Proxicast IPSec VPN Client

for Windows

User's Guide

Version 5.5x

proxicast®

www.proxicast.com

Copyright

Disclaimer

Proxicast does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Proxicast further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Proxicast is a registered trademark and ProxiOS (Proxicast Network Operating System), LAN-Cell, PocketPORT, Cell-Guard, Cell-Lock, Modem-LOCK, Modem-SAFE and Cell-Sentry are trademarks of Proxicast, LLC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Contents

1. Introducing The Proxicast IPSec VPN Client

1.1. What is The Proxicast IPSec VPN Client ?

The Proxicast IPSec VPN Client is IPSec VPN software for all Windows versions that allows a PC to establish a secure connection over the Internet to a LAN-Cell router or other IPSec-compliant device. IPSec is the most secure way to connect to a LAN-Cell as it provides strong user authentication, strong tunnel encryption with ability to cope with existing network and firewall settings.

Although designed for use with Proxicast LAN-Cell family of cellular routers, the Proxicast IPSec VPN Client can be used to connect with many other vendors' IPSec appliances. For example, the Proxicast IPSec VPN Client can also serve as a user's primary VPN connection to secure corporate networks via IPSec VPN concentrators from Cisco, SonicWall, WatchGuard, and many others.

The Proxicast 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 related areas. The IPSec VPN Client complements our range of network security products and like all our products is extremely easy to use and to install.

1.2. The Proxicast IPSec VPN Client Features

Windows versions	Win2000, WinXP 32-bit (incl.SP2), Windows Server 2003 32-bit, Windows Server 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8 32/64-bit.
Languages	Arabic, Chinese (simplified), Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Korean, Norwegian, Japanese, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai and Turkish.
Connection Mode	Operates as a peer-to-peer VPN as well as "point – to – multiple" mode, without a gateway or server. All connections types like Dial-up, DSL, Cable, 3G Cellular and Wi-Fi are supported. Allows IP Range networking. Can run in an RDP session (Remote Desktop connection).
Tunneling Protocol	Full IKE support: 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 Aggressive 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. Redundant Gateway allows The Proxicast VPN Client to open an IPSec tunnel with an alternate gateway in case the primary gateway is down or not responding.
Config Mode	"Config Mode" 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. IPSec 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. NOTE: Config Mode is not currently supported on Proxicast LAN-Cell Gateways.
USB Stick	VPN configurations and security elements (certificates, preshared key,…) can be saved into an USB Memory 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 Proxicast IPSec 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 debugging purposes.
Flexible User Interface	Silent install and invisible graphical interface allow IT managers to deploy solutions while preventing users from changing configurations. Tiny Connection Panel and VPN Configuration Panel can be available to end-users separately with Access Control. Drag & drop VPN Configurations into the IPSec VPN Client. Multiple keyboard shortcuts to easily navigate the IPSec VPN Client.
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.
Live update	Ability to check for online update.
Licensing	Evaluation and Lifetime based Licensing is available.

2. Installing The Proxicast IPSec VPN Client

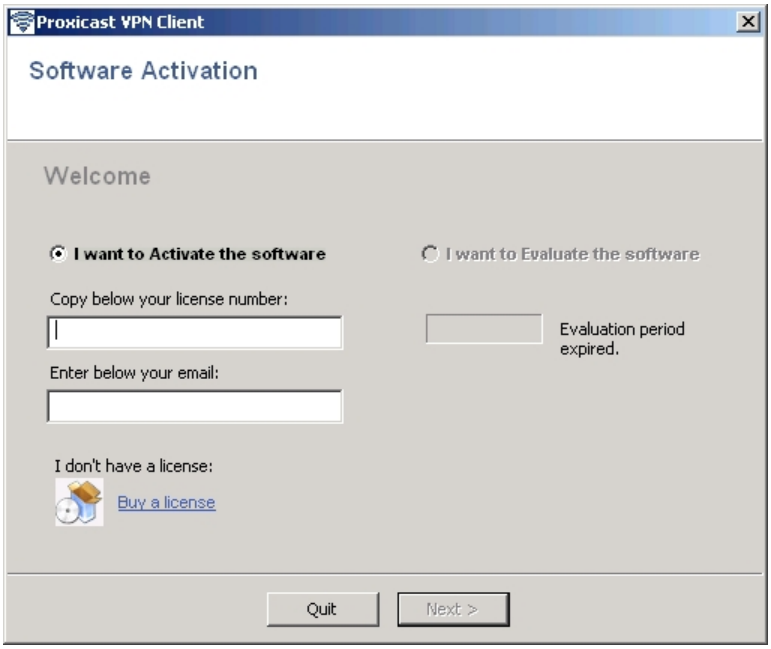
2.1. Software Installation

The Proxicast VPN Client installation is a classic Windows installation that does not require VPN specific information. After completing the installation, you will be asked to reboot your computer. After reboot and session login, The Proxicast VPN window can be launched:

- from user desktop, by double-clicking on The Proxicast VPN shortcut
- from VPN Client icon available in the taskbar
- from menu Start > Programs > Proxicast > VPN Client> Proxicast VPN Client

Once launched, 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 in the orange bar.
- "Activate' allows you to activate the software online. This requires a License Number. When clicking on the 'Activate' button, an Activation Wizard pops up.
- "Buy' allows you to go online and purchase a Software License from Proxicast's online shop.



Caution: On Windows 2000, XP and Vista, you must have administrator rights, otherwise the installation stops after the language choice with an error message.

Note: Software Installation can be customized with several command line parameter options.

A user might have restricted access rights on a given Windows computer. Here is what users can have access to:

Actions	Admin	Users
Software install	yes	no
Software activation	yes	yes
Software use	yes	yes

To make it even easier, The Proxicast IPSec VPN Client creates new rules into the Windows Firewall so that IPsec VPN traffic is enabled. Here are the Windows Firewall rules:

Vista Firewall Rule Name	Action
tgbphase1	authorize UDP 500
tgbphase2	authorize UDP 4500

On other versions of Windows or PCs or networks running firewall software, these UDP ports may need to be opened before The Proxicast IPSec VPN Client can make a connection to a remote gateway.

2.2. Software Evaluation

It is possible to use The Proxicast IPSec VPN Client during the evaluation period (i.e. limited to 30 days) by selecting the 'Evaluate' option. When the IPSec VPN Client is in "Evaluation" mode, the Register window appears at each start of the IPSec VPN Client.

During the Evaluation Period, the software has full functionality. Once the Evaluation Period expires, 'Evaluation' option is no longer available and the software is disabled.

2.3. Software Activation

2.3.1. Software Activation Wizard

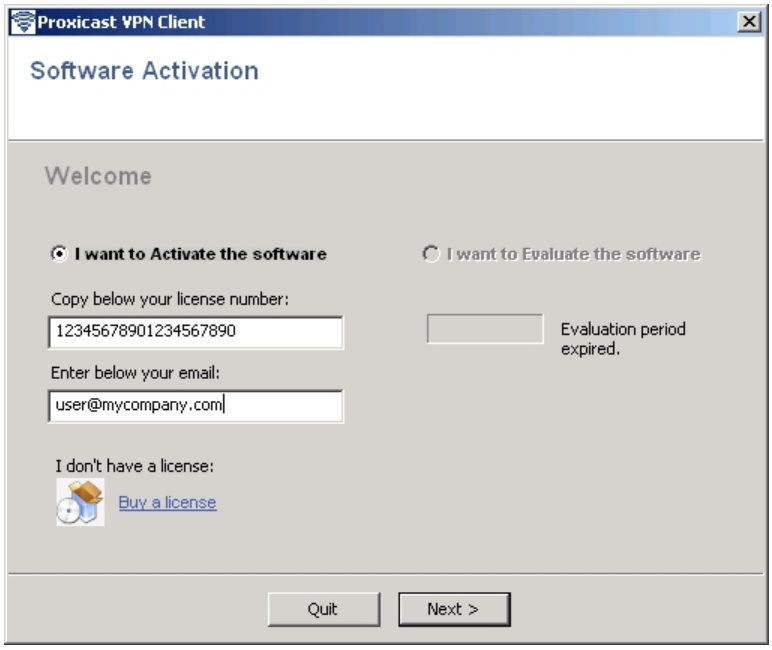
For use beyond the Evaluation Period, The Proxicast IPSec VPN Client software must be activated on your computer. To use the same License Number on new computer, you need to un-install the software on the previous computer – deactivation will be done automatically. The Software Activation is a two step 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 window when you start the 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 that is provided to you when a license is purchased.

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

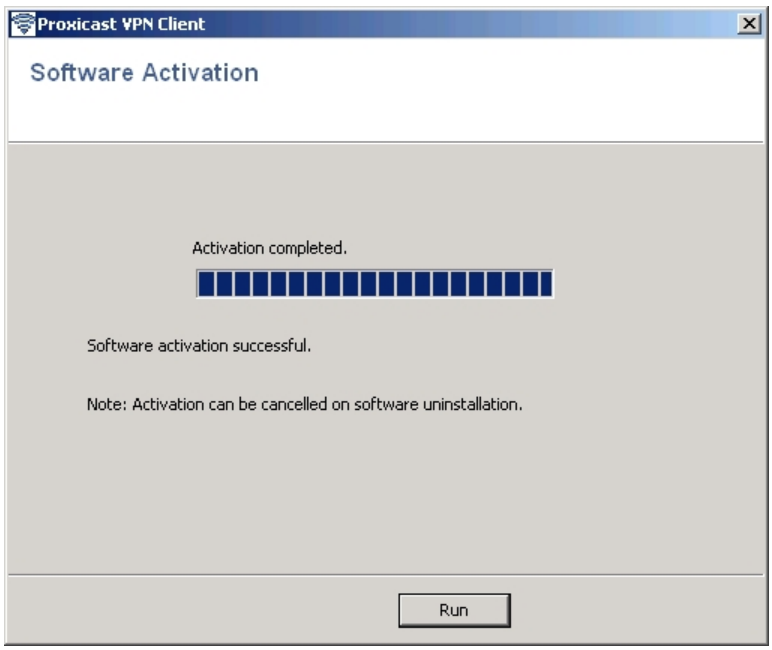


Note: The email address may not be required: IT Managers can force this value during the setup, then it will not be displayed by the Software Activation Wizard. This feature can be used to centralize all the Software Activation confirmation emails to a single email address.

2.3.3. Step 2 of 2: Online Activation

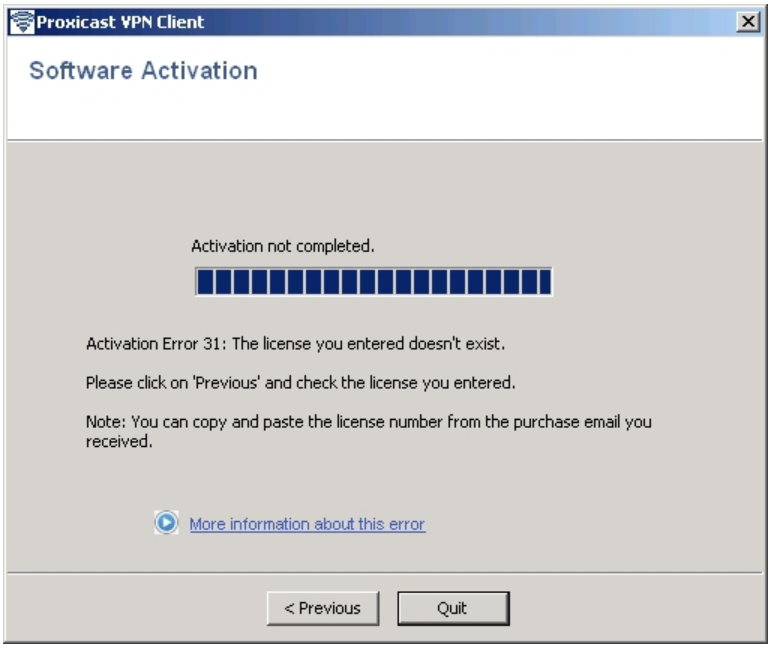
The 'Activation Wizard' will automatically connect to the online software activation server to activate the VPN Client Software. You can go back at any time to change the License Number.

