

Syswan VPN Client

User Guide

SYSWAN TECHNOLOGIES, INC.
2050 BEAVERCREEK RD, SUITE 101 #388
OREGON CITY, OR 97045 USA

1 - 877 - 6 - SYSWAN
WWW.SYSWAN.COM

1. Introducing the Syswan VPN Client.....	5
1.1 What is the Syswan VPN Client ?	5
1.2 Compatibility with Syswan Duolinks SW24 VPN series load balancers	5
1.3 Multi VPN Gateway solution.....	5
1.4 Multi USB Token and SmartCard solution	5
1.5 Linux Appliance Support	5
1.5 Syswan VPN Client Features	6
2. Installing the Syswan VPN Client.....	8
2.1 Software Installation.....	8
2.2 Software Evaluation	9
2.3 Software Activation	10
2.3.1 Software Activation Wizard.....	10
2.3.2 Step 1 of 2: Enter License Number.....	10
2.3.3 Step 2 of 2: Online Activation	11
2.3.4 Activation Troubleshooting	11
2.4 Software Upgrades	12
2.5 Software Uninstallation	13
3. Quick How To's	14
3.1 How To Open VPN tunnel?.....	14
3.2 How To Troubleshoot VPN tunnels?.....	14
3.3 How To Import by double clicking on a VPN Configuration icon?	14
4. Navigating the User Interface	15
4.1 User interface elements	15
4.2 System Tray Icon	16
4.3 System Tray Popup.....	17
4.4 Keyboard Shortcuts.....	18
4.5 Connection Panel.....	18
4.6 Configuration Panel.....	19
4.6.1 Main Menu.....	19
4.6.2 Status Bar.....	20
4.6.3 "About" window.....	20
4.6.4 Access Control & Hidden Interface.....	21
4.6.5 Wizards	22
4.6.6 Preferences	23
5. Connection Panel.....	24
5.1 Connection Panel basics.....	24
5.2. More information about Connections	25
6. Configuration Panel.....	26
6.1 Configuration Wizard.....	26
6.1.1 Three step Configuration Wizard.....	26
6.1.2 Step 1 of 3: Choice of remote equipment	27
6.1.3 Step 2 of 3: VPN tunnel parameters	27
6.1.4 Step 3 of 3: Summary.....	28
6.2 VPN Tunnel Configuration	28
6.2.1 How to create a VPN Tunnel ?	28
6.2.2 Multiple Authentication or IPSec Configuration Phase	29
6.2.3 Advanced Features	29
6.3 Authentication or Phase 1	29
6.3.1 What is Phase 1 ?	29
6.3.2 Phase 1 Settings Description	30
6.3.3 Phase1 Advanced Settings Description.....	31
6.4 IPSec Configuration or Phase 2.....	34
6.4.1 What is Phase 2 ?	34
6.4.2 Phase 2 Settings Description	34
6.4.3 Phase2 Advanced Settings Description.....	36
6.4.4 Script configuration.....	37
6.5 Global Parameters	38
6.5.1 Global Settings Description	38
6.6 VPN Tunnel View	40

- 6.6.1 How to view opened tunnels ? 40
- 6.7 USB Mode 41
 - 6.7.1 What is USB Mode ? 41
 - 6.7.2 How to set USB Mode ? 41
 - 6.7.3 How to enable a new USB Stick ? 42
 - 6.7.4 How to automatically open tunnels when a USB Stick is plugged in ? 42
- 6.8 Certificate Management 43
 - 6.8.1 Certificate Management overview 43
 - 6.8.2 How to configure IPsec VPN Client with PKCS#12 Certificates 43
 - 6.8.3 How to configure IPsec VPN Client with PEM Certificates 45
 - 6.8.4 Smart Card and Token Management 47
- 6.9 Configuration Management 50
 - 6.9.1 Import or Export VPN Configuration via menu 50
 - 6.9.2 Merging VPN Configurations 50
 - 6.9.3 Splitting a VPN Configuration 52
- 7. Deployment 53
 - 7.1 Embedded VPN Configuration 53
 - 7.2 Setup options 53
 - 7.2.1 Setup option overview 53
 - 7.2.2 Setup option for GUI mode 54
 - 7.2.3 Setup option for GUI mode access control 54
 - 7.2.4 Setup option for systray menu items 54
 - 7.2.5 Other Setup options 55
 - 7.3 Command line 55
 - 7.3.1 Command line options 55
 - 7.3.2 Stopping IPsec VPN Client: option "/stop" 55
 - 7.3.3 Import or Export VPN Configuration options 56
 - 7.3.4. Opening or closing VPN Tunnel options 56
- 8. Console and Logs 58
 - 8.1 Console Windows 58
- 9. Connecting to a Syswan Duolinks SW24 VPN series Load Balancer 59
 - 9.1 Requirements 59
 - 9.2 Configuring the Syswan Duolinks SW24 VPN series Load Balancer 60
 - 9.3 Configuring the Syswan VPN Client 63
 - 9.3 Opening the IPsec VPN Tunnel 66
 - 9.4 Troubleshooting 69
- 10. Contacts 70

Copyright and Trademarks

© 2007-2008 Syswan Technologies, Inc. All rights reserved.

Brands and product names are trademarks or registered trademarks of their respective holders.

Specifications are subject to change without notice.

V4.1 - REV A – EN

1. Introducing the Syswan VPN Client

1.1 What is the Syswan VPN Client ?

The Syswan VPN Client is an IPSec VPN software for all current Windows versions that allows users to establish secure encrypted connections over the Internet, usually between remote workers and their corporate network. IPSec is the most secure way to connect to the enterprise LAN as it provides strong user authentication, strong tunnel encryption with the ability to cope with existing networks and firewall settings. Syswan IPSec VPN Client is the result of many years of experience in network security and Windows network driver development, as well as extensive research in all related areas.

This IPSec VPN Client completes our range of networking and security products and like all our products, it is extremely easy to install and use.

1.2 Compatibility with Syswan Duolinks SW24 VPN series load balancers

The Syswan VPN Client offers total compatibility towards the Syswan Duolinks SW24 VPN series load balancers (Duolinks SW24 VPN and Duolinks SW24 VPN Plus routers) and guarantees a flawless hardware and software solution to secure any network. IT managers and remote users can rely on software and hardware products that come from the same vendor which are reliable, secure and cross platform compatible.

The Redundant Gateway option built into the Syswan VPN Client software and the dual WAN load balancing and redundancy capabilities of the Syswan Duolinks SW24 series load balancers offer remote users a unique feature that allows the Syswan VPN Client to automatically open a VPN tunnel with an alternate gateway in case the primary gateway is down or unreachable.

1.3 Multi VPN Gateway solution

The Syswan VPN Client strategy is to support as many VPN gateways and appliance vendors as possible in order to offer users a true multi vendor IPSec VPN software solution. A large number of IPSec VPN endpoints have been successfully tested for compatibility in our labs.

1.4 Multi USB Token and SmartCard solution

The Syswan VPN Client supports most popular USB Tokens and SmartCards that are available on the market today. New USB Token and SmartCard devices are regularly tested in our labs for compatibility and greater end user satisfaction.

By directly reading USB Tokens and SmartCards to obtain stored certificates, the Syswan VPN Client helps IT managers make use of existing corporate ID cards or employee cards that may carry digital credentials when implementing remote VPN solutions.

1.5 Linux Appliance Support

The Syswan VPN Client supports many implementations of Linux IPSec VPN like StrongS/WAN and FreeS/WAN. Therefore the Syswan VPN Client is compatible with most of the IPSec routers/appliances based on Linux implementations.

1.5 Syswan VPN Client Features

Supported OS	Windows 2000, Windows 2003, Windows XP, Vista 32 bits.
Connection Mode	Operates as a peer-to-peer VPN as well as a "point – to – multiple" mode without a gateway or server. All Internet connection types like Dial up, DSL, Cable, GSM/GPRS and WiFi are supported. Allows IP Range networking. It can run inside a RDP session (Remote Desktop connection).
Tunneling Protocol	Full IKE support: Our IKE implementation is based on the OpenBSD 3.1 implementation (ISAKMPD), thus providing best compatibility with existing IPSec routers and gateways. Full IPSec support: Main mode and Agressive mode MD5 and SHA hash algorithms Change IKE port
NAT Traversal	NAT Traversal Draft 1 (enhanced), Draft 2 and 3 (full implementation) Including NAT_OA support Including NAT keepalive Including NAT T Aggressive Mode Forced NAT-Traversal mode.
Encryption	Provides several encryption algorithms: 3DES, DES and AES 128/192/256bits encryption. Support of Group 1, 2, 5 and 14 (i.e. 768, 1024, 1536 and 2048).
User Authentication	X-AUTH support PreShared keying and X509 Certificates support. Compatible with most currently available IPSec gateways. USB Token & SmartCard support Flexible Certificate support: PEM, PKCS#12... Certificates can be directly imported from the user interface. Ability to configure one Certificate per tunnel. Hybrid Authentication Method support.
Dead Peer Detection (DPD)	DPD is an Internet Key Exchange (IKE) extension (i.e. RFC3706) for detecting a dead IKE peer.
Redundant Gateway	Redundant Gateway offers remote users a highly reliable secure connection to the corporate network. The Redundant Gateway feature allows the Syswan VPN Client to open an IPSec tunnel with an alternate gateway in case the primary gateway is down or unreachable.
Mode Config	"Mode Config" is an Internet Key Exchange (IKE) extension that enables the IPSec VPN gateway to provide LAN configuration to the remote user's machine (i.e. Syswan VPN Client). With Config-Mode the end-user is able to address all servers on the remote network by using their network name (e.g. //myserver/marketing/budget) instead of their IP Address.

USB Stick	VPN configurations and security elements (certificates, preshared key,...) can be saved into an USB Stick in order to remove security information (e.g.authentication) from the computer. Automatically open and close tunnels when plugging in or removing USB Stick.
Smart Card and USB Token	The Syswan VPN Client can read Certificates from Smart Cards to make full use of existing corporate ID card or employee cards that may carry Digital credentials.
Log console	All phase messages are logged for testing or staging purposes to easily narrow the view on specific aspects.
Flexible User Interface	Silent install and invisible graphical interface allow IT managers to deploy solutions while preventing user to misuse configurations. Tiny Connection Panel and VPN Configuration Panel can be available to end-users separately with Access Control. Drag & drop VPN Configurations into the Syswan VPN Client. Multiple keyboard shortcuts to easily navigate the Syswan VPN Client interface.
Scripts	Scripts or applications can be launched automatically on several events (e.g. before and after a tunnel opens, before and after a tunnel is closed).
Configuration Management	User Interface and Command Line. Password protected VPN configuration file. Specific VPN configuration file can be provided within the setup.

2. Installing the Syswan VPN Client

2.1 Software Installation

The Syswan VPN Client installation is a classical Windows installation that does not require specific information. After completing the installation, you will be asked to reboot your computer.

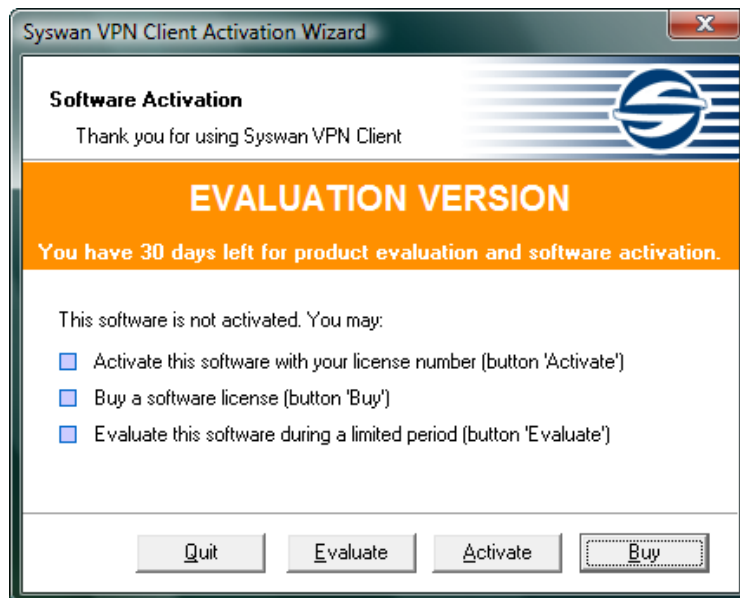
After reboot and session login, a window appears with several options:

"Quit" will close this window and software.

"Evaluate" allows you to continue software evaluation. Evaluation period left is displayed within the orange bar.

"Activate" allows you to activate the software online. This requires a License Number. When clicking on 'Activate' button, an Activation Wizard pops up.

"Buy" allows you to go online and obtain information on how to purchase a Syswan VPN Client Software License from our web site.



Caution:

On Windows 2000, XP and Vista, you must have administrator rights to perform the installation. Without these rights, the installation will stop after the language selection with an error message.

Shortcuts:

After software installation, the Syswan VPN Client window can be launched:

from user desktop, by double-clicking on Syswan VPN Client shortcut

from the VPN Client icon available in the taskbar

from Start Menu > Programs > Syswan > VPN Client > Syswan VPN Client

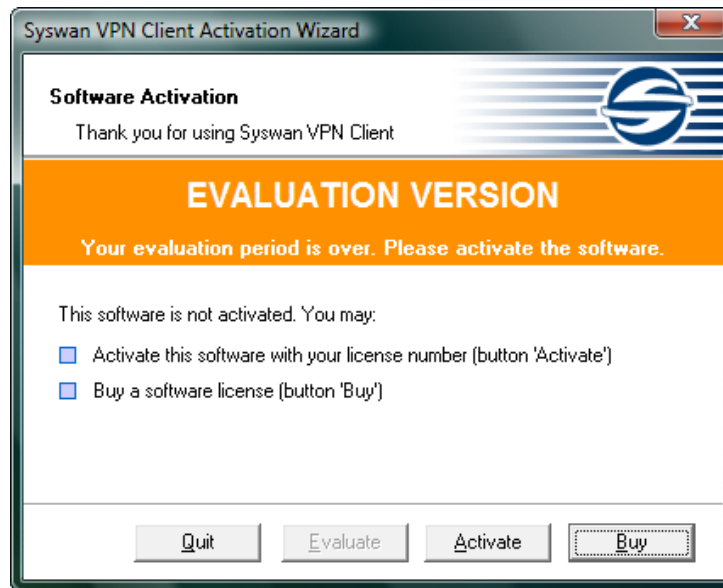
Note:

Software Installation can be customized with several parameter options in the command line. Please refer to the "Deployment Guide" document available on our web site for more information.

2.2 Software Evaluation

It is possible to use a fully functional copy of the Syswan VPN Client for an evaluation period limited to 30 days by clicking on the 'Evaluate' button. When the Syswan VPN Client is under "Evaluation" mode, the Software Activation window will appear at each start up of the Syswan VPN Client. Evaluation time left will be displayed inside the orange bar of that window.

Once the evaluation period expires, The 'Evaluate' button will no longer be available and the software will be disabled. You may activate the Syswan VPN Client software by using a purchased licence key. Any existing VPN tunnel configurations created during the evaluation period will be retained during the software activation.



2.3 Software Activation

2.3.1 Software Activation Wizard

For use beyond the evaluation period, the Syswan VPN Client software must be activated. The Software Activation is a two step process which requires a License Number and an email address.

The 'Activation Wizard' can be launched from the VPN Client software as followed:

Click on the 'Activate' button in the startup windows when you start the Syswan VPN Client.
Click on the '?' menu and then click on "Activation Wizard...".

2.3.2 Step 1 of 2: Enter License Number

Software Activation requires a License Number.

Enter your License Number, your email address and click 'Next' as shown below:

If you have a 20 character License Number, switch to the 20 character "License Number" field by clicking on the link "Click here to enter a 20 character License".

