Route*Finder*™

Internet Security Appliance

IPSec VPN Client

Install User Guide

MultiTech® Systems

RouteFinder™ IPSec VPN Client
Install User Guide
S000395A Revision A

Multi-Tech Systems, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Record of Revisions

Revision	Date	Description
A	01/09/06	Manual released. This user guide documents software version 3.00

Patents

This product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562**; **5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

Trademarks

Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, the Multi-Tech logo, and RouteFinder. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. SSH, ssh, SSH Secure Shell, and SSH Sentinel are trademarks or registered trademarks of SSH Communications Security Corp.

All products or technologies are the trademarks or registered trademarks of their respective holders.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Tech Support (800) 972-2439
Internet Address: http://www.multitech.com

Contents

Chapter 1 - Introduction and Description

The Multi-Tech Systems, Inc. RouteFinder VPN client is an IPSec VPN software for Windows that allows secure connections over the Internet usually between a remote worker and the corporate Intranet. IPSec is the most secure way to connect to the enterprise as it provides strong user authentication, strong tunnel encryption with the ability to cope with existing network and firewall settings.

The RouteFinder VPN client software is a companion software for Multi-Tech's RouteFinder product line. The RouteFinder products are an internet security applicance that lets you use data encryption and the internet to securely connect to telecommuters, remote offices, customers, or suppliers while avoiding the cost of expensive private leased lines.

VPN Client Features

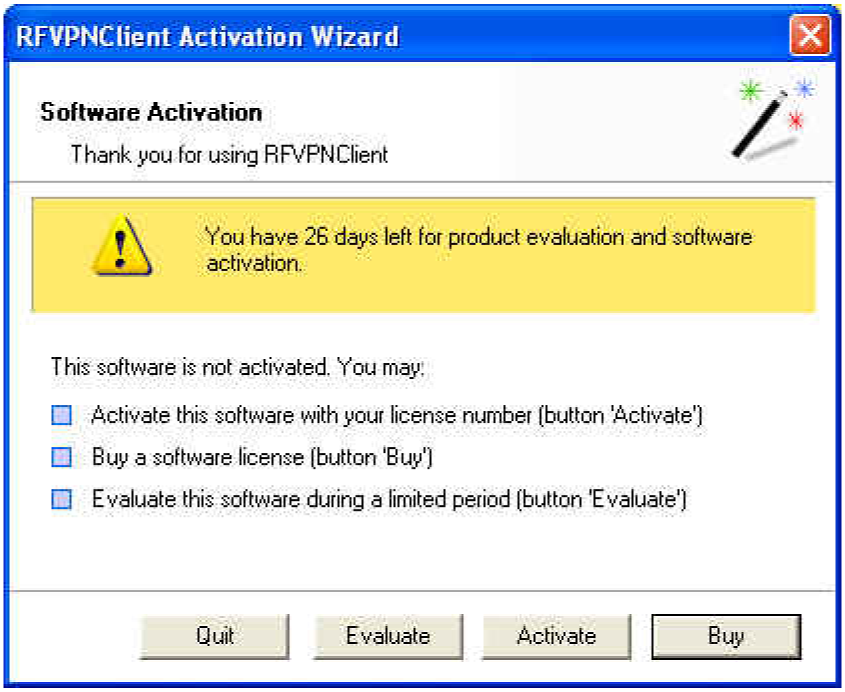
Windows supported versions	Win98 ,Me, Win2000, WinXP
Connection Mode	It operates as a peer-to-peer VPN in a "point – to – multiple" mode, without a gateway or server. All connections types like Dial up, DSL, Cable, GSM/GPRS and WiFi are supported.
Tunneling Protocol	Full IKE support: Our IKE implementation 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 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
Encryption	It provides 3DES, DES and AES 128/192/256bits encryption. Additional capabilities like DH1536, DH2048 and RSA 2048 key are also provided.
User Authentication	X-AUTH support PreShared keying and X509 Certificates support. It is compatible with most of the currently available IPSec gateways Support of Group 1, 2, 5 and 14 (i.e. 768, 1024, 1536 and 2048) Flexible Certificate support (PEM, PKCS12, ...)
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 can offer to remote users a highly reliable secure connection to the corporate network. Redundant Gateway feature allows the RouteFinder VPN Client to open an IPSec tunnel with an alternate gateway in case the primary gateway is down or not responding.