The 'Activation Wizard' will end with a 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 online full explanations and recommendations on how to proceed next.



Most 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 is already activated (error 033). Contact our sales team: sales@proxicast.com.

All activation errors are detailed online on our support website: http://support.proxicast.com

Note: If you didn't succeed in activating the software despite the previous recommendations, it is possible to manually activate the software. Please contact support@proxicast.com for further instructions on manual activation.

2.4. Software Upgrades

Warning: The VPN Client software needs to be activated after each software upgrade. Click on the menu "?" then "Check for update" on the Configuration Panel.

Note: The VPN Configuration is saved during a Software Upgrade and automatically enabled again within the new release.

2.5. Software Uninstallation

The Proxicast IPSec VPN Client can be uninstalled:

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

Your PC should have Internet access during the uninstall procedure so that your license key can be returned to the license server for reuse on a new PC.

3. Quick How To's

3.1. How To Setup a Tunnel to a LAN-Cell?

- Create a new Remote User IPSec VPN Rule on the LAN-Cell:
  - VPN Mode = Remote User
  - Preshared Key = any 8+ character string

- In the Proxicast IPSec VPN Client, select 'Wizard…' from the 'Configuration' menu.
  - IP address/DNS name of remote equipment = Public IP or DNS name of the LAN-Cell
  - Preshared Key = 8+ digit character string set in LAN-Cell
  - Private IP address of remote network = 192.168.1.0 (example)

Refer to Tech Note: *Proxicast IPSec VPN Client Example* on the Proxicast support web site for a detailed explanation of how to configure these settings on both the LAN-Cell and VPN Client.

3.2. How To Open a VPN tunnel?

To open a tunnel (once a VPN configuration is set) do any of the following:

- Configuration panel: Double-click the desired Tunnel (or right mouse, then select Open Tunnel)
- Connection panel: Right mouse button, then Open Tunnel (or Ctl+O)
- SystemTray > click on 'Open Tunnel'
- If Automatically open this tunnel when VPN Client starts is selected, launch the software
- If Automatically open this tunnel on traffic detection is selected, access the remote LAN
- If Automatically open this tunnel when USB stick is inserted, insert a configured USB Stick
- Double click on a VPN Configuration (e.g. icon on desktop, email attachment)
- Use one of the Command line options allows to open or close tunnels

3.3. How To import with a double click on a VPN Configuration icon?

Also known as 'Dial up mode': A tunnel may be opened via a double-click on a VPN Configuration file (i.e. extension '.tgb' file). This feature enables you to create various VPN Configurations on the windows desktop, and to open tunnels by clicking on VPN Configuration shortcut icons rather than launching the Proxicast IPSec VPN Client directly.

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 with a password as it is exported. This password will be required each time the tunnel icon is clicked on.

4. Navigating the User Interface

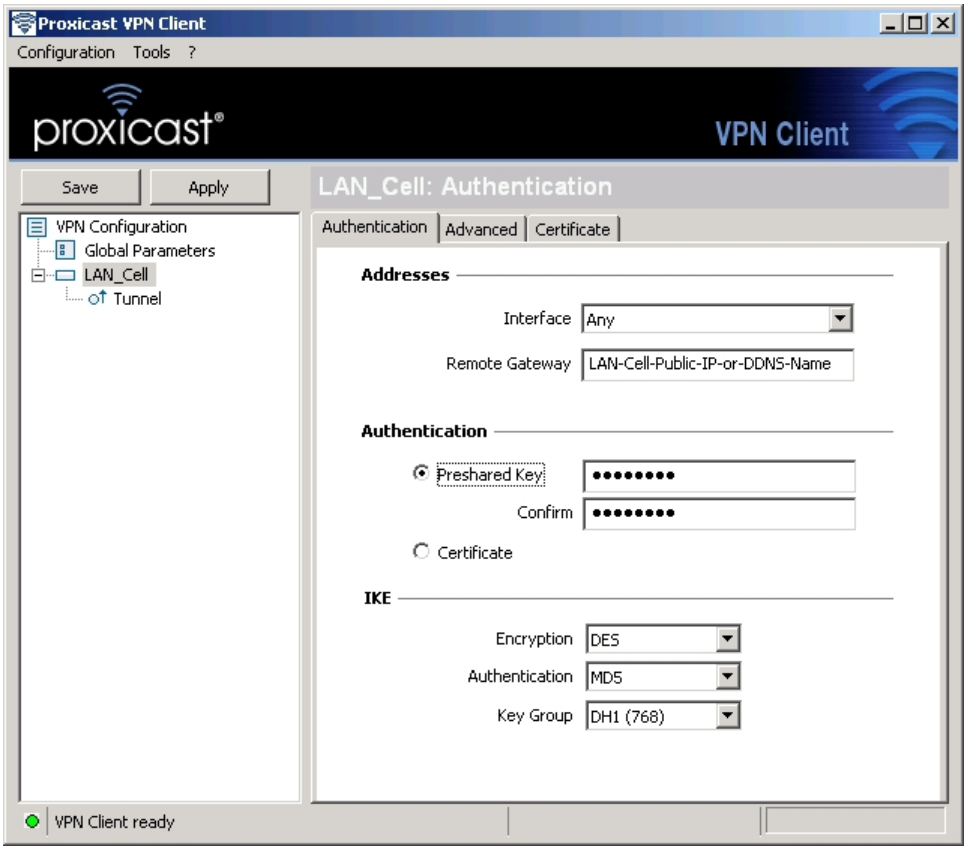
4.1. User interface elements

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

The IPSec 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



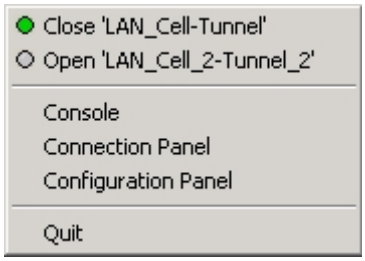
4.2. System Tray Icon

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

VPN Client application color codes:

Red icon: no VPN tunnel is opened
Green icon: at least one VPN tunnel is opened

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



A right-button click shows the following menu:

- "Console' shows log window.
- "Connection Panel" opens the Connection Panel which enables to open, close and get information about tunnels.
- "Configuration Panel" opens the main window. Tunnels can be opened or closed from this menu as well.
- "Quit' will close established VPN tunnels, then stop the configuration user interface.

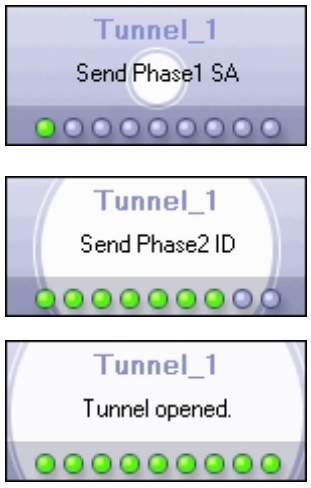
Tooltips over VPN Client icon shows the connection status of the VPN tunnel:

- "Tunnel <tunnelname>' when one or more tunnels are established
- "Wait VPN ready...' when the IKE service is reinitializing
- "The Proxicast VPN Client' when the VPN Client is up but with no opened tunnel.

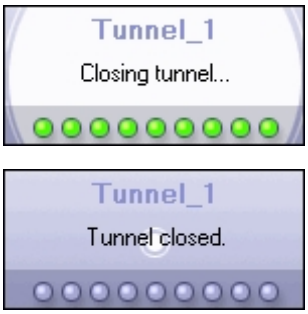
4.3. System Tray Popup

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

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



2. The popup shows tunnel closing as well.



3. In case the tunnel cannot open, it displays a warning with a description of the error condition.

4.4. Keyboard Shortcuts

Shortcut	Action
Ctrl + Enter	Switches back and forth 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 switching to the Configuration Panel.
Ctrl + D	Opens the VPN 'Console' for network 'Debug'.
Ctrl + S	'Save & Apply' a VPN Configuration.

4.5. Connection Panel

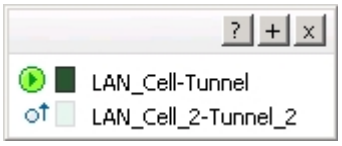
The Connection Panel enables users to open, close and get clear information about every tunnel that has been configured. This is all the end-user needs to open and close tunnels.

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

The Connection Panel is made of several elements:

- A list of all configured tunnels with 'open/close' button (below diagram)
- A link back to the 'Configuration Panel' (“+” menu button)

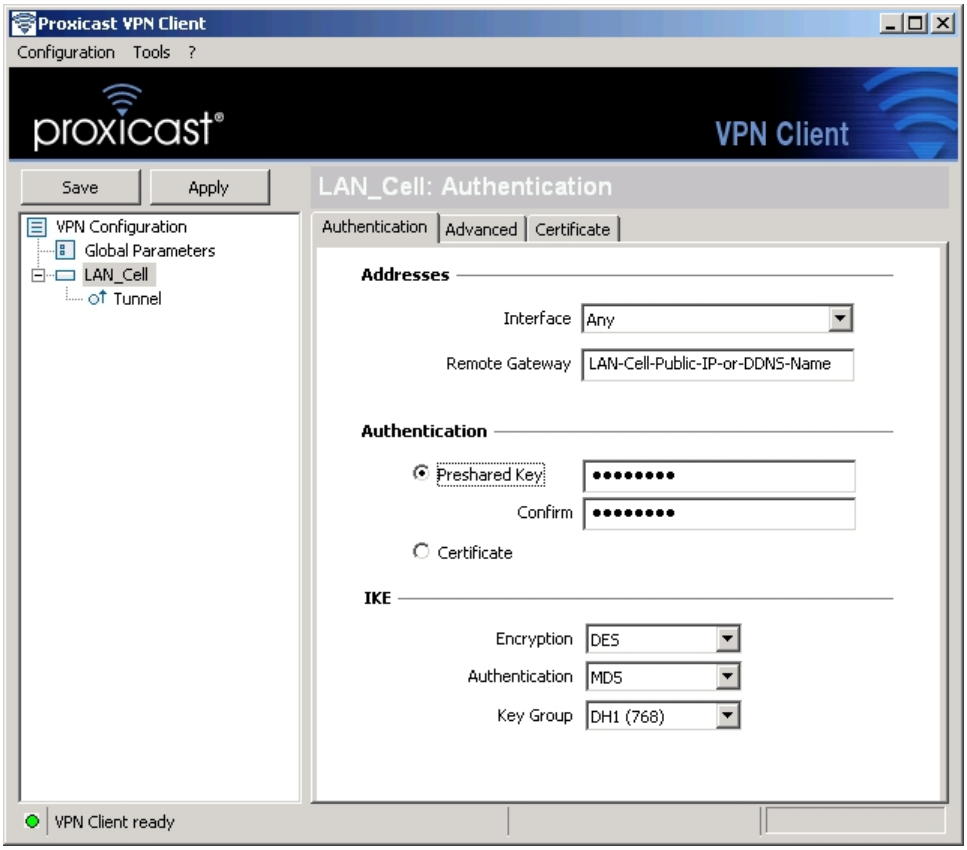
It's possible to switch back and forth between the 'Connection Panel' and the 'Configuration Panel' by using the shortcut 'Ctrl + Enter' (see section 'Shortcuts').