Note:

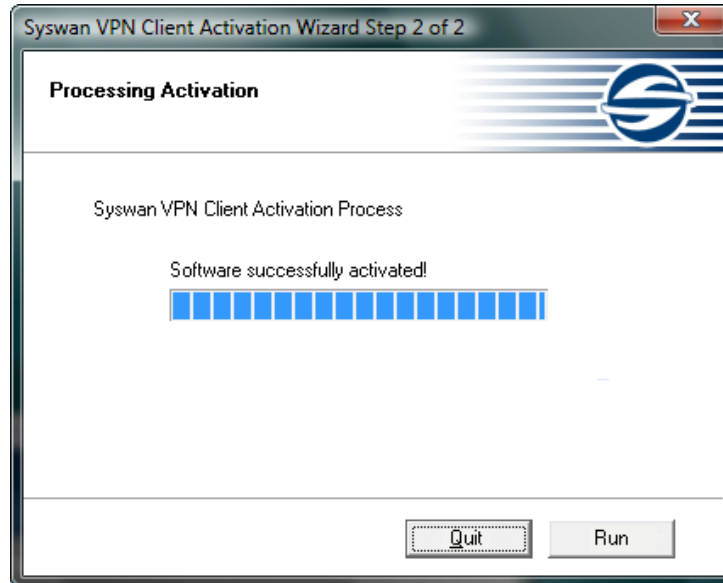
Please enter a valid email address here as it will be used to send you back the activation confirmation.

The email address may not be required as IT managers can force this value during the setup, then it will not be displayed by the Software Activation Wizard. This feature can be used to centralize all the Software Activation confirmation emails to a single email address during deployment. Please refer to the "Deployment Guide" document available on our web site for more information.

2.3.3 Step 2 of 2: Online Activation

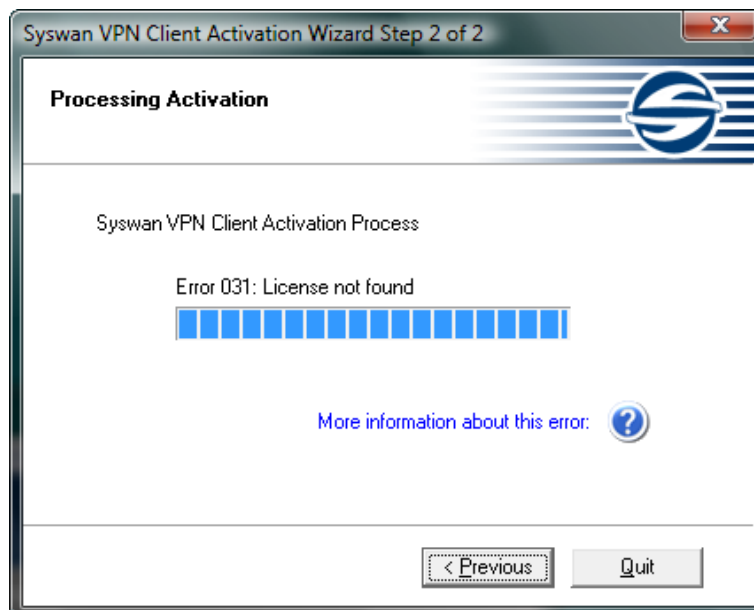
The 'Activation Wizard' will automatically connect to the online software activation server to activate the Syswan VPN Client Software.

The 'Activation Wizard' will end upon successful Activation.



2.3.4 Activation Troubleshooting

Errors may occur during the activation process. Each activation error is briefly explained on the step 2 activation window. The link "More information about this error" below the progress bar provides error explanation and recommendations on how to proceed next.



Most of the errors encountered may be fixed by carefully checking the following points:

1. Check you entered the correct License Number (error 031).
2. The communication with our activation server may be filtered by a proxy (error 053 or error 054). You should configure the proxy in the step 1 of the Software Activation Wizard by clicking the link at the bottom of the window.
3. The communication with our activation server may be filtered by a firewall (error 053 or error 054). Check if a personal firewall or a corporate firewall is filtering communications.
4. Our activation server may be temporarily unreachable. Try to activate the software a few minutes later.
5. Your License Number has already been activated (error 033). Please contact your network administrator as you may have the wrong licence number. You can also contact our support team for assistance or our sales team if you wish to purchase a new licence.

All activation errors are detailed on our web site:

<http://www.syswan.com/swvpnclient/vpnactivationerrors.htm>

Note:

If you did not succeed in activating the software despite the previous recommendations, it is always possible to manually activate the software on our web site :

http://www.syswan.com/swvpnclient/osa_manual.html

Please follow the instructions given on the manual activation page carefully.

2.4 Software Upgrades

Warning:

The Syswan VPN Client software needs to be **re-activated** once a software upgrade is applied. Depending on your maintenance contract, a software upgrade activation might be rejected. Please read the following recommendations carefully and check the current status of your maintenance and your software release by clicking on the menu "?" then "Check for update" on the Configuration Panel.

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

1. During your maintenance period of one year which starts from the day of your first activation, all software upgrades are allowed.
2. Once your maintenance period has expired (and if you have a maintenance renewal contract), only minor software upgrades are allowed. Minor software upgrades are identified by the last digit of a version.

During the upgrade process, the existing version of the software will be uninstalled and you may be required to reboot your computer to finish the uninstallation process. After the reboot, you can continue with the software upgrade.

Example:

My maintenance period has expired (i.e. more than one year has passed since my first software activation) and my current software Release is 4.10. I only can upgrade to Releases 4.11 till 4.19. I will not be able to upgrade to Releases 4.20, 4.30 or 5.00.

Note:

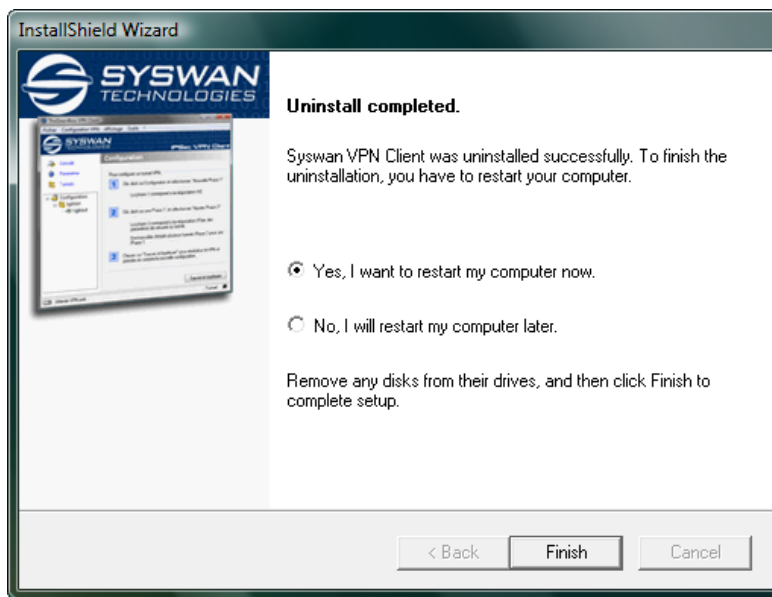
Any existing VPN Configurations are saved during the Software Upgrade and are automatically enabled again in the new release.

If you want to subscribe to or extend your maintenance period after the initial period of one year, please visit our web site or contact our sales team.

2.5 Software Uninstallation

Syswan IPSec VPN Client can be uninstalled:

from Windows Control Panel by selecting 'Add/Remove programs'
from Start Menu > Programs > Syswan > VPN Client > 'Uninstall Syswan VPN Client'



You will be requested to restart your computer after the Uninstallation Process is complete.

3. Quick How To's

3.1 How To Open VPN tunnel?

How to open a tunnel (once a VPN configuration is set):

- Connection panel > Open
- SystemTray > click on 'Open xxx'
- Automatically as soon as network traffic is detected
- Automatically as soon as USB stick is inserted
- Automatically as soon as Windows starts (before or after logon)
- By double clicking on a VPN Configuration file (e.g. icon on desktop, email attachment)
- By using the command line options to open or close tunnels

3.2 How To Troubleshoot VPN tunnels?

You will be able to find and troubleshoot issues, listed in the following documents or by consulting the FAQ and knowledgebase available on our web site:

- VPN TroubleShooting Documentation.
- Online help.
- Online Software Activation help.
- IPSec VPN Client FAQs.

3.3 How To Import by double clicking on a VPN Configuration icon?

Also known as the 'Dial up mode': A tunnel may be opened via a double-click on a VPN Configuration file (i.e. extension '.tgb' file). This feature permits the creation of various VPN Configuration on the windows desktop and to open tunnels by clicking on the shortcut icons.

To create a VPN Configuration shortcut icon on the desktop:

- Step 1: Configure the tunnel in 'Configuration Panel'
- Step 2: In 'Phase2 Advanced Settings', configure the tunnel to 'Automatically open this tunnel when the VPN Client starts'
- Step 3: Export the VPN Configuration onto your computer desktop.

Note: You may protect the VPN Configuration file with a password as it is exported. This password will be asked each time the tunnel configuration file is launched.

4. Navigating the User Interface

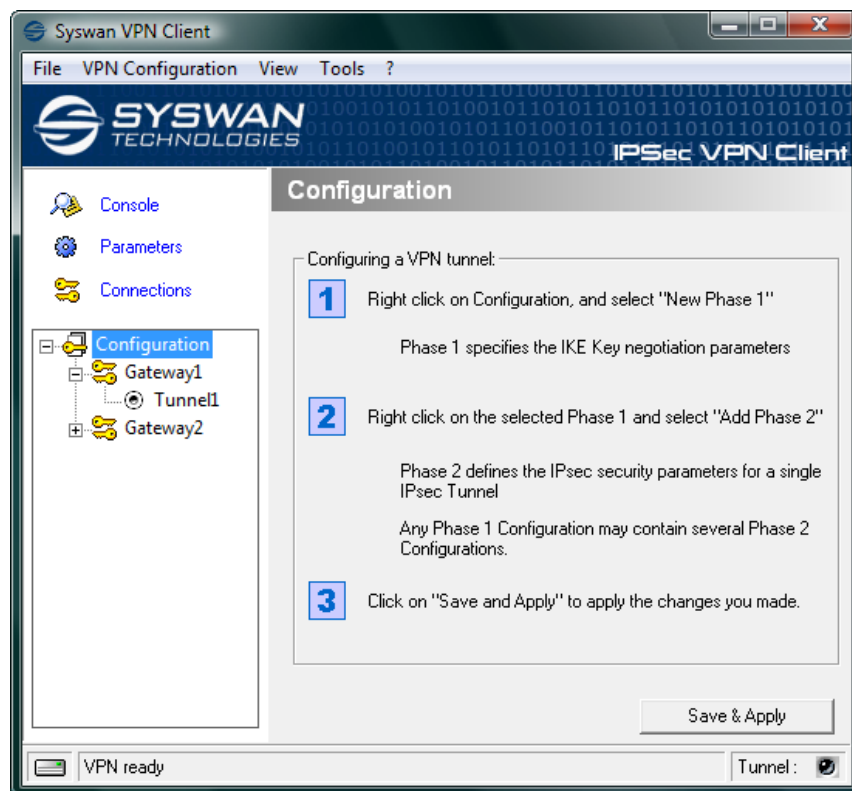
4.1 User interface elements

The Syswan IPsec VPN Client is fully autonomous and can start and stop tunnels without user intervention depending on network traffic to certain destinations. However, it requires that VPN tunnels are configured prior to connecting to a remote network using the VPN configuration options.

The Syswan 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 (e.g. Preshared key, Certificates, ...).

The user interface is made of several elements:

- Configuration Panel
- Connection Panel
- Main menus
- System Tray Icon & Popup
- Status bar
- Wizards
- Preferences



4.2 System Tray Icon

The VPN Client user interface can be launched via a double click on the application icon (Desktop or Windows Start menu) or by a single click on the 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. This is color coded.



VPN Client application system tray icon color represents the following :



Blue icon : no VPN tunnel is opened



Green icon : at least one VPN tunnel is opened

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

A right-button click shows the following menu:

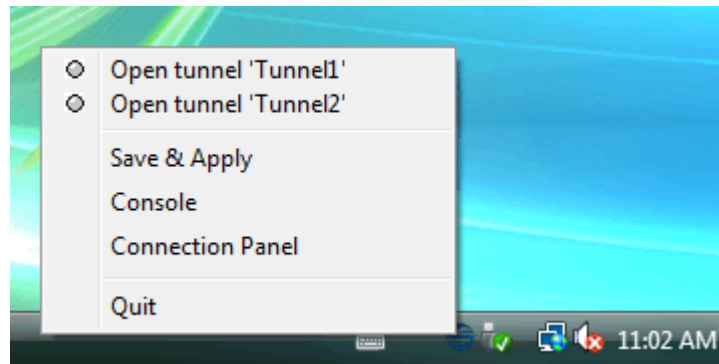
"Quit" will close established VPN tunnels, then stop the configuration user interface.

"Save & Apply" will close established VPN tunnels, apply latest VPN configuration modification and reopen VPN tunnels which are configured to be started automatically.

"Console" shows log window.

"Connection Panel" opens the Connection Panel which enables to open, close and get information about tunnels.

List of configured tunnels with current status. Tunnels can be opened or closed from this menu as well.



Tool tips over the VPN Client icon shows the connection status of the VPN tunnel:

"Tunnel <tunnelname>" when one or more tunnels are established

"Wait VPN ready..." when the IKE service is reinitializing

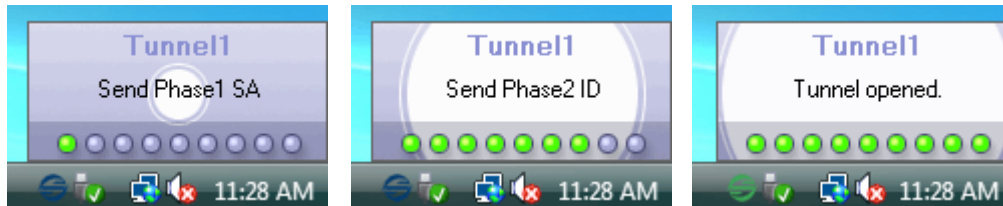
"Syswan VPN Client" when the VPN Client is up but with no opened tunnel.

4.3 System Tray Popup

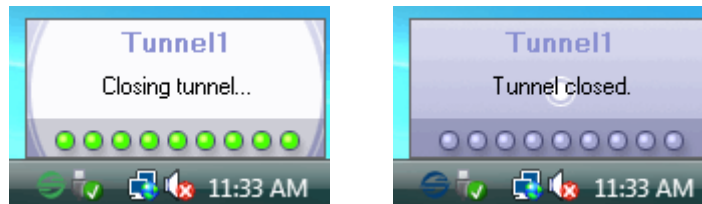
A tiny popup coming out from the systray icon shows up each time a tunnel is opening or closing.

This tiny popup has a simple behavior:

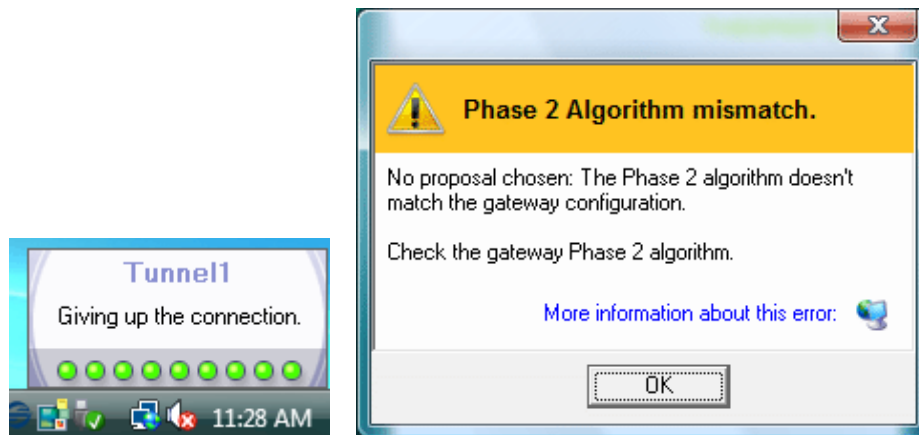
1. The popup shows tunnel opening with different phases and disappears after 6 sec unless the mouse pointer is moved over.