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. IPSec VPN Client).
USB Stick	VPN configurations and security elements (certificates, preshared key,…) can be saved into an USB Stick in order to remove authentication information from the computer.
Log console	All phase messages are logged for testing or staging purposes, and multiple filters (10) allows to easily narrow the view on specific aspects.
Invisible User Interface	Silent install and invisible graphical interface allow IT managers to deploy solutions while preventing user to misuse configurations.
Configuration building	User Interface and Command Line
Live update	Incremental install allows to replace encryption or authentication modules with new releases without rebooting the system. This works in addition to the live update feature which allows to update software from a central server.

Chapter 2 – Installing VPN Client

The RouteFinder 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, the Software Activation window appears with several options:



Software Activation

Thank you for using RFVPNClient

You have 26 days left for product evaluation and software activation.

This software is not activated. You may:

- □ Activate this software with your license number (button 'Activate')
- □ Buy a software license (button 'Buy')
- □ Evaluate this software during a limited period (button 'Evaluate')

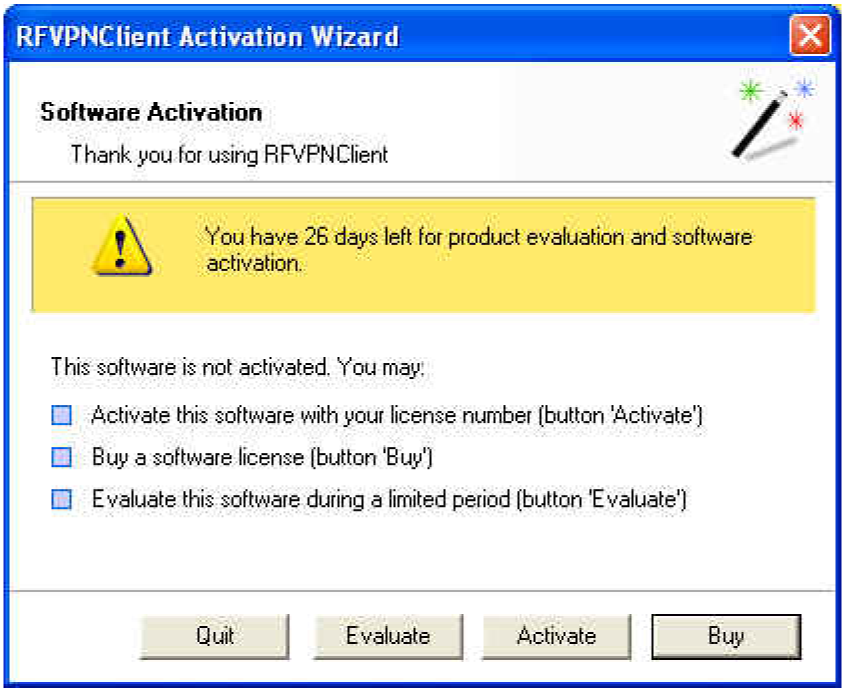
Button	Description
Quit	Closes this window and software.
Evaluate	Allows you to continue software evaluation. Evaluation period is displayed in the yellow bar above.
Activate	Allows you to activate the software online. This requires a License Number from your RouteFinder IPSec VPN Client CD. When clicking on the 'Activate' button, an Activation Wizard pops up.
Buy	Allows you to go online and purchase a license at the Multi-Tech Systems online store.

Caution: On Windows 2000 and XP, you must have administrator rights. If it is not the case, the installation stops after the language choice with an error message.

