want to Evaluate the software:	Lets you continue software evaluation. Evaluation time left is displayed in the orange banner.
I want to Activate the software:	Lets you activate the software license online. This requires a license number and Internet access.

Buy a license:	Lets you go online and purchase a software license. When you purchase a software license you must activate it before using the VPN Client.
-----------------------	--



Note:

When you run Windows 2000, Windows XP, Windows Vista, or Windows 7, you must have administrator rights otherwise the installation stops with an error message after the language selection.

After software installation, TheGreenBow VPN window can be launched:

- From user desktop, by double-clicking on TheGreenBow VPN shortcut.
- From VPN Client icon available in the taskbar.
- From menu **Start > Programs > TheGreenBow > TheGreenBow VPN > TheGreenBow VPNClient.**

2.1.1 Access Rights

Depending on your status, you might have restricted access rights on a Windows computer:

Actions	Admin	Users
Software install	Yes	No
Software activation	Yes	Yes
Software use	Yes	Yes

To make it easier, the VPN Client creates new rules in the Windows firewall (Vista and later) so that VPN traffic is enabled. The Windows firewall rules are:

Windows Firewall Rule Names	Actions
The IPSec VPN Client phase1	authorize UDP 500
The IPSec VPN Client phase2	authorize UDP 4500

2.2 Trial Software Evaluation

You can use the VPN Client during the evaluation period (usually limited to 30 days) by select the **I want to Evaluate the software** option. When the VPN Client is in evaluation mode, the register window appears each time that you start the VPN Client. The evaluation time remaining is displayed in the orange banner.

When the evaluation period expires, the **I want to Evaluate the software** option is no longer displayed and the software is disabled. In order to use the VPN Client you must purchase and activate a license.

During the time that a temporary software license number is used, the activation window is available from the Connection Panel screen. You can purchase and activate a permanent license while using a temporary license. The remaining time of the temporary license is available by clicking ? on the main menu of the Connection Panel screen.

When the temporary license expires, the Evaluate button is disabled. You must then click the **Buy a license** button to purchase a license and select the **I want to Activate the software** option and enter the license number to activate the purchased license.

2.3 Software Activation

2.3.1 Software Activation Wizard

In order to use the VPN Client beyond the evaluation period, the VPN Client license must be activated on your computer. You will need the license number or key and an email address.

To transfer a license to a new computer, you must uninstall the software from the old computer. Deactivation of the license on the old computer occurs automatically if the computer is connected to the Internet. The license can then be used to activate the VPN Client on a new computer.

To activate your software using the Activation Wizard:

1. Launch the Activation Wizard from the VPN Client by using either of the following methods:
 - Select **I want to Activate the software** option in the VPN Client startup window.
 - Click ? on the main menu of the Connection Panel screen, then click Activation Wizard.
2. Enter your license number. If you have a 20-character license number instead of a 24-character one, clicking on Click here to enter a 20 character License.

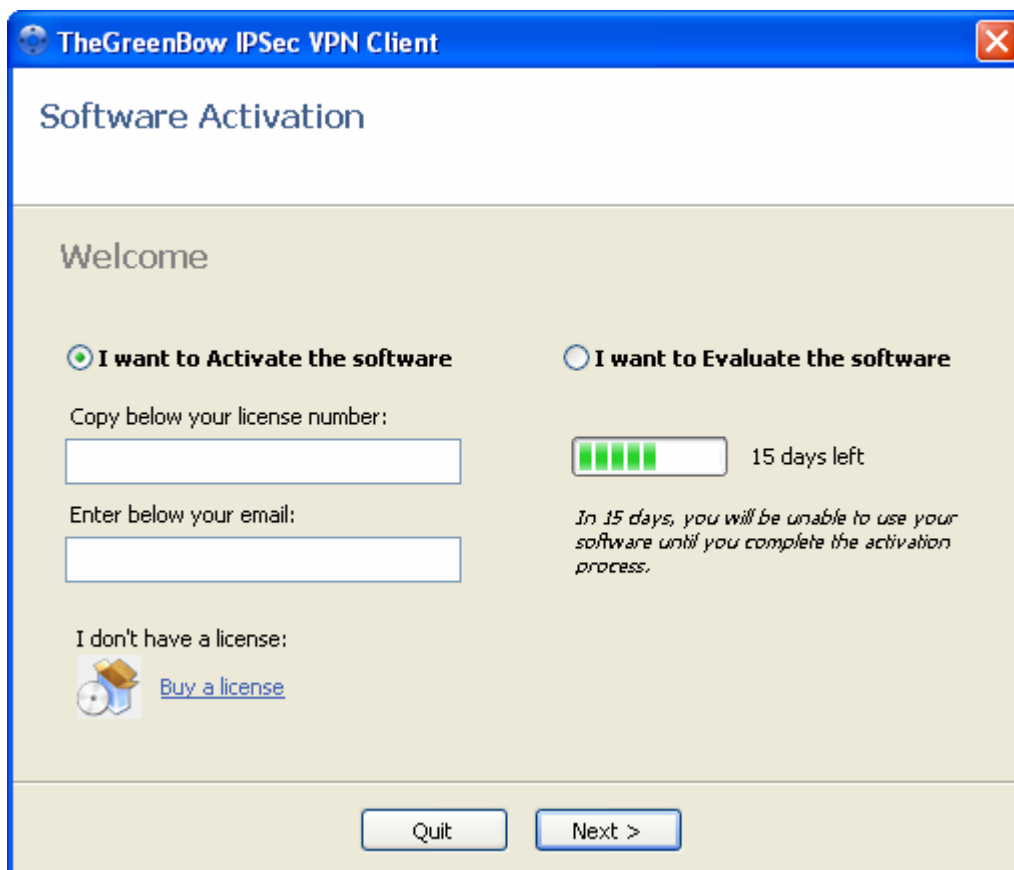


Figure 2-2

3. Enter your email address, which will be used to send you the activation confirmation.



Note:

The email address might not be required. If the administrator suppresses display of the **Email address** field during the software setup, it will not be displayed by the Activation Wizard. Suppression can be used to centralize all software activation confirmation emails to a single email address.

4. Click **Next**. The Activation Wizard attempts to automatically connect to the activation server to activate the VPN Client software. If the activation is successful, a message is displayed.



Tips:

After activation, save the license key number. You might need it again to reactivate your software in case of a problem. Also, keep the CD label for technical support.



Note:

- At any time you can change the license number, but you first need to uninstall the VPN Client.
- A license number is attached to a single computer after activation. However, you can deactivate the license number and transfer it to another computer.

2.3.2 Activation Troubleshooting

Errors might occur during the activation process. Each activation error type is displayed on the activation screen. Click **More information about this error** below the progress bar for explanation of the error and recommendations.

You can resolve most of errors by carefully checking the following:

- Verify that you entered the correct license number.
- Communication with the activation server may be blocked by a proxy. On the initial Activation Wizard screen, click on If you are using a Proxy, click here, and configure the proxy.
- Communication with the activation server may be blocked by a firewall (error 053 or error 054). Find out if a personal or corporate firewall is blocking communications.
- The activation server may be temporarily unreachable. Wait a few minutes and try again.
- Your license number could already be activated (error 033). Contact:sales@thegreenbow.com.



Note:

If you didn't succeed to activate the software despite the previous recommendations, it is always possible to manually activate the software on the website: www.thegreenbow.com/activation/osa_manual.html. This enables users to immediately fully activate the software.

2.4 Software Upgrade

The success of a software upgrade activation depends on your maintenance contract:

- During the maintenance period (which starts from your first activation), all software upgrades are allowed.

- If the maintenance period has expired or if you have no maintenance contract, only maintenance software upgrades are allowed. Maintenance software upgrades are identified by the last digit of a version.

Example: Your maintenance period has expired and your current software release is 3.12. You can upgrade to releases 3.13 through 3.19 but not to release 3.20, 3.30, or 4.00.

If you want to subscribe or extend your maintenance period, please contact the sales team: sales@thegreenbow.com.



Note:

- The VPN Client must be activated after each software upgrade. Depending on your maintenance contract, a software upgrade activation might be rejected. Carefully read the recommendations in this section and check the current status of your software release by clicking ? on the main menu of the Connection Panel screen and then Check for update.
- The VPN Configuration is saved during a Software Upgrade and automatically enabled again within the new release.
- If you have specified a password in the access control Configuration screen, you must enter it to be able to upgrade the software.

2.5 Software Uninstallation

TheGreenBow IPsec VPN Client can be uninstalled:

- from Windows Control Panel by selecting '**Add/Remove programs**'
- from Start **Menu** > **Programs** > **TheGreenBow** > **VPN** > '**Uninstall IPsec VPN Client**'

Uninstallation will reset your activation, allowing you to install and activate again the software on any other computer.



Note:

After uninstallation, save the license key number. You might need it again to reactivate your software.

Chapter 3 User Interface Overview

This chapter describes the user interface for the VPN Client. This chapter includes the following sections: **User Interface Elements**, **System Tray Popup Screens**, **Keyboard Shortcuts**, **Connection Panel Screen**, **Configuration Panel Screen**, and **VPN Console Active Screen**.

3.1 User Interface Elements

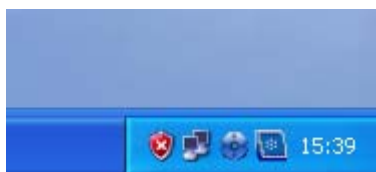
The VPN Client is fully autonomous and can start and stop tunnels without user intervention, depending on traffic to certain destinations. However it requires a VPN configuration.



The VPN Client configuration is defined in a VPN Configuration file. The software user interface allows creating, modifying, saving, exporting or importing the VPN configurations together with security elements such as a preshared key or certificates.

The user interface consists of several elements:

- Configuration Panel
- Connection Panel
- Main menus
- System tray icon and popup
- Status bar
- Wizards
- Preferences

The VPN Client software can be launched via a double click on application icon (Desktop or Windows Start menu) or by single click on application icon in system tray. Once launched, the VPN Client software shows an icon in the system tray that indicates whether a tunnel is opened or not, using color code.



Blue icon: 	No VPN tunnel is opened
Green icon: 	At least one VPN tunnel is opened

A right-button click on the VPN icon opens the configuration user interface.

The user interface shows the following menu items from top to bottom:

- Configured tunnels with their current status. You can open or close tunnels by clicking on **Open tunnel <tunnel name>** or **Close tunnel <tunnel name>**.
- **Save & Apply.** Closes all established VPN tunnels, applies the latest VPN configuration modification, and reopens the VPN tunnels that are configured to be started automatically.
- **Console.** Shows the VPN Console Active screen.
- **Connection Panel.** Opens the Connection Panel that lets you open and close VPN tunnels and displays information about VPN tunnels.
- **Configuration Panel.** Opens the Configuration Panel that lets you create and configure VPN tunnels.
- **Quit.** Closes all established VPN tunnels, and then closes the VPN Client.

3.2 System Tray Popup Screens

When a VPN tunnel opens or closes, a small popup screen comes out from the system tray icon and shows the following:

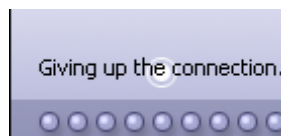
- VPN tunnel opening with different phases. The popup screen disappears after 6 seconds unless you move the mouse over the screen.



- VPN tunnel closing.



- If the VPN tunnel cannot open, the screen might display a warning with a link to more information.



3.3 Keyboard Shortcuts

The user interface supports the following keyboard shortcuts.

Shortcut	Action
Ctrl + Enter	Lets you switch back and forth between the Configuration Panel and the Connection Panel. If the Configuration Panel is protected with a password, you are asked for this password when you switch to the Configuration Panel.
Ctrl + D	Lets you open the VPN Console for network debugging.
Ctrl + S	Lets you save and apply a VPN Configuration.

3.4 Connection Panel

The Connection Panel enables users to open, close and get clear information about every tunnel that have been configured. This is all the end-user needs to open and close tunnels.

This feature clearly helps both IT Managers (who configure the VPN connections) and users (who only open or close VPN connections) with their own usage.

The Connection Panel is made of several elements for each configured tunnel:

- An icon (small grey or large green bullet) that shows if the tunnel is open or not.
- A gauge of traffic representing the volume of traffic back and forth within that particular tunnel.
- The tunnel name with format 'phase1-phase2'.

You can switch back and forth between the Connection Panel screen and the Configuration Panel screen by using the **Ctrl + Enter** shortcut.



3.5 Configuration Panel

The Configuration Panel enables to create VPN Configuration and is made of several elements:

- A tree list window (left column) that contains all the IKE and IPSec configurations.
- A configuration window (right side) that shows the associated parameters for every tree level.

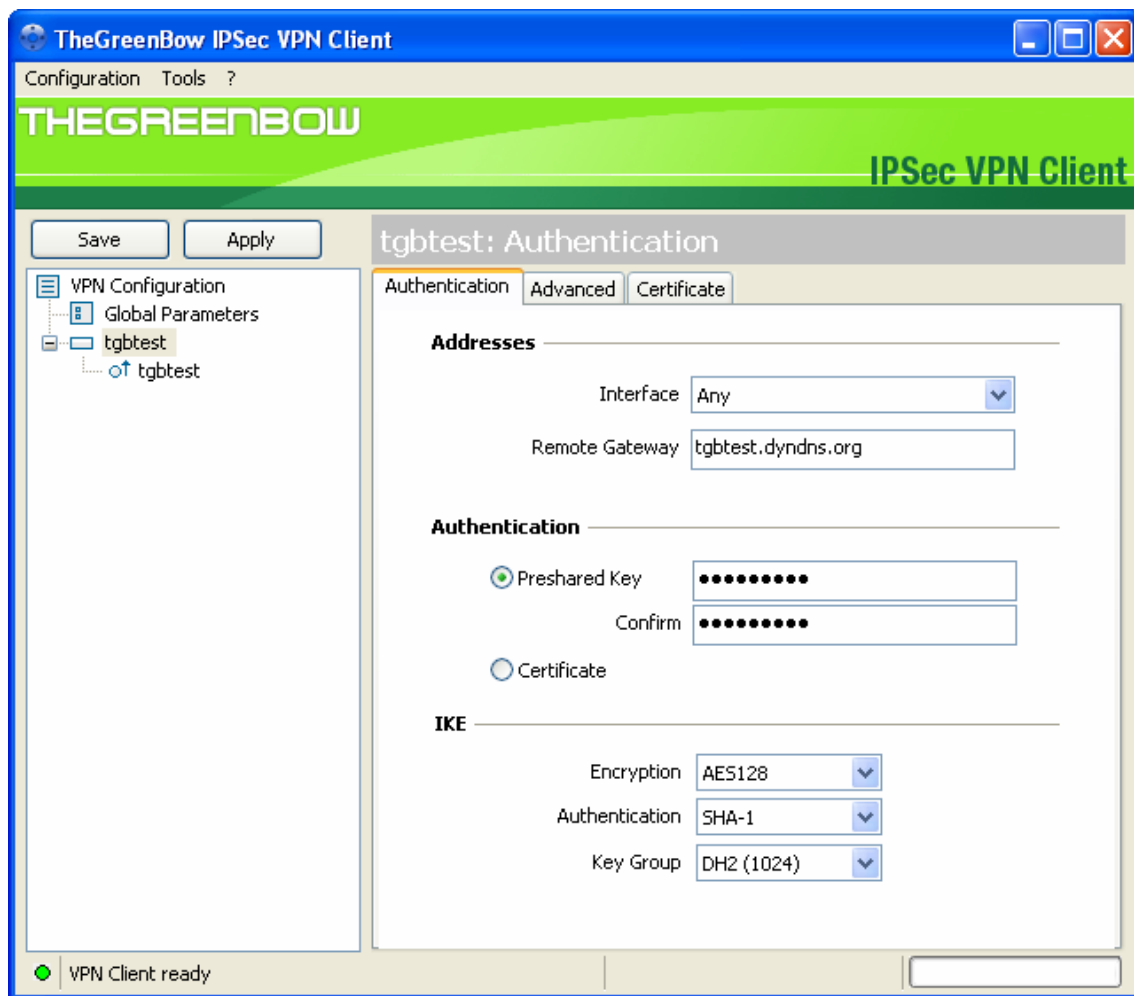


Figure 3-1

A VPN Configuration file (i.e. extension '.tgb') can be drag and dropped onto the Configuration Panel. This feature enables to easily apply a new VPN configuration. If a tunnel is configured to be 'opened when the VPN Client starts', it will be immediately opened as soon as the new VPN Configuration is applied ('Save & Apply').

3.5.1 Main Menus

The Main Menu is as followed:



Figure 3-2

Configuration:	It is used to Import or Export a configuration. It is also used to choose the location of the VPN Configuration: locally stored on computer or on USB Drive. It is finally used to configure miscellaneous preferences such as the way the VPN Client may start. 'Configuration' menu gives also access to the 'Configuration Wizard'.
Tools:	It contains 'Console', 'Connection Panel', 'Reset IKE' and 'Options...' choice.
?:	It gives access to 'check for update', 'online help', and 'Purchase license online' and window 'About'. '?' menu also gives access to the 'Activation Wizard' when the software is not activated yet.

3.5.2 Status Bar

The status bar displays several information:

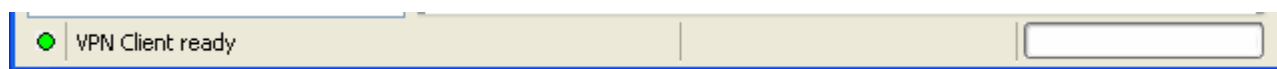


Figure 3-3

- The light box (left side) is green if the IKE services is up and running.
- The central box gives some information about VPN Client software status (e.g. "opening tunnel in progress", "saving configuration rules in progress", "VPN Client start up in progress", ...)
- The progress bar (right side) shows progress during saving or importing.

3.5.3 Windows "About"

The 'About' window provides the VPN Client software release number and software activation information. There is also an URL to our web site. License number (when activated), and module names with release numbers can be cut&paste if you need to send them to our tecsupport.

3.5.4 Options

The options can be configured via menu 'Tools' > 'Options....'.

Navigating the Options via three tabs:

- **View** tab to set access control & hidden interface preferences.
- **General** tab to set startup preferences and miscellaneous.
- **Language** tab to change language preferences and translate all strings.

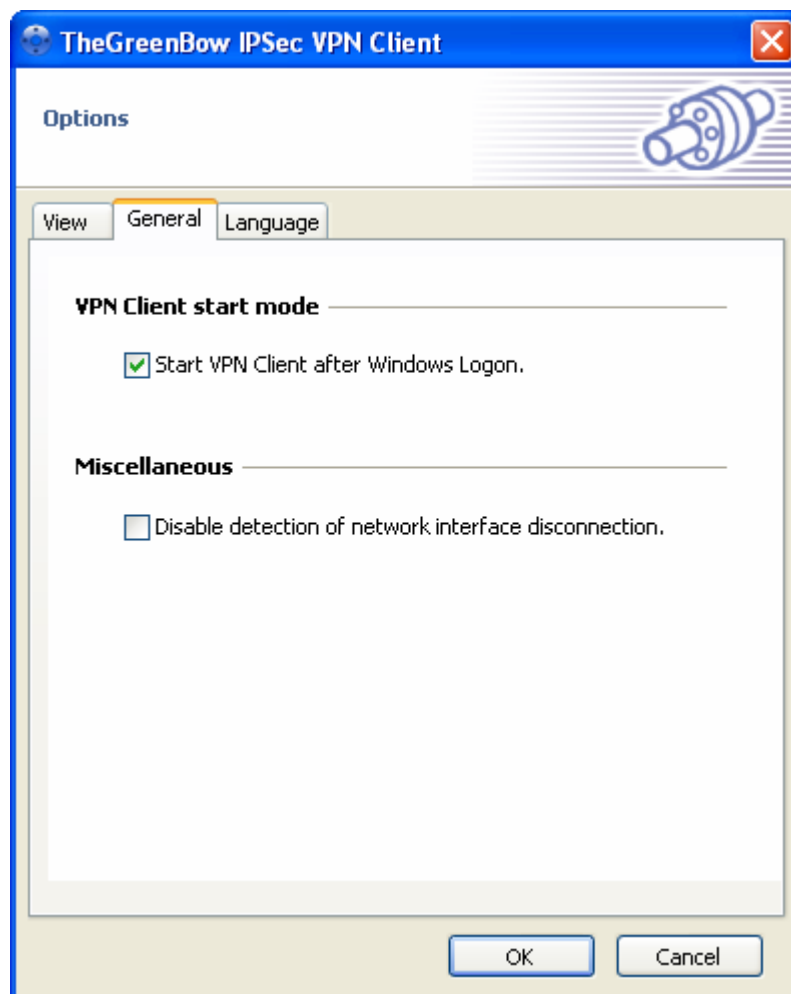


Figure 3-4

3.5.4.1 Access Control & Hidden Interface

This feature is especially designed for IT Managers. It enables to lock the access to the 'Configuration Panel', and to restrict with password the use of the IPsec VPN Client to the 'Connection Panel' and/or to the 'systray menu'.

The IT Manager can restrict the software access, from a full access to a completely hidden interface. Therefore, users cannot modify the VPN Configuration anymore, and mis-configuration are avoided.