2. The popup also show up when tunnels are closed.



3. In case the tunnel cannot open, a warning will display with a link to more information on our web site.



4.4 Keyboard Shortcuts

This feature improves the most common manipulations.

Shortcut	Action
Ctrl + Enter	Switches between the Configuration Panel and the Connection Panel. Note: in case, the Configuration Panel is protected with a password, the user will be asked for this password when he tries to switch to the Configuration Panel.
Ctrl + D	Opens the VPN Console in 'Debug' mode.
Ctrl + S	'Save & Apply' a VPN Configuration.

4.5 Connection Panel

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

This feature clearly helps both IT managers (who configure the VPN connections) and end users (who only open or close VPN connections) to access options depending on their usage.

The Connection Panel is made of several elements:

- An animated network diagram showing information on the current tunnel (upper half)

- A list of all configured tunnels with an 'open/close' button (lower half)

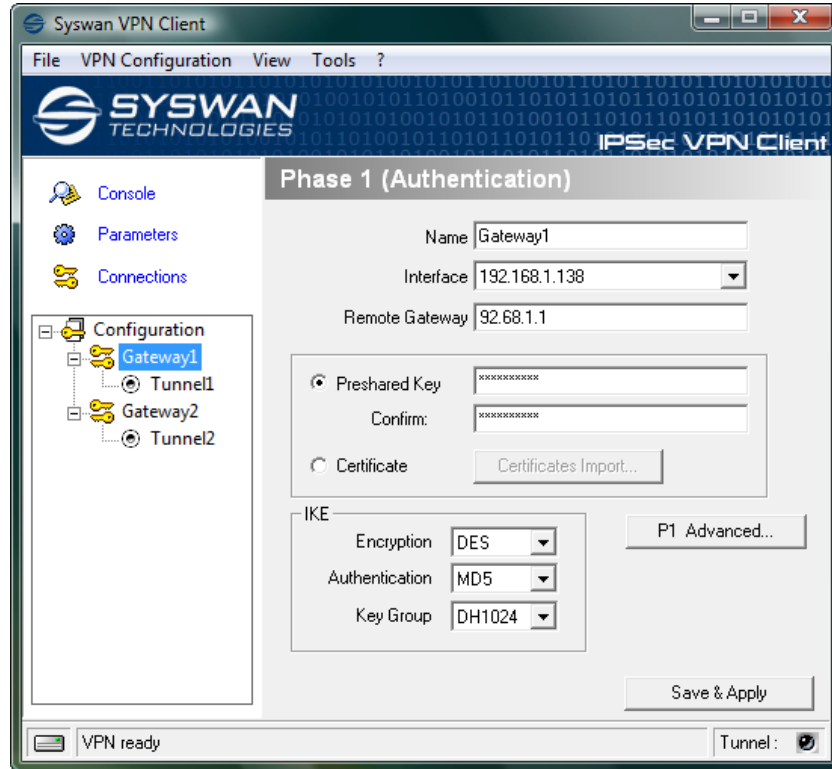
It is always possible to switch from the Connection Panel to the Configuration Panel through the system menu (menu 'Configuration Panel') or via the shortcut 'Ctrl + P' (see section 'Shortcuts').



4.6 Configuration Panel

The Configuration Panel enables to create VPN Configurations and offers several options:

- Three buttons 'Console', 'Parameters' and 'Connections' (left column)
- A tree list window (left column) that contains all the IKE and IPSec configurations
- A configuration window (right column) that shows the associated tree level.



A VPN Configuration file (i.e. extension '.tgb') can be dragged and dropped onto the Configuration Panel. This feature enables easy application of a new VPN configuration. If a tunnel is configured to be 'opened when the VPN Client starts' (see section 'Phase2 Advanced Settings'), it will be immediately opened when the new VPN Configuration is applied ('Save & Apply').

4.6.1 Main Menu

There are several menus as followed:

'File' menu is used to Import or Export a configuration. It is also used to choose the location of the VPN Configuration: local, USB, server, Token. It is finally used to configure miscellaneous preferences such as the way the VPN Client may start (e.g. before or after logon, ...).

'VPN Configuration' menu contains all actions from tree control right-click menu. 'Configuration' menu also gives access to the 'Configuration Wizard'.

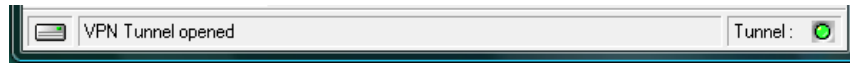
'View' menu contains the 'Configuration' of what the user can access.

'Tools' menu contains 'Console' and 'Connections' choice.

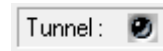
'?' menu gives access to 'check for update', 'online help' and window 'About'. 'The '?' menu also gives access to the 'Activation Wizard'.

4.6.2 Status Bar

The status bar displays several information:

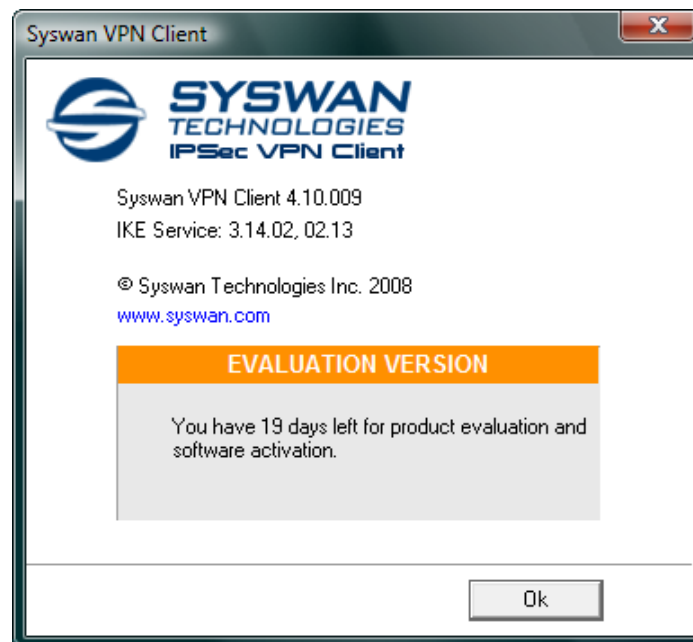


The left side box indicates the VPN configuration location. For example, if the "USB Mode" is set, the image will show a USB stick, enabled or not, depending on the presence of a valid VPN USB stick. The central box gives some information about VPN Client software status (e.g. "opening tunnel in progress", "saving configuration rules in progress", "VPN Client start up in progress", ...) The light box (right side) gives some information about tunnels : the green light indicates at least one tunnel is open and the gray light indicates no tunnels are open.



4.6.3 "About" window

The 'About' window provides the Syswan VPN Client software version and software activation information. There is also a URL to our web site.

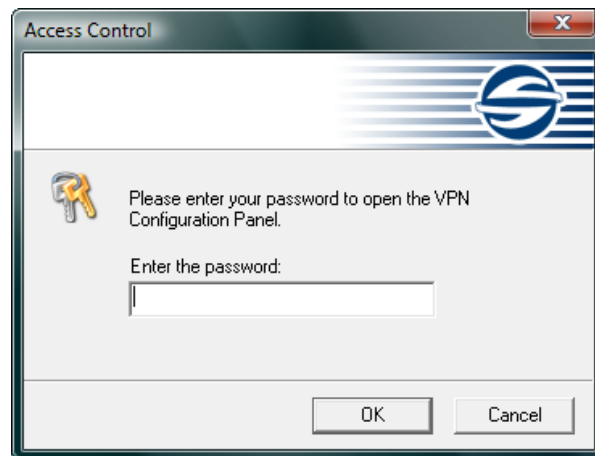


4.6.4 Access Control & Hidden Interface

This feature is especially designed for IT managers. It locks the access to the Configuration Panel, and restricts with password the use of the Syswan VPN Client 'Connection Panel' and/or the systray menu. Therefore, end users will not be able to modify the VPN Configuration so any misconfiguration is avoided.

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

1. when clicked (or double-clicked) on the systray Syswan VPN Client icon
2. when switching from the "Connection Panel" to the "Configuration Panel".



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

The Access Control Window available through the menu 'View > Configuration' in the Configuration Panel, also allows the configuration of the systray menu items. The IT manager can restrict software access, for example from full access rights to a completely hidden interface.

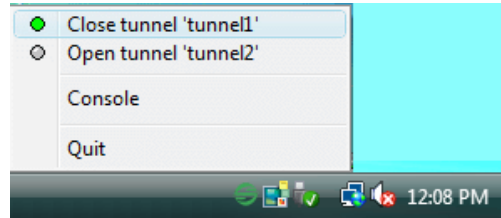


To remove the Access Control, just blank both fields 'Password' and 'Confirm' then click 'OK'.

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').

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

In case Access Control has been set, the 'Configuration Panel' cannot be opened by double-clicking on the desktop icon or by selecting it from the Start menu. Right-clicking on the icon on taskbar will be limited to "Console" access, quitting the software, and opening/closing the configured tunnels:



4.6.5 Wizards

There are two Wizards available:

VPN Configuration Wizard can be launched from Menu 'VPN Configuration' > 'Config Wizard'.
Software Activation Wizard can be launched from Menu '?' > 'Activation Wizard'.

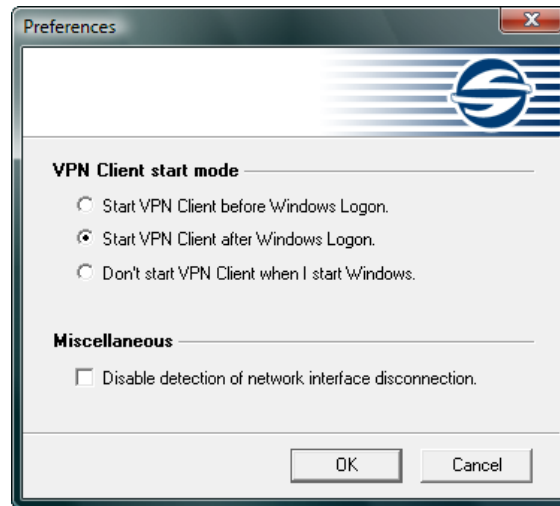
4.6.6 Preferences

'Preferences' window allows you to define:

Start up mode of the software. Modes that can be configured in the software setup (see section 'Setup options').

Enable/Disable the detection of interface disconnection feature.

Preferences are available via Menu 'File' and click 'Preferences'.



VPN Client start mode

Syswan IPsec VPN Client software has several start up mode, such as:

Start IPsec VPN Client software before MS Windows logon: this mode can be used for secure remote login

Start IPsec VPN Client software after MS Windows logon

Do not start IPsec VPN Client when starting MS Windows: IPsec VPN Client is launched either by the user or from within a script ("manual" mode)

Miscellaneous

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

5. Connection Panel

5.1 Connection Panel basics

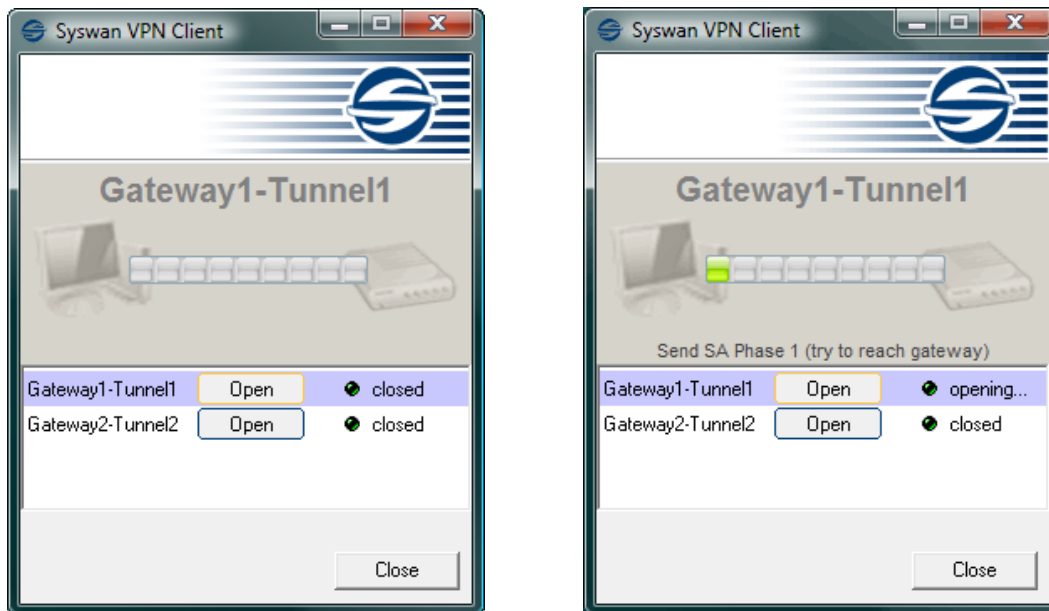
The Connection Panel enables users to open, close and get clear information about every tunnel that have been configured. This is all the end-user needs to open and close tunnels.

The Connection Panel is made up of several elements:

- An animated network diagram showing information on current tunnel (top)
- A list of all configured tunnels with 'open/close' button (bottom)

The user simply clicks on the 'Open' button of a tunnel to open this tunnel. The 'Open' button automatically switches to 'Close' when the tunnel is opened. One click on the name of the tunnel automatically opens the Configuration Panel, enabling to change the tunnel configuration. This feature is disabled when the Connection Panel is protected with a password (see section 'Access Control').

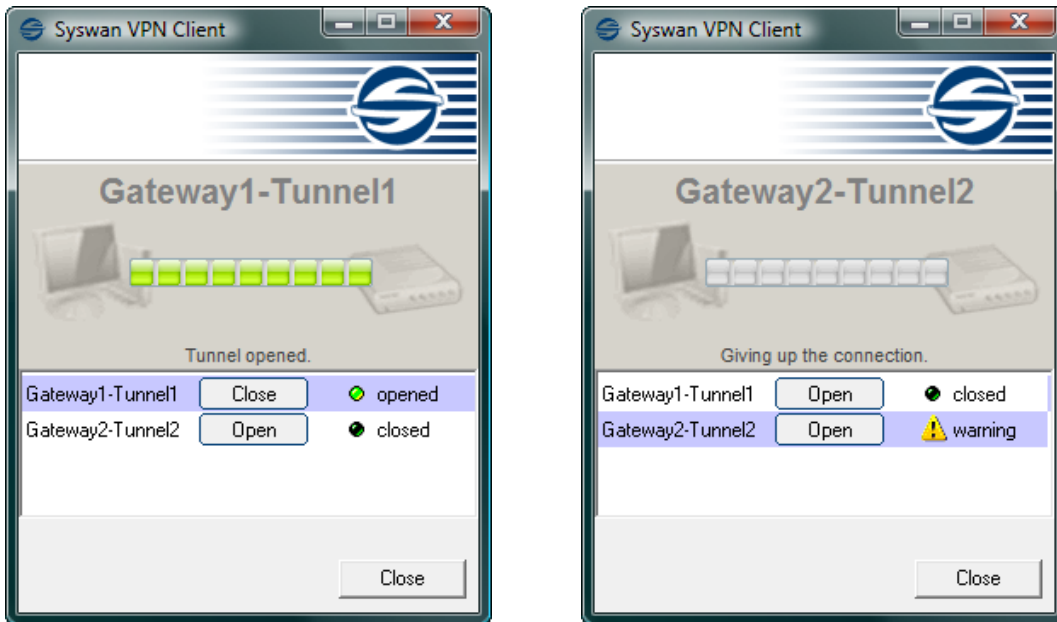
It is always possible to switch from the Connection Panel to the Configuration Panel through the system menu (menu 'Configuration Panel') or via the shortcut 'Ctrl + Enter' (see section 'Shortcuts').