Software Evaluation

It is possible to use the RouteFinder IPSec VPN Client during the evaluation period (i.e. limited to 30 days) by clicking on 'Evaluate' button. When the IPSec VPN Client is on "Evaluation" mode, the register window appears each time the client is rebooted. Evaluation period is displayed in the yellow bar above.

Once evaluation period expires, the **Evaluate** button is no longer available and the software is disabled.



RFVPNClient Activation Wizard

Software Activation

Thank you for using RFVPNClient

You have 26 days left for product evaluation and software activation.

This software is not activated. You may:

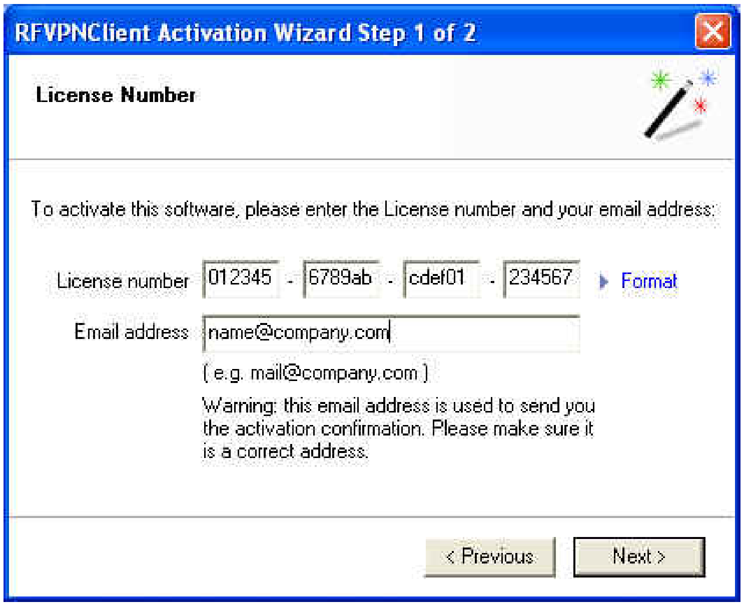
- Activate this software with your license number (button 'Activate')
- Buy a software license (button 'Buy')
- Evaluate this software during a limited period (button 'Evaluate')

Activation Wizard

The Activation Wizard is a two step Wizard that allows you to activate the software online. Activation requires the License Number from the RouteFinder IPSec VPN Client CD. Enter your License Number, email address and click 'Next' as shown below. Your email address will be used to send back an activation confirmation to the user.

Step 1 of 2: Enter License Number

Activation requires a License Number. Enter your License Number, your email address and click 'Next' as shown below. The email address will be used to send back an activation confirmation email to the user once activation has been successfully performed.



To activate this software, please enter the License number and your email address:

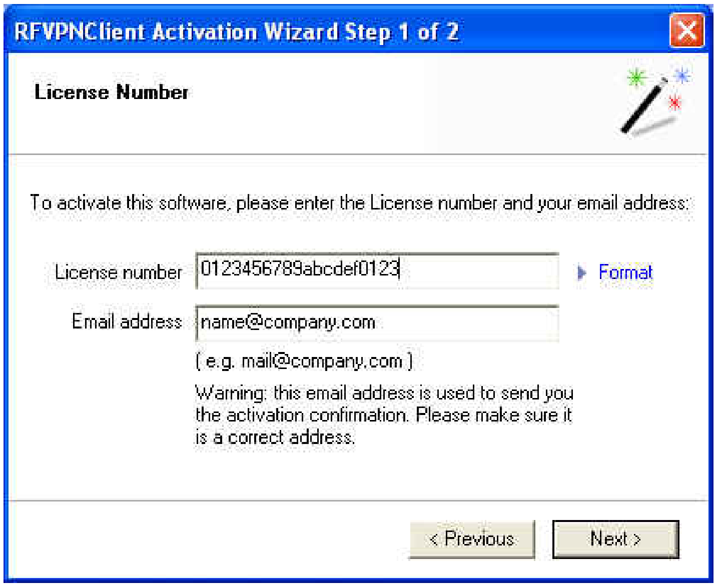
License number 012345 - 6789ab - cdef01 - 234567

Email address name@company.com

(e.g. mail@company.com)

Warning: this email address is used to send you the activation confirmation. Please make sure it is a correct address.