The Access Control with a password only concerns the 'Configuration Panel'. The access to the 'Connection Panel' is never controlled by password.

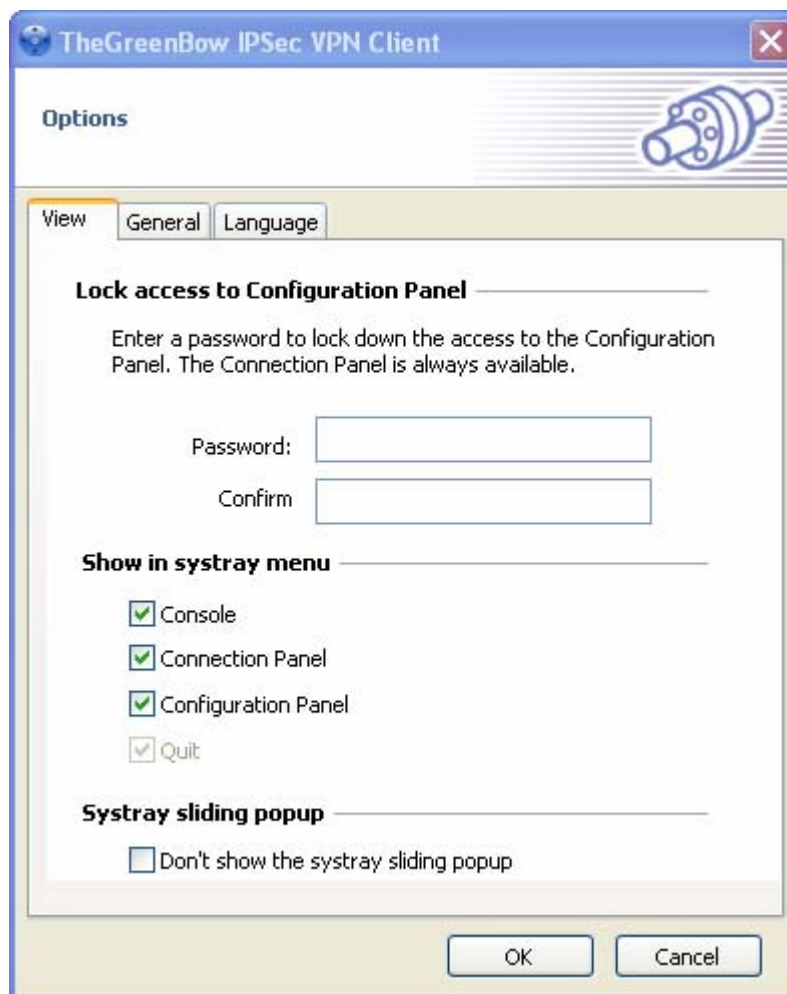


Figure 3-5

Once password configured, the user will be asked for the password:

1. When he clicks (or double-clicks) on the systray IPsec VPN Client icon.
2. When he switches from the "Connection Panel" to the **Configuration Panel**.
3. When he starts a **Software upgrade**.

Once password configured, the following **command lines** are not allowed:

1. 'vpnconf.exe /import' to import a new VPN configuration
2. 'vpnconf.exe /replace' to import and replace a new VPN configuration



Figure 3-6

This password may be configured as an option of the setup (see section '**Setup options**').

To remove the Access Control, just empty both fields '**Password**' and '**Confirm**' then click '**OK**'.

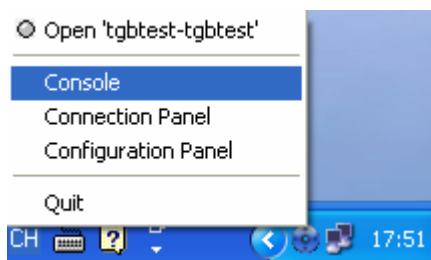


Note:

The 'Quit' item for the systray menu is disabled in the standard version of the software. It can nevertheless be removed during the software setup, through the setup option "-menuitem" (see section '**Setup option**')

In case Access Control has been set, the 'Configuration Panel' can not be opened and showed by double-clicking on desktop icon, by selecting Start menu. Right-click over the systray icon in taskbar is limited to "Console" access, quitting the software, and opening/closing the configured tunnels.

Here is an example:



3.5.4.2 General

'General' tab allows to define:

- Start up mode of the software. Those modes can be configured in the software setup (see section '**Setup options**').
- Enable/Disable the detection of interface disconnection feature.

Those preferences are available via Menu 'Tools' > 'Options..' and click 'General..'.

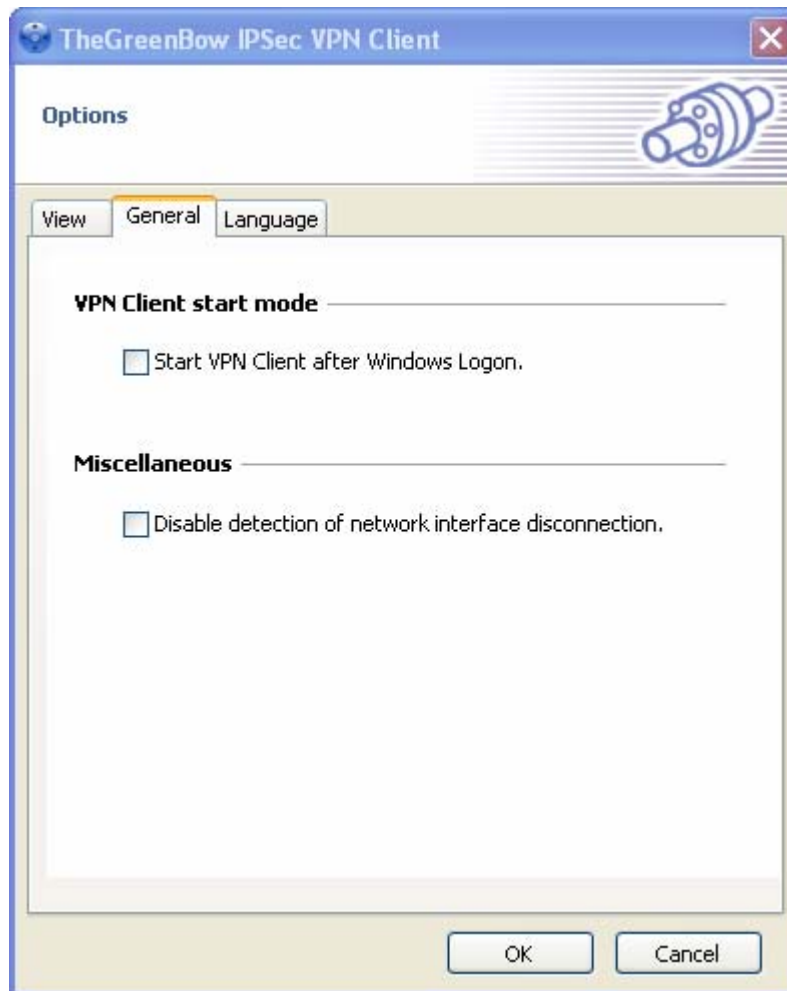


Figure 3-7

VPN Client start mode

TheGreenBow IPsec VPN Client software has several start up mode, such as start or don't start IPsec VPN Client software after MS Windows login

Miscellaneous

Disable detection of interface disconnection allows the IPsec VPN Client maintain tunnels opened while the network interface disconnects momentarily but very often. This type of behavior occurs when the interface used to open tunnels is unstable such as WiFi, GPRS and all 3G interfaces.

3.5.4.3 Language & Translation

The 'Language' option is available from menu 'Options..' then click on 'Language'. This option allows to select, and apply the selected language to the software on the fly (no restart).

It also allows anyone to localize the software. This feature is especially designed for our partners around the world who localize the IPsec VPN Client. It enables to translate the entire software in a new language directly from the software and to see the changes right away.

Select any language in the list:

- Click 'OK' to apply the selected language to the software.
- Click 'Edit language ...' to start translation of a new language. If you want to improve or adapt an existing language, find the closest language in the list.

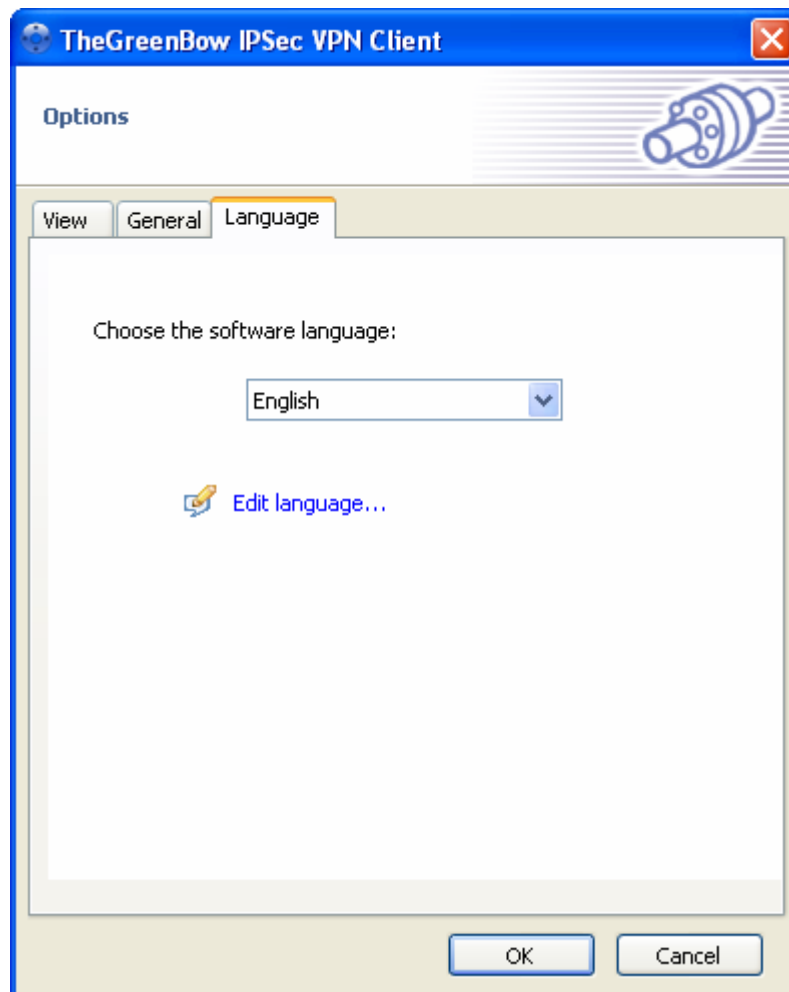


Figure 3-8



Note:

If you are returning back to this tool, the language you previously saved after editing has now a '!' mark at the end of the language name like 'English !'.

The software will display all the strings from the system language file (e.g. eng.dll).

You can see 4 columns:

- Line number
- String ID: name of the string
- Original: string in English
- Translation: translated string

Now, you can...

- Start translating by clicking on any string. A popup appears with the sentence to translate.
- 'Find' any word in the list. Click on 'F3' to find next.
- 'Apply' instantly the strings you have just translated to the software, to see if it fits into the software fields.
- 'Save' your work into a language file (.lng). The default folder is TheGreenBow IPsec VPN Client install folder, but you may choose any folder.
- 'Submit' the new language file (.lng) you've just translated to TheGreenBow so we can include it in the next software release.

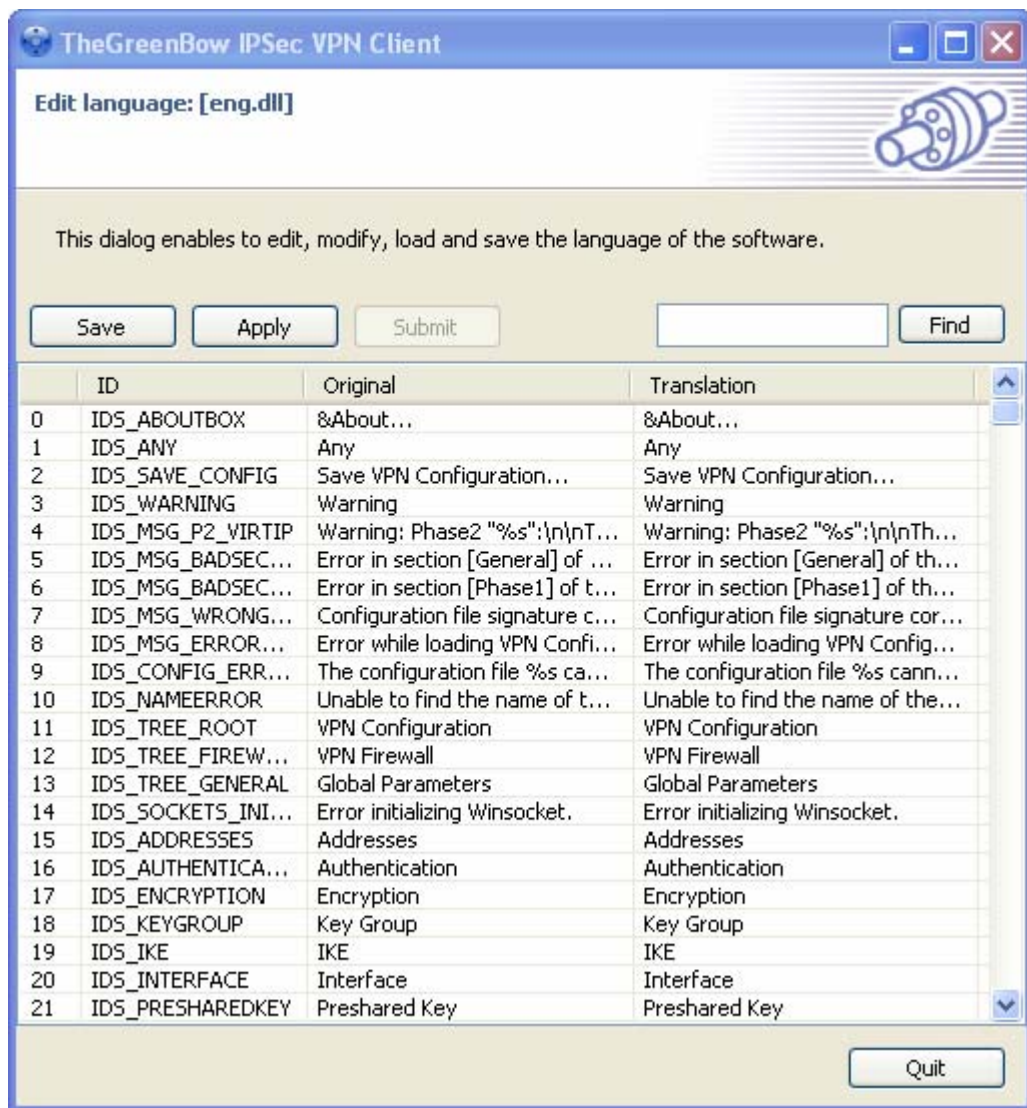


Figure 3-9



Note:

the language file you are working on is always displayed on the top left corner. A newlanguage file (.lng) can always be deleted from TheGreenBow IPsec VPN Client install folder incase you want to start again from scratch.

During translation, the following characters are generic expression which must not be changed:

"%s": is replaced by a string"

%d": is replaced by a number"

\n": stands for carriage return"

&": underlines the following character e.g. in menus

Modify IDS_DATE_FORMAT = " %m-%d-%Y " only if you know the appropriate syntax.

IDS_SC_P11_3 is not expected to be translated.

3.5.5 Wizards

There are several Wizards available:

- **VPN Configuration Wizard** can be launched from Menu 'Configuration' > 'Wizard'.
- **USB Drive mode Wizard** can be launched from Menu 'Configuration' > 'Move to USB Drive'.
- **Software Activation Wizard** can be launched from Menu '?' > 'Activation Wizard'

Chapter 4 Connection Panel

4.1 Connection Panel basics

The Connection Panel enables users to open, close and get clear information about every tunnel that have been configured. This is all the end-user needs to open and close tunnels.

The Connection Panel is made of several elements for each configured tunnel:

- An icon (small grey or large green bullet) that shows if the tunnel is open or not.
- A gauge of traffic representing the volume of traffic back and forth within that particular tunnel.
- The tunnel name with format 'phase1-phase2'



Figure 4-1

Navigating the Connection Panel:

- [?] icon to open the '**About**' window.
- [+] icon to switch back to the '**Configuration Panel**'.
- [x] icon to close the Connection Panel.
- It's possible to switch back and forth between the '**Connection Panel**' and the '**Configuration Panel**' by using the shortcut '**Ctrl + Enter**' (see section '**Shortcuts**').
- Double click on any line will open or close the tunnel.

It's possible to switch back and forth between the '**Connection Panel**' and the '**Configuration Panel**' by using the shortcut '**Ctrl + Enter**' (see section '**Shortcuts**').

Chapter 5 Configuration Panel

5.1 VPN Configuration Overview

5.1.1 How to create a VPN Tunnel?

To create a VPN tunnel from the '**Configuration Panel**' (without using the **Configuration Wizard**), you must follow the following steps:

1. Reset Configuration Panel to remove any prior configurations.

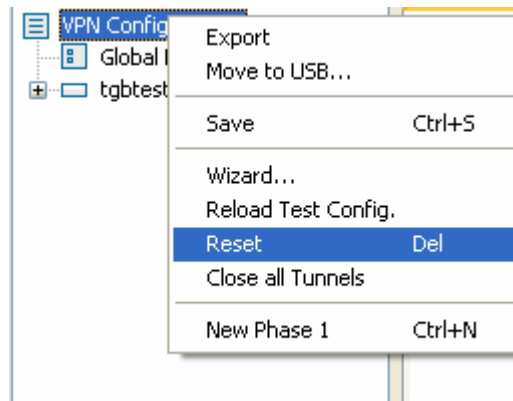


Figure 5-1

2. Right-click on 'VPN Configuration' in the tree list window and select 'New Phase 1'.

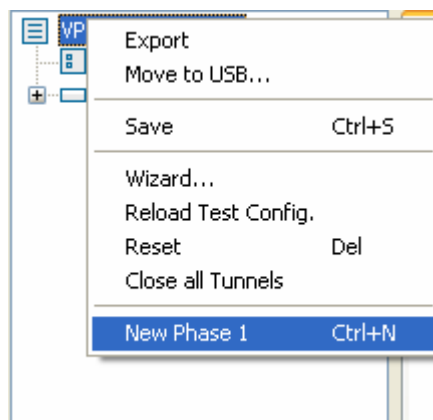


Figure 5-2

3. Configure Authentication Phase (**Phase 1**).
4. Right-click on the new Phase 1 in the tree control and select "New Phase 2'.

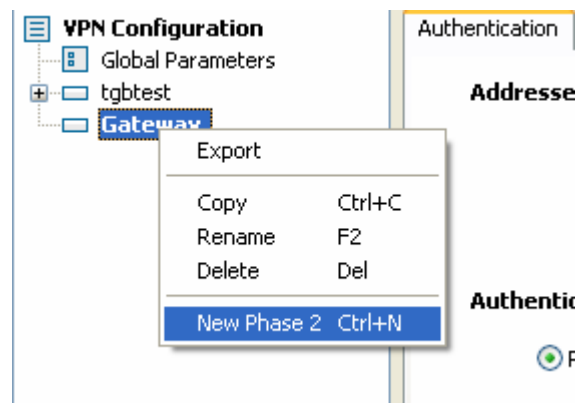


Figure 5-3

5. Configure IPsec Phase (**Phase 2**).
6. Change the name of any Phase 1 or Phase 2 once selected via a single click on the name, or a right click > 'Rename'.
7. Once the parameters are set, 'Apply' to take into account the new configuration. That way the IKE service will run with the new parameters. Click on 'Save' to save it into the configuration file for future use.
8. Double click on any phase2 in the tree (light grey bullet) for opening the IPsec VPN tunnel.

Please refer to **Phase 1** and **Phase 2** for more settings descriptions.

5.1.2 Multiple Authentication or IPsec Configuration Phase

Several Authentication Phases (**Phase1**) can be configured. Therefore, one computer can establish IPsec VPN connections with several gateways or other computers (peer to peer).

Similarly, several IPsec Configuration (**Phase 2**) can be created for a same Authentication Phase (**Phase 1**).

5.1.3 Advanced Features

Advanced features and parameters can be defined for Phase 1 and Phase 2.

Those defined in Phase 1 apply to all Phase 2 created in current VPN Configuration:

- Enable/Disable **Config-Mode**
- Enable/Disable **NAT-T Aggressive Mode**
- Enable/Disable **Redundant Gateway**
- Select **NAT-T mode** (Forced, Disabled or Automatic)
- Set **X-Auth Login/password** with pop up option

- Enable/Disable **Hybrid Mode** which is an Hybrid Authentication Method

Those defined in Phase 2 only apply to the associated Phase 2:

Automatic Open Mode

- Choose **Script/Application** to be launched when tunnel opens
- Manual settings of **DNS/WINS** server addresses
- Enable Windows logon via VPN tunnel using Vista Credential Providers (aka GINA on W2K/WXP).