4.6. Configuration Panel

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

- Menus across the top
- 'Save', and 'Apply' buttons
- 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 with tabs for groups of related parameters.



A VPN Configuration file (i.e. extension '.tgb') can be dragged and dropped onto the Configuration Panel. This feature enables you to easily apply 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 as soon as the new VPN Configuration is applied ('Save or Apply').

4.7. Configuration Panel Menus

Configuration

- Import: Importing a VPN security policy (VPN Configuration VPN)
- Export: Exporting a VPN security policy (VPN Configuration VPN)
- Move to USB drive: USB Mode settings and enable the USB mode
- Wizard: Automate the creation of a new tunnel configuration
- Quit: Close the open VPN tunnels and quit the software

Tools

- Connection Panel
- Console: IKE connection trace Window
- Reset IKE: Reboot IKE

- Options: Options protective display startup, language management, management PKI

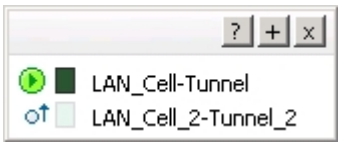
? Menu

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

5. Connection Panel

5.1. Connection Panel Basics

The Connection Panel enables users to open, close and get status information about every tunnel that has been configured.

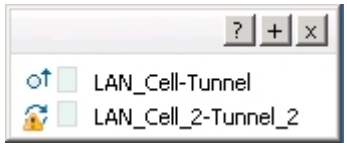


The user simply double-clicks on the 'Open/Close' icon of a tunnel to open or close a tunnel. The 'Open' button automatically switches to 'Close' when the tunnel is opened.

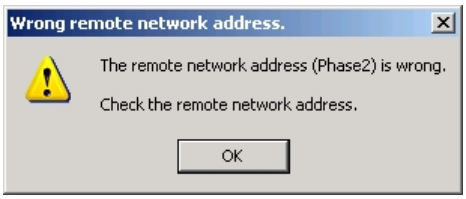
It's possible to switch back and forth between the 'Connection Panel' and the 'Configuration Panel' by using the shortcut 'Ctrl + Enter' (see section 'Shortcuts').

5.2. More About Connections

If problems occur during the tunnel opening process, a warning icon is shown to the left of the tunnel name.



Double-clicking the warning icon opens a message box with details of the issue preventing the tunnel from opening.



6. Configuration Panel

6.1. Configuration Wizard

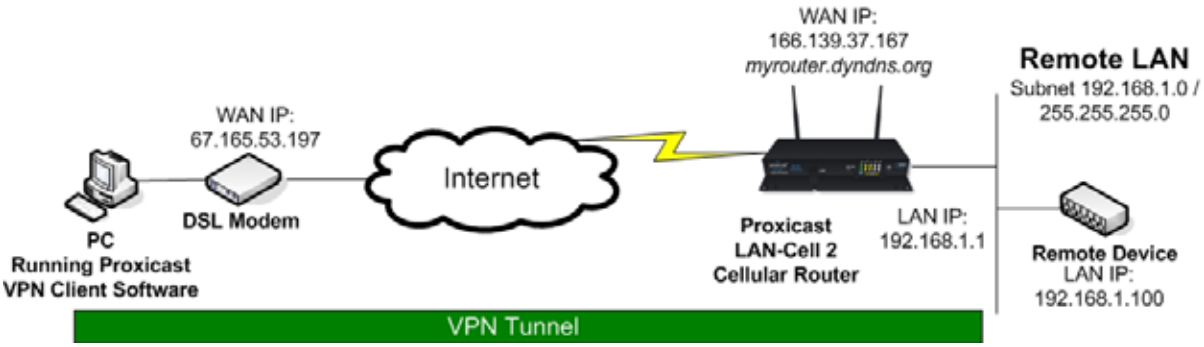
6.1.1. Two step Configuration Wizard

The Proxicast IPSec VPN Client provides a Configuration Wizard which is designed to make it easy to create a VPN connection to a LAN-Cell gateway in two simple steps.

The Configuration Wizard is for remote computers that need to get connected to a LAN-Cell gateway using the default Phase 1 and Phase 2 parameters set in the LAN-Cell's VPN firmware. IPSec configurations for other remote gateway devices should be made through the 'Configuration Panel'.

Consider the following example:

- Your PC has a dynamically provided public IP address (DSL, cable, 3G modem, etc).
- You want to connect to a remote LAN-Cell that has a dynamic IP address. You have already configured the LAN-Cell to use the DynDNS service to update "*myrouter.dyndns.org*" with the IP address as it assigned from your cellular carrier.
- The remote LAN-Cell's private address is 192.168.1.1 with a subnet is 192.168.1.0 /255.255.255.0. (e.g. the remote device want to reach is a server with the IP address: 192.168.1.100.)

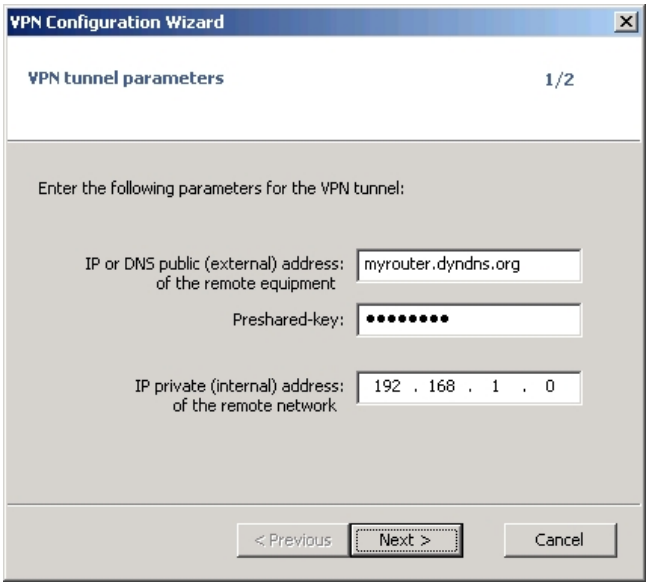


To configure this connection, open the Wizard by selecting the "**Configuration > Wizard**" menu.

6.1.2. Step 1 of 2: VPN tunnel parameters

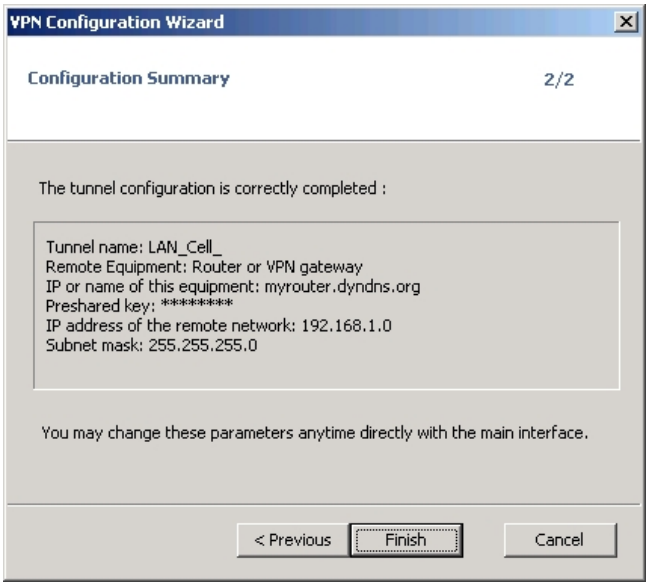
You must specify the following information:

- The public (Wide Area Network side) address or DNS name of the remote gateway (LAN-Cell) (*myrouter.dyndns.org* or *serial#.proxidns.com* or 166.139.37.167 in this example)
- The preshared key you will use for this tunnel (this preshared key must be the same as the one you set in the LAN-Cell)
- The private IP subnet of your LAN-Cell (e.g. 192.168.1.0 not 192.168.1.1)



6.1.3. Step 2 of 2: Summary

The second step summarizes your new VPN configuration. Other parameters may be further configured directly via the 'Configuration Panel' (e.g. Certificates, virtual IP address, etc..) if you have changed the LAN-Cell's VPN configuration parameters.



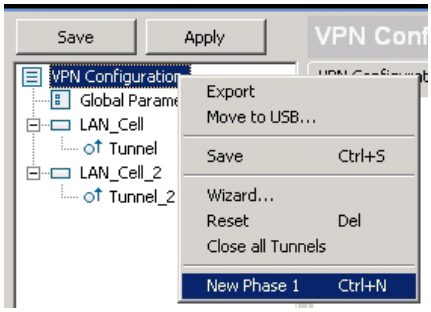
6.2. VPN Tunnel Configuration

6.2.1. How to create a VPN Tunnel ?

The Configuration Wizard will automatically create an IPSec tunnel with the default parameters which match the default IPSec tunnel parameters on the LAN-Cell. You only have to supply the LAN-Cell's IP address (or DDNS name), the LAN-Cell's local IP subnet and the preshared key. This is the easiest way to create a VPN tunnel to a LAN-Cell gateway.

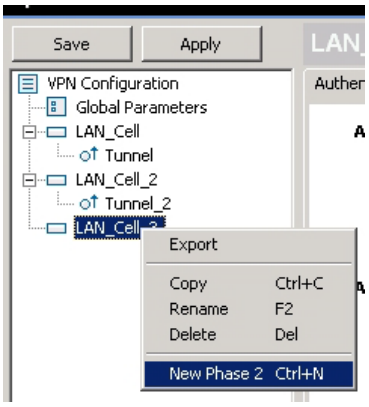
To create a VPN tunnel from the Configuration Panel (without using the Configuration Wizard), you must follow the following steps:

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



2. Configure the Authentication Phase (Phase 1), making sure to confirm that the settings match those chosen when creating the VPN tunnel configuration on the LAN-Cell and click 'Save & Apply'.

3. Right-click on the 'new LAN_Cell_' in the tree control and select 'Add Phase 2'.



4. Configure the IPSec Phase parameters (Phase 2) to match those set on the LAN-Cell's VPN configuration.

5. Once the parameters are set, click on 'Save" to take into account the new configuration.

6. Double-click (or Ctl+O) on the new tunnel name to open the IPSec VPN tunnel.

Please refer to Phase 1 and Phase 2 for descriptions of each parameter.

6.2.2. Multiple Authentication Configuration Phases

Any number Authentication Phases (Phase1) can be configured. Therefore, one computer can establish IPSec VPN connections with multiple different gateways.

Similarly, several IPSec Configurations (Phase 2) can be created for a same Authentication Phase (Phase 1) (i.e. multiple tunnels to the same remote gateway).