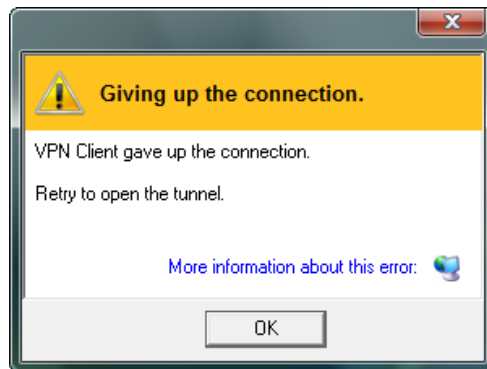
It is also possible to automatically apply a new VPN Configuration by dragging & dropping a VPN Configuration file onto the Connection Panel. If a tunnel is configured to be automatically opened when the VPN Client starts (see section 'Phase2 Advanced Settings'), it will immediately appear open.

5.2. More information about Connections

If problems occur during the tunnel opening process, a warning is shown on the right of the tunnel list.



Click on the associated warning link to automatically open the 'Warning' popup which shows a detailed message about the problem. Explicit warning messages help users and IT managers to troubleshoot VPN errors. These popups are also linked ("More information about this error:" link) to our online help web pages that detail symptoms and give clues for troubleshooting.



6. Configuration Panel

6.1 Configuration Wizard

6.1.1 Three step Configuration Wizard

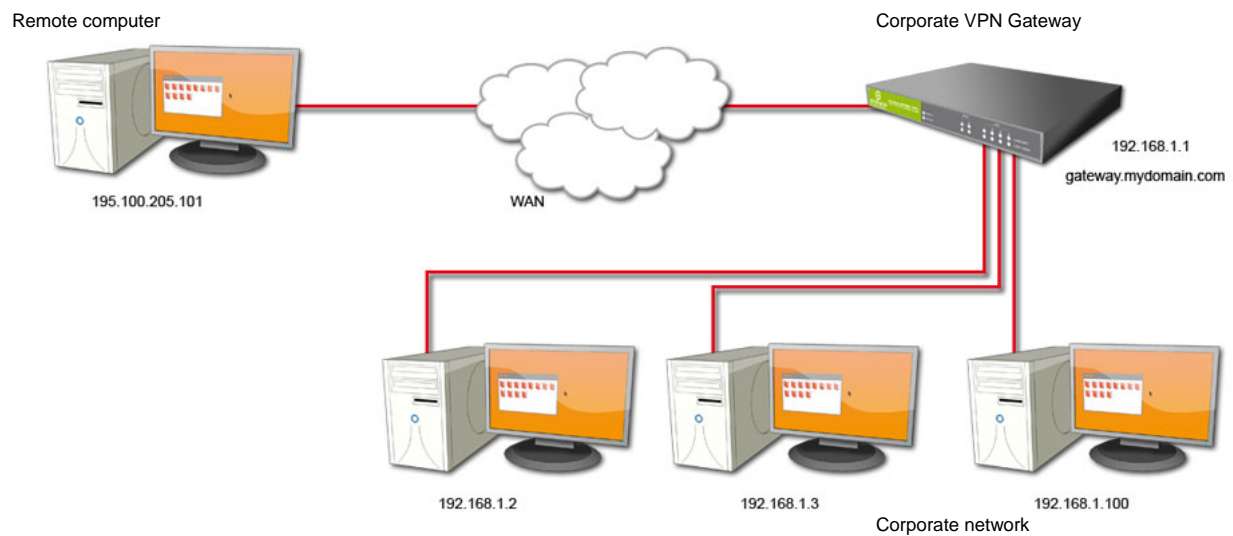
The Syswan VPN Client provides a Configuration Wizard which enables the creation of a VPN configuration in three easy steps. This Configuration Wizard is designed either for remote computers that need to get connected to a corporate LAN through a VPN gateway or Peer-to-Peer mode.

Lets take the following example:

The remote computer has a dynamically provided public IP address.

It tries to connect to the corporate LAN behind a VPN gateway that has a DNS address "gateway.mydomain.com".

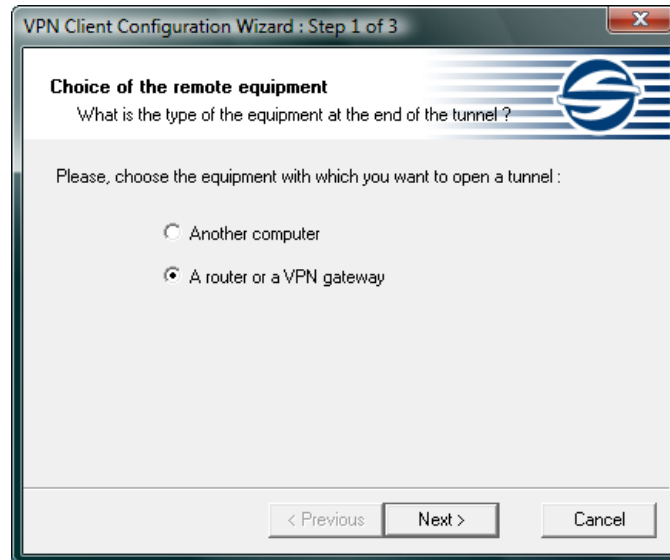
The Corporate LAN address is 192.168.1.xxx. e.g. the remote computer wants to reach a server with the IP address: 192.168.1.100.



For configuring this connection, open the wizard window by selecting menu "Configuration > Wizard"

6.1.2 Step 1 of 3: Choice of remote equipment

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



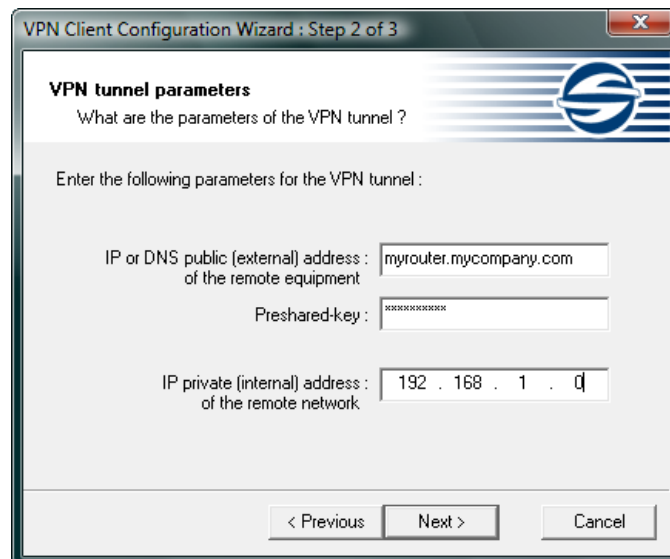
6.1.3 Step 2 of 3: VPN tunnel parameters

You must specify the following information:

- The public (Wide Area Network) address of the remote gateway

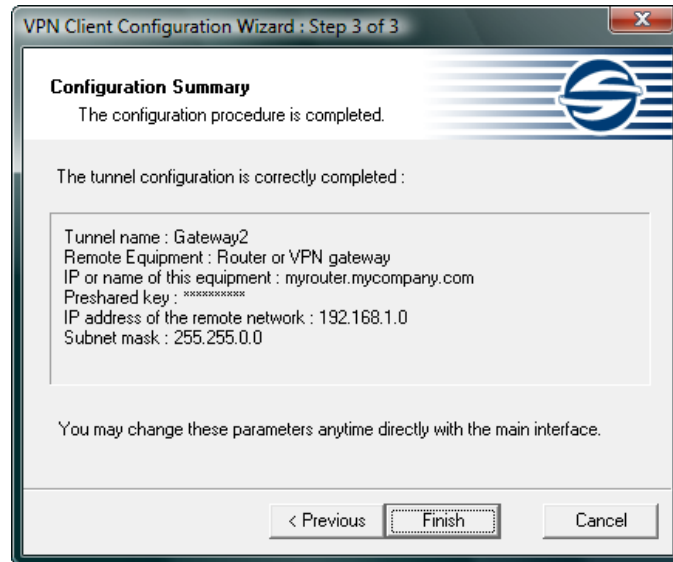
- The preshared key you will use for this tunnel (this preshared key must be the same in the gateway)

- The IP address of your company LAN (e.g. specify 192.168.1.0)



6.1.4 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..).

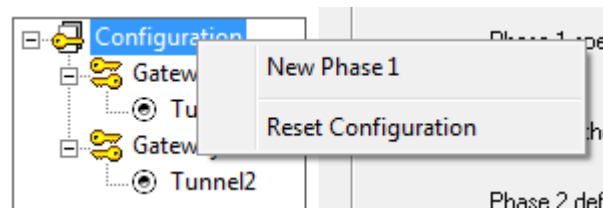


6.2 VPN Tunnel Configuration

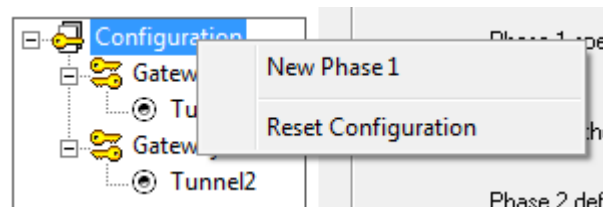
6.2.1 How to create a VPN Tunnel ?

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

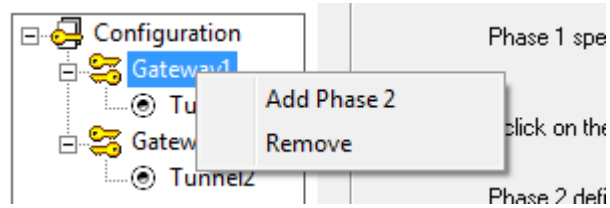
1. Reset Configuration Panel to remove any prior configurations.



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



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



5. Configure IPsec Phase (Phase 2).
6. Once the parameters are set, click on 'Save & Apply' to save the new configuration. The IKE service will run with these new parameters.
7. Click on the 'Open Tunnel' button available on the "IPsec Configuration" window to establish an IPsec VPN tunnel .

Please refer to Phase 1 and Phase 2 for setting descriptions.

6.2.2 Multiple Authentication or IPsec Configuration Phase

Several Authentication Phases (Phase 1) 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).

6.2.3 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

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

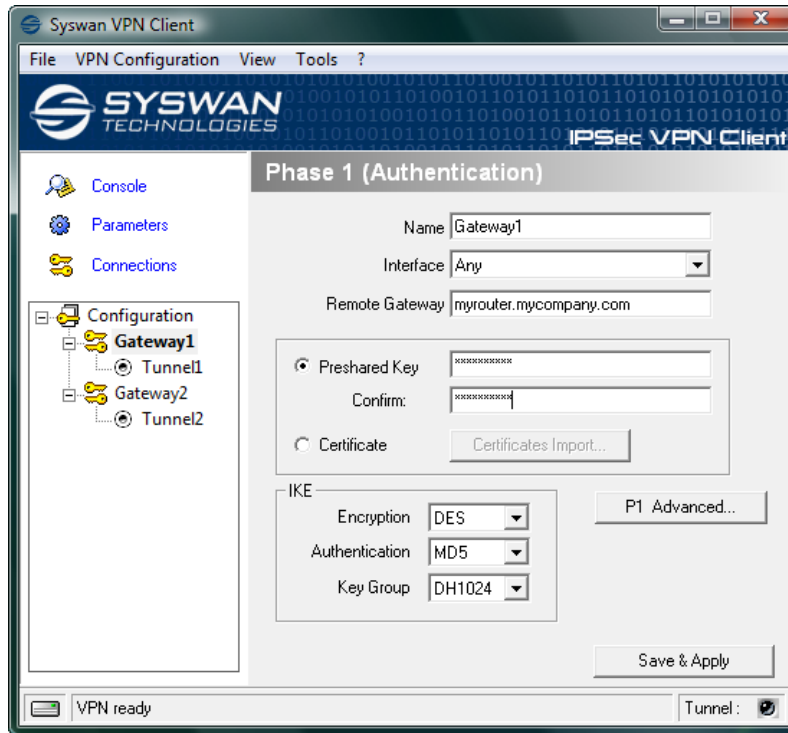
6.3 Authentication or Phase 1

6.3.1 What is Phase 1 ?

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

The purpose of Phase 1' 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.

6.3.2 Phase 1 Settings Description



- Name** Label used only for reference in the configuration user interface. This value is never used during IKE negotiation. It is possible to change this name after initial configuration. No two Phase 1 can have the same name.
- Interface** IP address of the network interface of the computer, through which VPN connection is established. If the IP address changes (ie when it is received dynamically from an ISP), select "Any".
- Remote Gateway** IP address or DNS address of the remote gateway (example: 10.20.0.1 or myrouter.mycompany.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 Import..' to choose the certificate source: PEM files, PKCS#21 file or SmartCard (see section How to configure Certificates). 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, ...).
- IKE key group** Diffie-Hellman key length.

For more advanced settings, click on 'P1 Advanced'.

6.3.3 Phase1 Advanced Settings Description

For advanced features & parameters, click on 'P1 Advanced' button in the Phase 1 panel.

Phase1 Advanced

Advanced features

Config Mode Redund.GW

Aggressive Mode NAT-T

X-Auth

X-Auth Popup Login

Hybrid Mode Password

Local and Remote ID

Choose the type of ID: Set the value for the ID:

Local ID user@mycompany.com

Remote ID myrouter.mycompany.cor

Ok Cancel

Config-Mode

When 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):

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

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 Syswan VPN Client.

Aggressive Mode

When checked, the VPN Client will use aggressive mode as the negotiation mode with the remote gateway.

Redundant GW

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).

Syswan 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.

If the primary gateway can be reached but tunnel establishment fails (e.g. VPN configuration problems) then the VPN Client will not try to establish tunnels with the redundant gateway. Check your configuration.

If a tunnel is successfully established to the primary gateway with the DPD feature (i.e. Dead Peer Detection) negotiated on both sides, when the primary gateway stops responding (e.g. DPD detects non-responding remote gateway) the VPN Client immediately starts opening a new tunnel towards the Redundant Gateway.

The same behavior will apply to the redundant gateway. This means that the VPN Client will try to open primary and redundant gateways until the user exits the software or clicks on 'Save & Apply'.

NAT-T mode

The NAT-T mode allows Forced, Disabled and Automatic.

The NAT-T "Disabled" prevents the IPSec VPN Client and the VPN gateway to start NAT-Traversal.

The NAT-T "Automatic" mode leaves the VPN Gateway and VPN Client negotiate the NAT-Traversal.

In NAT-T "Forced" mode Syswan VPN Client will force NAT-T by encapsulating IPSec packets into UDP frames to solve traversal with intermediate NAT routers.

Local ID

Local ID is the identity the VPN Client is sending during Phase 1 to VPN gateway.

This identity can be:

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. support@Syswan.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 Client's IP address is used.

Remote ID

Remote ID is the identity the VPN Client is expecting to receive during Phase 1 from the VPN gateway. This identity can be:

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

Define the login and password of an X-Auth IPSec 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. The end user has 20 seconds to enter its login and password before X-Auth authentication fails.

If X-Auth authentication fails then the tunnel establishment will fail too.

Hybrid Authentication Mode 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 uni-directionally 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. Syswan IPSec VPN Client implements the RFC 'draft-ietf-ipsec-isakmp-hybrid-auth-05.txt'.