5.2 Configuration Wizard

5.2.1 Three step Configuration Wizard

The GreenBow IPsec VPN Client provides a Configuration Wizard which enables the creation of VPN configuration in three easy steps. This Configuration Wizard is designed either for remote computers that need to get connected to a corporate LAN through a VPN gateway or Peer to Peer mode.

Let take the following example:

- The remote computer has a dynamically provided public IP address.
- It tries to connect the Corporate LAN behind a VPN gateway that has a DNS address "gateway.mydomain.com".
- The Corporate LAN address is 192.168.0.xxx. e.g. the remote computer want to reach a server with the IP address: 192.168.0.100.

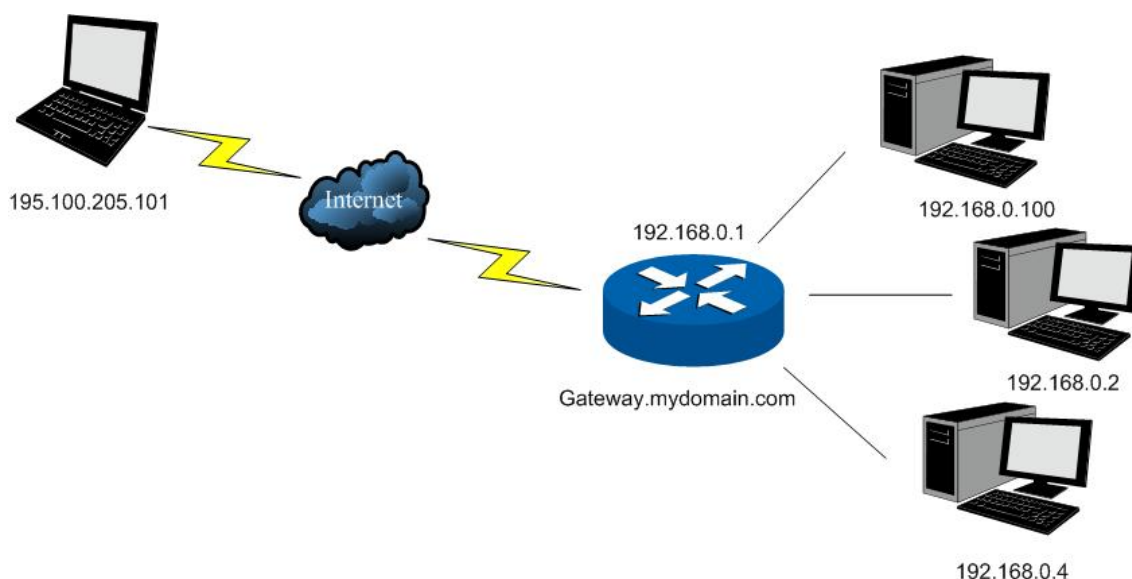


Figure 5-4

For configuring this connection, open the Configuration Wizard's window by selecting menu 'Configuration' > 'Wizard'.

5.2.2 Step 1 of 3: Choice of remote equipment

You must specify the type of the equipment at the end of the tunnel: VPN gateway.

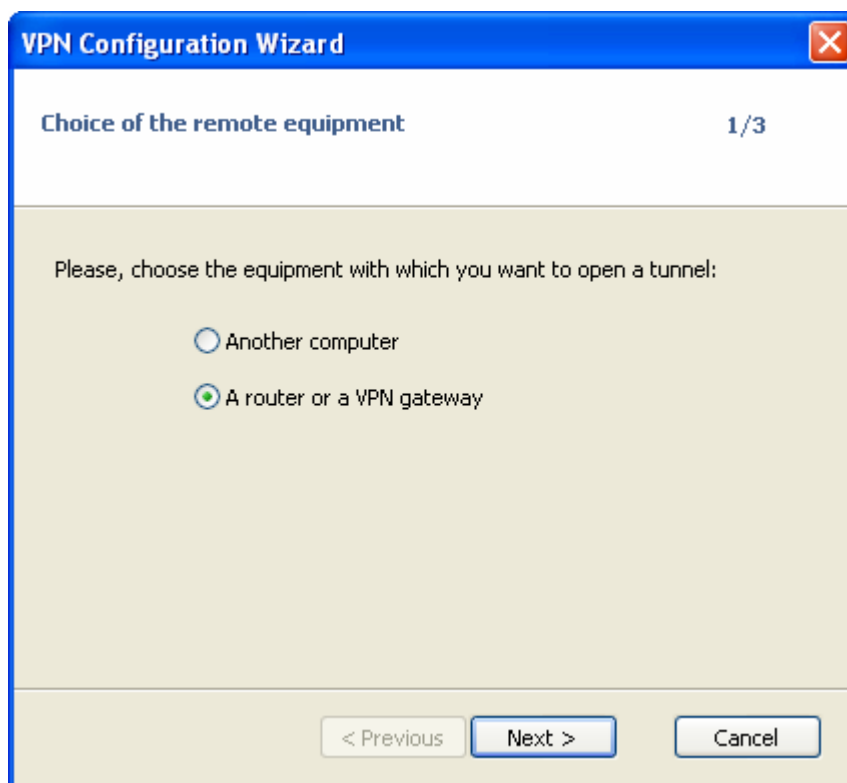
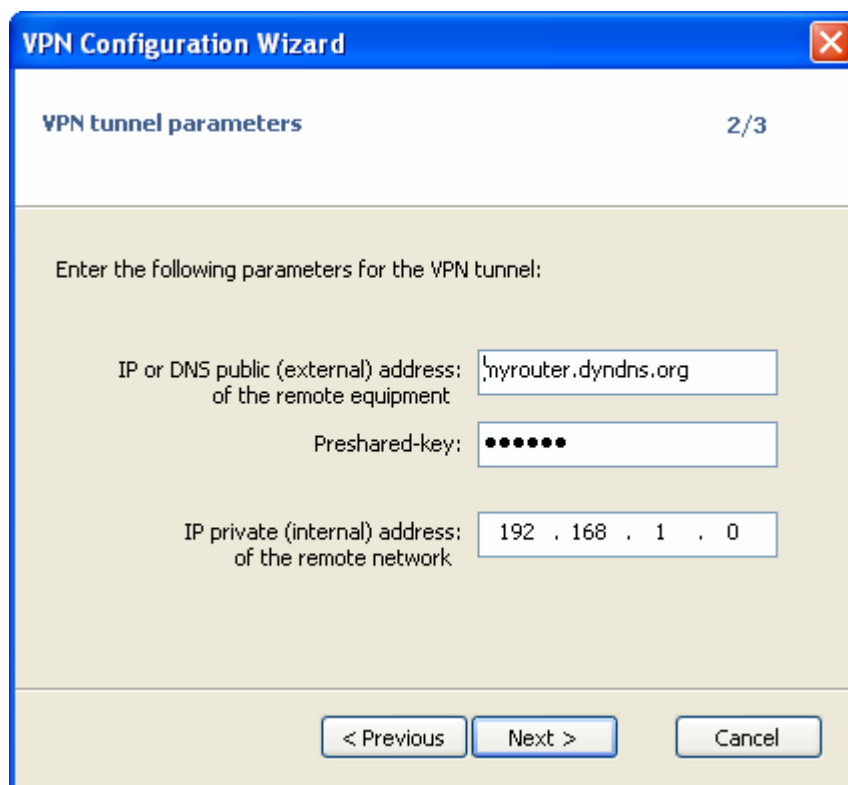


Figure 5-5

5.2.3 Step 2 of 3: VPN tunnel parameters

You must specify the following information:

- The public (Wide Area Network side) address of the remote gateway
- The preshared key you will use for this tunnel (this preshared key must be the same in the gateway)
- The IP address of your company LAN (e.g. specify 192.168.1.0)



The image shows a 'VPN Configuration Wizard' window with a blue title bar and a close button. The window is titled 'VPN Configuration Wizard' and shows '2/3' steps. The current step is 'VPN tunnel parameters'. The instructions say 'Enter the following parameters for the VPN tunnel:'. There are three input fields: 'IP or DNS public (external) address: of the remote equipment' with the value 'myrouter.dyndns.org', 'Preshared-key:' with a masked value of seven dots, and 'IP private (internal) address: of the remote network' with the value '192 . 168 . 1 . 0'. At the bottom are three buttons: '< Previous', 'Next >', and 'Cancel'.

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 equipment myrouter.dyndns.org

Preshared-key:

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

< Previous Next > Cancel

Figure 5-6

5.2.4 Step 3 of 3: Summary

The third step summarizes your new VPN configuration. Other parameters may be further configured directly via the 'Configuration Panel' (e.g. Certificates, virtual IP address, etc..).

The tunnel has been created and you can open it.

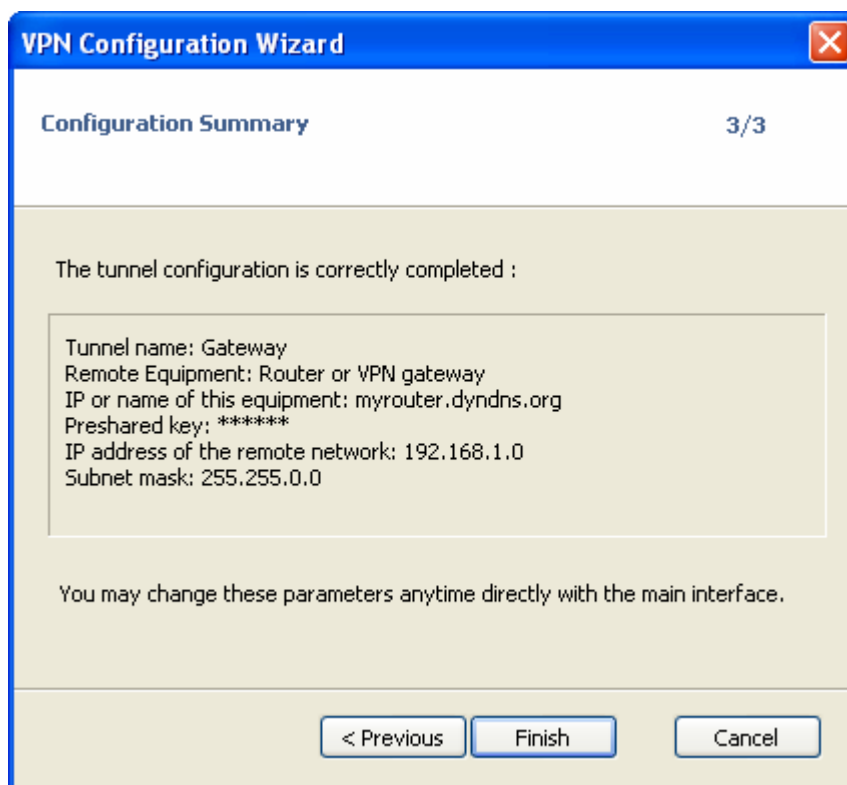


Figure 5-7

5.3 Authentication or Phase 1

5.3.1 What is Phase 1 ?

'Authentication' or 'Phase 1' window will concern settings for Authentication Phase or Phase 1. It is also called IKE Negotiation Phase.

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.

You must specify the following information:

- The public (Wide Area Network side) address of the remote gateway
- The preshared key you will use for this tunnel (this preshared key must be the same in the gateway)
- The IP address of your company LAN (e.g. specify 192.168.1.0)

5.3.2 Phase 1 Settings Description

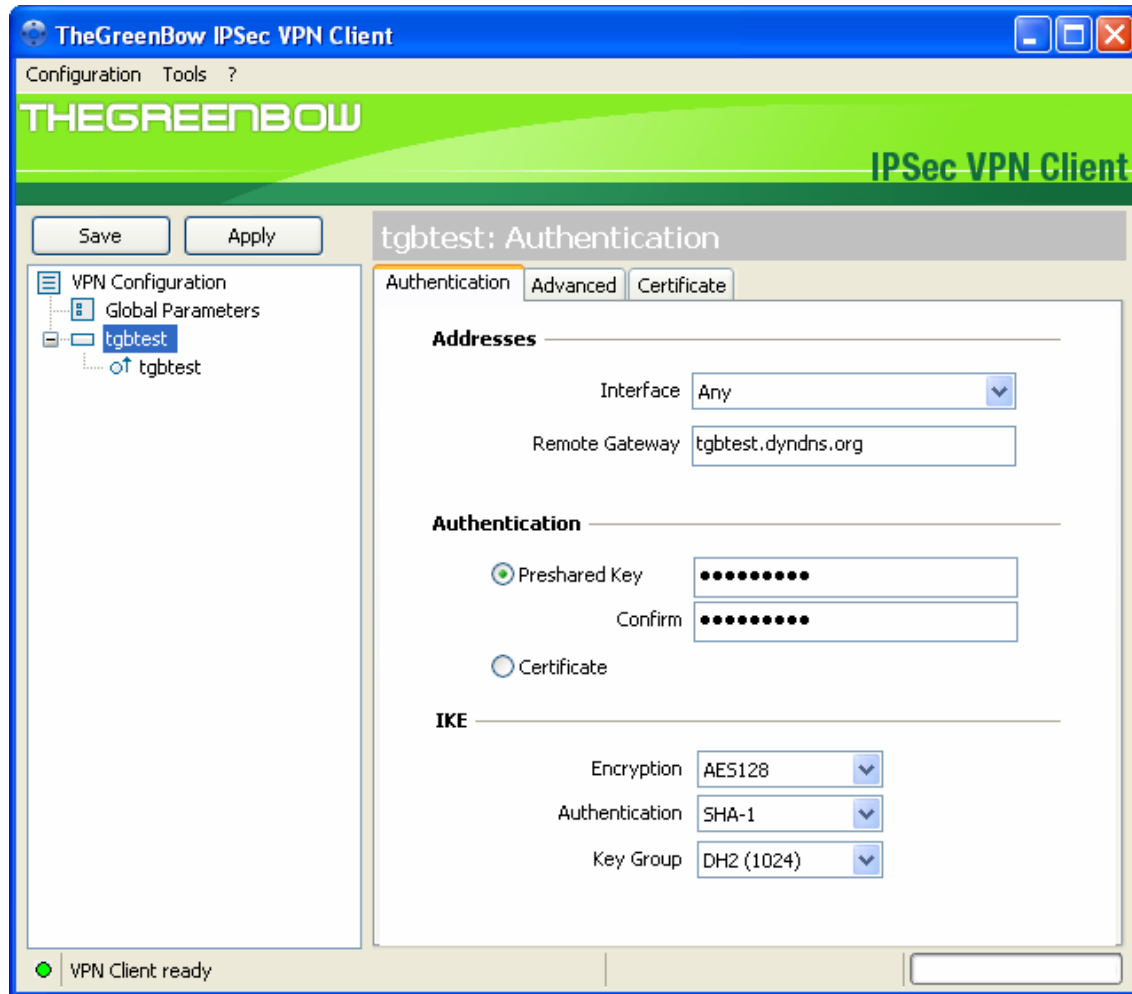


Figure 5-8

Interface:	IP address of the network interface of the computer, through which VPN connection is established. If the IP address may change (when it is received dynamically by an ISP or router), select "Any". In case the IP address configured into the VPN Configuration file refers to an IP address that does not exist on the computer then the default "Any" is forced upon this parameter.
Remote Gateway:	IP address or DNS address of the remote gateway (in our example: gateway.mydomain.com). This field is mandatory.
Pre-shared key:	Password or key shared with the remote gateway.

Certificate:	X509 certificate used by the VPN Client. Click on 'Certificate Management..' to choose the certificate source: PEM files, PKCS#12 file, SmartCard and tokens, or the Windows Certificate Store. One Certificate per tunnel can be configured.
IKE encryption:	Encryption algorithm used during Authentication phase (3DES, AES, ...).
IKE authentication:	Authentication algorithm used during Authentication phase (MD5, SHA, ...). SHA1 and SHA2-256-bit are supported.
IKE key group:	Diffie-Hellman key length.

For more advanced settings, go to 'Advanced' tab.

5.3.3 Phase1 Advanced Settings Description

For advanced features & parameters, click on 'Advanced' tab into Phase1 panel.

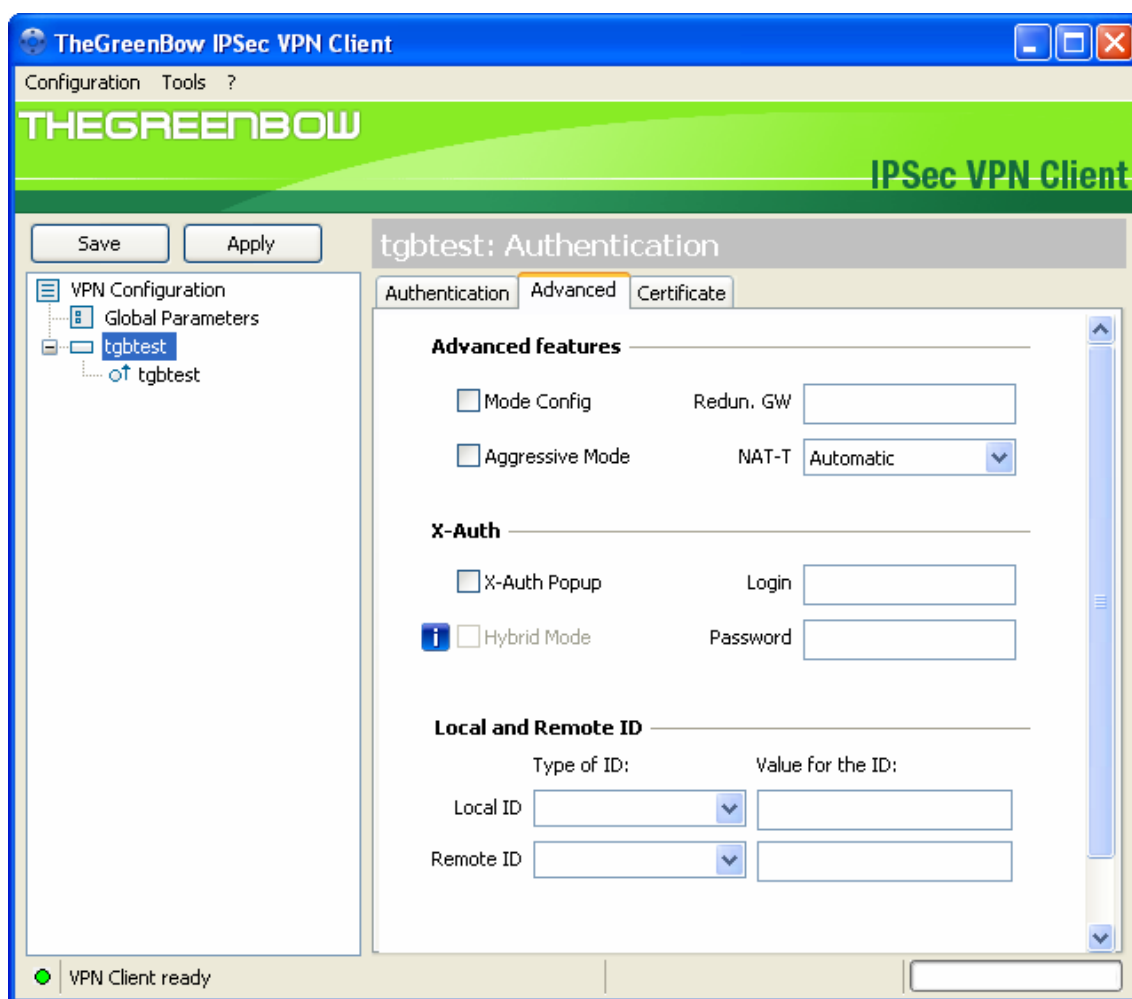


Figure 5-9

Config-Mode:	<p>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. If Config-Mode is enabled, and provided that the remote Gateway supports Config-Mode, the following parameters will be negotiated between the VPN Client and the remote Gateway during the IKE exchange (Phase 1):</p> <ul style="list-style-type: none"> • Virtual IP address of the VPN Client • DNS server address (optional) • WINS server address (optional) <p>In case Config-Mode is not available on the remote gateway, you may refer to section 'Phase2 Advanced' settings to manually set DNS and WINS server addresses into the IPSec VPN Client.</p>
Aggressive Mode:	<p>If checked, the VPN Client will used aggressive mode as negotiation mode with the remote gateway.</p>
Redundant GW:	<p>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).</p> <ul style="list-style-type: none"> • VPN Client will contact the primary gateway to establish a tunnel. If it fails after several tries (default is 5 tries, configurable in "Parameters" panel > "Retransmissions" field) the Redundant Gateway is used as the new tunnel endpoint. Delay between two retries is about 10 seconds. • In case primary gateway can be reached but tunnel establishment fails (e.g. VPN configuration problems) then the VPN Client won't try to establish tunnels with the redundant gateway. Configurations need modifications. • If a tunnel is successfully established to the primary gateway with DPD feature (i.e. Dead Peer Detection) negotiated on both sides, when the primary gateway stops responding (e.g. DPD detects non-responding remote gateways) the VPN Client immediately starts opening a new tunnel with the Redundant Gateway. • The exact same behavior will apply to the redundant gateway. This means that the VPN Client will try to open primary and redundant gateway until the user exits software or click on 'Save & Apply'.