From VPN Client release 3.0 and later, the License Number format is a 24 digit number (i.e. 4 times 6 digits). Older License Number format is a 20 digit number. You can select the right format by clicking on 'Format' on the right end side next to the License Number field as follow:



To activate this software, please enter the License number and your email address:

License number 0123456789abcdef0123

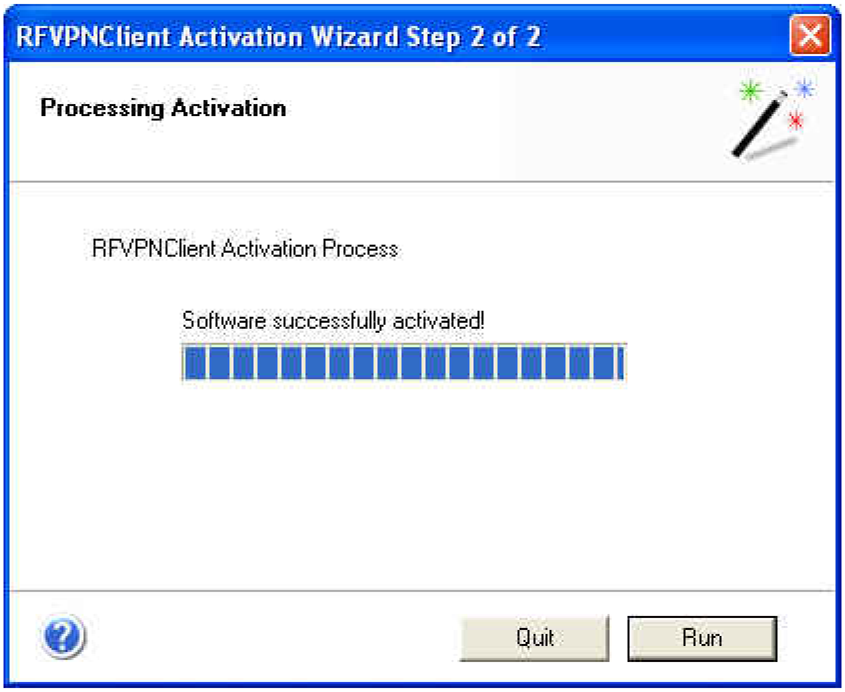
Email address name@company.com

(e.g. mail@company.com)

Warning: this email address is used to send you the activation confirmation. Please make sure it is a correct address.

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 anytime to change the License Number.