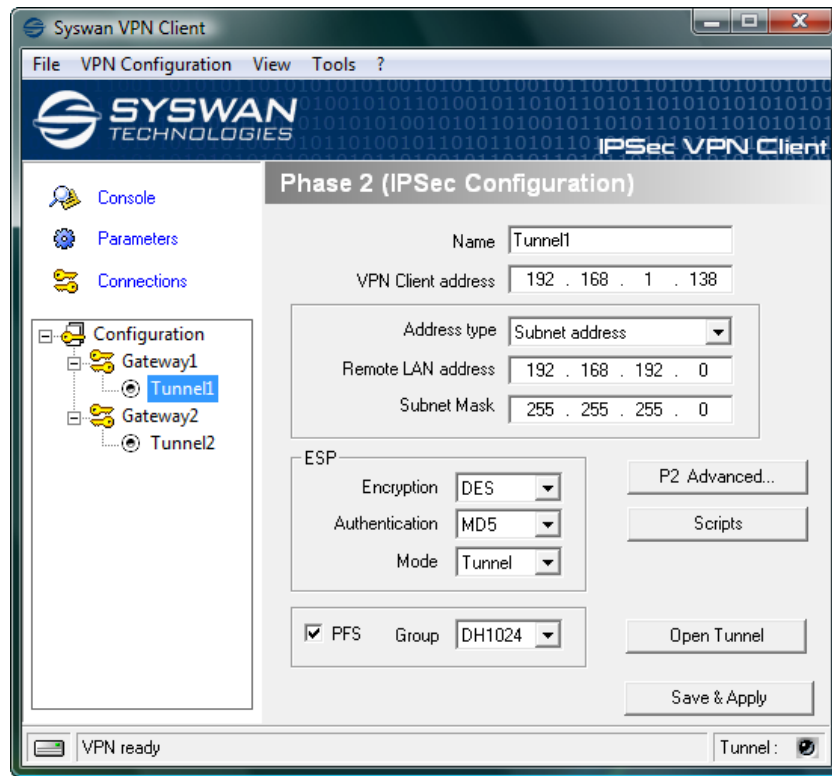
6.4 IPsec Configuration or Phase 2

6.4.1 What is Phase 2 ?

The 'IPsec Configuration' or 'Phase 2' window concerns 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.

6.4.2 Phase 2 Settings Description



- Name** Label used only for reference in the configuration user interface. This parameter is never transmitted during IPsec Negotiation. It is possible to change this name after initial configuration. No two Phase 2 can have the same name.
- VPN Client address** Virtual IP address used by the VPN Client inside the remote LAN: The computer will appear in the LAN with this IP address. **It is important that this IP address does not belong to the remote LAN.** (Example : You should avoid an IP address like 192.168.192.138 if your remote LAN address is 192.168.192.0 and the Subnet Mask is 255.255.255.0).

Address type	<p>The remote endpoint may be a LAN or a single computer, 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 Syswan VPN Client to establish a tunnel only within the range of 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	This field may be "Remote host address" or "Remote LAN address" depending on the address type. It is the remote IP address, or LAN network address of the gateway, that opens the VPN tunnel.
Subnet mask	Subnet mask of the remote LAN. Only available when address type is equal to "Subnet address".
ESP encryption	Encryption algorithm negotiated during IPSec phase (3DES, AES, ...)
ESP authentication	Authentication algorithm negotiated during IPSec phase (MD5, SHA, ...)
ESP mode	IPSec encapsulation mode: tunnel or transport.
PFS group	Diffie-Hellman key length.
Open Tunnel	This button opens the selected tunnel. As soon as the tunnel is opened, this button changes to "Close Tunnel".
Scripts	Scripts may be configured in the Script configuration window.

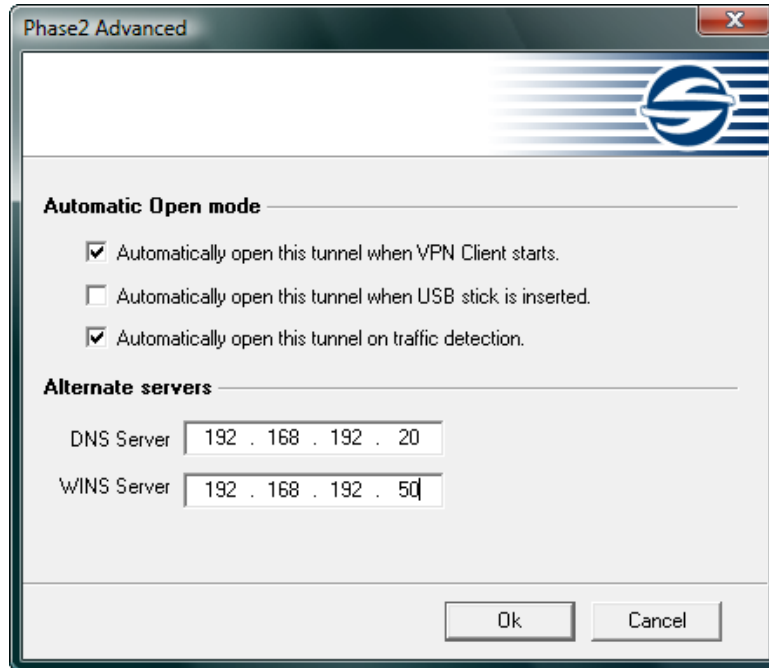
Note: "IP Range" feature combined with "Open tunnel when traffic" feature allows to automatically open tunnel when traffic is detected for a specific range of IP addresses. However, the range of IP addresses must be authorized in the configuration of VPN gateway.

For more advanced settings, click on 'P2 Advanced'.

Once the parameters are set, click on 'Save & Apply' to save and to take into account the new configuration.

6.4.3 Phase2 Advanced Settings Description

For advanced features & parameters, click on 'P2 Advanced' button into Phase 2 panel.

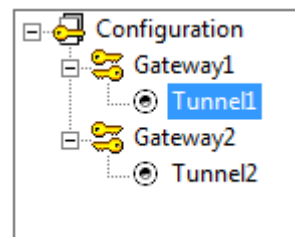


Automatic Open Mode The VPN Client can automatically open the specified tunnel (Phase 2) on specific events such as:

Auto open this tunnel when the VPN Client starts up.

Auto open this tunnel when USB stick is inserted (see section "USB Mode").

Auto open this tunnel when the VPN Client detect traffic towards remote LAN. If selected, the Phase 2 icon in the Configuration Panel tree list changes its shape/color to reflect that this feature is now active:

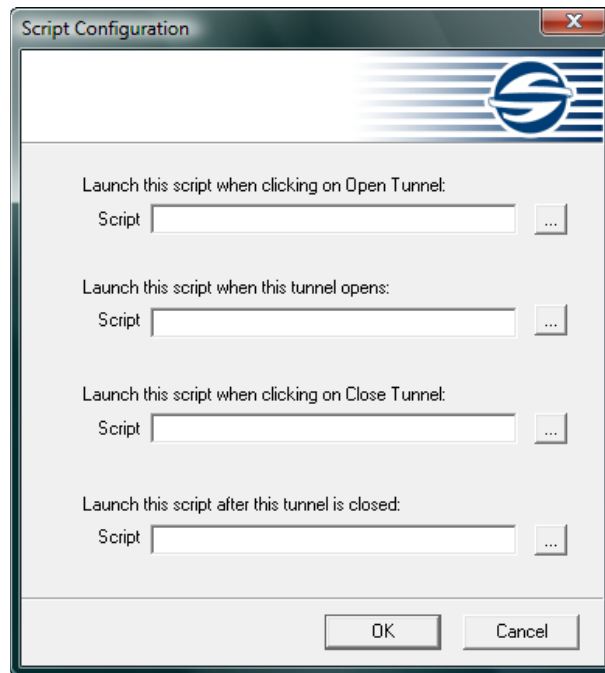


Alternate Servers

DNS and/or WINS server IP addresses of the remote LAN can be entered here, to help users resolve intranet addressing. The DNS or WINS addresses are taken into account as soon as the tunnel is opened, and for as long as it remains open.

6.4.4 Script configuration

Scripts may be configured in the Script configuration window. This window can be opened through the button 'Scripts' of a Phase 2 Settings window.



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

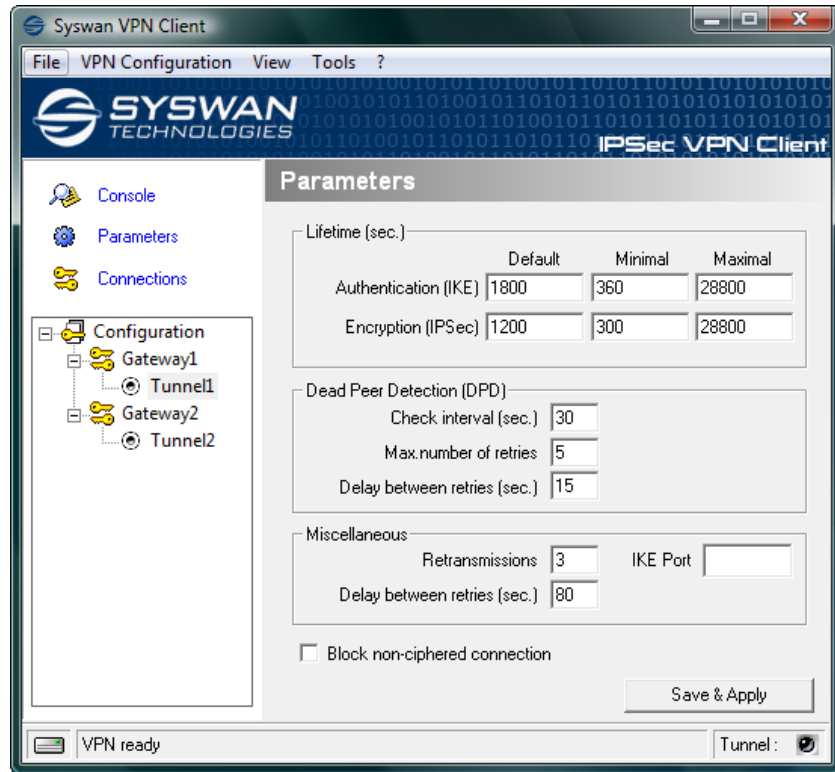
This feature enables to execute scripts (batches, scripts, applications...) at each step of a tunnel connection for a variety of purposes e.g. to check current software release, to check database availability before launching backup application, to check a software is running...

It also enables to configure various network configuration before, during and after a tunnel connection.

6.5 Global Parameters

6.5.1 Global Settings Description

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



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.
	Delay between retries	Minimum time before any attempts by user to restart IKE negotiation.
	Block non-ciphered connection	When this option is checked, only encrypted traffic is authorized.
	IKE Port	User can change port number for IKE negotiation. Exchanges are still on UDP but they can be on another port other than 500 as some firewalls do not allow IKE Port 500. The remote gateway must support this feature.

Dead Peer Detection (i.e. DPD) is an Internet Key Exchange (IKE) extension (i.e. RFC3706) for detecting a dead IKE peer. Syswan IPSec VPN Client uses DPD:

- to delete opened SA in the VPN Client when a peer has been detected dead.
- to re-start IKE negotiations with the Redundant Gateway if activated in the 'Phase 1 Advanced' Configuration Panel.

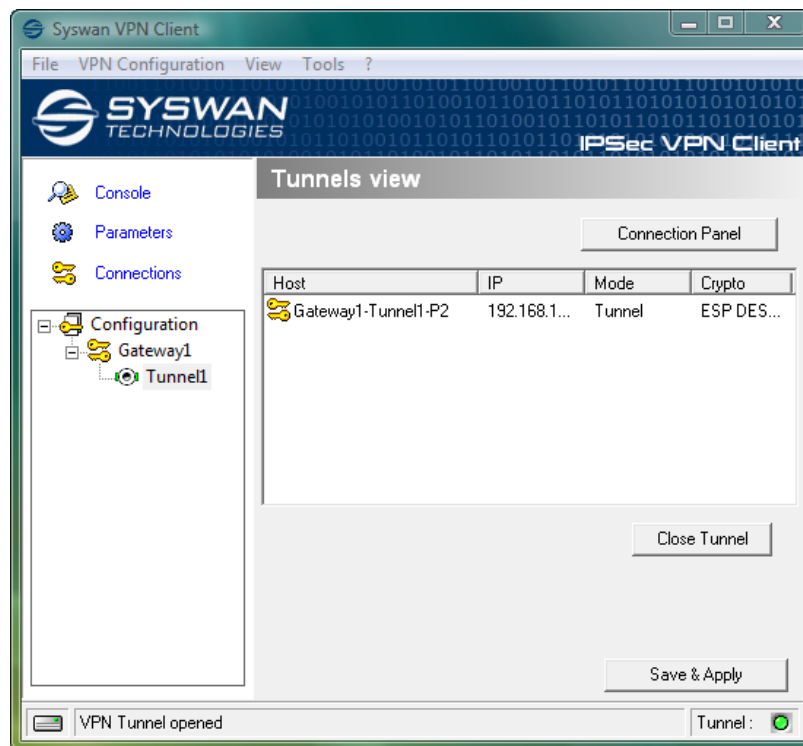
Once the parameters are set, click on 'Save & Apply' to retain the new configuration.

6.6 VPN Tunnel View

6.6.1 How to view opened tunnels ?

'Tunnel View' screen shows VPN tunnels that are currently open. This screen may also be used to close opened tunnels. To close a VPN tunnel, select the tunnel in the list and click on 'Close Tunnel'. Tunnels may also be viewed, opened and closed directly from the context menu of the system tray icon and from the Connection Panel.

The Connection Panel can be opened with the button "Connection Panel". It is possible to switch between the Connection Panel and the Configuration Panel with the shortcut key "Ctrl+Enter" (see section 'Shortcuts').



6.7 USB Mode

6.7.1 What is USB Mode ?

The Syswan VPN Client gives the possibility to secure VPN configurations and security elements (e.g. PreShared key, Certificates...) by the use of an USB Stick.

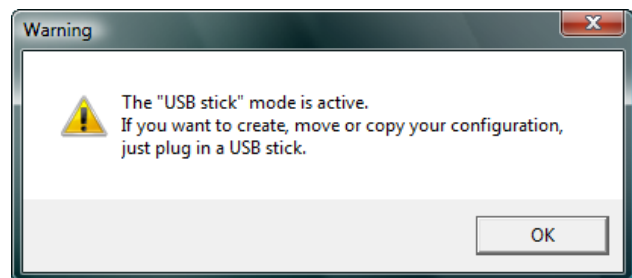
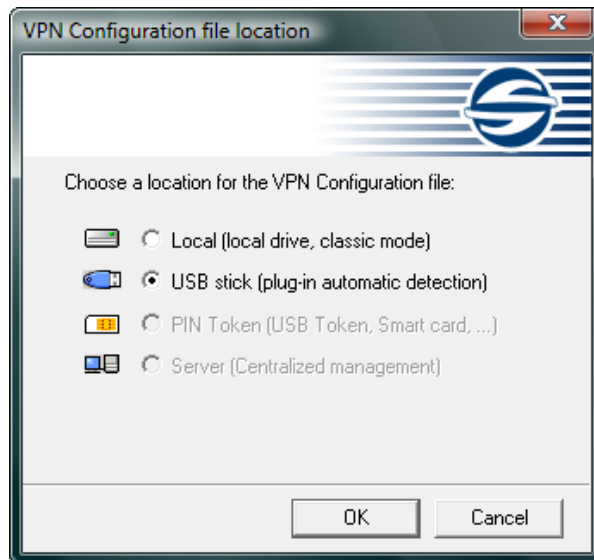
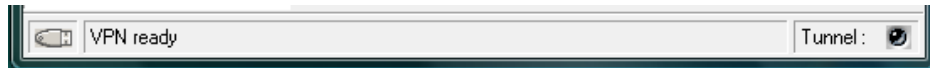
When you select "USB mode", the VPN configuration and security elements contained into the configuration are stored onto the USB Stick the first time you plug it in.

When complete, you just need to insert the USB Stick to automatically open tunnels. And then unplug the USB Stick to automatically close any established tunnels.

6.7.2 How to set USB Mode ?

The USB Mode can be set by clicking on the 'USB Stick' icon in the status bar of the Configuration Panel or via the menu:

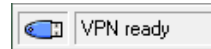
- Select menu 'File' > 'VPN Configuration File...'
- Select 'USB Stick'



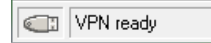
Note: At this stage, if an USB Stick containing a VPN configuration and security elements is already plugged in, the associated drive will be automatically recognized. Please note also that it is not necessary to insert an USB Stick during this step. In case no USB Stick is plugged in, the following warning window will appear:

Once USB mode is set, the left side box in the status bar shows a USB stick icon.