NAT-T mode:	<p>The NAT-T mode allows Forced, Disabled and Automatic.</p> <p>The NAT-T "Disabled" prevents the [PRODUCTNAME] and the VPN gateway to start NAT-Traversal.</p> <p>The NAT-T "Automatic" mode leaves the VPN Gateway and VPN Client negotiate the NAT-Traversal.</p> <p>In NAT-T "Forced" mode [COMPANY] [PRODUCTNAME] will force NAT-T by encapsulating IPSec packets into UDP frames to solve traversal with intermediate NAT routers.</p>
Local ID:	<p>Local ID is the identity the VPN Client is sending during Phase 1 to VPN gateway. This identity can be:</p> <ul style="list-style-type: none"> • an IP address (type = IP address), for example: 195.100.205.101 • a domain name (type = DNS), e.g. mydomain.com • an email address (type = Email), e.g. [EMAILSUPPORT] • a string (type = KEY ID), e.g. 123456 • a certificate issuer (type=DER ASN1 DN) (see Certificates configuration) If this identity is not set, VPN Client's IP address is used.
Remote ID:	<p>Remote ID is the identity the VPN Client is expecting to receive during Phase 1 from the VPN gateway. This identity can be:</p> <ul style="list-style-type: none"> • an IP address (type = IP address), for example: 80.2.3.4 • a domain name (type = DNS), e.g. gateway.mydomain.com • an email address (type = Email), e.g. admin@mydomain.com • a string (type = KEY ID), e.g. 123456 • a certificate issuer (type=DER ASN1 DN) (see Certificates configuration) If this identity is not set, VPN gateway's IP address is used.
X-Auth:	<p>Define the login and password of an X-AuthIPSec negotiation. If "X-Auth Popup" is selected, a popup window asking for a login and a password will appear each time an authentication is required to open a tunnel with the remote gateway. For more details go to Using X-Auth section.</p> <p>If X-Auth authentication fails then the tunnel establishment will fail too.</p>

Hybrid Authentication Mode:	<p>The Hybrid mode is a specific authentication method used within IKE Phase 1. This method assumes an asymmetry between the authenticating entities. One entity, typically an Edge Device (e.g. firewall), authenticates using standard public key techniques (in signature mode), while the other entity, typically a remote User, authenticates using challenge response techniques. These authentication methods are used to establish, at the end of Phase 1, an IKE SA which is unidirectionally authenticated. To make this IKE bi-directionally authenticated, this Phase 1 is immediately followed by an X-Auth Exchange [XAUTH]. The X-Auth Exchange is used to authenticate the remote User. The use of these authentication methods is referred to as Hybrid Authentication mode. [COMPANY] [PRODUCTNAME] implements the RFC 'draft-ietf-ipsec-isakmp-hybrid-auth-05.txt'.</p>
------------------------------------	--

5.4 IPsec Configuration or Phase 2

5.4.1 What is Phase 2?

'IPsec Configuration' or 'Phase 2' window will concern settings for Phase 2.

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**.

5.4.2 Phase 2 Settings Description

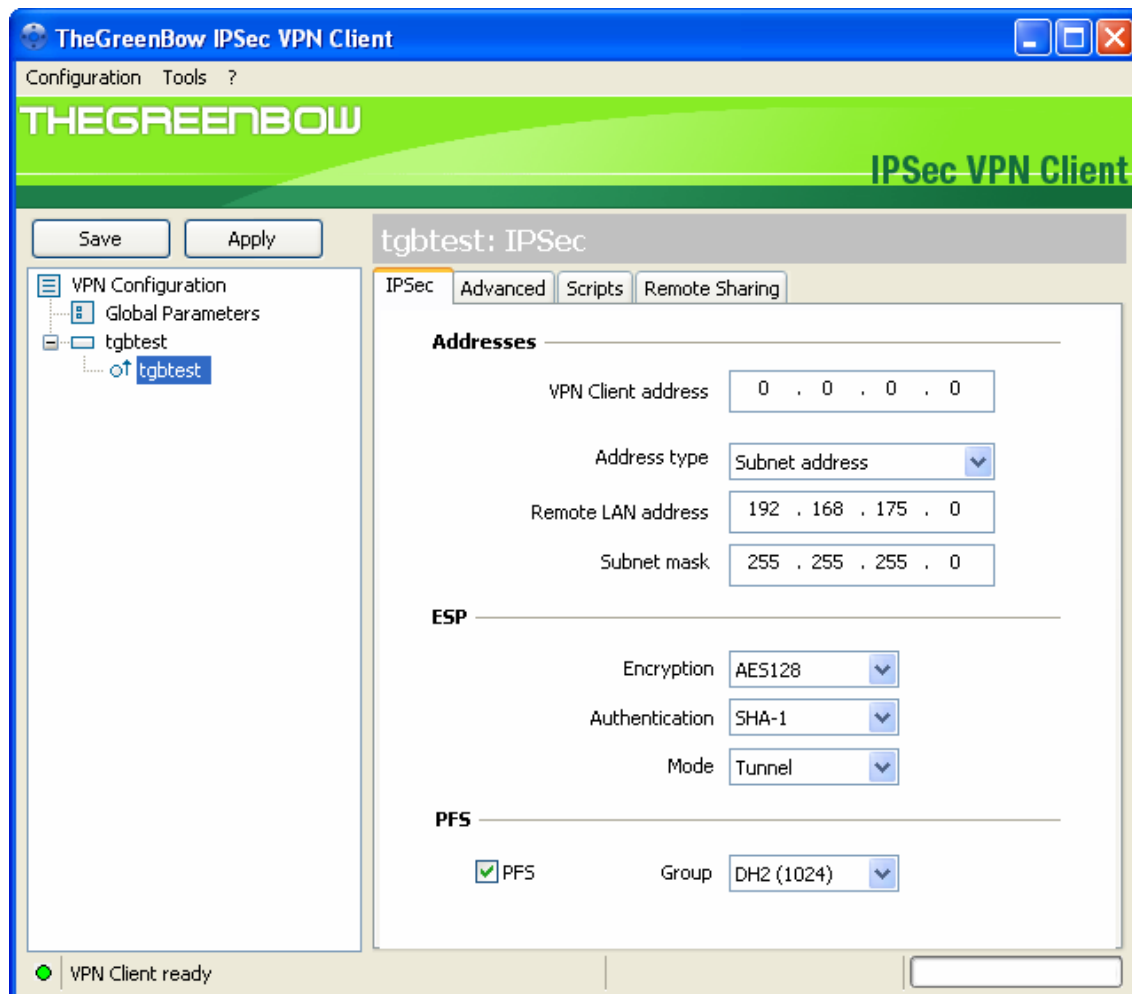


Figure 5-10

VPN Client address:	<p>Virtual IP address used by the VPN Client inside the remote LAN: your computer will appear in the remote LAN with this IP address.</p> <ul style="list-style-type: none"> • This address can be configured manually by entering an IP address here. • This address can be provided by the remote gateway if 'Mode-Config' has been selected in Phase 1. In that case the field is disabled and a bleu [i] icon appears to remind you. <p>This IP address can belong to the same remote LAN subnet (e.g., in the example, you have an IP address like 192.168.204.10). In this case, it is important to read the note below.</p>
Address type:	<p>The remote endpoint may be a LAN or a single computer,</p> <p>In case the remote endpoint is a LAN, choose "Subnet address" or "IP Range". When choosing "Subnet address", the two fields "Remote LAN address" and "Subnet mask" become available. When choosing "IP Range", the two fields "Start address" and "End address" become available, enabling the VPN Client to establish a tunnel only within a range of a predefined IP addresses. The range of IP addresses can be just one IP address.</p> <p>In case the remote end point is a single computer, choose "Single Address". When choosing "Single address", only the field "Remote host address" is available.</p>
Remote address:	<p>This field may be "Remote host address" or "Remote LAN address" depending of the address type. It is the remote IP address, or LAN network address of the gateway, that opens the VPN tunnel.</p>
Subnet mask:	<p>Subnet mask of the remote LAN. Only available when address type is equal to "Subnet address".</p>
ESP encryption:	<p>Encryption algorithm negotiated during IPSec phase (3DES, AES, ...)</p>
ESP authentication:	<p>Authentication algorithm negotiated during IPSec phase (MD5, SHA, ...). SHA1 and SHA2-256-bit are supported.</p>
ESP mode:	<p>IPSec encapsulation mode: tunnel or transport</p>
PFS group:	<p>Diffie-Hellman key length if selected.</p>



Note:

It is possible to have both local IP address of your computer and remote LAN as part of the same subnet. To be able to do so, you must select "Auto open this tunnel on traffic detection" ('P2 Advanced'). Once the VPN tunnel opened in this configuration, all the traffic with remote LAN is allowed but communication with local network becomes impossible.

For more advanced settings, click on **Advanced** tab.

Once the parameters are set, 'Apply' to take into account the new configuration. That way the IKE service will run with the new parameters. Click on 'Save' to save it into the configuration file for future use.

You'll find a set of useful VPN Client configuration documents available for each of the VPN gateway we support. Please go to our [knowledge base](#) on our website.

5.4.3 Phase2 Advanced Settings Description

For advanced features & parameters, click on 'Advanced' tab into Phase2 panel.

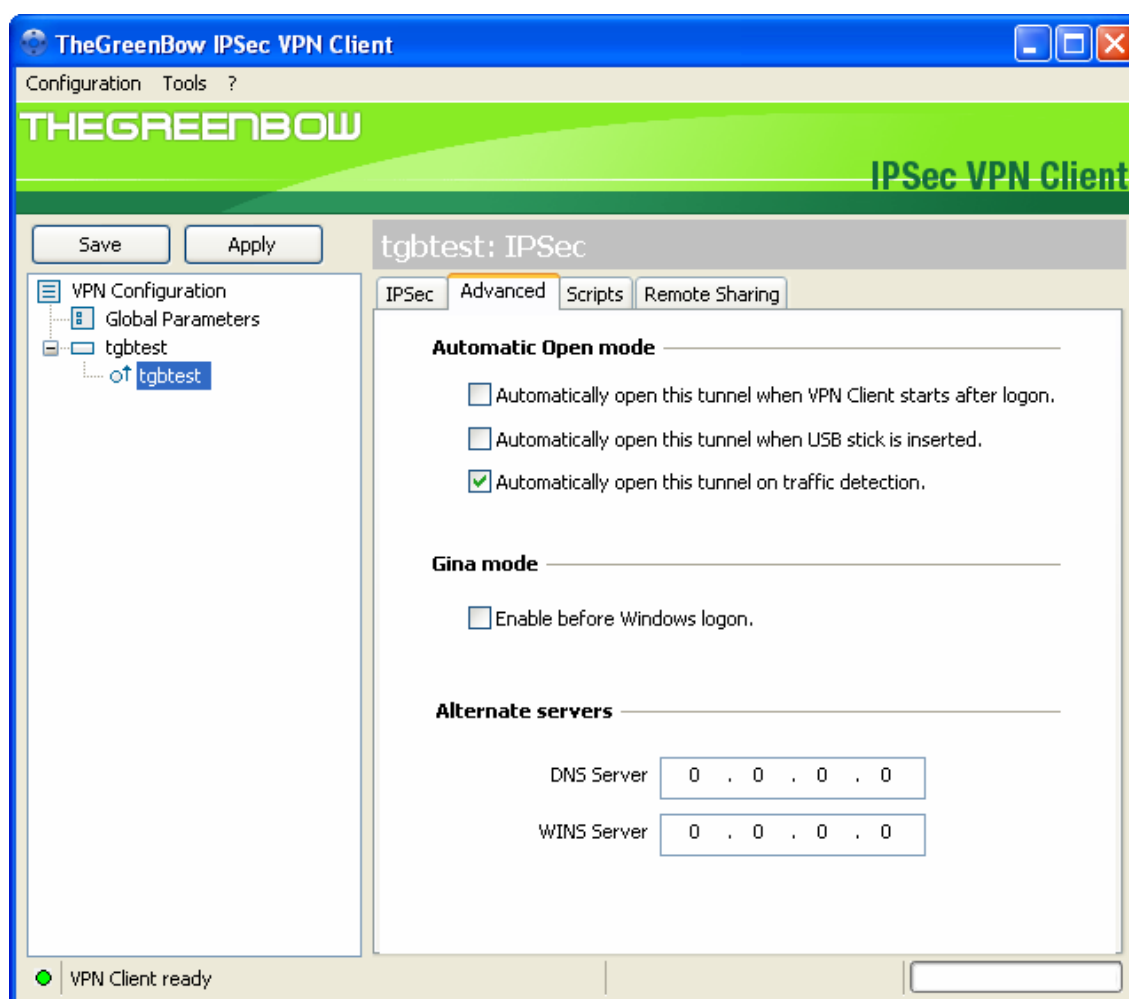


Figure 5-11

Automatic Mode:	<p>The VPN Client can automatically open the specified tunnel (Phase2) on specific events such as:</p> <ul style="list-style-type: none"> • Auto open this tunnel when the VPN Client starts up. • Auto open this tunnel when USB Drive is plugged in (see section "USB Mode"). • Auto open this tunnel when the VPN Client detect traffic towards remote LAN.
Gina Mode:	<p>If Gina Mode selected, this tunnel can be used by Vista Credential Providers (aka GINA on W2K/WXP) to process Windows logon. This is useful when using a corporate employee Dbase for logon and the remote computer need to connect to the corporate network before processing the Windows logon.</p>
Alternate Servers:	<p>DNS and WINS server IP addresses of the remote LAN that help users to resolve intranet addressing.</p> <ul style="list-style-type: none"> • Those addresses can be configured manually by entering an IP addresses here. • Those addresses can be provided by the remote gateway if 'Mode-Config' has been selected in Phase 1. In that case the field is disabled and a blue [i] icon appears to remind you. <p>The DNS or WINS addresses are taken into account as soon as the tunnel is opened, and as long as it is opened.</p>

5.4.4 Script configuration

Scripts may be configured in the 'Scripts' tab. This tab can be found in **Phase 2 Settings** panel.

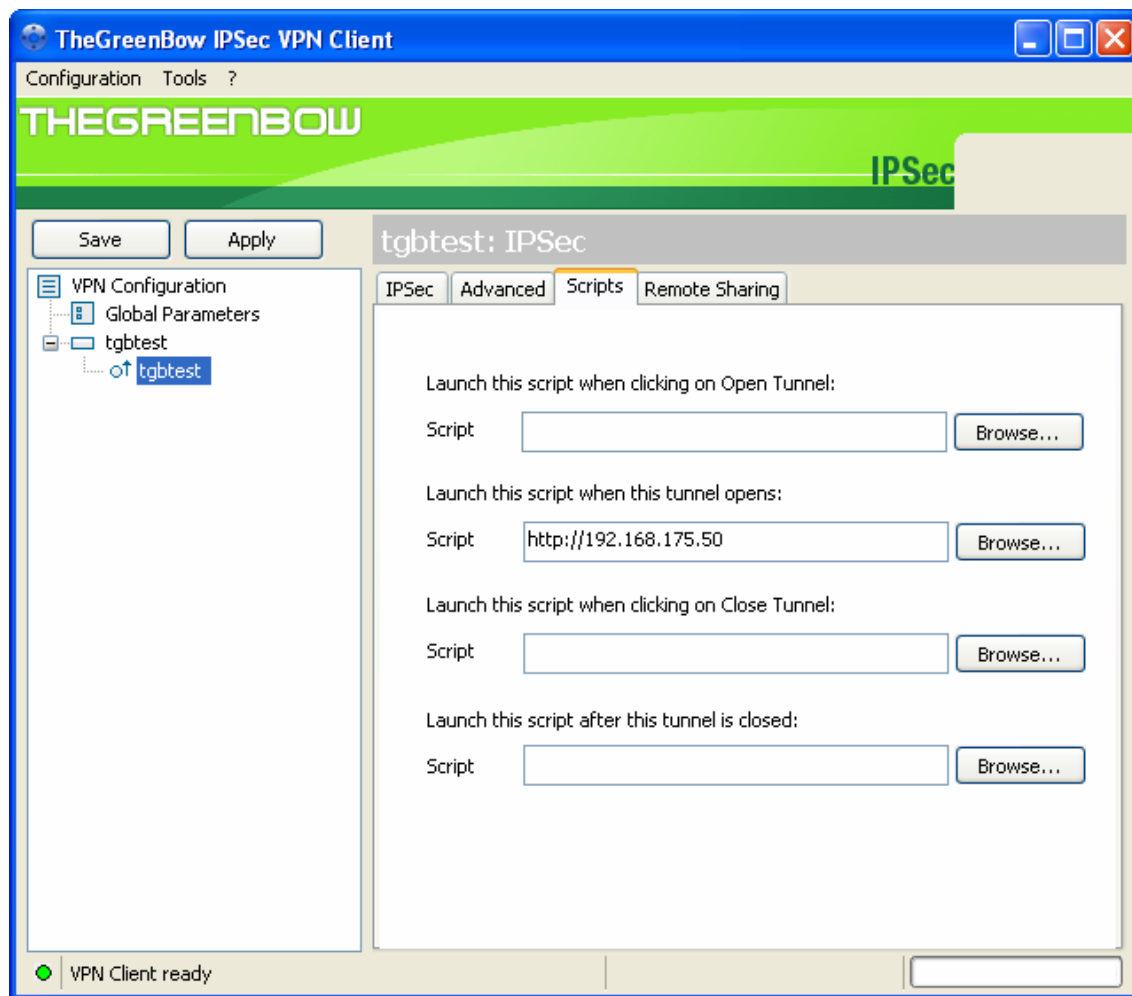


Figure 5-12

Scripts or applications can be enabled for each step of a VPN tunnel opening and closing process:

- Before tunnel is opened
- Right after the tunnel is opened
- Before tunnel closes
- Right after tunnel is closed

This feature enables to execute scripts (batches, scripts, applications...) at each step of a tunnel connection for a variety of purposes e.g. to check current software release, to check database availability before launching backup application, to check a software is running, a logon is set... .

It also enables to configure various network configurations before, during and after tunnel connections.

5.4.5 Remote Desktop Sharing

Multiple Remote Desktop Sharing sessions may be configured in the 'Remote Sharing' tab. This tab can be found in Phase 2 Settings panel.

This feature enables a user to share his machine on the corporate network from a remote location like home. When the user click on one of the Remote Desktop Sharing session, the associated VPN tunnel automatically opened, and an RDP session is launched to reached the remote machine.



Note:

Only Windows RDP session is supported.

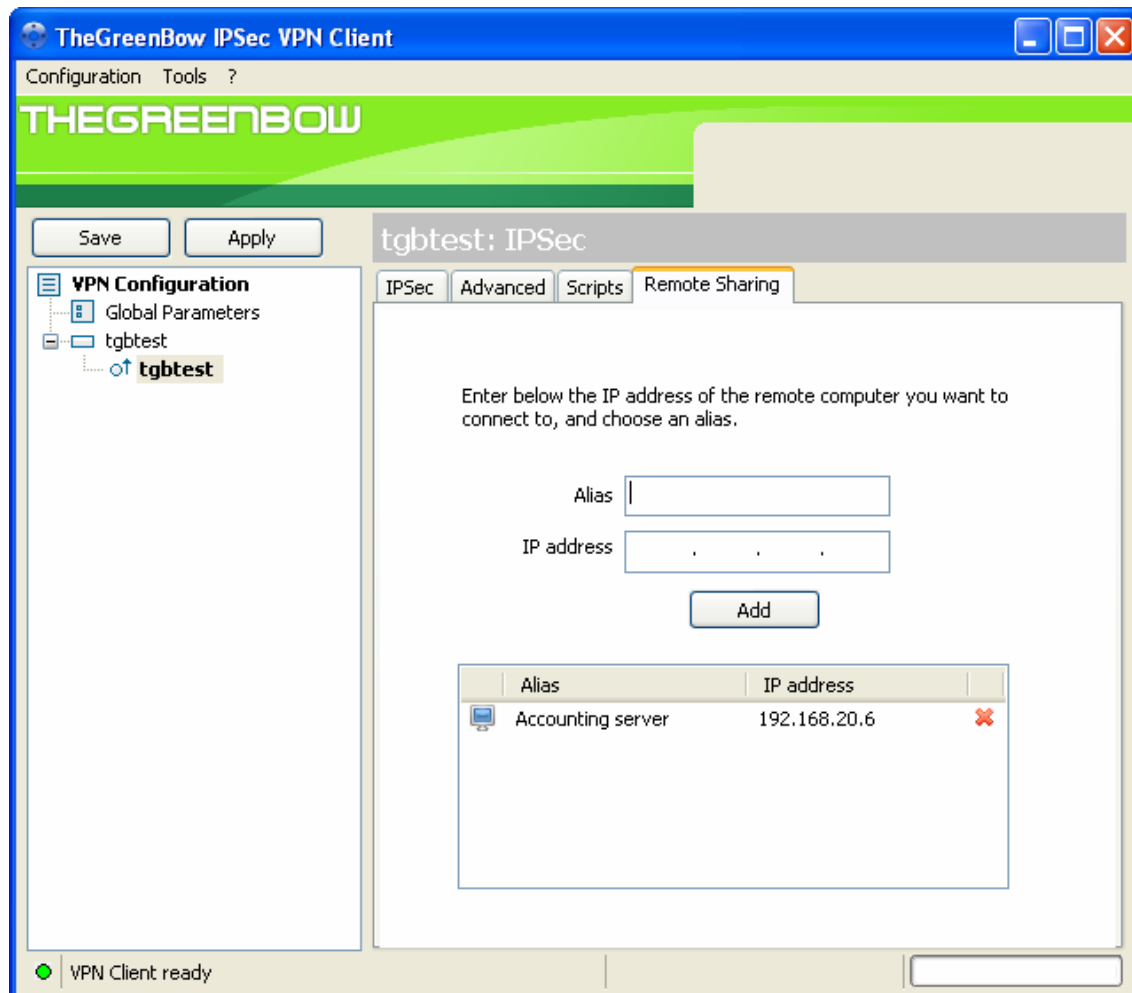


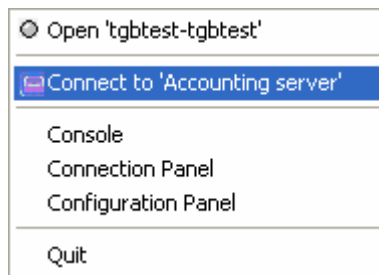
Figure 5-13

To add a new Remote Desktop Sharing session, proceed as follow:

1. Enter an alias for your remote desktop session
2. Enter an IP address of the machine your are trying to reach
3. Click 'Add'

To open one of the Remote Desktop Sharing session:

1. Click on any of the alias you have created in the Configuration Panel
2. Click on any of the alias in the systray menu



5.5 Global Parameters

5.5.1 Global Settings Description

Global Parameters are generic settings that apply to all created VPN tunnels. Once modified, click on <Save> or <Apply> to take into account your modifications.