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 Agressive Mode
- Enable/Disable Redundant Gateway
- Select NAT-T mode (Forced, Disabled or Automatic)
- Set X-Auth Login/password with pop up option
- Import PKI Certificates used for authentication

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

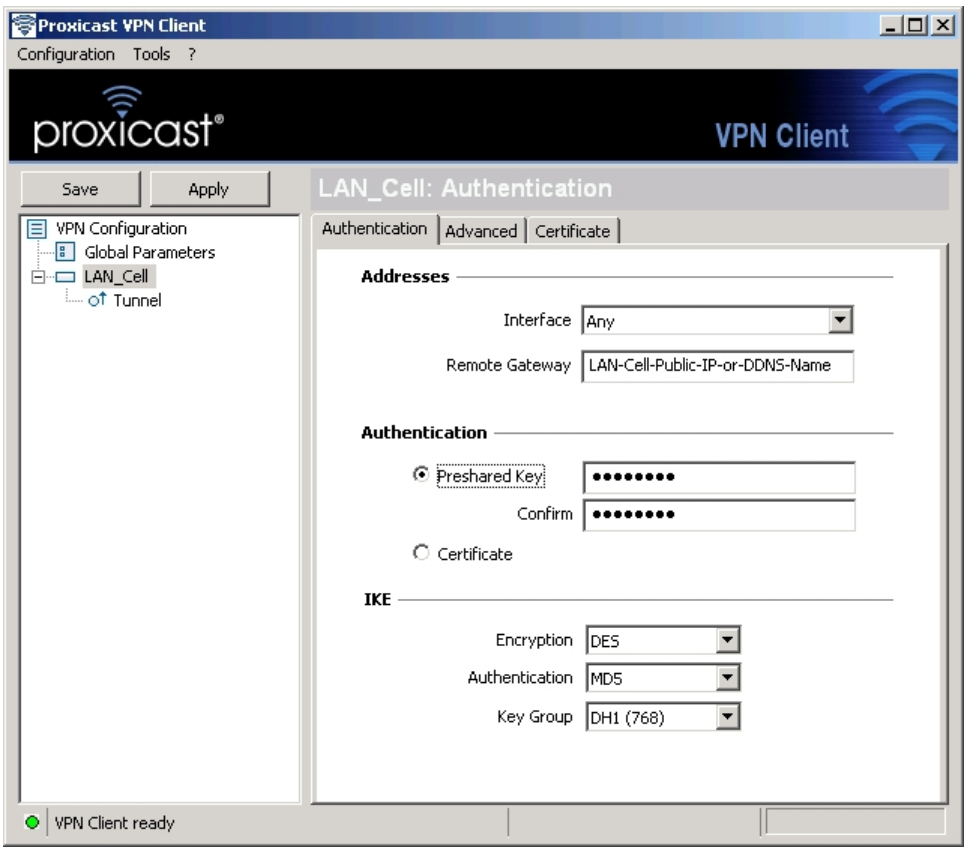
- Automatic Open Mode
- Manual settings of DNS/WINS server addresses
- Choose Script/Application to be launched when tunnel opens

6.3. Authentication or Phase 1

6.3.1. What is Phase 1 ?

'Authentication' or 'Phase 1' is also called the IKE Negotiation Phase. Phase 1's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of Phase 1, each end system must identify and authenticate itself to the other.

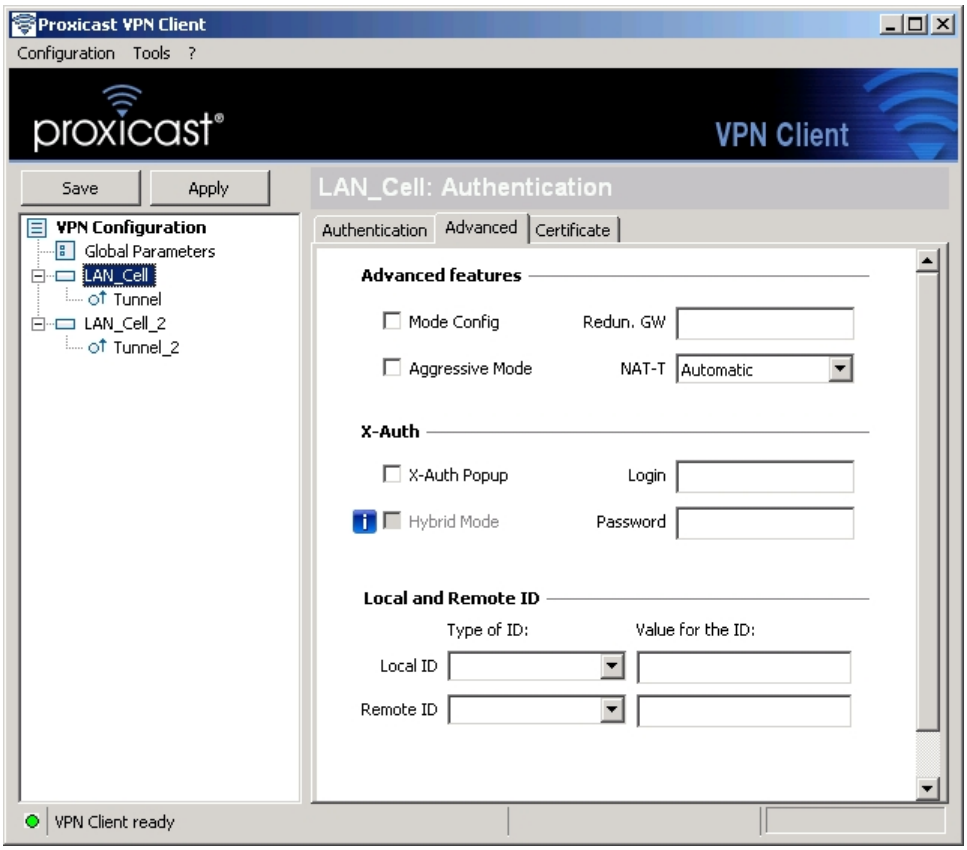
6.3.2. Phase 1 Settings Description



Interface	IP address of the network interface of the computer, through which VPN connection is established. If the IP address may change (when it is received dynamically by an ISP), select "Any".
Remote Gateway	IP address or DNS address of the remote gateway (in our example: myrouter.dyndns.org). **This field is mandatory**.
Pre-shared key	Password or key shared with the remote gateway.
Certificate	X509 certificate used by the VPN Client . When selected, the Import Certificate tab is displayed. Click on 'Import Certificate..' to choose the certificate source: PEM files or P12 files (see section How to configure Certificates).
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.

6.3.3. Phase1 Advanced Settings Description

For advanced features & parameters, click on 'Advanced' tab on the Authentication panel.



Mode-Config	If checked, the VPN Client will activate Mode-Config for this tunnel. Mode-Config allows to the VPN Client to fetch some VPN Configuration information from the VPN gateway: · Virtual IP address of the VPN Client · DNS server address (optional) · WINS server address (optional) If Mode-Config is not available on the remote gateway, refer to section 'Phase2 Advanced' settings to manually set DNS and WINS server addresses.

	NOTE: Mode-Config is not currently supported on Proxicast LAN-Cell.
Aggressive Mode	If checked, the VPN Client will used aggressive mode as 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 DNS name of the Redundant Gateway (e.g. backup-router.dyndns.org). · The Proxicast VPN Client will contact the primary gateway to establish a tunnel. If it fails after several tries (default is 5 tries, configurable in "Parameters" panel > "Retransmissions" field) the Redundant Gateway is used as the new tunnel endpoint. Delay between two retries is about 10 seconds. · In case the primary gateway can be reached but tunnel establishment fails (e.g. VPN configuration problems) then the VPN Client won't try to establish tunnels with the redundant gateway. · If a tunnel is successfully established to the primary gateway with DPD feature (i.e. Dead Peer Detection) negotiated on both sides, when the primary gateway stops responding (e.g. DPD detects non-responding remote gateways) the VPN Client immediately starts opening a new tunnel with the Redundant Gateway. · The exact same behavior will apply to the redundant gateway. This means that the VPN Client will try to open primary and redundant gateway until the user exits software or click on 'Save & Apply'.
NAT-T	The NAT-T mode allows Forced, Disabled and Automatic. The NAT-T "Disabled" prevents the IPSec VPN Client and the VPN gateway from starting NAT-Traversal. The NAT-T "Automatic" mode allows the VPN Gateway and VPN Client to negotiate NAT-Traversal. In NAT-T "Forced" mode, The Proxicast IPSec VPN Client will force NAT-T by encapsulating IPSec packets into UDP frames to solve traversal with intermediate NAT routers.
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 60 seconds (i.e. default) to enter a 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 unidirectionally authenticated. To make this IKE bi-directionally authenticated, this Phase 1 is immediately followed by an X-Auth Exchange [XAUTH]. The X-Auth Exchange is used to authenticate the remote User. The use of these authentication methods is referred to as Hybrid Authentication mode. The Proxicast IPSec VPN Client implements the RFC 'draft-ietf-ipsec-isakmp-hybrid-auth-05.txt'.
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@proxicast.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.

6.3.4. Modify X-Auth popup duration

It is possible to modify the X-Auth popup window display duration. The default value is 60 sec. In some cases, it might be required to extend the duration. In this software release, modification can only be done in the VPN Configuration file with any text editor.

Note: Remember that VPN Configuration file cannot be edited if encrypted. If you need password protection, modify **`Xauth-interval`** parameter in the VPN configuration file, then Import the modified VPN Configuration, then go to 'File' > 'Export VPN Configuration' and select 'Password protection'.

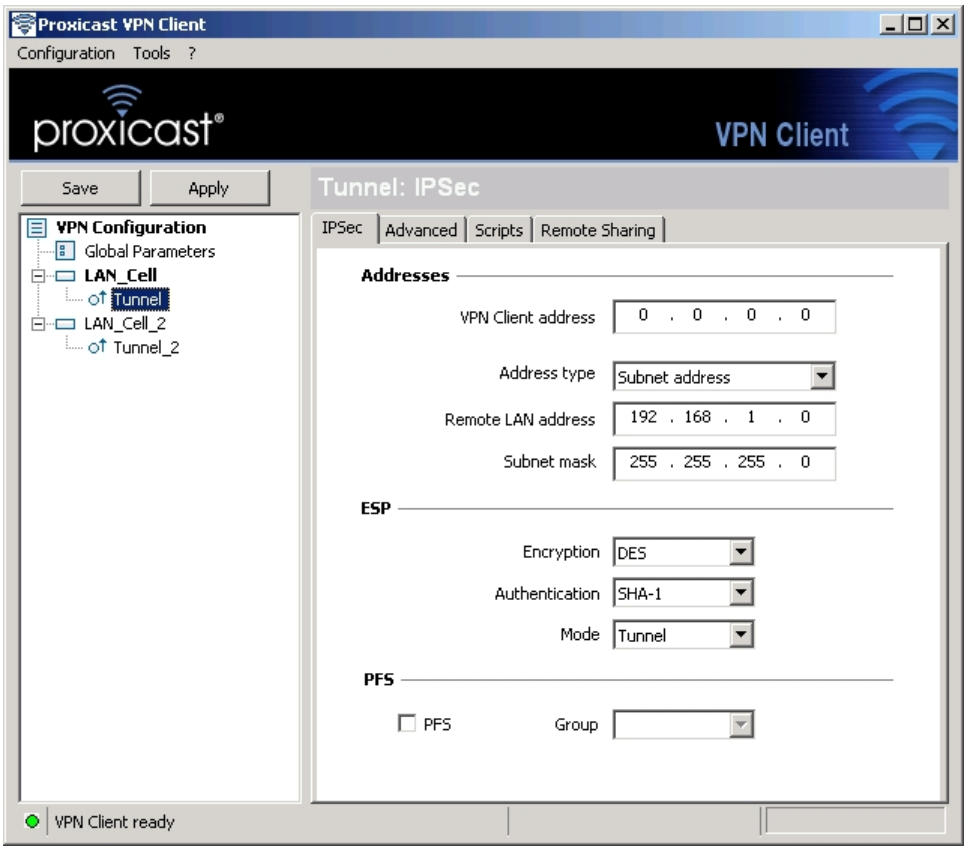
```
[General]
Shared-SADB = Defined
Retransmits = 5
Exchange-max-time = 15
Default-phase-1-lifetime = 28800,300:28800
Bitblocking = 0
Xauth-interval = 60
DPD-interval = 15
DPD_retrans = 2
DPD_wait = 15
```

6.4. IPSec Configuration or Phase 2

6.4.1. What is Phase 2 ?

'IPSec Configuration' or 'Phase 2' negotiates the IPSec security parameters that are applied to the traffic going through tunnels negotiated during Phase 1.