The USB Stick icon is blue when a USB Stick is plugged in:



The USB Stick icon is gray when no USB Stick is plugged in:



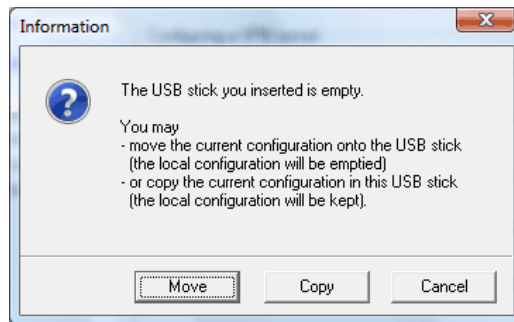
6.7.3 How to enable a new USB Stick ?

A blank USB Stick (new or freshly formatted) is enabled by copying VPN configuration and security elements onto it.

When you insert a new USB Stick, the IPsec VPN Client automatically proposes to enable the USB Stick through the following options:

Copying the VPN configuration and security elements onto the USB Stick: the VPN Client will copy the security information onto the USB Stick and leave a copy in the computer. This feature is specially designed for IT managers to enable multiple USB Sticks for multiple users in no time.

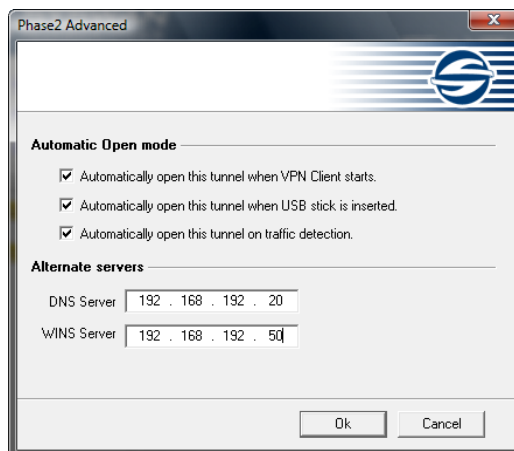
Moving the configuration onto the USB Stick: the IPsec VPN Client will copy the security information onto the USB Stick and remove all security information from the computer. This method is used to secure a computer once the VPN configuration has been setup.



6.7.4 How to automatically open tunnels when a USB Stick is plugged in ?

Each and every tunnels may be configured individually:

In the IPsec Configuration (Phase 2) of the relevant tunnel, click on 'P2 Advanced' button
 Select the 'Automatically open this tunnel when USB stick is inserted' mode



6.8 Certificate Management

6.8.1 Certificate Management overview

The Syswan VPN Client can use Certificates from PEM files, PKCS#12 file or SmartCard.

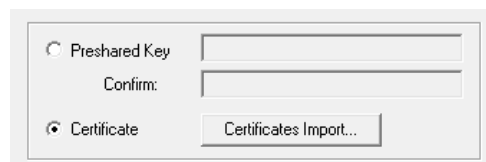
Note: Syswan VPN Client does not allow creation of Certificates. Certificates must be created (and stored on SmartCard) by a third party software. You will find additional support documents on "How to generate Certificates" or "How to convert Certificate formats" on our web site.

6.8.2 How to configure IPsec VPN Client with PKCS#12 Certificates

PKCS#12 certificates are supported by a lot of gateways. Syswan IPsec VPN Client can import PKCS#12 certificates into the VPN Configuration, directly from the main interface. One PKCS#12 certificate can be defined per tunnel. Therefore, it is possible to connect to several gateways that do not use the same PKI (Public Key Infrastructure).

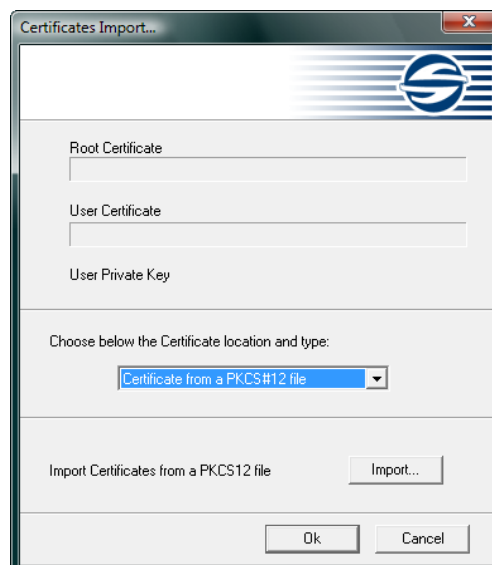
Here are the steps to configure the IPsec VPN Client with **PKCS#12 Certificates**:

Step 1: Select radio button 'Certificate' in the 'Phase 1' window and click on 'Certificates Import...'



Step 2: Select 'Certificate from a PKCS#12 file' in the list box, then click on the 'Import...' button.

Step 3: Select the PKCS#12 Certificates you want to import. If the PKCS#12 Certificate is protected, enter the password in the password pop up window. Once the Certificate is correctly imported, its subject is automatically displayed in the top fields of the 'Certificates Import ...' window. Also, key icons are displayed next to each certificate component (root certificate, user certificate, private key) as shown below.



Step 4: PKCS#12 Certificates will be stored in the VPN Configuration file as soon as you click on "Save & Apply".

Note: Once the Certificate is imported, its subject is used for the local ID of the associated Phase 1. This is shown in the P1 Advanced window with the following indication:

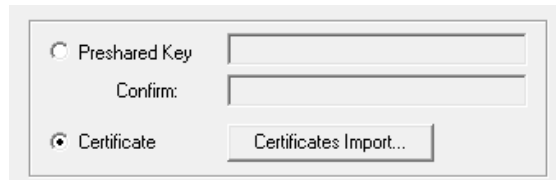
Local and Remote ID	
Choose the type of ID:	Set the value for the ID:
Local ID	local
Remote ID	

6.8.3 How to configure IPsec VPN Client with PEM Certificates

Syswan IPsec VPN Client can import PEM Certificates into the VPN Configuration directly from the Configuration Panel. One PEM Certificate can be defined per tunnel. Therefore, it is possible to connect to several gateways that do not use the same PKI (Public Key Infrastructure).

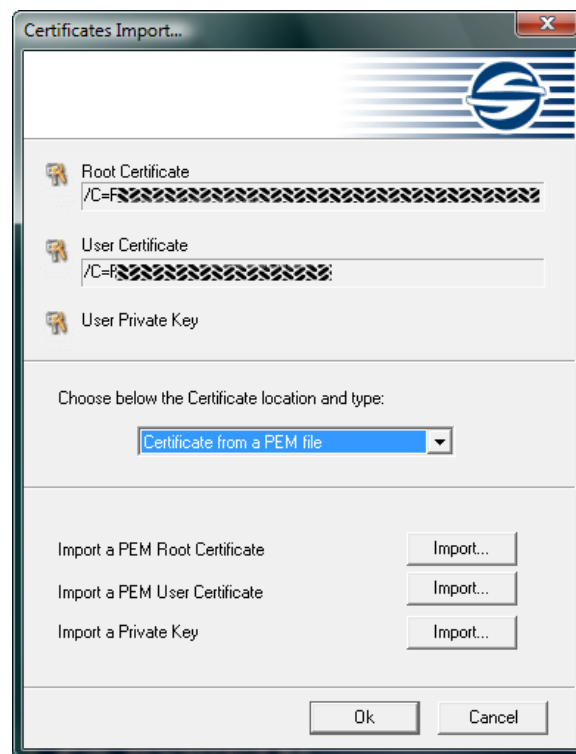
Here are the steps to configure the IPsec VPN Client with PEM Certificate

Step 1: Select radio button 'Certificate' in the Phase 1 window and click on 'Certificates import...'



Step 2: Choose "Certificate from a PEM file" in the list box

Step 3: Import the Root Certificate, the User Certificate and the Private Key by clicking on the associated button. Once the certificate is correctly imported, its subjects are filled in the 'Certificate Import...' window.



Step 4: PEM Certificates will be stored in the VPN Configuration file as soon as you click on "Save & Apply".

Once the Certificate is imported, its subject is used for the local ID of the associated Phase1. This is shown in the P1 Advanced window with the following indication:

Local and Remote ID		
	Choose the type of ID:	Set the value for the ID:
Local ID	Subject from X509	local
Remote ID		

Note: The PEM file enclosing the private key must not be encrypted or protected with a password.

6.8.4 Smart Card and Token Management

How to configure a tunnel with Certificates from a Smart Card

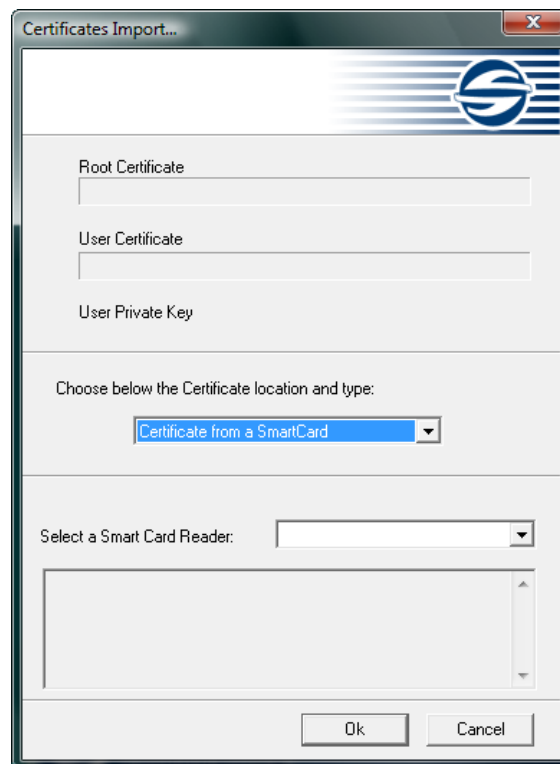
The Syswan VPN Client can read Certificates from Smart Cards. Smart Cards can be used for securing X509 certificates that can be protected by a PIN code.

Here are the steps to configure a tunnel using Certificates from Smart Cards:

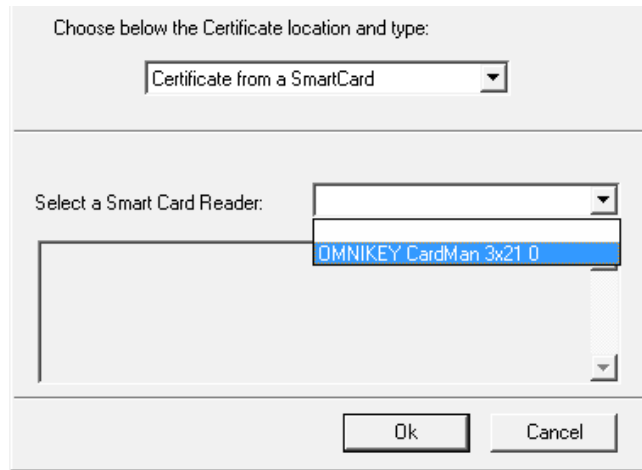
Step 1: Select radio button 'Certificate' in the 'Phase 1' window and click on 'Certificates Import...'



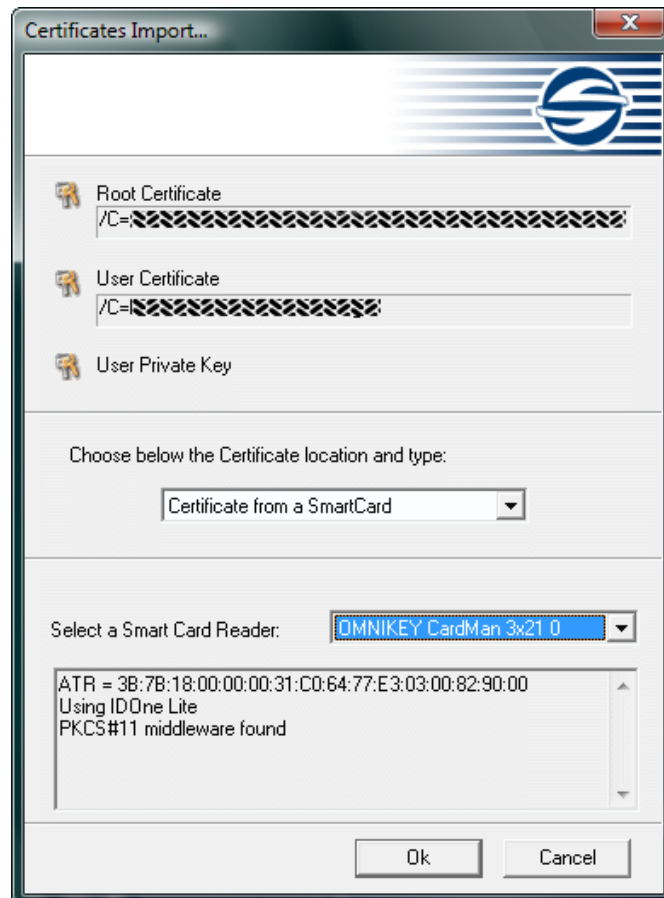
Step 2: Select 'Certificate from a Smart Card' in the list box. The bottom part of the window shows a list of Smart Card Reader.



Step 3: Select the Smart Card Reader you want to use. The Smart Card Reader identification process starts and a PIN code may be required. Enter your 'Smart Card PIN code' and click 'OK'.



Once the Smart Card is successfully read, information about the Smart Card Reader and the Smart Card are displayed in the text area below the list box, while the subjects of the Certificates are displayed in the top two fields of the window:



Step 4: Smart Card Reader information will be stored in the VPN Configuration file as soon as you click on "Save & Apply".

How to use a tunnel with Certificates from a Smart Card

When a tunnel is configured to use Certificates from a Smart Card, the PIN code of the Smart Card is required each time the tunnel is opened (excepted on automatic VPN renegotiations).

To open a tunnel with Certificates from a Smart Card, it is required to have:

1. The Smart Card Reader correctly installed and configured in the IPsec VPN Client
2. A readable Smart Card inserted in the Smart Card Reader
3. The correct PIN code for reading the Smart Card.

Each problem encountered when using a Smart Card is displayed in the Software Console. See section 'Smart Card Troubleshooting' below.

Smart Card Troubleshooting

Users may encounter issues while configuring Smart Card and Smart Card Readers.

Smart Card Trouble	Message displayed (*)
No Smart Card Reader is found	No smart card found
If no Smart Card is found, it is probably because the SmartCard Reader middleware is missing. The procedure to easily add a Smart Card Reader middleware is displayed in the text area below the list box.	No ATR Unknown ATR: this smart card may not be supported. No PKCS#11 middleware for this smart card was found. You can set PKCS#11 middleware with the command line: Vpnconf.exe /addmiddleware:path_to_the_dll
The Smart Card cannot be read	ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Using IDOne Lite PKCS#11 middleware found Error 0x00000015
The PIN code is wrong	ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Using IDOne Lite PKCS#11 middleware found Wrong PIN code
No certificate can be found in the Smart Card	ATR = 3B:7B:18:00:00:00:31:C0:64:77:E3:03:00:82:90:00 Using IDOne Lite PKCS#11 middleware found No configuration or no certificate found in the smart card

(*) Message displayed in the text area below the Smart Card listbox.

Users may encounter issues while opening a tunnel which requires Certificates on a Smart Card.

Smart Card Trouble	Message displayed in the Console.
No Smart Card Reader is found	Missing Smart Card Reader
The PIN code is wrong	Wrong PIN code
No certificate can be found in the Smart Card or The Smart Card cannot be read	Empty or unreadable Smart Card

6.9 Configuration Management

6.9.1 Import or Export VPN Configuration via menu

The Syswan 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 "File > Import VPN Configuration".

Exporting a configuration, select menu "File > Export VPN Configuration".

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

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



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: Import/Export in 'USB Mode'

When the Syswan VPN Client is configured in "USB Mode" and when a USB stick is inserted, the importation of a VPN Configuration is directly written on the USB stick. If the VPN Client is configured in "USB mode" but no USB stick is inserted (the USB icon in the bottom left corner of the GUI is disabled), the exportation and importation of a VPN Configuration are disabled.