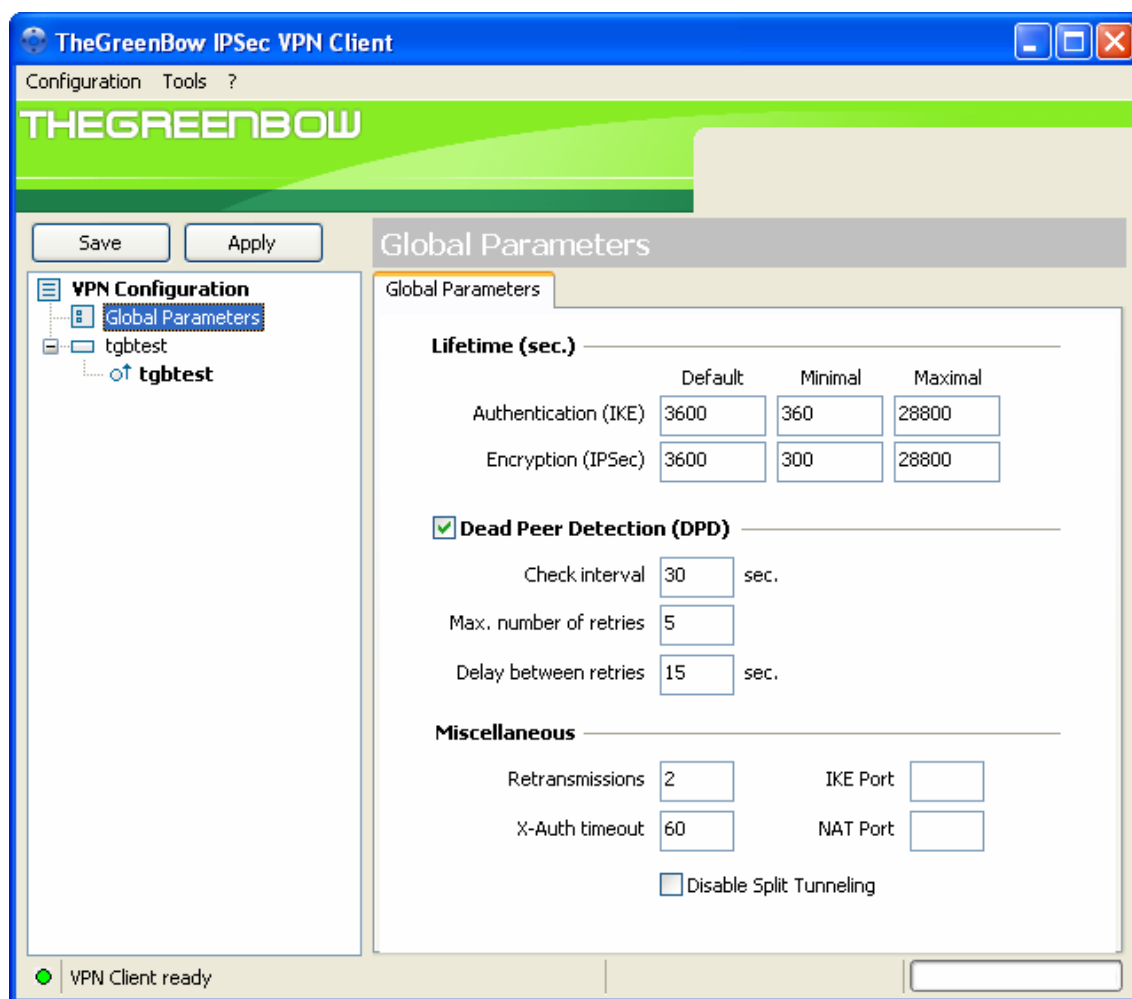


Figure 5-14

Lifetime (sec.)	IKE default lifetime	Default lifetime for IKE rekeying.
	IKE minimal lifetime	Minimal lifetime for IKE rekeying.
	IKE maximal lifetime	Maximal lifetime for IKE rekeying.

	IPSec minimal lifetime	Default lifetime for IPSec rekeying.
	IPSec maximal lifetime	Maximal lifetime for IPSec rekeying.
	IPSec minimal lifetime	Minimal lifetime for IPSec rekeying.
Dead Peer Detection (DPD)	Check interval (sec.)	Interval between DPD messages.
	Max number of retries	Number of DPD messages sent.
	Delay between retries (sec.)	Interval between DPD messages when no reply from remote gateway.
Miscellaneous	Retransmissions	How many times a message should be retransmitted before giving up.
	IKE Port	UDP port 500 is the port used by default during Phase1 IKE negotiation. User can change port number for IKE negotiation. Exchanges are still on UDP but they can be on another port than port 500 as some firewalls do not allow IKE Port 500 or outgoing traffic on Port 500 might not be allowed in some places. The remote gateway must support this feature and reroute the incoming traffic associated with the new selected IKE ports onto the default UDP 500 so that it is properly routed to the IPSec service.
	NAT Port	UDP port 4500 is the port used by default during Phase2 IPSec negotiation. User can change port number for IPsec negotiation. Exchanges are still on UDP but they can be on another port than port 4500 as some firewalls do not allow IPsec Port 4500 or outgoing traffic on Port 4500 might not be allowed in some places. The remote gateway must support this feature and reroute the incoming traffic associated with the new selected IPSec port onto the default UDP 4500 so that it is properly routed to the IPSec service.
	X-Auth timeout	Time allowed to the user to enter X-Auth credentials.
Disable Split Tunneling		When this option is checked, only encrypted traffic is authorized therefore all traffic goes through VPN tunnels once opened.

Dead Peer Detection (i.e. DPD) is an Internet Key Exchange (IKE) extension (i.e. RFC3706) for detecting a dead IKE peer. The Greenbow IPsec VPN Client is using DPD:

- to delete opened SA in the VPN Client when peer has been detected dead.
- to re-start IKE negotiations with the Redundant Gateway if activated in the **Phase1 Advanced** Configuration Panel.

Once the parameters are set, 'Apply' to take into account the new configuration. That way the IKE service will run with the new parameters. Click on 'Save' to save it into the configuration file for future use.

5.6 USB Mode

5.6.1 What is USB Mode?

The Greenbow VPN Client brings the capability to secure VPN configurations and VPN security elements (e.g. PreShared key, Certificates, ...) onto an USB Drive and out of the computer. This gives users the ability to attach a VPN Configuration:

- to a specific computer: therefore the VPN tunnels defined in the VPN configuration can only be used on that specific computer, or,
- to a specific USB drive: therefore the VPN tunnels defined in the VPN configuration can only be used with specific USB Drive.

When you select 'Configuration' > 'Move to USB Drive..', the VPN configuration and security elements contained into the configuration are moved onto the USB Drive the first time you plug it in.

Once done, you just need to plug in the USB Drive to automatically open tunnels. And you just need to unplug the USB Drive to automatically close all opened tunnels.

5.6.2 How to enable a new USB Drive?

A new USB Drive (no data) is enabled by copying VPN configuration and security elements onto it. There are several ways to do that:

- Export VPN Configuration via menu 'Configuration' > 'Export' and then copy the VPN Configuration file onto the USB Drive.
- Use the 'USB Mode Wizard' via menu 'Configuration' > 'Move to USB Drive..'.

Here is how the 'USB Mode Wizard' works.

1. The 'USB Mode Wizard' starts with 'USB Mode Wizard' step1.

In case an USB drive is already plugged in, the [PRODUCTNAME] will detect it as shown below. Potentially, the Wizard will ask to select one USB Drive, because several USB Drives could be plugged in at the same time:



Figure 5-15



Note:

- If an USB Drive is plugged in while in 'USB Mode Wizard' step1 and it appears to be the only one, the VPN Client will also detect it and jump to 'USB Mode Wizard' step2.
- If an USB Drive containing a VPN Configuration is plugged-in while a first USB drive with another VPN Configuration is already plugged-in, a warning message asks the user to unplug one of them before continuing.

2. 'USB Mode Wizard' step2

The wizard proposes to enable the USB Drive through the following options:

- 'With this computer only': therefore the VPN tunnels defined in the VPN configuration can only be used on this specific computer
- 'On any computer': therefore the VPN tunnels defined in the VPN configuration can be used with specific USB Drive only, on any computer.

The VPN Configuration can be protected (not mandatory) by a password so that the USB Drive would be lost without compromising company security.

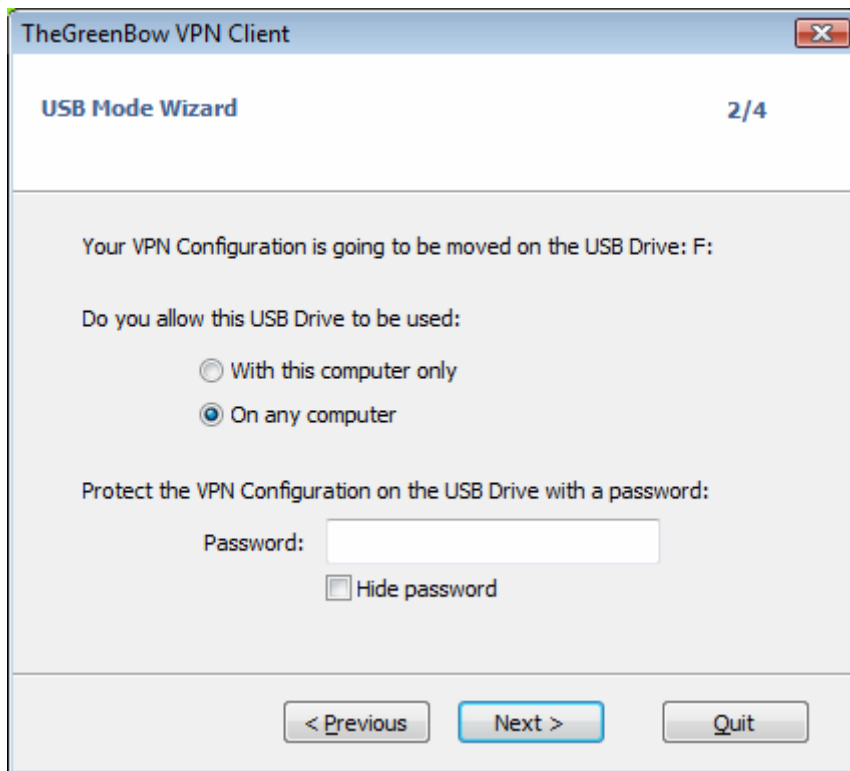


Figure 5-16



Note:

- At this step, if the USB Drive is unplugged, the wizard will automatically go back to step1.
- The VPN Client software doesn't enable to change the password or the computer association with the USB Drive. Nevertheless, it is always possible to plug the USB Drive containing the VPN Configuration, [export the VPN Configuration](#) to a local disk, unplug the USB Drive, [import the VPN Configuration](#), and start the 'USB Mode Wizard' all over again to set new password or new association with computer.

3. 'USB Mode Wizard' step3

Then the wizard proposes to selected the VPN tunnels that need to be opened next time the USB Drive is plugged in. The same 'Phase2 Advanced settings' option 'Auto open this tunnel when USB Drive is plugged in' is used here for every tunnel.

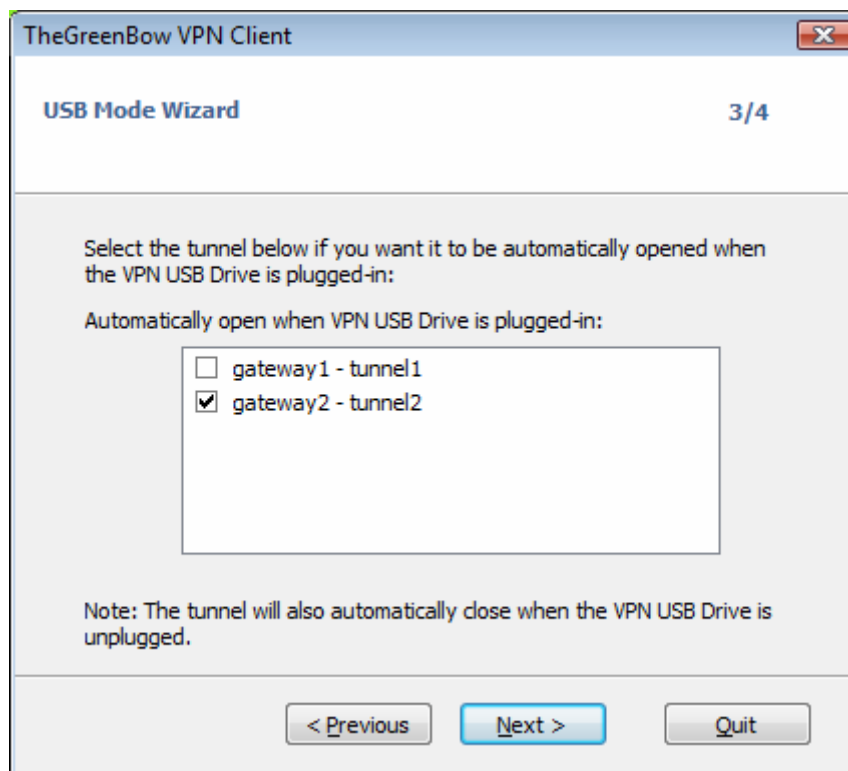


Figure 5-17

4. 'USB Mode Wizard' step4

Step4 is a summary of previous settings. Upon confirmation, the [PRODUCTNAME] will copy the VPN Configuration onto the USB Drive and remove all security information from the computer and the VPN Client is considered in 'USB Mode'.

Note: Once moved to the USB Drive, the VPN Configuration is kept as long as the USB Drive is plugged-in. As soon as the USB Drive is unplugged, the VPN Configuration is reset (an empty configuration is shown in the 'Configuration Panel'). Next time the VPN Client starts, the VPN Configuration will be empty.

5.6.3 How to automatically open tunnels when an USB Drive is plugged in?

Each and every tunnels may be configured individually using the option 'Auto open tunnels when USB Drive is plugged in'.

If an USB Drive containing a VPN Configuration is plugged in, all VPN tunnels set with this feature will open automatically. They will close when the USB Drive is un-plugged. Same behavior if the USB Drive is already plugged-in when the VPN Client starts.

In this case, a little bleu icon like an USB drive appears in the VPN Configuration tree.

Obviously, if a USB Drive without any VPN Configuration is plugged-in or if no USB Drive is plugged in, the VPN Client starts in local mode (using whatever VPN Configuration available on local disk).

This option can be configured in the 'Configuration Panel':

- IPsec Configuration (Phase 2) of the relevant tunnel, click on <Advanced> tab,
- Select the 'Automatically open this tunnel when USB Drive is inserted' option.

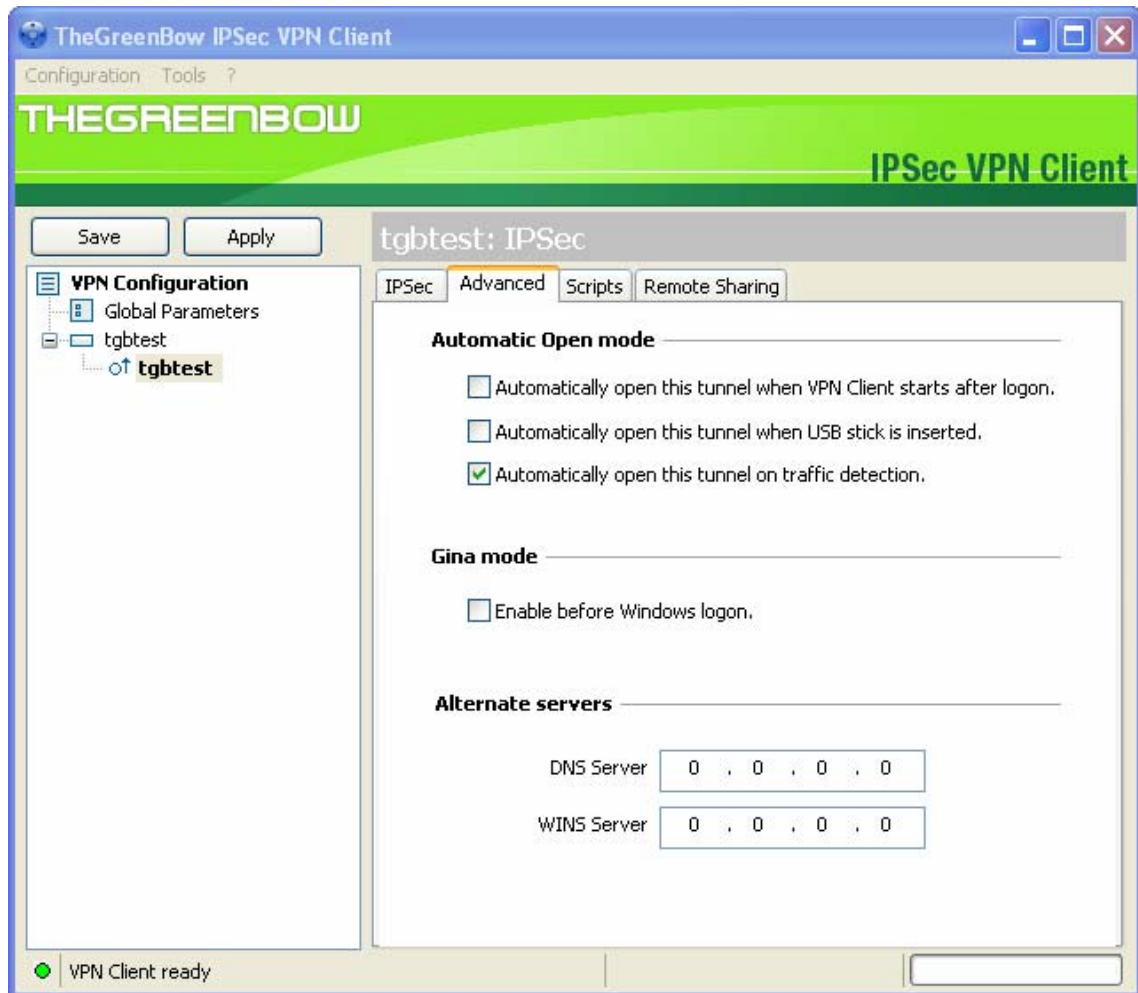


Figure 5-18

See also **USB Mode Wizard** and [How to enable a new USB Drive?](#) via menu 'Configuration' > 'Move to USB Drive..'



Note:

The option 'Automatically open this tunnel when USB Drive is inserted' is disabled before Windows logon.

5.7 Configuration Management

5.7.1 Import or Export VPN Configuration via menu

The Greenbow VPN Client can import or export a VPN Configuration. With this feature, IT managers can prepare a configuration and deliver it to other users.

- Importing a configuration, select menu 'Configuration' > 'Import'.
- Exporting a configuration, select menu 'Configuration' > 'Export'.

An exported VPN configuration file will have a ".tgb" extension.

Exported VPN Configuration can be protected by a password. When the user wants to export a configuration, a window automatically asks if the exported VPN configuration must be protected with a password or not.