6.4.2. Phase 2 Settings Description



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. Typically, the VPN Client address is not part of the remote LAN subnet behind the remote gateway. Normally you can leave the VPN Client IP address at 0.0.0.0 when connecting to a remote LAN-Cell gateway. **This IP address can belong to the same remote LAN subnet (e.g., in the example, you set a VPN Client IP address like 192.168.1.10). If your IP address on the VPN Client overlaps with the remote subnet on the remote gateway, it is important to read the note below.**
Address type	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 Proxicast IPSec VPN Client to establish a tunnel only within a range of a predefined IP addresses. The range of IP addresses can be just one IP address. Incase the remote end point is a single computer, choose "Single Address". When choosing "Single address", only the field "Remote host address" is available.
Remote LAN address	This field may be "Remote host address" or "Remote LAN address" depending of the address type. It is the remote IP address, or LAN network address of the gateway, that opens the VPN tunnel.
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.

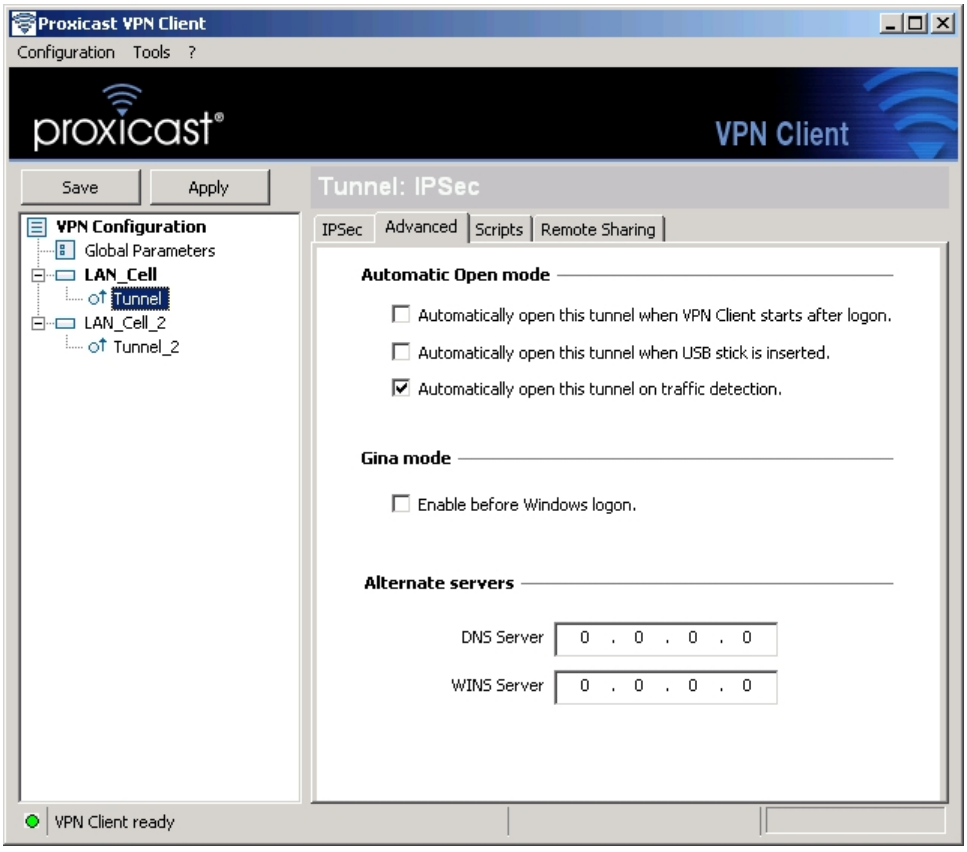
Note 1: "IP Range" feature combined with "Open tunnel when traffic" feature allows the VPN Client to automatically open tunnel when traffic is detected for a specific range of IP Addresses. However, the range of IP addresses must be authorized in the configuration of the remote VPN gateway.

Note 2: It is possible to have both local IP address of your computer and remote LAN as part of the same subnet. To be able to do so, you must select "Auto open this tunnel on traffic detection" ('P2 Advanced'). Once the VPN tunnel opened in this configuration, all the traffic with remote LAN is allowed but communication with local network becomes impossible. You may also need to configure the remote gateway (LAN-Cell) to enable overlapping local and remote subnets. Please consult the Proxicast knowledgebase for more information on this type of VPN configuration.

Once the parameters are set, click on 'Save' to save the new configuration.

6.4.3. Phase2 Advanced Settings Description

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

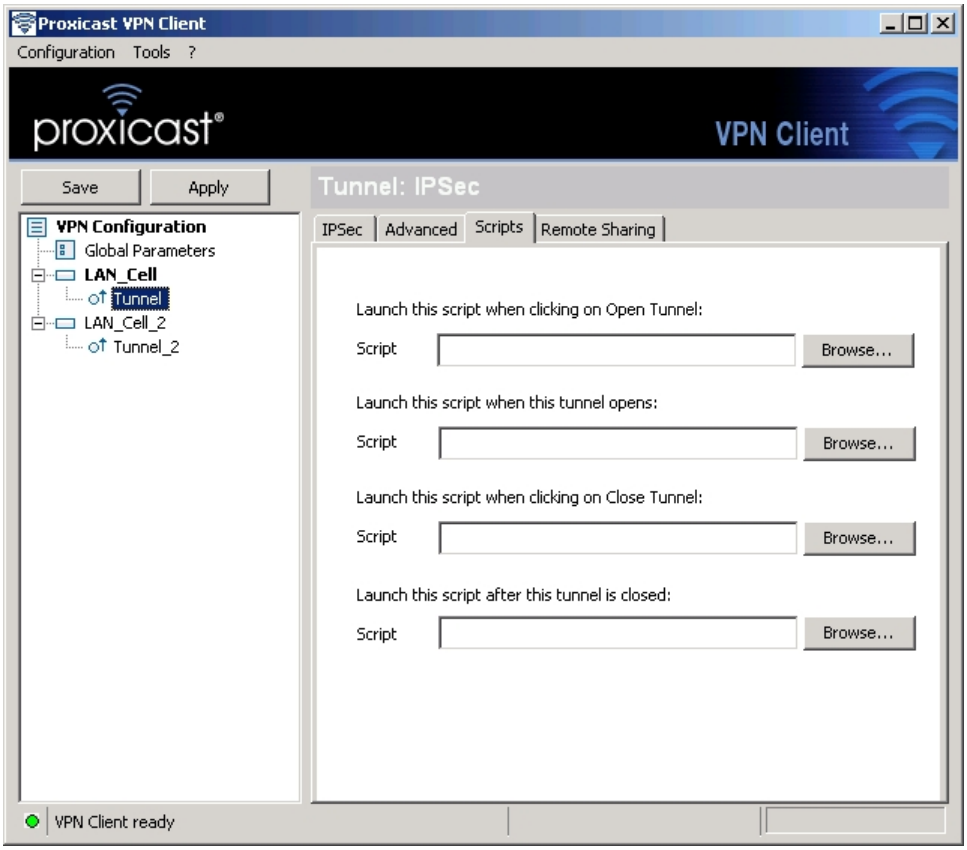


Automatic Open Mode	The VPN Client can automatically open the specified tunnel (Phase 2) on specific events such as: · Auto open this tunnel when the VPN Client starts up. · Auto open this tunnel when USB stick is inserted (see section "USB

	Mode"). · Auto open this tunnel when the VPN Client detects traffic destined for the 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 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 as long as it is opened.

6.4.4. Script Configuration

Scripts may be configured in the Script configuration tab.



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

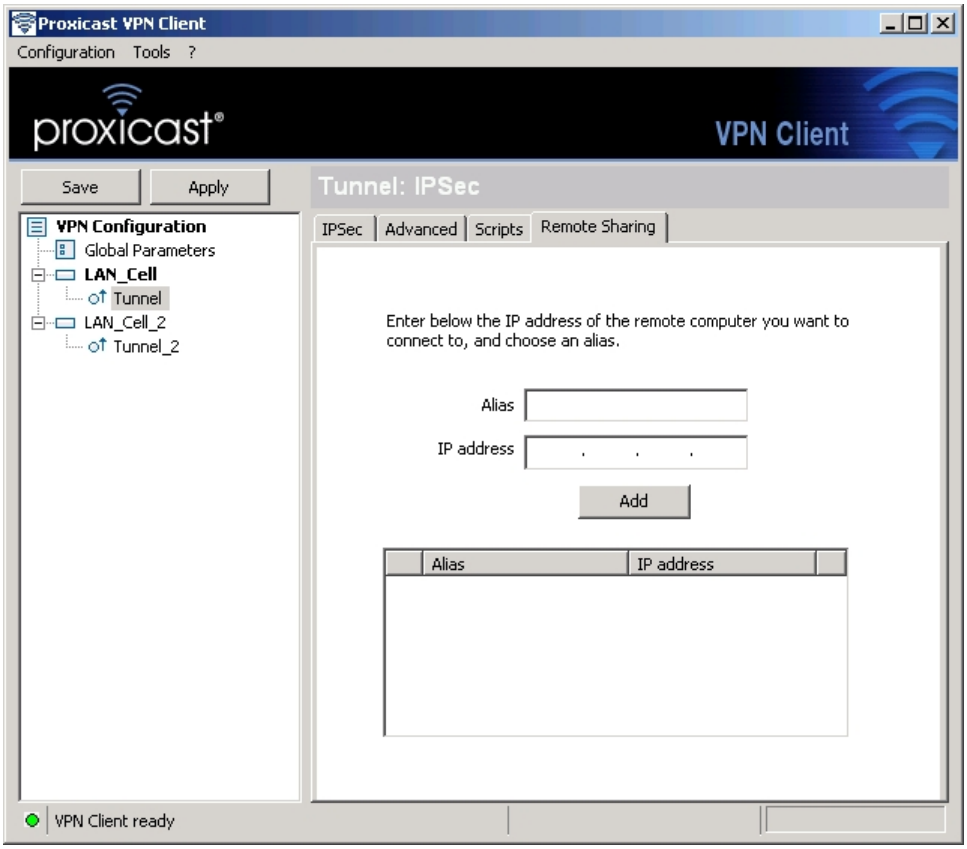
This feature enables you execute scripts (batches, scripts, applications...) at each step of a tunnel connection for a variety of purposes e.g. to check current software release, to check database availability before launching backup application, to check that software is running, a logon is set, etc.