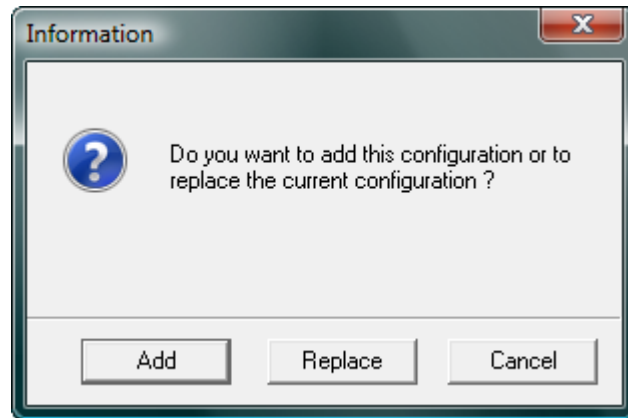
Note: A VPN Configuration file can also be imported via the command line.

6.9.2 Merging VPN Configurations

Syswan IPsec VPN Client 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.

Merging VPN Configurations can be done in several ways.

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



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 does not handle relative paths (e.g. "..\..\file.tgb"). For more details, see import command line section.

Any way you choose to import a VPN Configuration, here are some 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.

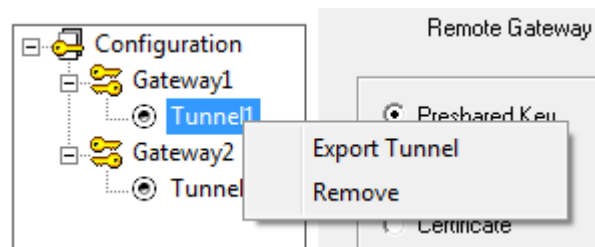
Tunnel name conflict between existing and imported VPN Configurations are solved by software automatically by adding an increment between bracket e.g. tunnel_office(1) to the imported tunnel names (i.e. both Phase1 and Phase 2).

6.9.3 Splitting a VPN Configuration

The Syswan 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:

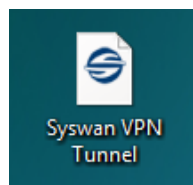
1. Right click on any tunnel Phase 2 from your VPN Configuration, then select 'Export Tunnel'.



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



3. Once exported, the VPN Configuration can be sent to users. Any VPN Configuration can be double clicked to directly launch the Syswan IPsec 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.

Export of a Phase 2 will export the Global Parameters as well.

7. Deployment

7.1 Embedded VPN Configuration

A pre-created VPN Configuration may be enclosed into the Syswan VPN Client Setup.

Enclosing VPN Configuration within the Syswan VPN Client Setup enables IT manager to deploy pre-configured IPSec VPN Client software in a single package to all company users.

A VPN Configuration ".tgb" file embedded within the IPSec VPN Client Setup folder (see 'Deployment Guide' description on our web site) is automatically imported by the IPSec VPN Client during software installation.

The process to create a setup with a VPN Configuration is as follows:

1. Create the VPN Configuration that needs to be embedded into the Setup. This step must be processed from a formerly installed IPSec VPN Client, from which the VPN Configuration is exported (e.g. "myconfig.tgb").
2. Create a silent installation, or copy the Syswan VPN Client Setup into a setup folder.
3. Add the VPN Configuration (e.g. "myconfig.tgb") file into the same folder.
4. Deploy the package to the user. The VPN Configuration found in the folder will be added 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 encryption (without being protected with a password).

7.2 Setup options

7.2.1 Setup option overview

Several options are available with the IPSec VPN Client Setup:

1. Configuration of the GUI mode: 'full', 'user' or 'hidden'
2. Protection of the GUI mode Access Control with password
3. Configuration of the Systray menu items.
4. Other options for Software Start, License Number and Activation email

Command line syntax example:

```
Setup.exe -s --license=0123456789ABCDEF0123 --start=boot --activmail=admin@mycompany.com
```

Warning:

All the switches '--gui', '--menuitem', '--license', '--start', '--activmail' can only be used with the switch '-s' (silent mode install).

7.2.2 Setup option for GUI mode

Syntax: **--vpngui=full|user|hidden**

enables to define the GUI appearance when the IPsec 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.

Remark:

--vpngui=hidden is equivalent to option **--hide=yes**. This option can still be used (as it is maintained for compatibility reasons).

7.2.3 Setup option for GUI mode access control

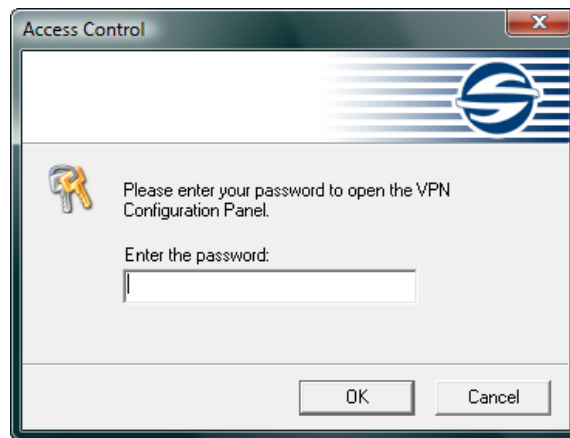
Syntax: **--password=mypwd**

Control the access to the VPN GUI with a password.

The user will be asked for a 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.



Example: **--vpngui=user --password=admin01**

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

7.2.4 Setup option for systray menu items

Syntax: **--menuitem=[0...15]**

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**.

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

Note 1: the tunnels are always shown in the systray menu, and can always be opened and closed from this systray menu.

Note 2: **'menuitem'** and **'vpngui=hidden'**.

By default, **vpngui=hidden** (or **hide=yes**) will 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 **'vpngui'**. This means that: **"--vpngui=hidden --menuitem=1"** will set a systray menu with only the 'Quit' item.

7.2.5 Other Setup options

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

Syntax: **--license=[license_number]**

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

Syntax: **--start=[logon|boot|manual]**

Allows the configuration of the start mode for the VPN Client: after the logon windows, during the boot, or manually. Default is [logon].

Syntax: **--activmail=[activation_email]**

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

Example:

Setup -s --license=0123456789ABCDEF0123 --start=boot --activmail=admin@mycompany.com

7.3 Command line

7.3.1 Command line options

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

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

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

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

" [path]vpnconf.exe /stop " where **[path]** is the IPsec 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 launches the VPN Client after establishing a dialup connection and exits it just before disconnection.

7.3.3 Import or Export VPN Configuration options

Syswan 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 does not 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.

" **/importance:** " imports a VPN configuration file without running the VPN Client. This command is especially useful in installation scripts: it runs a silent installation and imports a configuration automatically.

" **/replace:** " replaces 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 /importance option to import a VPN configuration file without running the VPN Client.

" **/export:** " exports the current VPN Configuration (including certificates) in the specified file. This command start the VPN Client if it is not already running.

" **/exportonce:** " exports the current VPN Configuration (including Certificates) in the specified file. This command does not start the VPN Client if it is not already running.

" **/add:** " imports a new VPN Configuration into an existing VPN Configuration and merge both into one single VPN Configuration. This command line may be used whether the VPN Client is running or not. This command does not start the VPN Client if it is not already running.

All 6 arguments "**import**", "**importance**", "**export**", "**exportonce**", "**replace**" and "**add**" are exclusive and cannot be used together.

7.3.4. Opening or closing VPN Tunnel options

The Syswan VPN Client can open or close a VPN tunnel by the command line. Both command lines can be invoked while Syswan IPsec 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. This command does not handle relative paths (e.g. "..\..\file.tgb"). Double-quotes are supported, allowing paths containing spaces.

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. This command doesn't handle relative paths (e.g. "..\..\file.tgb"). Double-quotes are supported allowing paths containing spaces.

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

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

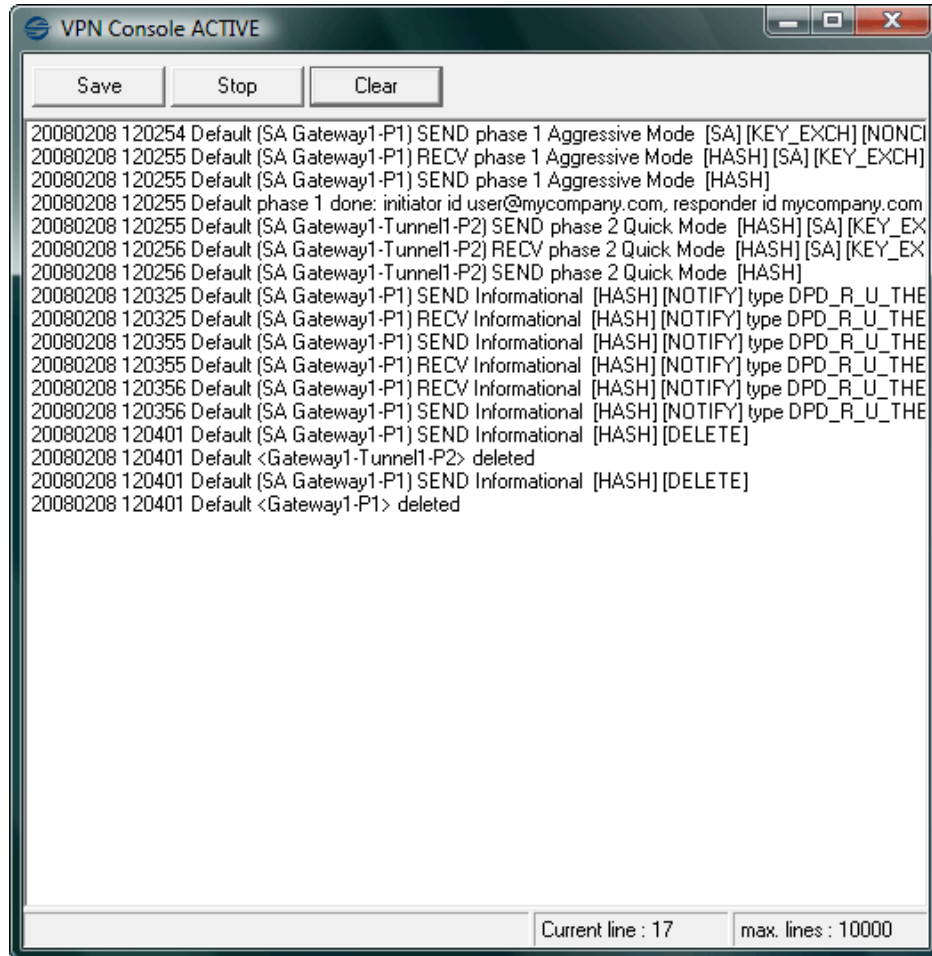
Restriction note:

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

8. Console and Logs

8.1 Console Windows

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



Button	Description
Save	Save current logs in a file. Future logs will not be saved in the selected file.
Start/Stop	Start/Stop collecting logs.
Clear	Clear console window content

9. Connecting to a Syswan Duolinks SW24 VPN series Load Balancer

9.1 Requirements

This section is intended for IT managers and network administrators.

It provides a comprehensive guide on how to configure your Syswan Duolinks SW24 VPN series load balancer and a remote IPSec VPN configuration using the Syswan VPN Client software, including the configuration of a redundant gateway.

If you are not familiar with network configurations and related tasks, please contact your IT manager or network administrator for assistance.

Requirements to implement this example VPN configuration :

1. A Syswan Duolinks SW24 VPN or a Syswan Duolinks SW24 VPN Plus load balancer with basic configuration and at least one WAN link connected to the Internet.
2. A computer on the load balancer network or a remote computer with Internet access for VPN configuration on the Syswan Duolinks SW24 VPN series load balancer.
3. A remote computer on another network with Internet access and no firewall restrictions for IPSec traffic.
4. Syswan VPN Client software.

All data given in this VPN network configuration are given as example only.

You will need to replace this information to suit your network settings and configuration.

Corporate network settings :

WAN Link 1	:	10.20.0.1	Your WAN Link 1	:	_____
WAN Link 2	:	10.30.0.1	Your WAN Link 2	:	_____
Local LAN	:	192.168.192.0	Your local LAN	:	_____
Subnet Mask	:	255.255.255.0	Your Subnet Mask	:	_____

Remote network settings :

Remote LAN	:	192.168.1.0	Your remote LAN	:	_____
Remote Pc	:	192.168.1.100	Your remote Pc	:	_____

Other required settings :

User ID	:	user@mycompany.com	Your user ID	:	_____
Preshared Key	:	1234567890	Your Preshared Key	:	_____

Important note:

During IKE Phase 1 activation, your load balancer will need to reboot as you will be changing primary settings.

9.2 Configuring the Syswan Duolinks SW24 VPN series Load Balancer

First, login to your Syswan Duolinks SW24 VPN Series load balancer.

Step 1 :

Go to “VPN Configuration > IKE Global setup” page.

Enable both WAN links and make sure that Phase 1 DH Group is set to DH Group 2 (1024-bit), Encryption Method is set to DES and Authentication Method is set to MD5.

You may leave all other settings on this page as default.

Choose “Submit and Reboot” to save your IKE configuration.



www.syswan.com/support



IKE Global Setup



Basic Configuration
Advanced Port
Advanced Configuration
Security Management
VPN Configuration
IKE Global Setup
IPSec Policy Setup
VPN Logs
QoS Configuration
Management Assistant
Network Info

Global List (Phase 1)					
WAN	State	ISAKmp Port	DH Group	Encryption Method	Authentication Method
WAN 1	Enabled	500	DH Group 2 (1024-bit)	DES	MD5
WAN 2	Enabled	500	DH Group 2 (1024-bit)	DES	MD5

Global Parameters	WAN 1
Enable Setting	<input checked="" type="checkbox"/>
ISAKmp Port	500
Phase 1 DH Group	DH Group 2 (1024-bit) ▾
Phase 1 Encryption Method	DES ▾
Phase 1 Authentication Method	MD5 ▾
Phase 1 SA Lifetime	28800 Seconds
Retry Counter	5
Retry Interval	10 Seconds
Maxtime to complete Phase 1	180 Seconds
Maxtime to complete Phase 2	120 Seconds
Count Per Send	1
NAT Traversal Port	4500

Log Level
Log Level

Tunnel Action
All Tunnels

Important note:

During IKE Phase 1 activation, your load balancer will need to reboot as you will be changing primary settings.

Remember these settings as they must match those in the Phase 1 settings of your Syswan VPN Client software.

Step 2 :

Once step 1 is completed, go to “VPN Configuration > IPSec Policy Setup” page

Choose “New Policy” and create a VPN Configuration for WAN1 as per following screen capture.

Click “Add” when done :

Information required in this example :

- Local Security Network : Type Subnet / IP 192.168.192.0 / Mask 255.255.255.0
- Remote Security Network : Any
- Remote Security Gateway : Distinguished ID / user@mycompany.com
- Encryption Method : DES / Authentication Method : MD5
- Key Type : Autokey(IKE)
- Perfect Forward Secrecy : DH Group 2 (1024-bit) / Preshared Key : 1234567890

Remember these settings as they must match those in the Phase 2 settings of your Syswan VPN Client software.

Step 3 :

If you have a second WAN link connected to your load balancer, you may choose to activate the “Redundant Gateway” option on the Syswan VPN Client.

In order to benefit from the Redundant Gateway option for your remote user, you will need to create a second VPN configuration for the same user pointing to WAN 2 on your Syswan Duolinks SW24 VPN series load balancer.

Choose “New Policy” and create a second VPN Configuration for the same remote user.