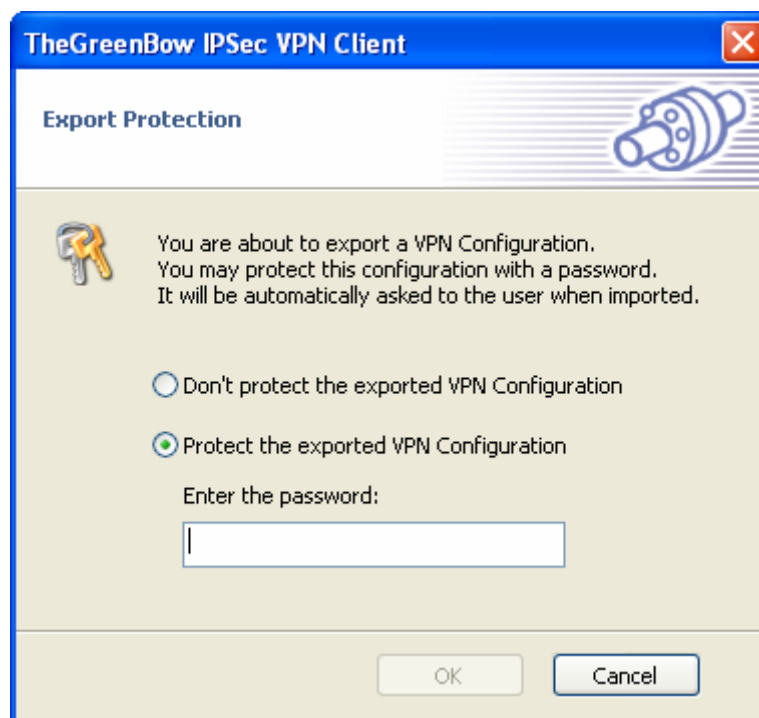


Figure 5-19

When a VPN Configuration is protected with a password, its importation will automatically ask the user to enter the password. An exported VPN Configuration which is not protected with a password will be automatically imported without any request to the user.

**Note:**

- When the VPN Client is configured in "USB Mode" and when a USB Drive is plugged in, the importation of a VPN Configuration is directly written on the USB Drive. If the VPN Client is configured in "USB mode" but no USB Drive is plugged in, the exportation and importation of a VPN Configuration are disabled.
- A VPN Configuration file can also be imported via the [command line](#).

5.7.2 Merge of VPN Configurations

The Greenbow can import one or several tunnels into an existing VPN Configuration. With this feature, IT managers can merge a new VPN Configuration with new gateways into an existing VPN Configuration and deliver it to users or group of users.

Merge of VPN Configurations can be done in several ways.

1. Import new VPN Configuration via menu 'Configuration' > 'Import' and then select 'Add' instead of 'Replace'.

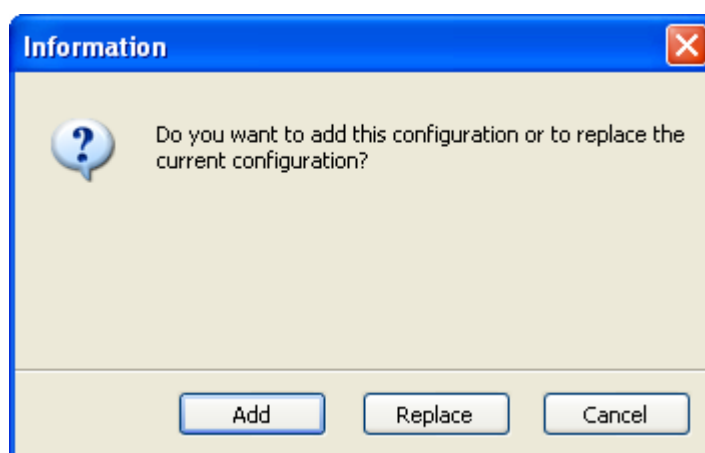


Figure 5-20

2. Drag&drop a new VPN Configuration into the software with an existing VPN Configuration already opened. The exact same popup window (see above) will appear asking if the user wants to 'Add' or 'Replace' existing VPN Configuration.
3. Import new VPN Configuration via command line.

`"[path]\vpnconf.exe /add:[file.tgb] "` where `[path]` is the VPN Client installation directory, and `[file.tgb]` is the VPN Configuration file. This command doesn't handle relative paths (e.g. `"..\..\file.tgb"`).

Anyway you choose to import VPN Configuration, here are common behaviors:

- Global parameters are not imported in case at least one tunnel was already configured prior to import and user selects 'Add' VPN Configuration in the popup.

- Global parameters are imported in case the user selects 'Replace' or no tunnel was configured prior to import.
- Tunnel name conflict between existing and imported VPN Configurations are solved by software automatically by adding an increment between bracket e.g. tunnel_office(1) to the imported tunnel names (i.e. both Phase1 and Phase 2).

5.7.3 Split of VPN Configuration

The VPN Client can export one tunnel from an existing VPN Configuration. With this feature, IT managers can split existing VPN Configuration into smaller VPN Configuration and deliver it to users or group of users.

To export a single tunnel, you must follow the following steps:

1. Right click on any tunnel Phase 2 from your VPN Configuration, and then select 'Export'

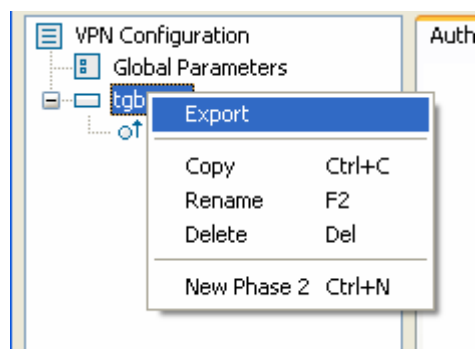


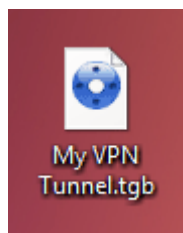
Figure 5-21

2. A popup windows appears to ask for VPN Configuration password protection.



Figure 5-22

3. Once exported, the VPN Configuration can be sent to users or you can double click on it to start the VPN Client.



Note:

- Export of a Phase 2 will export the associated Phase 1 as well. This means also export of Certificates that might have been defined in this Phase 1. A VPN Configuration file can also be imported via the command line.
- Export of a Phase 2 will export the Global Parameters as well.

5.7.4 Embed your own VPN Configuration into VPN Client Setup

A (pre-created) VPN Configuration may be enclosed into the VPN Client Setup. Enclosing VPN Configuration within the VPN Client Setup enables IT Manager to deploy pre-configured [PRODUCTNAME] software in a single package to all company users.

5.7.5 Demo VPN Configuration

The VPN Client Setup embeds a Demo VPN Configuration. This Demo VPN Configuration enables to open a tunnel to our Greenbow Demo Server as soon as the VPN Client software is installed.

It is particularly useful to check if a tunnel can be opened from my computer to an operational remote network for test – and eventually for debug – purpose.

Chapter 6 VPN Client Software Setup and Deployment

The VPN Client is designed to be easily deployed and managed. It implements several features that enable an administrator to preconfigure the VPN Client software setup before deployment, to remotely install or upgrade the VPN Client, and to centrally manage VPN configurations.

6.1 Embedded VPN Configuration

An unzipped VPN configuration .tgb file is embedded within the VPN Client software setup and is automatically imported by the VPN Client during its installation.

The process to create a setup with a VPN Configuration is the following:

1. Create the VPN Configuration that need to be embedded into the Setup. This step must be processed from a formerly installed [PRODUCTNAME], from which the VPN Configuration is exported (e.g. "myconfig.tgb").
2. Create a silent installation, or simply unzip the [PRODUCTNAME] Setup.
3. Add the VPN Configuration (e.g. "myconfig.tgb") file into the unzipped setup directory.
4. Deploy the package to the user (the VPN Configuration will be used during the setup)

Important note: the Setup cannot import and use an encrypted (protected) VPN Configuration. When creating your VPN Configuration make sure it is exported without being encrypted (without being protected with a password).

6.2 Setup options

6.2.1 Setup option overview

Several options are available with the VPN Client Setup.

1. Configuration of the **GUI mode**: *'full'*, *'user'* or *'hidden'*.
2. Protection of the **GUI mode Access Control** with a password.
3. Configuration of the **Systray menu** items.
4. Other options for **Software Start**, **License Number**, **Auto Software Activation**, **no trial windows**, **languages** and **Activation email**.

Syntax example:

```
Setup.exe /S --license=0123456789ABCDEF0123 --start=1  
--activmail=smith@smith.com
```

Warning: all the switches '--guidefs', '--menuitem', '--license', '--start', '--activmail', '--password', '--autoactiv', '--noactiv', '--lang' can only be used with the switch '/S' (silent mode install, case sensitive).

6.2.2 Setup option for GUI mode

Syntax: `--guidefs=full|user|hidden`

enables to define the GUI appearance when the VPN Client starts.

"**full**": [Default] The Configuration Panel is displayed.

"**user**": The Connection Panel is displayed.

"**hidden**": Both VPN Configuration Panel and Connection Panel are not displayed. Only the systray menu can be opened. Tunnels can be opened from the systray menu.

Here is an example using `--guidefs=hidden`

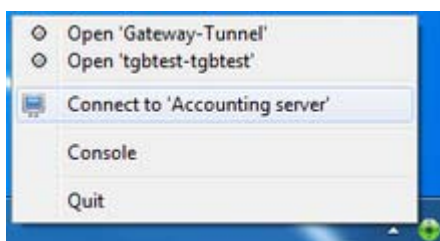


Figure 6-1

6.2.3 Setup option for GUI mode access control

Syntax: `--password=mypwd`

Enables to control the access to the **Configuration Panel** with a password. See 3.5.4.1 Access Control & Hidden Interface for more info.

The user will be asked for the password:

- When the user clicks or double-clicks on the VPN systray icon
- When the user wants to switch from the Connection Panel to the Configuration Panel.



Figure 6-2

Example: `--guidefs=user --password=admin01`

These 2 options enable the VPN Client to be locked in "Connection Panel" mode only, while the access to the Configuration Panel is protected with a password.

6.2.4 Setup option for systray menu items

Syntax: `--menuitem=[0...31]`

Enables to specify the items of the systray menu that the IT manager wants to keep.

The value is a 'bitfield': 1 = Quit, 2 = Connection panel, 4 = Console, 8 = Save&Apply, 16 = Configuration panel, Default is 31: All menus.

Example: `--menuitem=5` will configure a systray menu with the items: Quit + Console.



Note:

- the tunnels are always shown in the systray menu, and can always be opened and closed from this systray menu.
- 'menuitem' and 'guidefs=hidden'. By default, `guidefs=hidden` set the systray menu item list to Quit + Console. (The items 'Save&Apply' and 'Connection Panel' are not visible). However the use of 'menuitem' overrides 'guidefs'. That means the following: "`--guidefs=hidden --menuitem=1`" will set a systray menu with only the 'Quit' item.

6.2.5 Other Setup options

Here are the other installation parameters for the setup command line:

Syntax: `/s` ("S" must be preceded by only 1 slash, case sensitive)

Usage: Enables a silent installation (no dialog are displayed to the user during the installation)

Example: "TheGreenBow_VPN_Client.exe /S"

Syntax: `/D=[install path]` ("D" must be preceded by only 1 slash, case sensitive)

Usage: [install path] is the path where to install the software. No quotation marks even if space in the path.

Warning: This options must be used with the option `/S` (silent mode) and must be placed at the end of the command line, as the last option if any others.

Syntax: `--license=[license_number]`

Allows to configure the license number. The License Number is a set of 24 hexadecimal characters. Old License Numbers might be 20 hexadecimal characters.

Syntax: `--start=[1|2]`

Allows to configure the start mode for the VPN Client: after the logon windows [1] or manually [2]. Default is [1].

Syntax: `--reboot=[1]`

Allows to reboot automatically after silent installation. Default is [1].

Syntax: `--activemail=[activation_email]`

Allows to force the email used for activation confirmation. During the activation process, the edit box used for entering this email will be disabled

Syntax: `--autoactiv=1`

In case of software upgrade (i.e. license number and activation email have already been entered in previous installation) and `--autoactiv=1` option is added, the software will try to activate software automatically when starting if network is available or when requesting to open a tunnel if network was not available at startup.

Syntax: `--noactiv=1`

No display of the 'Trial window' once software started until trial period ends. User doesn't know he is in trial period and software will be disabled at the end of trial period. It means that if the user tries to launch the software after the end of trial period, the software will start and open the 'Trial window' but the 'Evaluate' button will be disabled.

Syntax: `--lang=[language code]`

This option specifies the language for the [COMPANY] [PRODUCTNAME] software and installation software. Available languages are listed below.

ISO 639-2 code	Language code	English name
EN	1033 (default)	English
FR	1036	French
ES	1034	Spanish
PT	2070	Portuguese
DE	1031	German
NL	1043	Dutch
IT	1040	Italian
ZH	2052	Chinese simplified
SL	1060	Slovenian
TR	1055	Turkish
PL	1045	Polish
EL	1032	Greek
RU	1049	Russian
JA	1041	Japanese
FI	1035	Finnish
SR	2074	Serbian
TH	1054	Thai
AR	1025	Arabic
HI	1081	Hindi
DK	1030	Danish
CZ	1029	Czech
HU	1038	Hungarian

NO	1044	Norwegian
FA	1065	Farsi

Example:

```
TheGreenBow_VPN_Client.exe /S --license=0123456789ABCDEF0123 --start=2
--activmail=smith@smith.com
```

6.3 Command line

6.3.1 Command line options

Several command lines are available, they are meant to be used by IT managers to adapt the VPN Client behavior to their needs and to help integration with other applications.

- Stopping VPN Client
- Importing or Exporting VPN Configuration
- Opening or Closing VPN tunnels

For more details..

- Please see the **Deployment Guide** on our website
- Best software implementation of command line (e.g. Remote Desktop Manager from devolutions.net,..) & video tutorial

6.3.2 Opening or closing VPN Tunnel options

The Greenbow VPN Client can open or close a VPN tunnel by the command line. Both command lines can be invoked while the Greenbow VPN Client is running:

" [path]\vpnconf.exe /open:[phase1-phase2] " where [path] is the VPN Client installation directory, and [phase1-phase2] are the Phase1 and the Phase2 names in the VPN Configuration file.

In case the specified tunnel is already open, this command line has no effect.

" [path]\vpnconf.exe /close:[phase1-phase2] " where [path] is the VPN Client installation directory, and [phase1-phase2] are the Phase1 and the Phase2 names in the VPN Configuration file.

In case the specified tunnel is already close, this command line has no effect.

Both arguments "open" and "close" are exclusives and cannot be used together.

Restriction note:

- Execution of those command lines will open the Software Graphical User Interface (GUI). This restriction will be removed in further software release.

6.3.3 Stopping IPsec VPN Client: option **"/stop"**

The Greenbow VPN Client can be stopped at any time by the command line:

`"[path]\vpnconf.exe /stop"` where `[path]` is the VPN Client installation directory.

If there is several active tunnels, they will close properly.

This feature can be used, for example, in a script that launch the VPN Client after establishing a dialup connection and exit it just before the disconnection.

6.3.4 Import or Export VPN Configuration options

The Greenbow VPN Client can import a specific configuration file by the command line:

`" [path]\vpnconf.exe /import:[file.tgb] "` where `[path]` is the VPN Client installation directory, and `[file.tgb]` is the VPN Configuration file. This command doesn't handle relative paths (e.g. `"..\file.tgb"`). Double-quotes are supported allowing paths containing spaces.

`" /import: "` may be used either if the VPN Client is running or not. When the VPN Client is already running, it imports dynamically the new configuration and automatically applies it (i-e: restarts the IKE service). If the VPN Client is not running, it is launched with the new configuration.

`" /importonce: "` enables to import a VPN configuration file without running the VPN Client. This command is especially useful in installation scripts: it allows to run a silent installation and to import a configuration automatically.

`" /export" /exportonce:"` enables to export the current VPN Configuration (including Certificates) in the specified file. This command doesn't start the VPN Client if it is not running already. Please note that `/pwd:` is mandatory.

`" /add:"` enables to import a new VPN Configuration into an existing VPN Configuration and merge both into a single VPN Configuration. This command line may be used either if the VPN Client is running or not. This command doesn't start the VPN Client if it is not running already.

`" /replace: "` enables to replace the current configuration by a new VPN Configuration. This feature is available in software release 4.1 and older, and may be used instead of the `/importonce` option to import a VPN configuration file without running the VPN Client.

`" /pwd:[password]"` enables to set a password for import operations. This option can be used together with the `/import`, `/importonce`, `/export`, `/exportonce`, `/add` and `/replace` options but it must be placed after one of those options.

All arguments `"import"`, `"importonce"`, `"export"`, `"exportonce"`, `"add"` and `"replace"` are exclusives and cannot be used together.

Chapter 7 Configuring the VPN Client with a TP-LINK VPN Router

This chapter describes how to configure the VPN Client with a TP-LINK router. This chapter includes the following sections: **Example VPN Network Topology**, **Configure the TP-LINK VPN Router**, **Configure the VPN Client**.

7.1 Example VPN Network Topology

In the VPN network example shown in the figure below, the VPN router functions as a gateway for a main office. The Windows PC VPN Client is installed on a remote laptop that runs Windows XP and that connects to the Internet. The Windows PC VPN Client connects to the VPN router and establishes a secure IPSec VPN connection with the router so the laptop user can gain access to the file server or any other resources at the main office.

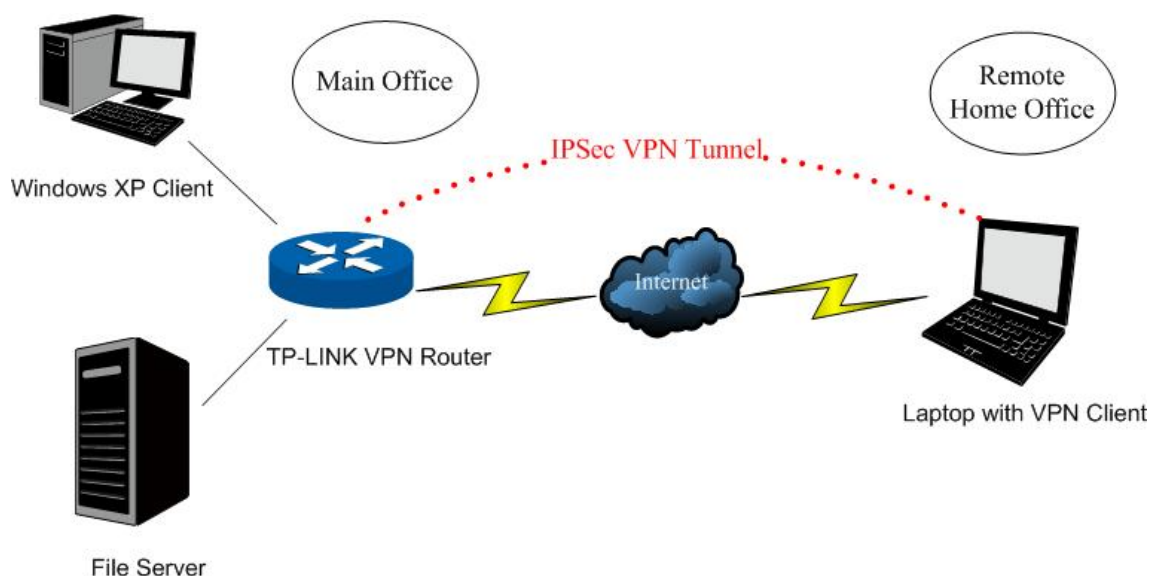


Figure 7-1

The following table shows the IP addresses that are used in the VPN network example shown in Figure 7-1.

Main Office	Remote Home Office
Main office router: WAN IP: 110.200.13.18 VPN Router IP address: 192.168.0.1 Subnet mask: 255.255.255.0	Home office router: Windows XP laptop with VPN Client: 116.31.85.133 Subnet mask: 255.255.255.0 Default gateway: 116.31.85.1

File server IP: 192.168.0.2 Subnet mask: 255.255.255.0 Default gateway: 192.168.0.1 Client IP: 192.168.0.3 Subnet mask: 255.255.255.0 Default gateway: 192.168.0.1	VPN Client settings: Pre-shared key:123456
---	--



Note:

All the addresses in this chapter are for example only. You can adjust the settings and configuration to suit your network.

7.2 Configuring the TP-LINK VPN Router

To configure a VPN connection between the VPN router and a client, access the router's Web management interface, create an IKE policy, and then create a VPN policy.

1) IKE Setting

To configure the IKE function, you should create an IKE Proposal firstly.

- **IKE Proposal**

Choose the menu **VPN→IKE→IKE Proposal** to load the configuration page.

Settings:

Proposal Name: proposal_IKE_1

Authentication: MD5

Encryption: 3DES

DH Group: DH2

Click the <Add> button to apply the setting.

IKE Proposal	
Proposal Name:	<input type="text" value="proposal_IKE_1"/>
Authentication:	<input type="text" value="MD5"/> ▼
Encryption:	<input type="text" value="3DES"/> ▼
DH Group:	<input type="text" value="DH2"/> ▼
<div>Add</div> <div>Clear</div> <div>Help</div>	

Figure 7-2

- **IKE Policy**

Choose the menu **VPN→IKE→IKE Policy** to load the configuration page.

Settings:

Policy Name:	IKE_1
Exchange Mode:	Main
IKE Proposal:	proposal_IKE_1 (you just created)
Pre-shared Key:	123456
SA Lifetime:	28800
DPD:	Disable

Click the <Add> button to apply.