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

6.4.5. Remote Desktop Sharing

The Proxicast IPsec VPN Client allows you to configure the "Remote Desktop" logon in the VPN tunnel. With one click, the VPN tunnel opens to the remote computer, and the RDP (Windows Remote Desktop Protocol) session is automatically opened on the remote computer.

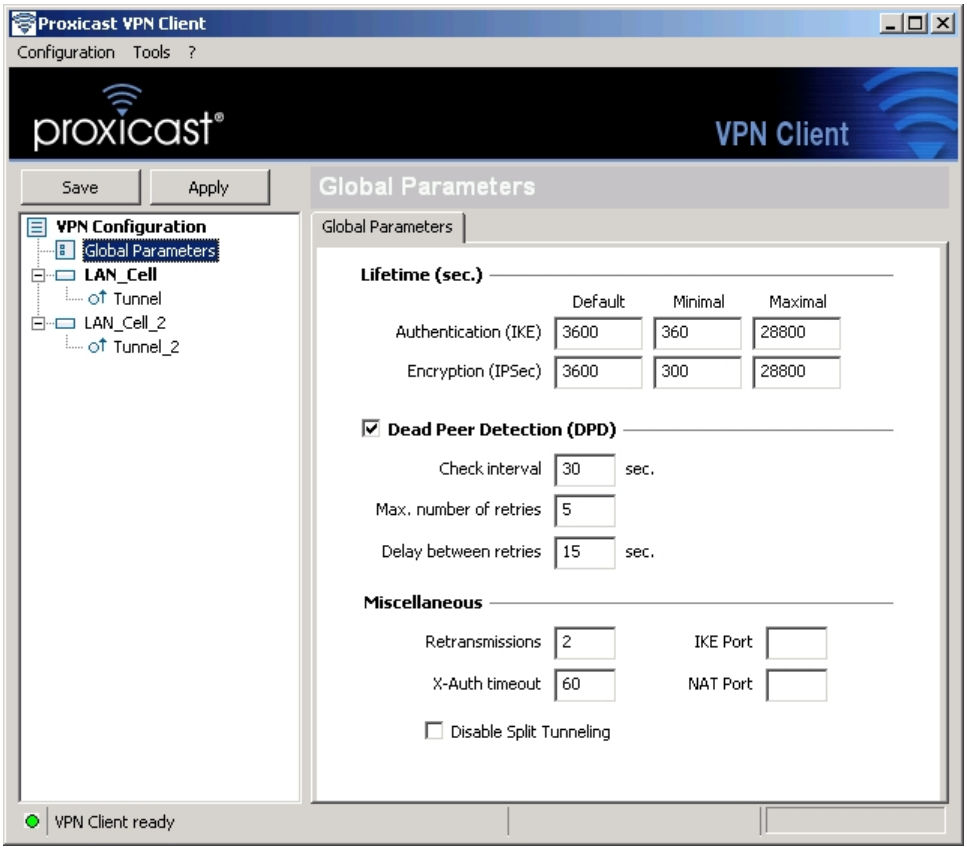
1. Select the VPN tunnel (Phase 2) in which the "Remote Desktop" session will be opened.
2. Select the "Remote Sharing" tab.
3. Enter an alias for the connection (this name is used to identify the connection in the different software menus), and enter the IP address of the remote computer.
4. Click on "Add": The Remote Desktop Sharing session is added to the list of sessions.



6.5. Global Parameters

6.5.1. Global Settings Description

Global Parameters are generic settings that apply to all created VPN tunnels.



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 than 500. The remote gateway must support this feature.
	NAT Port	User can change UDP port number used for NAT Traversal (default 4500).
	Disable Split Tunneling	Forces all network traffic to go through the tunnel rather than to the Internet

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

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

Once the parameters are set, click on 'Save' to save the new configuration.

6.6. Configuration Management

6.6.1. Import or Export VPN Configuration via menu

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

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

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

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

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.

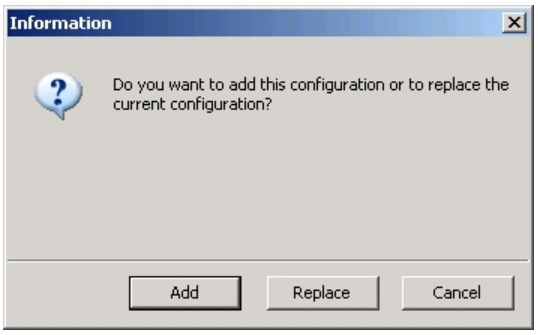
Note: Import/Export in 'USB Mode'
When the VPN Client is configured in "USB Mode" and when a USB stick is inserted, the importation of a VPN Configuration is directly written on the USB stick. If the VPN Client is configured in "USB mode" but no USB stick is inserted (the USB icon in the bottom left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

6.6.2. Merge of VPN Configurations

The Proxicast 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.

Merge of VPN Configurations can be done in several ways.

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



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

3. Import new VPN Configuration via command line.

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

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

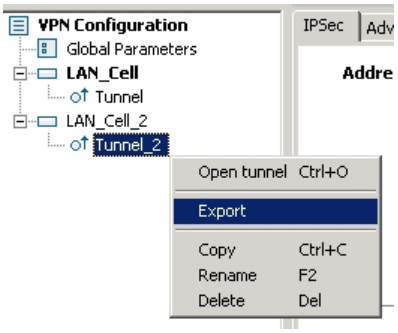
- Global parameters are not imported in case at least one tunnel was already configured prior to import and user selects 'Add' VPN Configuration in the popup.
- Global parameters are imported in case the user selects 'Replace' or no tunnel was configured prior to import.
- Tunnel name conflict between existing and imported VPN Configurations are solved by software automatically by adding an increment between bracket e.g. tunnel_office(1) to the imported tunnel names (i.e. both Phase1 and Phase 2).

6.6.3. Splitting a VPN Configuration

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

To export a single tunnel, follow these steps:

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



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

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

6.7. USB Mode

6.7.1. What is USB Mode ?

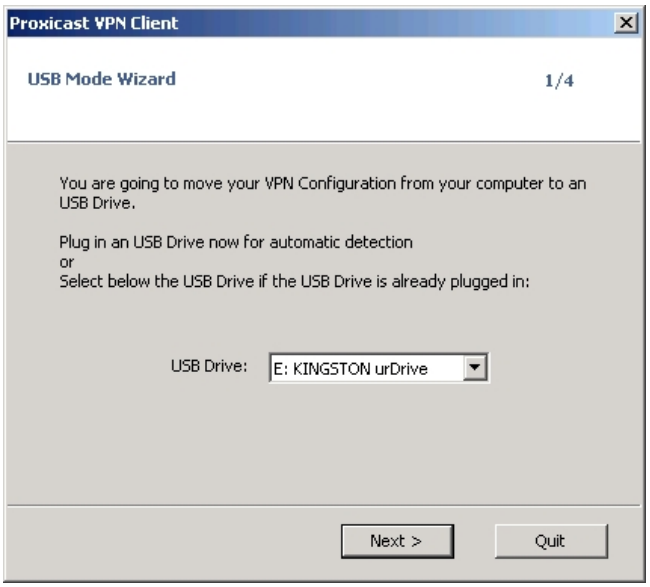
The Proxicast VPN Client brings the capability to secure VPN configurations and VPN security elements (e.g. PreShared key, Certificates, …) by the use of an USB Memory Stick.

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

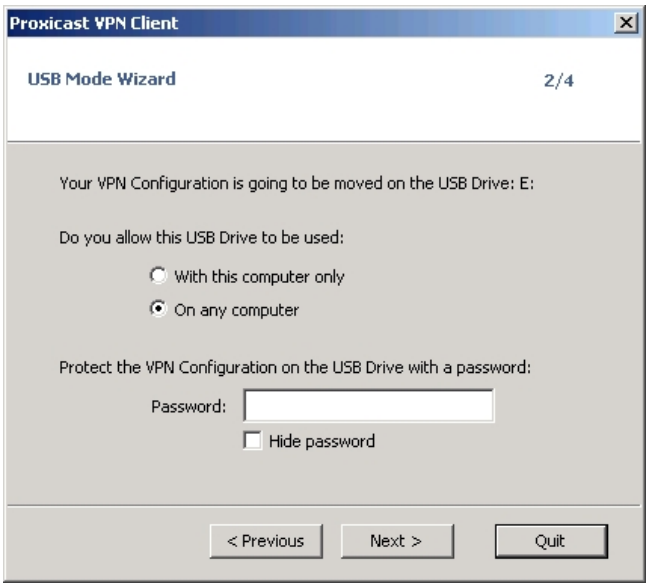
Once done, you just need to insert the USB Stick to automatically open tunnels. And you just need to unplug the USB Stick to automatically close all established tunnels.

6.7.2. How to set USB Mode ?

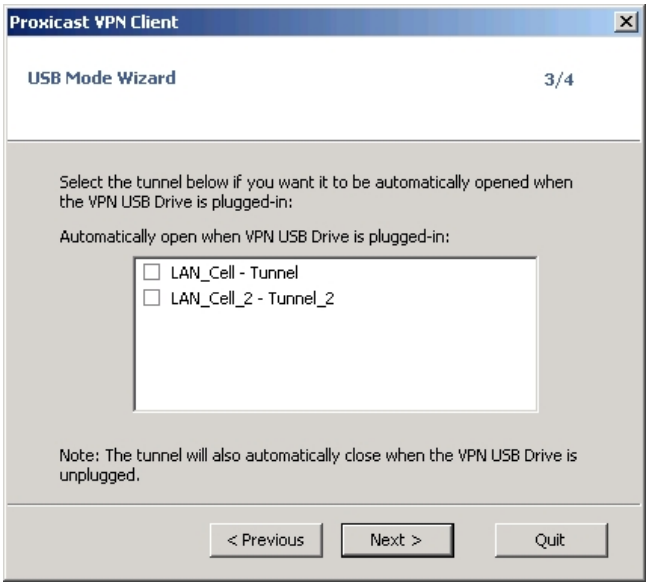
The USB Mode is initiated from the ‘Configuration > Move to USB Drive’ menu



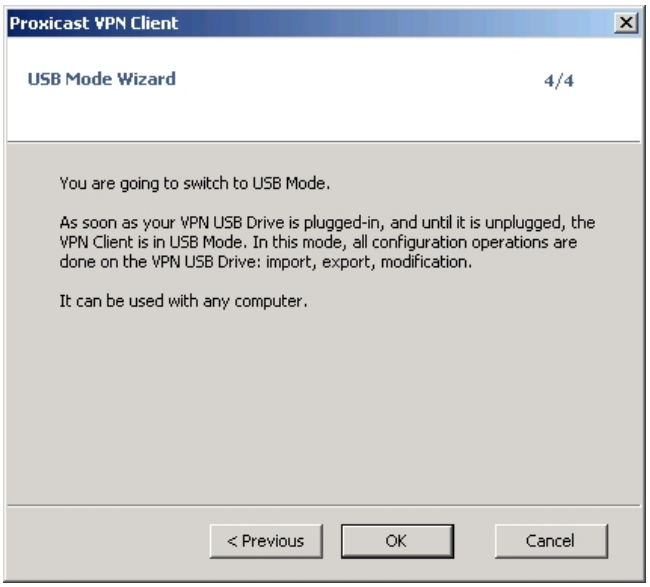
Select which computers the USB stick should be associated with. Optionally protect the USB stick with a password that will be required when it is inserted.