Everything in the second configuration will be identical to the first one. You will need to define a new name for this configuration and change the “Traffic Binding Interface” to WAN 2 as the example screen capture below:



www.syswan.com/support



IPSec Policy Setup



Basic Configuration		Traffic Binding		Local Identity Option	
Advanced Port Advanced Configuration Security Management VPN Configuration		<input type="button" value="New Policy"/>	Name: Roaming-W2 State: <input checked="" type="checkbox"/> Enabled	Interface: WAN 2 Session: Session 1	Type: IP Address
Traffic Selector					
Protocol Type	Any				
Local Security Network	Local Type: Subnet	IP Address: 192.168.192.0	Subnet Mask: 255.255.255.0	Port Range: 0 ~ 0	
Remote Security Network	Remote Type: Any				
Remote Security Gateway	Identity Type: Distinguished ID, user@mycompany.com				
Security Level					
Encapsulation Format	ESP				
Encryption Method	DES				
Authentication Method	MD5				
Key Management					
Key Type	Autokey (IKE)				
Phase 1 Negotiation	Aggressive Mode				
Perfect Forward Secrecy	DH Group 2 (1024-bit)				
Preshared Key	1234567890			Characters / Hex:0x	
Key Lifetime	In Time	3600	Seconds	Note : 0 for no expiry	
	In Volume	0	Kbytes		
Action					
<input type="button" value="Connect"/> <input type="button" value="Flush Tunnel"/> <input type="button" value="Reload Policy"/> <input type="button" value="Tunnel Status .."/> <input type="button" value="Set Options .."/>					
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Update"/> <input type="button" value="Refresh"/>					

Click “Add” when done.

The configuration of your Syswan Duolinks SW24 VPN series load balancer is now complete. Next, you will need to configure the Syswan VPN Client software on the remote user’s PC with the same Phase 1 and Phase 2 information.

9.3 Configuring the Syswan VPN Client

Make sure that the Syswan VPN Client software is installed on the remote computer.

You will find this software on the CD ROM included with your purchase.

You may also download the latest version of the Syswan VPN Client from our web site (<http://www.syswan.com>).

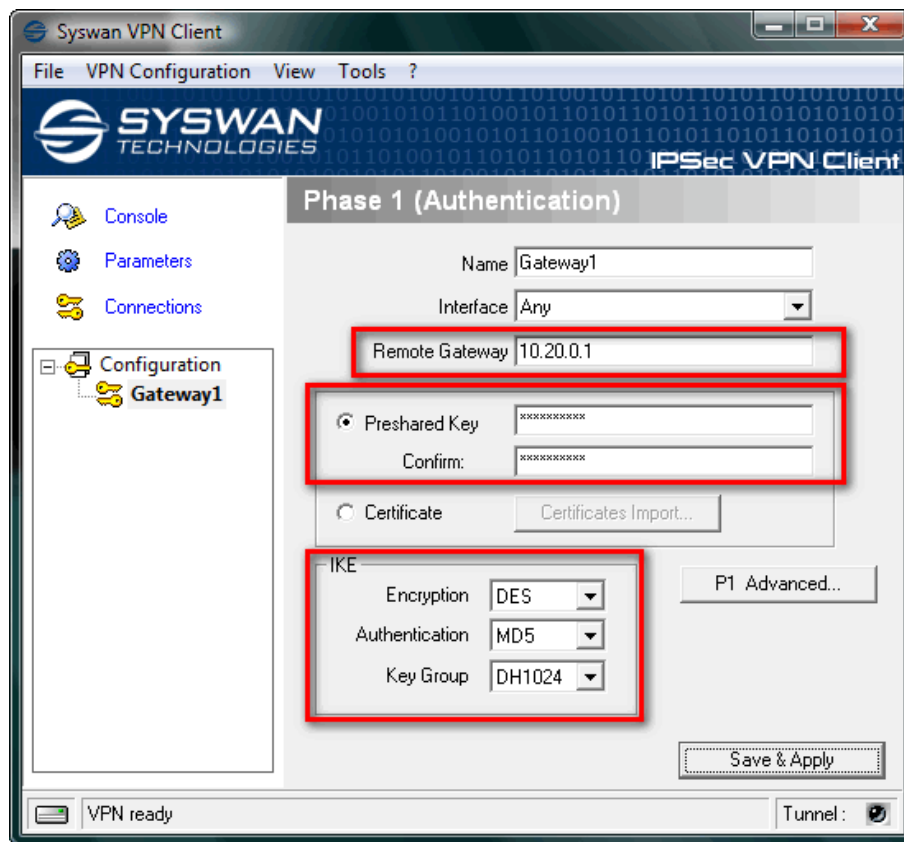
Step 1 : Phase 1 configuration

Open the Syswan VPN Client software user interface.

Right click on “Configuration” and select “New Phase 1”

Enter your remote gateway IP address (WAN Link 1 IP address of your Syswan Duolinks SW24 VPN series load balancer. Example : 10.20.0.1)

Make sure that you enter correctly the previously defined preshared key as well as the other IKE options for Phase 1 here. (Example : 1234567890, DES, MD5 and Group2-DH1024).



Click “Save & Apply”.

Now select “P1 Advanced”.

In the P1 Advanced screen, select “Aggressive Mode”.

In Redund.GW enter the second IP address of your remote gateway (WAN Link 2 IP address of your Syswan Duolinks SW24 VPN series load balancer. Example : 10.30.0.1)

The Local ID type must be defined as “Email” as the previously defined settings.

Enter the email address as the ID value (Example : user@mycompany.com).

Phase1 Advanced

Advanced features

Config Mode

Aggressive Mode

Redund.GW: 10.30.0.1

NAT-T: Automatic

X-Auth

X-Auth Popup

Hybrid Mode

Login: _____

Password: _____

Local and Remote ID

Choose the type of ID: Local ID: Email

Set the value for the ID: user@mycompany.com

Remote ID: _____

Ok Cancel

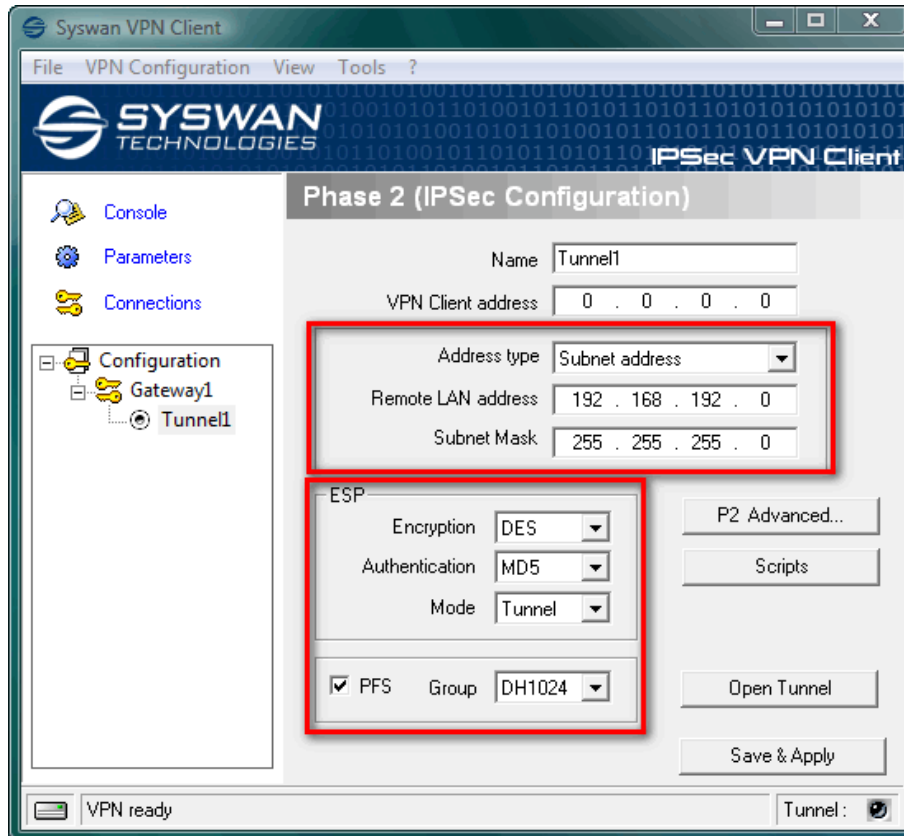
Click “Ok” and then “Save & Apply”.

Step 2 : Phase 2 configuration

Create a Phase 2 configuration by right clicking on the Phase 1 setting and choosing “Add Phase 2”.

Change the address type to read “Subnet address”.

Add the remote LAN address and the subnet mask. (example: 192.168.192.0 / 255.255.255.0)



Make sure that ESP Algorithms and PFS/DH Group match the previously defined settings. (Example : DES, MD5 and PFS/DH Group2-DH1024).

Note : Most SMB networks are configured with a subnet mask of 255.255.255.0 to permit one private Class C network. A Class C network will provide 253 IP V4 addresses which is enough for these types of networks. If you do not know or are not sure of your subnet mask, please contact your IT manager or network administrator for assistance.

The VPN Client Address should not belong to the remote network subnet range (ie: to the 192.168.192.0/24 network in our example). If you leave the default settings of 0.0.0.0, the VPN Client Address will be the same as the physical address of the remote machine either directly by the ISP or by a remote network.

If the remote network subnet range is equal to your corporate network subnet, then the remote user VPN connection will not be established. In this case, you must manually specify another IP address from another subnet range (ie 192.168.1.1 or 10.0.0.1) in the VPN Client address field.

When complete, click “Save & Apply”.

Note : You can optionally use the “Phase 2 Advanced” options to define tunnel opening modes and declare alternate DNS and/or WINS servers prior for this tunnel.

9.3 Opening the IPSec VPN Tunnel

Make sure that your local firewall permits IPSec traffic from within your remote network.

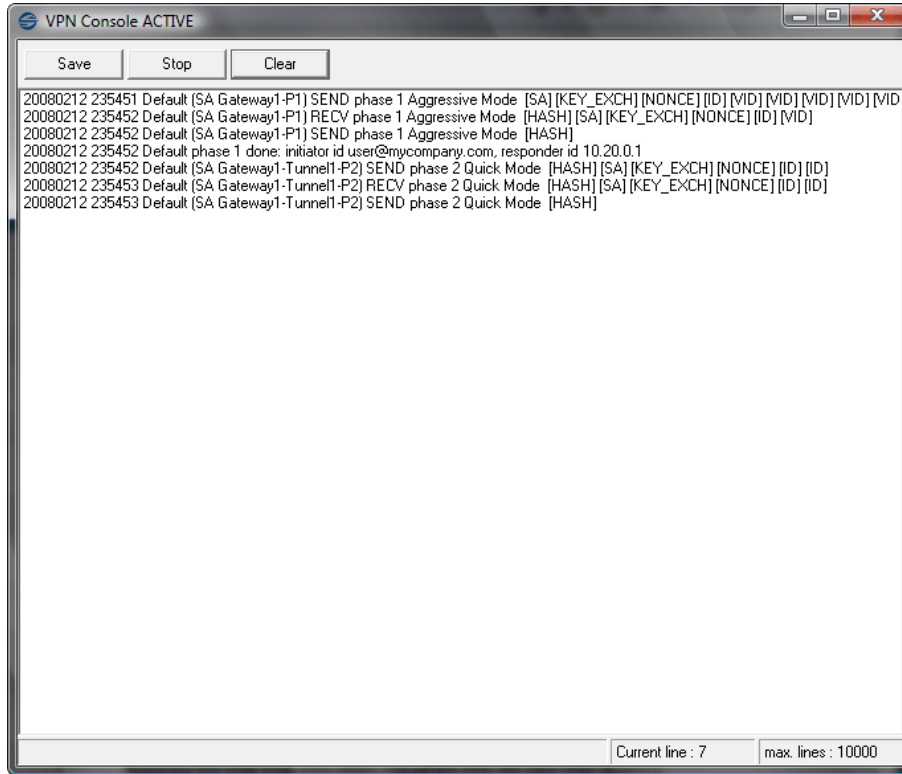
Click on “Save & Apply” on the Syswan VPN Client software window to make sure that all configuration modifications are saved.

Click on “Open Tunnel” to open the secure IPSec VPN Tunnel you just created between your remote computer and the corporate network.



You may select “Connections” to see opened VPN tunnels or try to access any remotely available services (ie: ping a PC on the corporate LAN or access a server resource) to test your configuration.

Select “Console” to access the Syswan VPN Client software IPsec logs on the remote computer.



Select “VPN Configuration > VPN Logs” on your Syswan Duolinks SW24 VPN Series load balancer to access IPsec VPN logs on the Corporate gateway.

2008/02/12 11:54:48	Info.	ike	Phase2 Responder(Quick) : established [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:47	Info.	ike	Phase2 Responder(Quick) : 1st [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:47	Info.	ike	Phase2 Responder(Quick) : 1st [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:47	Info.	ike	Respond phase 2 negotiation [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:46	Info.	ike	ISAKMP SA established [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:46	Info.	ike	Phase1 Aggressive Responder state=9 [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:46	Info.	ike	Phase1 Responder(Aggressive) : 1st [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:46	Info.	ike	Set DPD Vendor ID
2008/02/12 11:54:45	Info.	ike	Received DPD Vendor ID
2008/02/12 11:54:45	Info.	ike	received Vendor ID: RFC 3947
2008/02/12 11:54:45	Info.	ike	received Vendor ID: draft-ietf-ipsec-nat-t-ike-03
2008/02/12 11:54:45	Info.	ike	received Vendor ID: draft-ietf-ipsec-nat-t-ike-00
2008/02/12 11:54:45	Info.	ike	Start Aggressive mode [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]
2008/02/12 11:54:45	Info.	ike	Respond phase1 negotiation [Remote(82.111.111.131:500), Local(82.111.111.2:500 Wan1)]

Statistics for an active tunnel can be viewed by choosing the active tunnel in the “Tunnel list” under “VPN Configuration > IPsec Policy Setup” and by clicking on the “Tunnel Status...” button.

Example configuration test results :

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d89f:c777:e3b4:d5d7%8
    IPv4 Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>ping 192.168.192.254

Pinging 192.168.192.254 with 32 bytes of data:

Reply from 192.168.192.254: bytes=32 time=75ms TTL=128
Reply from 192.168.192.254: bytes=32 time=74ms TTL=128
Reply from 192.168.192.254: bytes=32 time=75ms TTL=128
Reply from 192.168.192.254: bytes=32 time=74ms TTL=128

Ping statistics for 192.168.192.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 74ms, Maximum = 75ms, Average = 74ms

C:\>ping 192.168.192.1

Pinging 192.168.192.1 with 32 bytes of data:

Reply from 192.168.192.1: bytes=32 time=73ms TTL=254
Reply from 192.168.192.1: bytes=32 time=74ms TTL=254
Reply from 192.168.192.1: bytes=32 time=75ms TTL=254
Reply from 192.168.192.1: bytes=32 time=75ms TTL=254

Ping statistics for 192.168.192.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 73ms, Maximum = 75ms, Average = 74ms
```

The above screen capture shows the result of IPSec traffic transiting through the VPN tunnel.

Remote network settings : 192.168.1.0 / 24

Remote network gateway : 192.168.1.1

IP address of remote PC : 192.168.1.100

Corporate network settings : 192.168.192.0 / 24

Corporate network gateway : 192.168.192.1

IP address of server on Corporate network : 192.168.192.254

Remote to corporate LAN - Test 1 :

PING (ICMP echo) from 192.168.1.100 to 192.168.192.254 (Corporate server) – Successful.

Remote to corporate LAN - Test 2 :

PING (ICMP echo) from 192.168.1.100 to 192.168.192.1 (Corporate LAN gateway) – Successful.

9.4 Troubleshooting

The Chapter 9 details a working example of a remote-to-LAN IPSec VPN configuration using Syswan hardware and software solutions.

Configuring a VPN tunnel can be a difficult task as any missing parameter can prevent a VPN connection from being established.

Hint : If your configuration is not working, double check all the configurations entries (Phase 1 and Phase 2) at both ends and make sure that there are no errors.

Troubleshooting and other help documentations are available in the FAQ & Knowledgebase section of our web site.

You may also contact your IT manager or the network administrator for assistance.

10. Contacts

Information and updates are available at: www.syswan.com
Technical support available by email at: [support @ syswan.com](mailto:support@syswan.com)
Pre sales support available by email at: [sales @ syswan.com](mailto:sales@syswan.com)