IKE Policy

Policy Name:
Exchange Mode: ☒ Main ☐ Aggressive
Local ID Type: ☒ IP Address ☐ FQDN
Local ID:
Remote ID Type: ☒ IP Address ☐ FQDN
Remote ID:
IKE Proposal 1:
IKE Proposal 2:
IKE Proposal 3:
IKE Proposal 4:
Pre-shared Key:
SA Lifetime: Sec (60-604800)
DPD: ☐ Enable ☒ Disable
DPD Interval: Sec (1-300)

Add

Clear

Help

List of IKE Policy

No.	Name	Mode	Proposal 1	Proposal 2	Proposal 3	Proposal 4	Action
No entries.							

Select All

Delete

Search

Figure 7-3

2) IPsec Setting

To configure the IPsec function, you should create an IPsec Proposal firstly.

● IPsec Proposal

Choose the menu **VPN→IPsec→IPsec Proposal** to load the following page.

Settings:

Proposal Name: proposal_IPsec_1

Security Protocol: ESP

ESP Authentication: MD5

ESP Encryption: 3DES

Click the <Save> button to apply.

IPsec Proposal	
Proposal Name:	<input type="text" value="proposal_IPsec_1"/>
Security Protocol:	<input type="text" value="ESP"/> ▼
ESP Authentication:	<input type="text" value="MD5"/> ▼
ESP Encryption:	<input type="text" value="3DES"/> ▼

Figure 7-4

- **IPsec Policy**

Choose the menu **VPN→IPsec→IPsec Policy** to load the configuration page.

Settings:

IPsec:	Enable
Policy Name:	IPsec_1
Status:	Activate
Mode	Client-to-LAN
Local Subnet:	192.168.0.0/24
WAN:	WAN1
Remote Host:	116.31.85.133
Exchange Mode	IKE
IKE Policy:	IKE_1
IPsec Proposal:	proposal_IPsec_1 (you just created)
PFS:	NONE
SA Lifetime:	3600

Click the <Add> button to add the new entry to the list and click the <Save> button to apply.



Note:

It is suggested to set the Remote Host to be 0.0.0.0, which means there is no limit to the IP address of the remote host with VPN Client.

General

IPsec:

☒ Enable
 ☐ Disable

Save

IPsec Policy

Policy Name:

IPsec_1

Add

Mode:

Client-to-LAN

Clear

Local Subnet:

192.168.2.0 / 24

Help

Remote Subnet:

0.0.0.0 / 0

WAN:

WAN1

Remote Host:

116.31.85.133

Policy Mode:

☒ IKE
 ☐ Manual

IKE Policy:

IKE_1

IPsec Proposal 1:

proposal_IPsec_1

IPsec Proposal 2:

IPsec Proposal 3:

IPsec Proposal 4:

PFS:

NONE

SA Lifetime:

3600

Sec (120-604800)

Status:

☒ Activate
 ☐ Inactivate

List of IPsec Policy

No.	Name	Mode	Local Subnet	Remote Subnet	Policy Mode	Status	Action
No entries.							

Select All

Activate

Inactivate

Delete

Search

Figure 7-5

7.3 Configuring the VPN Client

The VPN Client lets you to set up the VPN connection manually or with the integrated Configuration Wizard, which is the easier and preferred method. The Configuration Wizard uses the default settings and provides basic interoperability so that the VPN Client can easily communicate with TP-LINK or third-party VPN devices. However, the Configuration Wizard does not let you enter the local and remote IDs, so you must manually enter this information.

7.3.1 Use the Configuration Wizard to Configure the VPN Client

1. Access the VPN Client's user interface, and select VPN Configuration > Wizard from the main menu on the Configuration Panel screen. The VPN Client Configuration Wizard Step 1 of 3 screen displays.

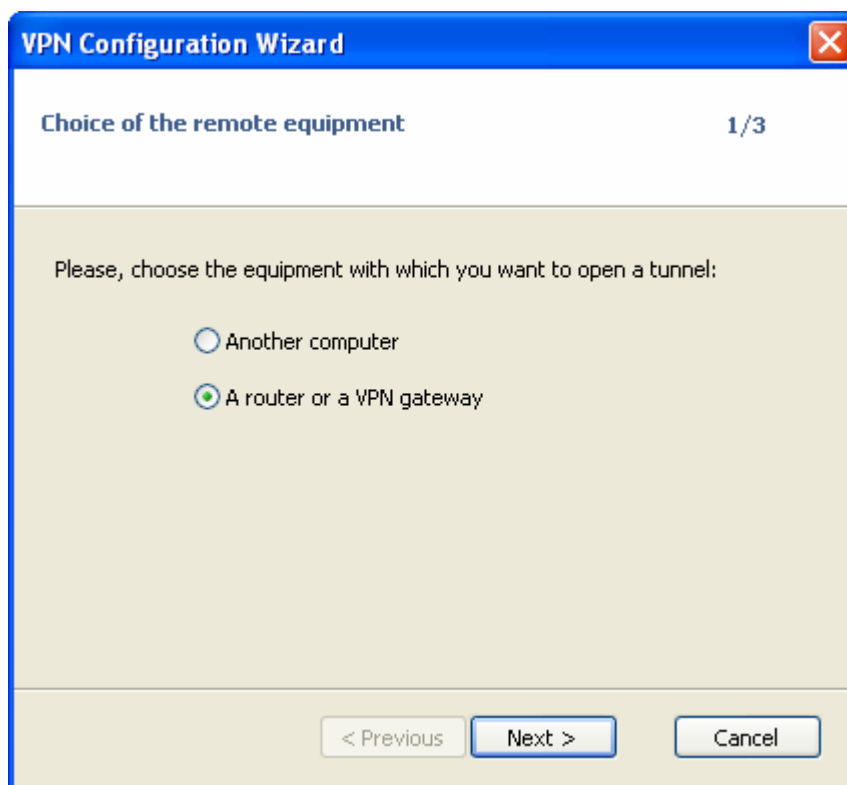


Figure 7-6

2. Select the **A router or a VPN gateway** radio button, and click Next. The VPN Client Configuration Wizard Step 2 of 3 screen displays.

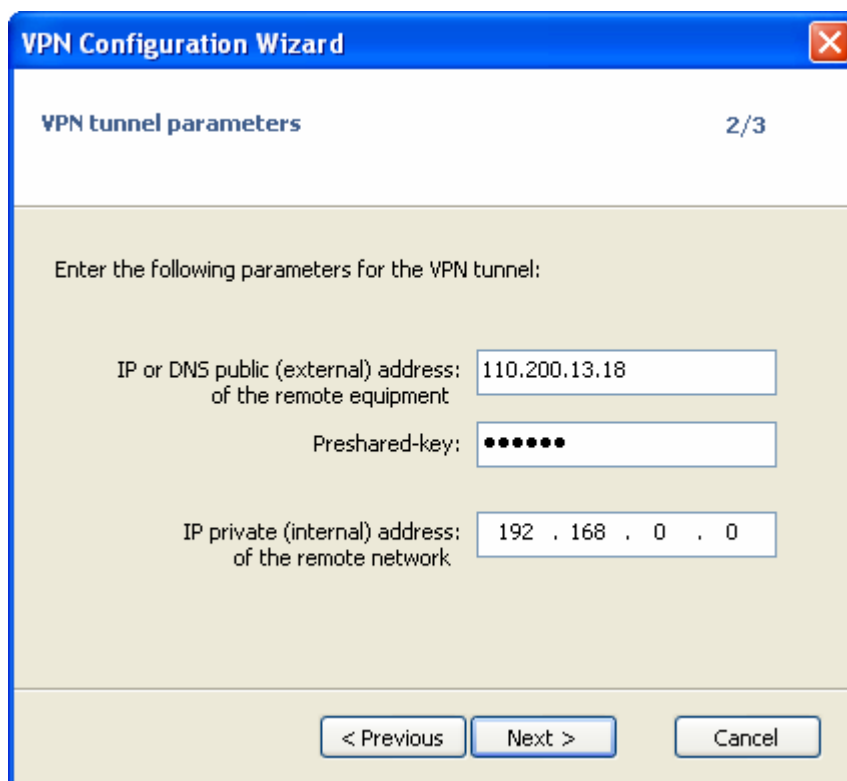


Figure 7-7

3. Specify the following VPN tunnel parameters:

IP or DNS public (external) address of the remote equipment: Enter the remote IP address or DNS name of the VPN router: 110.200.13.18.

Preshared-key: Enter 123456, which is the preshared key that you already specified on the VPN router.

IP private (internal) address of the remote network: Enter 192.168.0.0, which is the remote private IP address of the remote VPN router. This IP address enables communication with the entire 192.168.0.x subnet.



Note:

All the addresses in this chapter are for example purposes only. You can adjust the settings and configuration to suit your network.

4. Click **Next**. The VPN Client Configuration Wizard Step 3 of 3 screen displays.

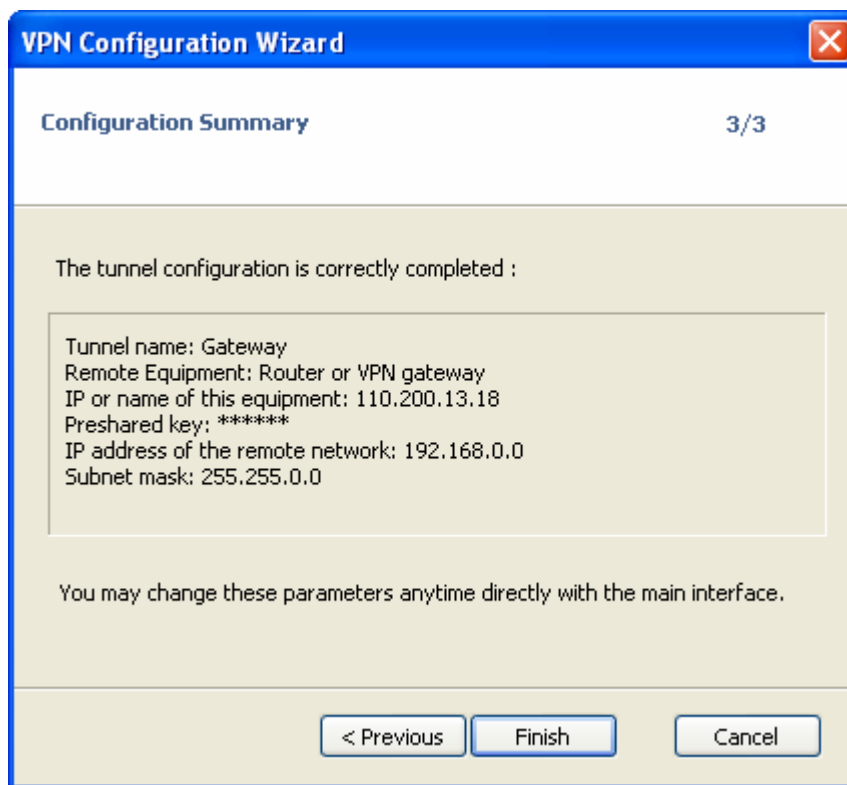


Figure 7-8

5. This screen is a summary screen of the new VPN configuration. Click **Finish**.

6. Specify the local and remote IDs:

- a) Click on the default name Gateway1 in the tree list window of the Configuration Panel screen. The Phase 1 (Authentication) window displays in the Configuration Panel screen.

- b) Click **Advanced**. The Phase 1 Advanced screen displays.

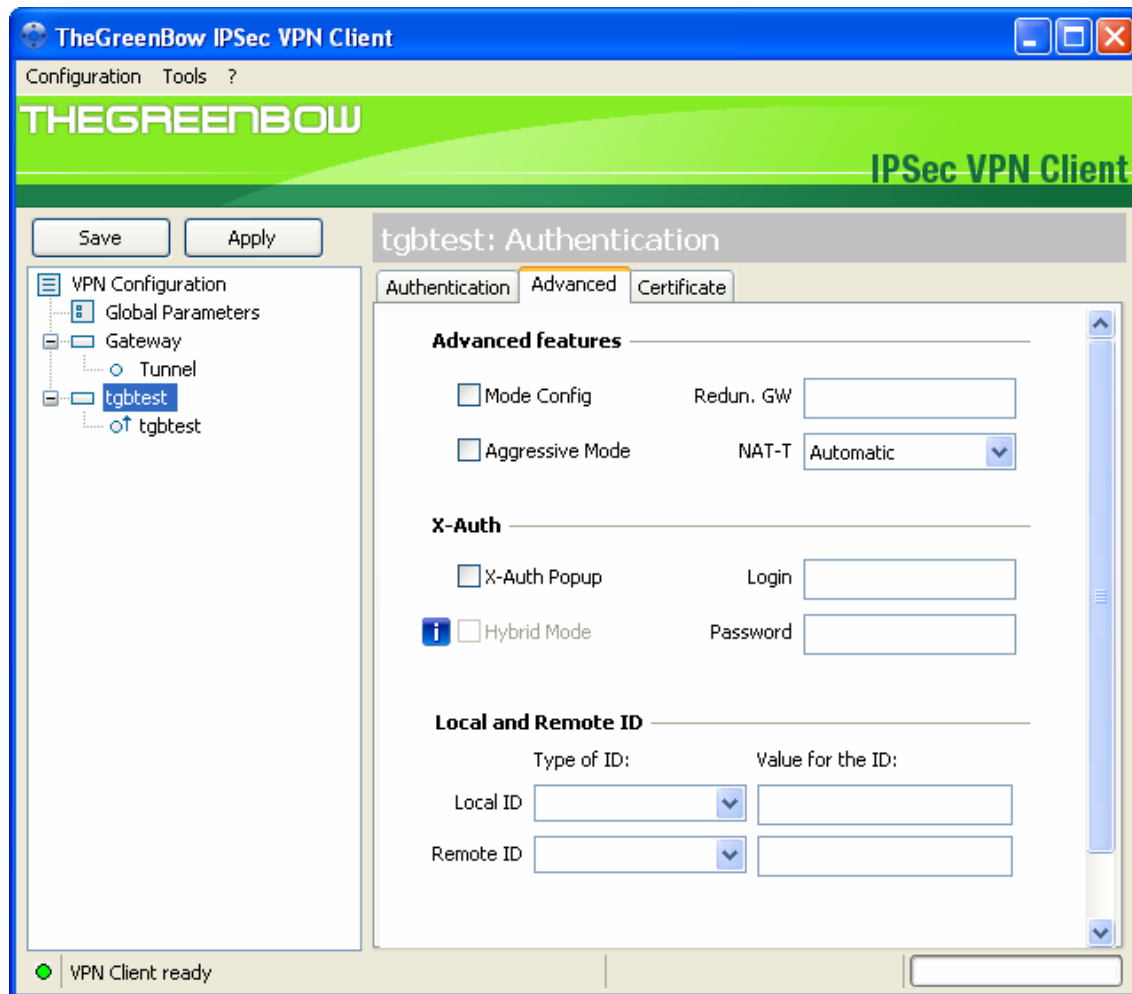


Figure 7-9

- c) Specify the settings that are explained in the following table.

Setting	Description
Aggressive Mode:	Enable or disable aggressive mode as the negotiation mode with the VPN router.
NAT-T:	Select Automatic from the drop-down list to enables the VPN Client and VPN router to negotiate NAT-T. It is suggested to enable it.

Local ID:	As the type of ID, select DNS from the Local ID drop-down list if you specified FQDN in the VPN router configuration or select the IP Address if you specified IP Address in the VPN router configuration. The VPN router only supports IP Address and DNS.
Remote ID:	As the type of ID, select DNS from the Remote ID drop-down list if you specified FQDN in the VPN router configuration or select the IP Address if you specified IP Address in the VPN router configuration. The VPN router only supports IP Address and DNS.

d) Click **OK** to save the settings.

7. Specify the global parameters:

a) Select VPN Configuration > Parameters from the main menu. The Parameters window is displayed in the Configuration Panel screen.

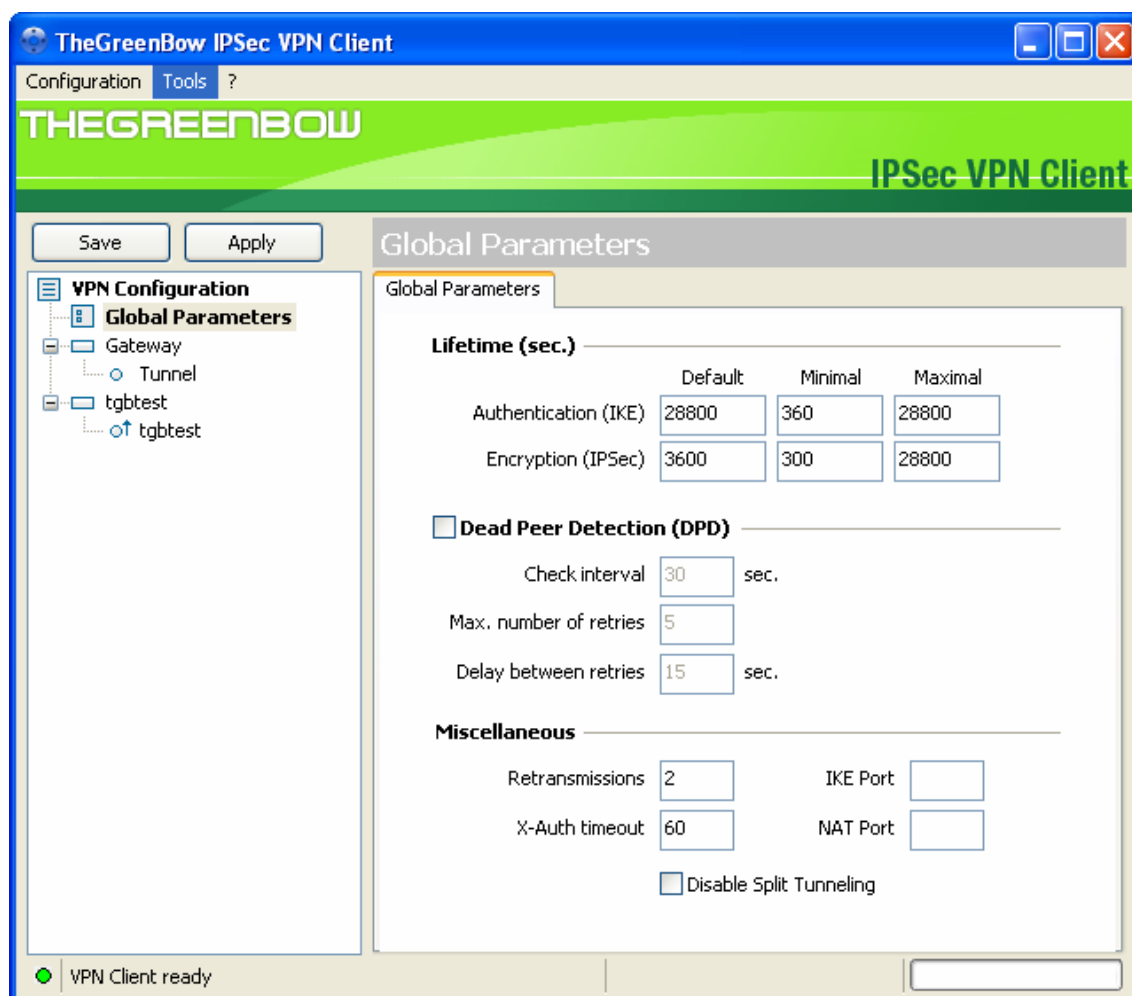


Figure 7-10

b) Specify the default lifetimes in seconds:

- Authentication (IKE), Default: The default lifetime value is 3600 seconds. Replace this setting to 28800 seconds to match the configuration of the VPN router.
- Encryption (IPSec), Default: The default lifetime value is 1200 seconds. Replace this setting to 3600 seconds to match the configuration of the VPN router.

c) Click **Save**.

The VPN Client configuration is now complete.

To connect the VPN Client to the VPN router, see **Establish a VPN connection**.

7.3.2 Manually Configure the VPN Client

To manually configure a VPN connection between the VPN Client and a router, access the VPN Client's user interface, create an IKE phase 1 configuration, an IPSec phase 2 configuration, and then specify the global parameters.