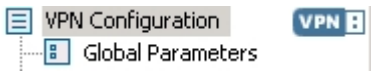
Next, select which tunnels are to be opened automatically when the USB stick is inserted.



Confirm that you are ready to switch to USB Mode.



When the USB stick is removed, all configuration information in the VPN Client will be erased. When the USB stick is reinserted, the configuration will be automatically loaded and the USB stick icon will be displayed Configuration and Connection Panels



6.8. Options

The **'Tools' > 'Options'** menu allows users to configure a number of system-wide parameters including password protections, GUI options, start-up behavior, and certificate management.

6.8.1. Password Protection

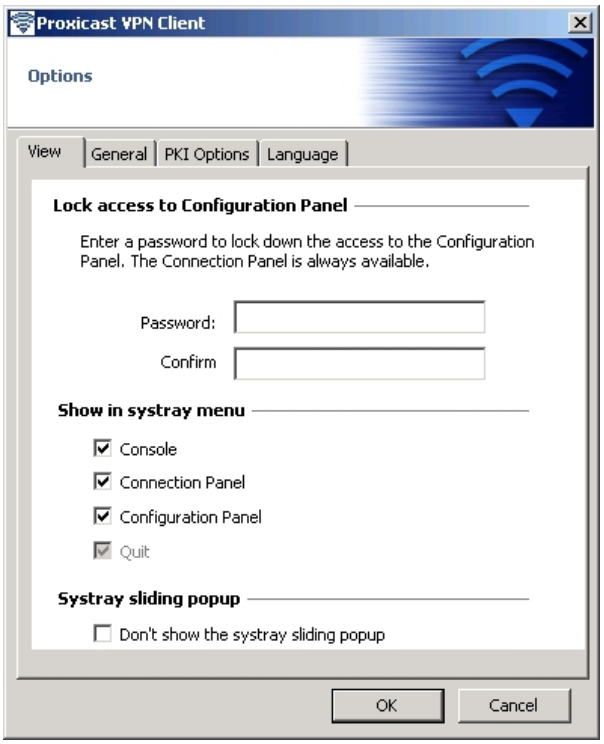
The Proxicast VPN Client software allows IT managers to protect access to the VPN security policy by a password. From this point forward, this password is called "Administrator password".

The provided protection applies on one hand to the Configuration Panel access (regardless of which way the Configuration Panel is opened, the password is requested), on the other hand to all possible operations on the VPN security policy: changes, registration, import, export. Thus, any import of a VPN security policy will be enabled if the right Administrator password is provided.

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

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

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



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

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

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

To remove the protection via password, empty both "Password" and "Confirm" fields and click OK.

6.8.2. GUI Appearance

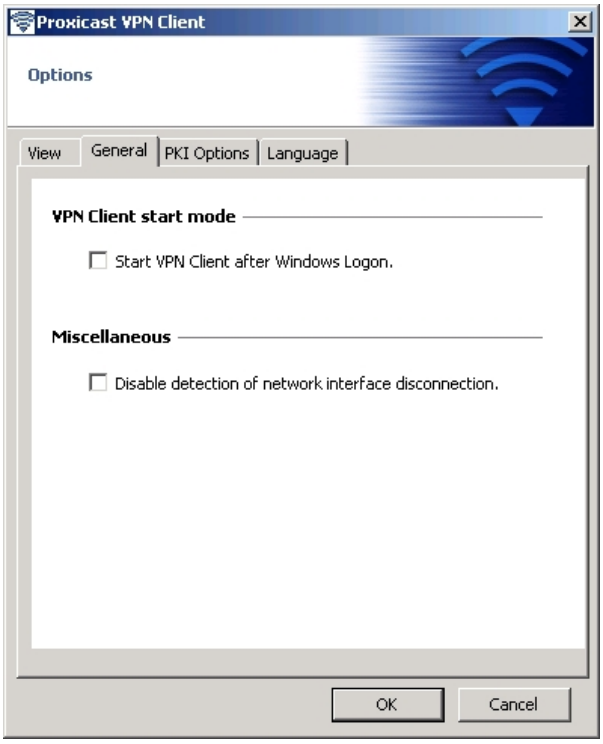
The options on the "View" tab of the "Options" window also allow to hide all software interfaces, by removing from the taskbar menu the "Console", "Configuration Panel" and "Connection Panel" items.

The menu in the taskbar is then reduced to the single list of available VPN tunnels.

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

Note: The 'Quit' item for the systray menu is disabled in the GUI software. It can nevertheless be removed during the software setup, through the setup option "`-menuitem`" (see section 'Setup Options')

6.8.3. General Options



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

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

Disabling the disconnection detection
In its generic behavior the VPN Client closes the VPN tunnel (on its side), when it finds a problem communicating with the remote VPN gateway. In unreliable local networks, prone to frequent micro-disconnections, this feature can have drawbacks (which can go up to unable to open a VPN tunnel).

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

6.9. Certificate Management

6.9.1. Certificate Management overview

The Proxicast IPsec VPN Client is fully integrated with most PKI solutions in the market. The software implements a set of features for different certificates storage (files, Windows Certificate Store, Smart Card and Token) and a set of rules to define the certificates to use (CRL topic key usage, etc...)

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

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

The certificate configuration is divided into three steps:

1. "Certificate" tab of the Phase 1 involved
2. "PKI Options" tab in the window ‘Tools’ > ‘Options’ in the Configuration Panel
3. An optional startup configuration file: vpnconf.ini

6.9.2. Setup a Certificate

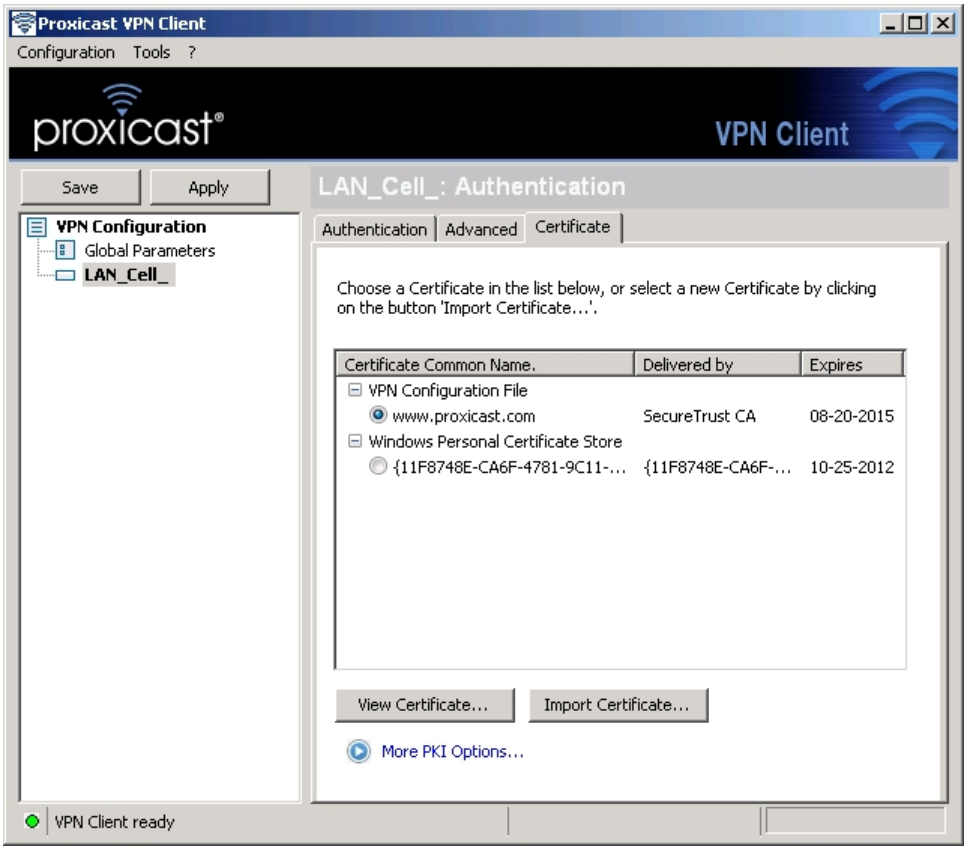
VPN Client allows you to assign a user certificate to a VPN tunnel. There can be only one certificate per tunnel, but each tunnel can have its own certificate.

The VPN Client allows you to select a certificate stored:

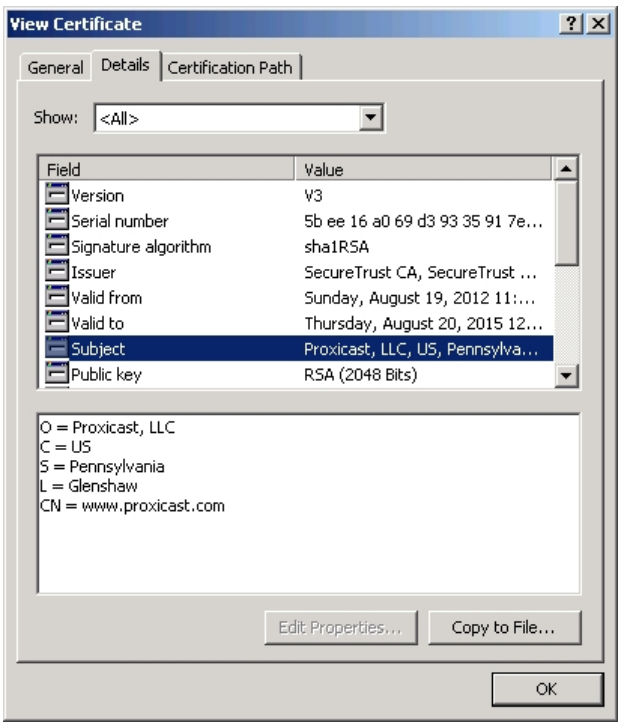
- In the VPN Configuration file (see "Import Certificate")
- In the Windows certificate store (see "Windows Certificate Store")
- On a smart card or a token (see "Configure a Smart Card or Token")

The Phase 2 "Certificate" tab lists all relevant media available on the computer, which contain certificates. If a media does not have a certificate, it is not displayed in the list (e.g. if the VPN Configuration file contains no certificate, it does not appear in the list).

By clicking one of the media, the list of certificates it contains is displayed. Click on the desired certificate to assign to the VPN tunnel.



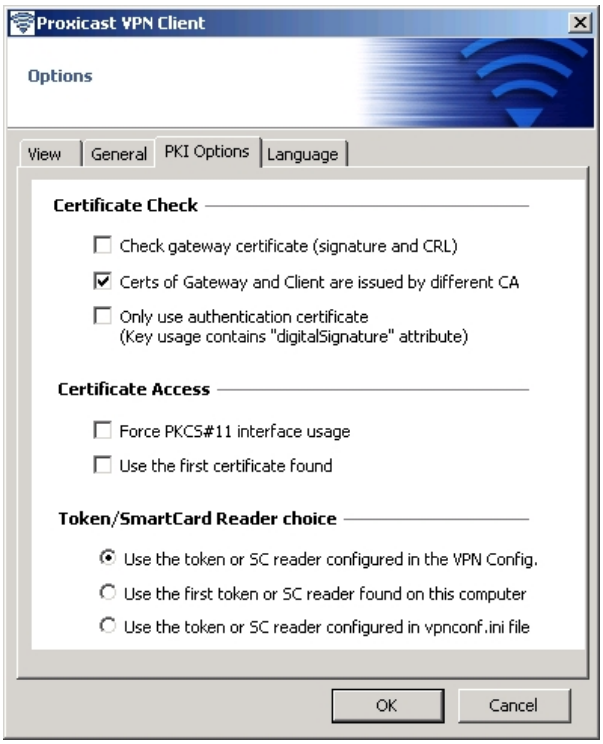
Once the certificate is selected, the button "View Certificate" allows to view the details of the certificate.



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

6.9.3. PKI Certificate Options

The Proxicast IPsec VPN Client offers many possibilities to define the certificate to use, as well as smart cards or tokens.



Check Gateway Certificate	This option forces the VPN Client to check the certificate of the VPN gateway during the opening of the tunnel. The certificate expiration date is checked, as well as the signature of certificates in the certification chain and the associated CRL (certificate not revoked).
Gateway and Client certificate issued by different CA	If the VPN Client and Gateway use certificates from a different CA, this box must be checked (it allows the VPN Client to adapt the opening protocol of the VPN tunnel)
Only use authentication certificate	When this option is checked, only the "Authentication" Certificate type (i.e. "Key Usage" is "Digital signature") are taken into account by the VPN Client. (2)
Force PKCS#11	The VPN Client can manage PKCS11 and CSP readers. When this option is checked, the VPN Client takes into account PKCS11 readers and Tokens.
First Certificate found	When this option is checked, the VPN Client uses the first certificate found on the specified smart card or token, regardless of the subject of the certificate that may be configured in the Local ID field of the Phase 1 "Advanced" tab involved.
Use VPN Configuration	Smart Card or Tokens readers used are stored in the VPN onfiguration. The VPN Client favors readers or Token specified in the VPN Configuration file.
Use first reader found	The VPN Client uses the first Smart Card reader or Token found on the computer to search for a certificate.
Use VpnConf.ini	The VPN Client favors the configuration file vpnconf.ini to consider smart card readers or tokens to be used.

6.9.4. Import a Certificate

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

1. In the "Certificates" tab of a Phase 2, click on "Import a Certificate..."
2. Select "PEM Format" or “P12 Format”
3. Select ("Browse") root certificates, user and private key to import Note: The file with the private key must not be encrypted.
4. Validate

6.9.5. Using Windows Certificate Store

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

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

6.9.6. Use a VPN Tunnel with a Certificate from a Smart Card

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

If the smart card is not inserted, or if the token is not available, the tunnel does not open.

If the certificate does not fulfill the required conditions (see "Rules for certificate ("PKI Options" tab)"), the tunnel does not open. If the PIN code entered is incorrect, the VPN Client notifies the user that has 3 consecutive attempts before locking out the Smart Card.

The VPN Client implements a mechanism for automatically detecting the insertion of a smart card. Thus, the tunnels associated with the certificate contained on the smart card are opened automatically upon inserting the Smart Card. Conversely, removal of the smart card automatically closes all associated tunnels.

This functionality is achieved by checking the option "Open tunnel automatically when the USB drive is inserted" (see chapter "IPsec Advanced").

7. Deployment

7.1. Embedded VPN Configuration

A VPN Configuration ".tgb" file embedded within the IPSec VPN Client Setup (unzipped) is automatically imported by the IPSec VPN Client during software installation.

To create a setup with a VPN Configuration:

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 simply unzip the IPSec VPN Client Setup.
3. Add the VPN Configuration (e.g. "myconfig.tgb") file into the unzipped setup directory.
4. Deploy the package to the user (the VPN Configuration will be used during the setup)

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

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 a password.
3. Configuration of the Systray menu items.
4. Other options for Software Start, License Number, Auto Software Activation, no trial windows, languages and Activation email.

Syntax example:
```
Proxicast_VPNClient_Setup.exe /S --license=0123456789ABCDEF0123
--start=1 --activmail=smith@smith.com
```

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

7.2.2. Setup option for GUI mode

Syntax: **`--guidefs=full|user|hidden`**
Enables 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.

7.2.3. Setup option for GUI mode access control

Syntax: **`--password=mypwd`**
Controls access to the VPN GUI with a password.

The user will be asked for the password:

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

Example: **`--guidefs=user --password=admin01`**
These 2 options enable the GUI to be locked in "Connection Panel" mode only, while access to the Configuration Panel is protected with a password.

7.2.4. Setup option for systray menu items

Syntax: **`--menuitem=[0...31]`**
Specifies the items of the systray menu that the IT manager wants to keep.

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

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

Note 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 **`'guidefs=hidden'`**.
By default, **`guidefs=hidden`** sets the systray menu item list to Quit + Console. (The items 'Save & Apply' and 'Connection Panel' are not visible). However the use of **`'menuitem'`** overrides **`'guidefs'`**.
That means the following: "**`--guidefs=hidden --menuitem=1`**" will set a systray menu with only the 'Quit' item.

7.2.5. Other Setup options

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

Syntax: **`--license=[license_number]`**
Configures the license number. The License Number is a set of 24 hexadecimal characters. Old License Numbers might be 20 hexadecimal characters.

Syntax: **`--start==[1|2|3]`**
Configures the start mode for the VPN Client: **`after the logon windows [1], during the boot [3], or manually [2]. Default is [1].`**

Syntax: **`--activmail=[activation_email]`**
Define the email address used for activation confirmation. During the activation process, the edit box used for entering this email will be disabled

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

Syntax: **`--noactivwin=1`**
No display of the 'Trial window' once software started until trial period ends. User doesn't know he is in trial period and software will be disabled at the end of trial period. It means that if the user tries to launch the software after the end of trial period, the software will start and open the 'Trial window' but the 'Evaluate' button will be disabled.

Syntax: **`--lang=[language code]`**
This option specifies the language for the The Proxicast IPSec VPN Client software and installation software. Available languages are listed below.

ISO 639-2 code	Language code	English name
EN	1033 (default)	English
FR	1036	French
ES	1034	Spanish
PT	2070	Portuguese
DE	1031	German
NL	1043	Dutch
IT	1040	Italian
ZH	2052	Chinese simplified
SL	1060	Slovenian
TR	1055	Turkish
PL	1045	Polish
EL	1032	Greek
RU	1049	Russian
JA	1041	Japanese

FI	1035	Finnish
SR	2074	Serbian
TH	1054	Thai
AR	1025	Arabic
DK	1030	Danish
CZ	1029	Czech
HU	1038	Hungarian
NO	1044	Norwegian
FA	1065	Persian
KO	1042	Korean

Example:
Proxicast_VPNClient_Setup.exe /S --license=0123456789ABCDEF0123 --start=1 --activmail=smith@smith.com

7.3. Command Line Options

7.3.1. Command line options

Several command line options 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 Proxicast 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 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 just before the disconnection.

7.3.3. Import or Export VPN Configuration options

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

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

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

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

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

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

" **/add:** " imports a new VPN Configuration into an existing VPN Configuration and merges both into a single VPN Configuration. This command line option may be used either if the VPN Client is running or not. This command doesn't start the VPN Client if it is not running already.

" **/pwd:[password]**" sets a password for import operations. This option must be used together with the /import or /importonce options.

All 5 arguments "**import**", "**importonce**", "**export**", "**exportonce**" and "**add**" are mutually exclusive and cannot be used together.

7.3.4. Opening or closing VPN Tunnel options

The Proxicast VPN Client can open or close a VPN tunnel from the command line. Both command line options can be invoked while The Proxicast 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 doesn't handle relative paths (e.g. "..\..\file.tgb"). Double-quotes are supported allowing paths containing spaces.
If the specified tunnel is already open, this command line has no effect.

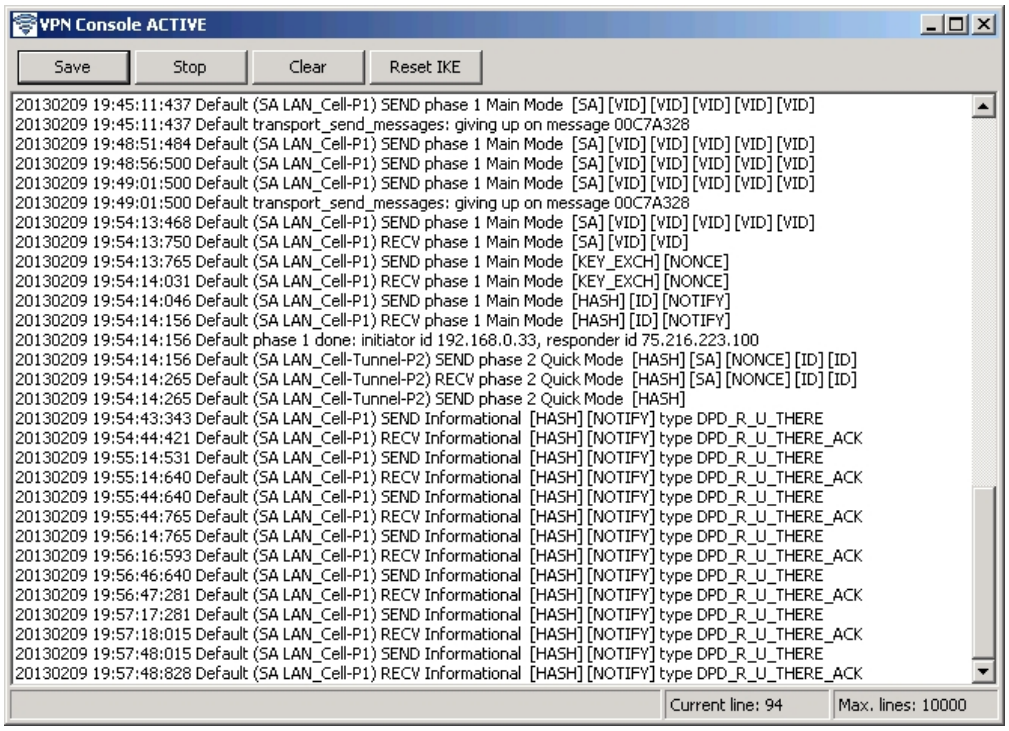
" **[path]\vpnconf.exe /close:[phase1-phase2]** " where **[path]** is the VPN Client installation directory, and **[phase1-phase2]** are the Phase1 and the Phase2 names in the VPN Configuration file. This command doesn't handle relative paths (e.g. "..\..\file.tgb"). Double-quotes are supported allowing paths containing spaces.
If specified tunnel is already closed, this command line has no effect.

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

Restriction note:
- Execution of these command line options will open the Software Graphical User Interface (GUI). This restriction will be removed in further software release.

8. Console and Logs

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 and troubleshooting connection issues.



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

9. Contacts

Online Web Support

Please refer to support.proxicast.com for additional support documentation and access to our Knowledgebase which contains many resources such as.TechNotes, Frequently Asked Questions, sample configurations and software updates.

E-Mail Support

Support E-mail: support@proxicast.com

Please provide the following information when you contact customer support:

- Software version number
- Operating system
- Brief description of the problem and the steps you've taken to try to solve it

Corporate Headquarters (Worldwide Customer Support)

- Sales E-mail: sales@proxicast.com
- Telephone: 877-777-7694 (412-213-0018)
- Fax: 412-492-9386
- Web Site: www.proxicast.com, support.proxicast.com
- Regular Mail:

  Proxicast, LLC
  312 Sunnyfield Drive, Suite 200
  Glenshaw, PA 15116-1936

INDEX

V

W

X