To set up an IKE phase 1 configuration:

1. Right-click on 'VPN Configuration' in the tree list window and select 'New Phase 1'.

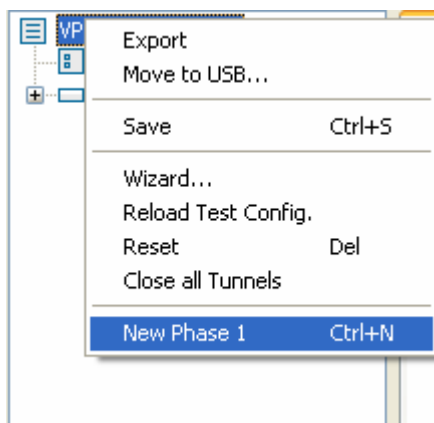


Figure 7-11

2. The Phase 1 (Authentication) window displays in the Configuration Panel screen.

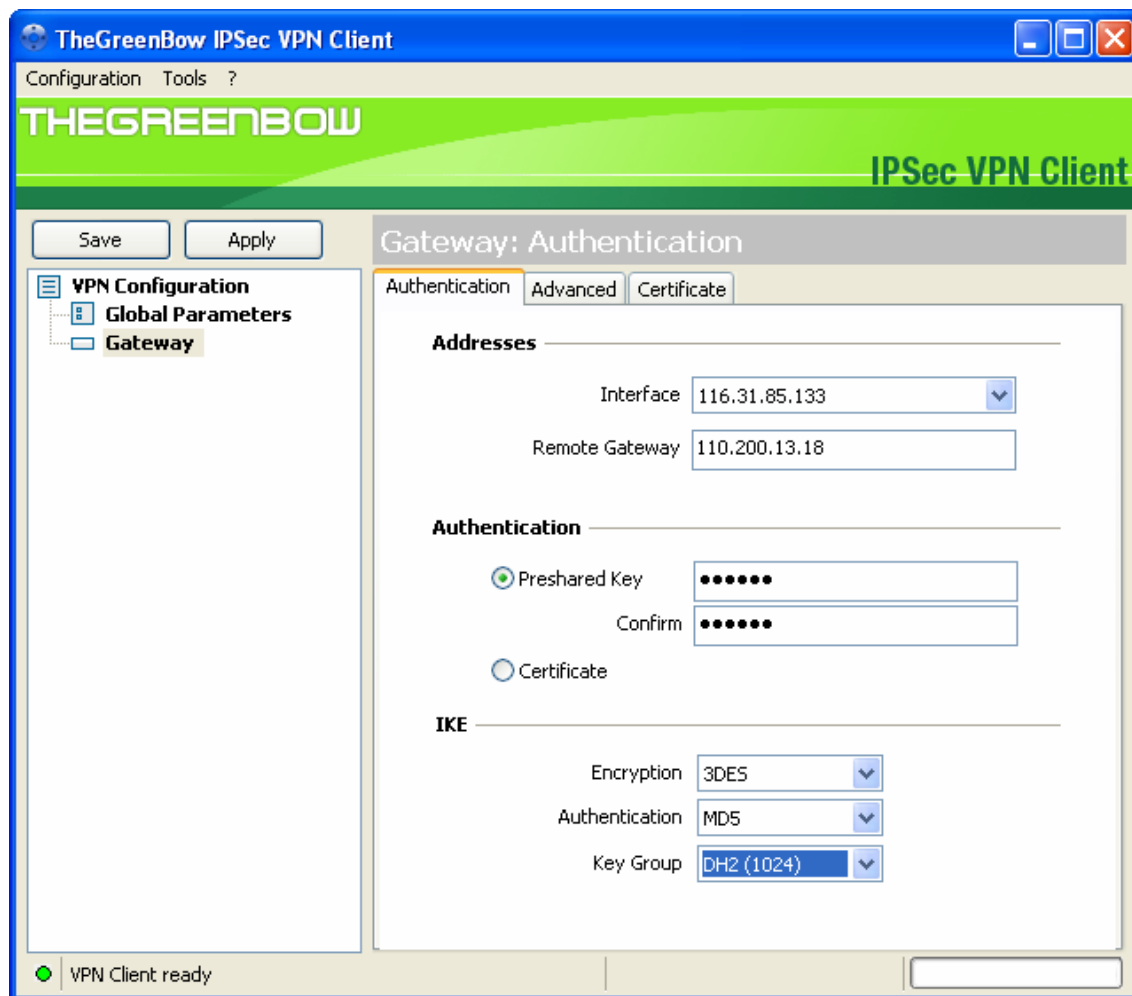


Figure 7-12

3. Specify the settings that are explained in the following table.

Setting	Description	
Interface:	Select the IP Address of the home office router from the drop-down list.	
Remote Gateway:	Enter the remote IP address of the VPN router: 110.200.13.18.	
Preshared Key:	Select the Preshared Key radio button. Enter 123456, which is the preshared key that you already specified on the VPN router. Confirm the key in the Confirm field.	
IKE:	Encryption	Select the 3DES encryption algorithm from the drop-down list.

	Authentication	Select the MD5 authentication algorithm from the drop-down list.
	Key Group	Select the DH2 (1024) key group from the drop-down list.



Note:

The IKE Proposal you created for the VPN Client must be the same as the Proposal on the VPN router.

4. Click **Save** to save the settings.
5. On the same screen, click **Advanced** The Phase 1 Advanced screen displays.

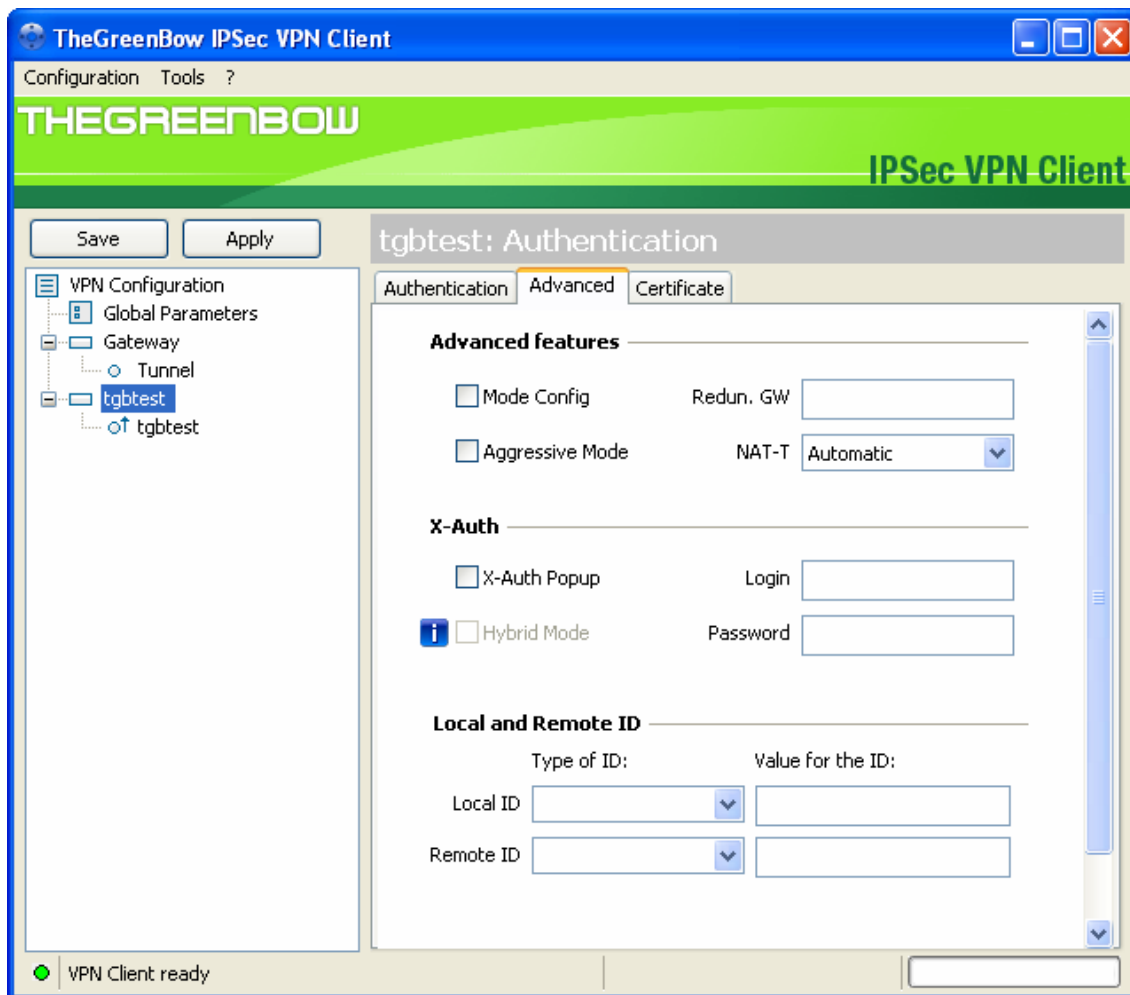


Figure 7-13

6. Specify the settings that are explained in the following table.

Setting	Description
Aggressive Mode:	Enable or disable aggressive mode as the negotiation mode with the VPN router.
NAT-T:	Select Automatic from the drop-down list to enables the VPN Client and VPN router to negotiate NAT-T.
Local ID:	As the type of ID, select DNS from the Local ID drop-down list if you specified FQDN in the VPN router configuration or select the IP Address if you specified IP Address in the VPN router configuration. The VPN router only supports IP Address and DNS.
Remote ID:	As the type of ID, select DNS from the Remote ID drop-down list if you specified FQDN in the VPN router configuration or select the IP Address if you specified IP Address in the VPN router configuration. The VPN router only supports IP Address and DNS.

- Click **Save** to save the settings.

To set up an IPSec phase 2 configuration:

- Right-click on the new Phase 1 in the tree control and select "New Phase 2'.

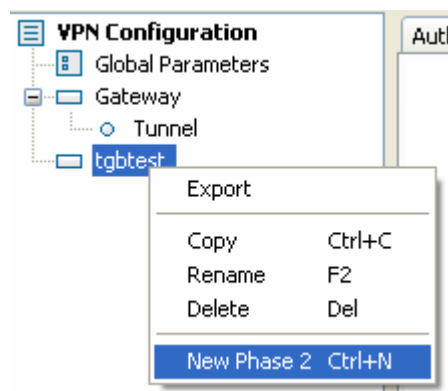


Figure 7-14

- Click on the new Phase 2 in the tree control, the Phase 2 (IPSec Configuration) screen displays.

Establish a VPN connection

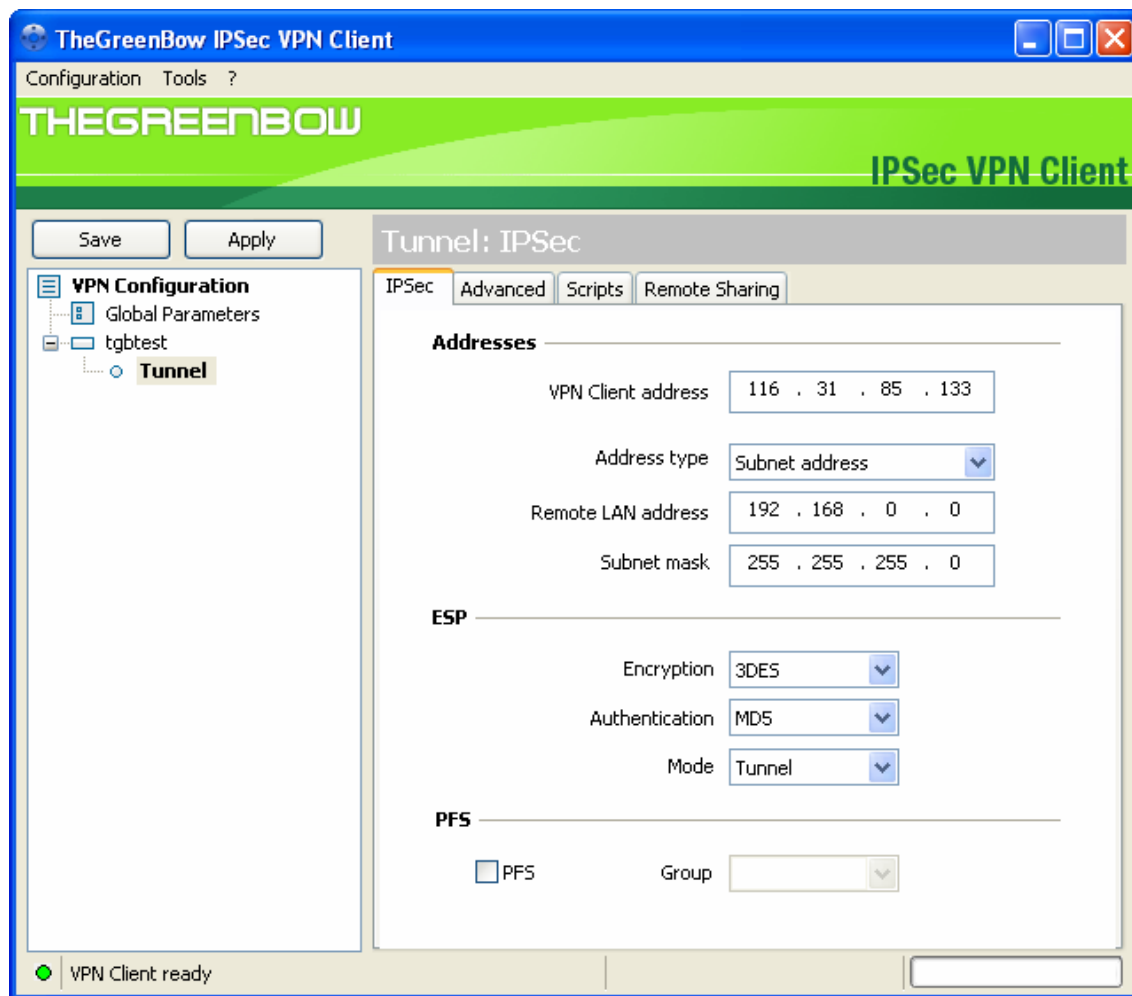


Figure 7-15

3. Specify the settings that are explained in the following table.

Setting	Description
VPN Client address:	It is suggest keeping 0.0.0.0 in this field. You can also enter the IP address of the host with VPN Client, but the IP address cannot be the same as the interface IP address of the VPN router or belong to the remote subnet.
Address Type:	You can only select the Subnet address type.
Remote LAN Address:	Enter 192.168.0.0 as the remote IP address. It must be the same as the LAN address of the remote VPN router.

Subnet Mask:	Enter 255.255.255.0 as the remote subnet mask of the gateway that opens the VPN tunnel. It must be the same as the Local Subnet set in the VPN router.	
ESP:	Encryption	Select 3DES as the encryption algorithm from the drop-down list.
	Authentication	Select MD5 as the authentication algorithm from the drop-down list.
	Mode	Select Tunnel as the encapsulation mode from the drop-down list. The VPN client supports Tunnel Mode only.

4. Click the **Save**.

There are more options within **P2 Advanced**, however for this document we won't be going into these features.

Global parameters

1. Select VPN Configuration > Parameters from the main menu. The Parameters window displays in the Configuration Panel screen.

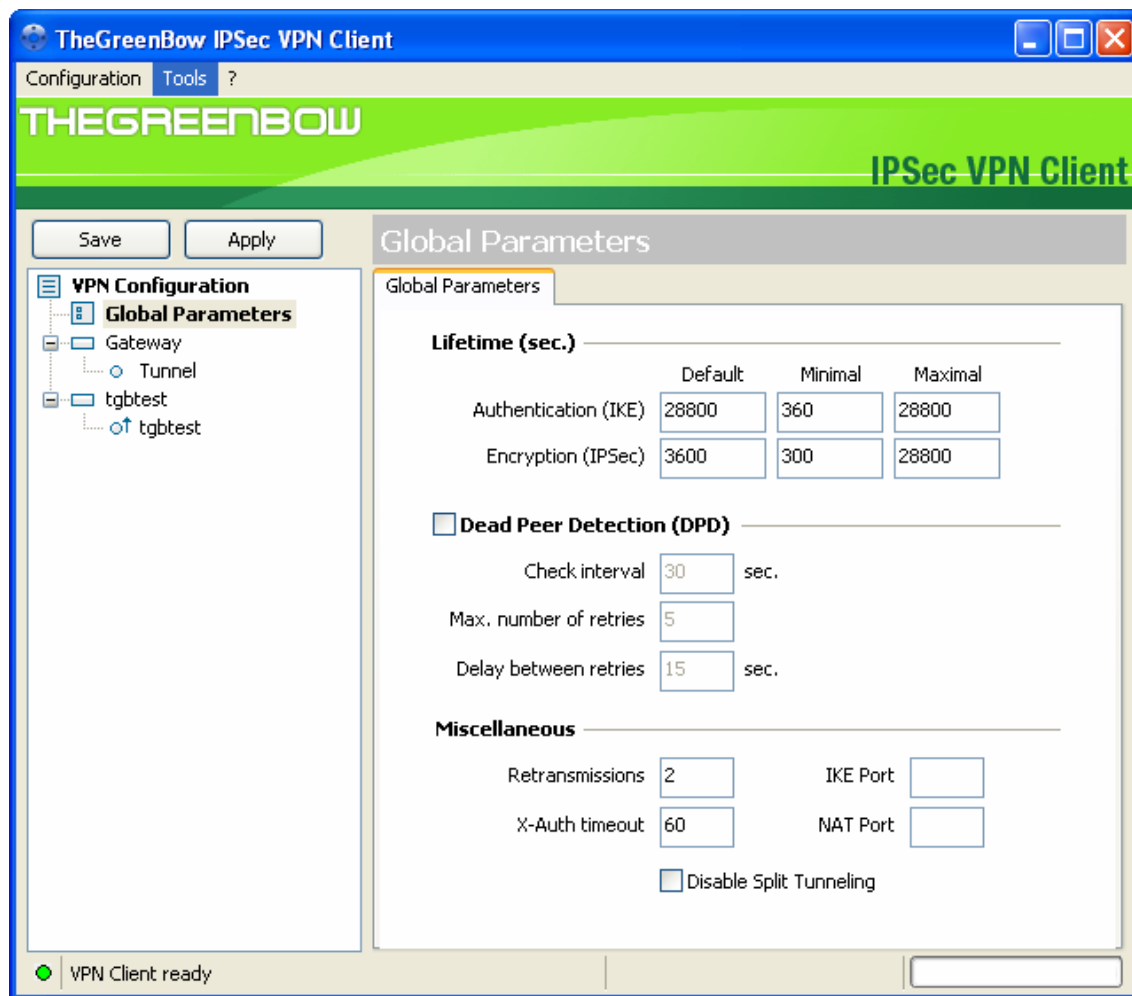


Figure 7-16

2. Specify the default lifetimes in seconds:

- Authentication (IKE), Default: The default lifetime value is 3600 seconds. It is suggested to keep the default value.
- Encryption (IPSec), Default: The default lifetime value is 1200 seconds. It is suggested to keep the default value.

3. Click **Save**.

7.3.3 Establish a VPN connection

There are several ways to establish a connection.

- Right-click on the new Phase 2 in the tree control, and then click **Open Tunnel**.
- Right-click on the system tray icon, then click the name of the tunnel to open it.

Chapter 8 Console and Logs

8.1 Console Windows

The 'Console' window is available from the context menu of the systray icon or from the menu Tools > Console. This window can be used to analyze VPN tunnels. This tool is particularly useful for IT managers in setting up their network.

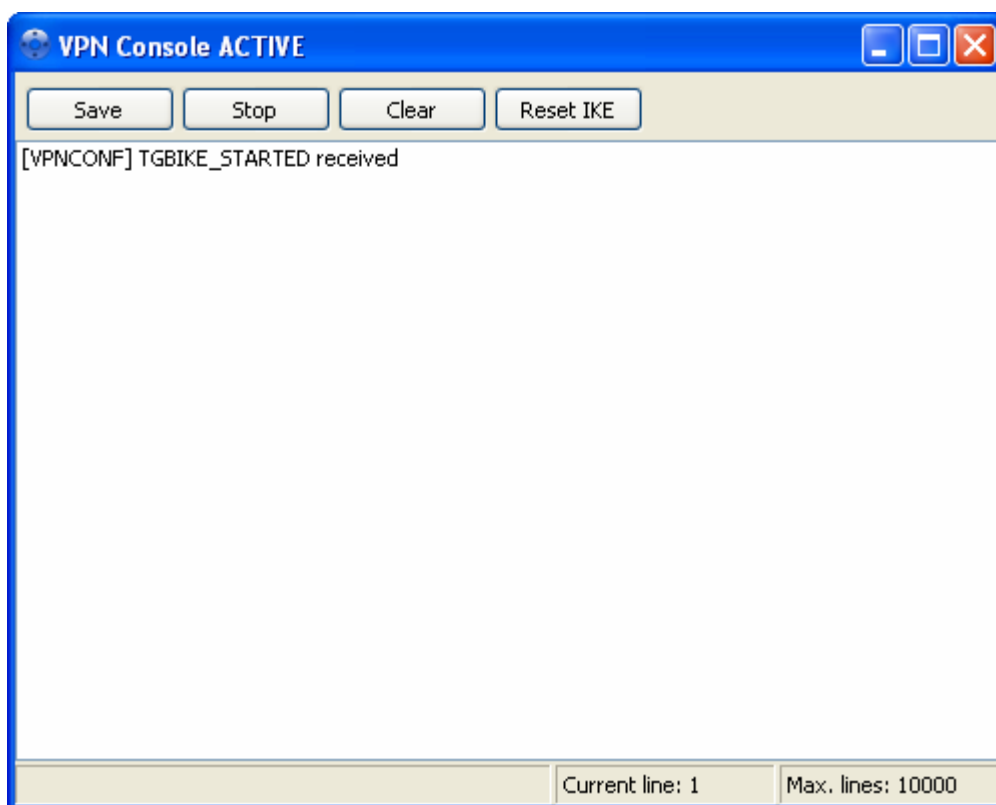


Figure 8-1

Button	Description
Save:	Save current logs in a file. Future logs won't be saved in the selected file.
Start/Stop:	Start/Stop collecting logs.
Clear:	Clear console window content
Reset IKE:	Restart IKE process.