RFVPNClient Activation Wizard Step 2 of 2

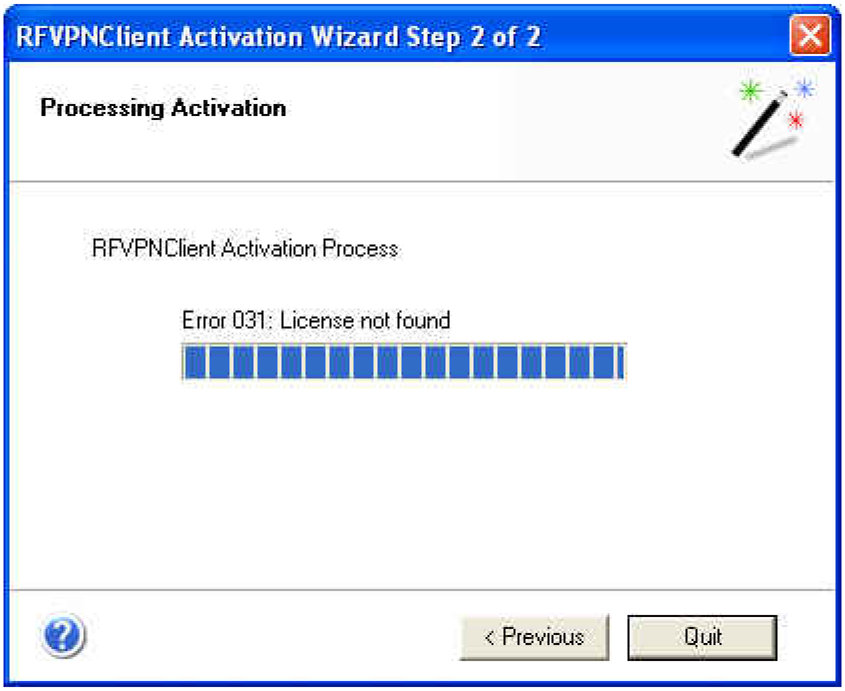
Processing Activation

RFVPNClient Activation Process

Software successfully activated!

Activation errors

In case of an error is returned by the online software activation server, as shown below, you shall click on the help button available in the window to get more online explainations and recommandations on how to proceed next.



RFVPNClient Activation Process

Error 031: License not found

Error	Error messages	Error explanations
031	License not found	License number doesn't exist in the activation server database. There must be an error in entering the license number. Also some old licenses are 20 digits only while new licenses are 24 digits.
032	Reserved	Reserved
033	Activation quota exceeded	Too many installations and activations have been processed for this specific license number. License numbers can not be used more than allowed by your IT department.
034	Wrong product code	The License number you've entered is not allowed on this software product. This software product requires a specific license number that is provided by the distributor of this software.
035	Wrong product code	The License number you've entered is not allowed on this software product. This software product requires a specific license number that is provided by Multi-Tech Systems, Inc. for this software.
036	Not allowed to activate this software release	Maintenance period is expired. In this case, you are not allowed to process any software upgrade. However you are allowed to continue using the previous version installed and activated on your computer.
050	Impossible to complete activation process	Activation server can not generate activate code for this license at the moment of activation

Error	Error messages	Error explanations
051	Impossible to complete activation process	Activation server can not generate activate code for this license at the moment of activation
052	Impossible to complete activation process	Activation server can not generate activate code for this license at the moment of activation
053	Cannot connect activation server	The activation server can't be contacted. Reasons can be broken Internet connection, activation server down, firewall and security policies.
054	Cannot connect activation server	The activation server can't be contacted. Reasons can be broken Internet connection, activation server down, firewall and security policies.
055	Activation code error	Activation code might have been modified after activation.

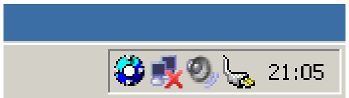
Chapter 3 - Navigating the User Interface

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

The VPN Client configuration is defined in a VPN configuration file. The software user interface allows creating, modifying, saving, exporting or importing the VPN configurations together with security elements (e.g. Preshared key, Certificates, ...).

System Tray

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

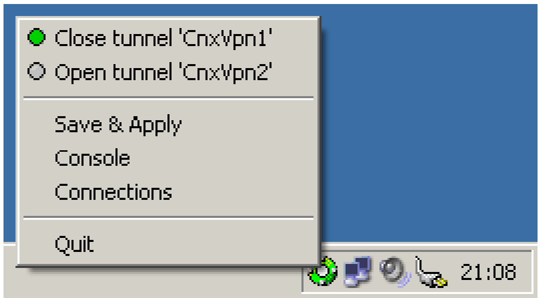


VPN Client application color code is the following:

Blue icon: no VPN tunnel is opened

Green icon: at least one VPN tunnel is opened

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



A right-button click shows the following menu:

Button	Description
Quit	Closes established VPN tunnels, stops the configuration user interface.
Save & Apply	Closes established VPN tunnels, apply latest VPN configuration modification and reopen all the VPN tunnels.
Console	Shows log window.
Connections	Opens the list of already established VPN tunnels. You can configure tunnels to open up automatically when the software starts.

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

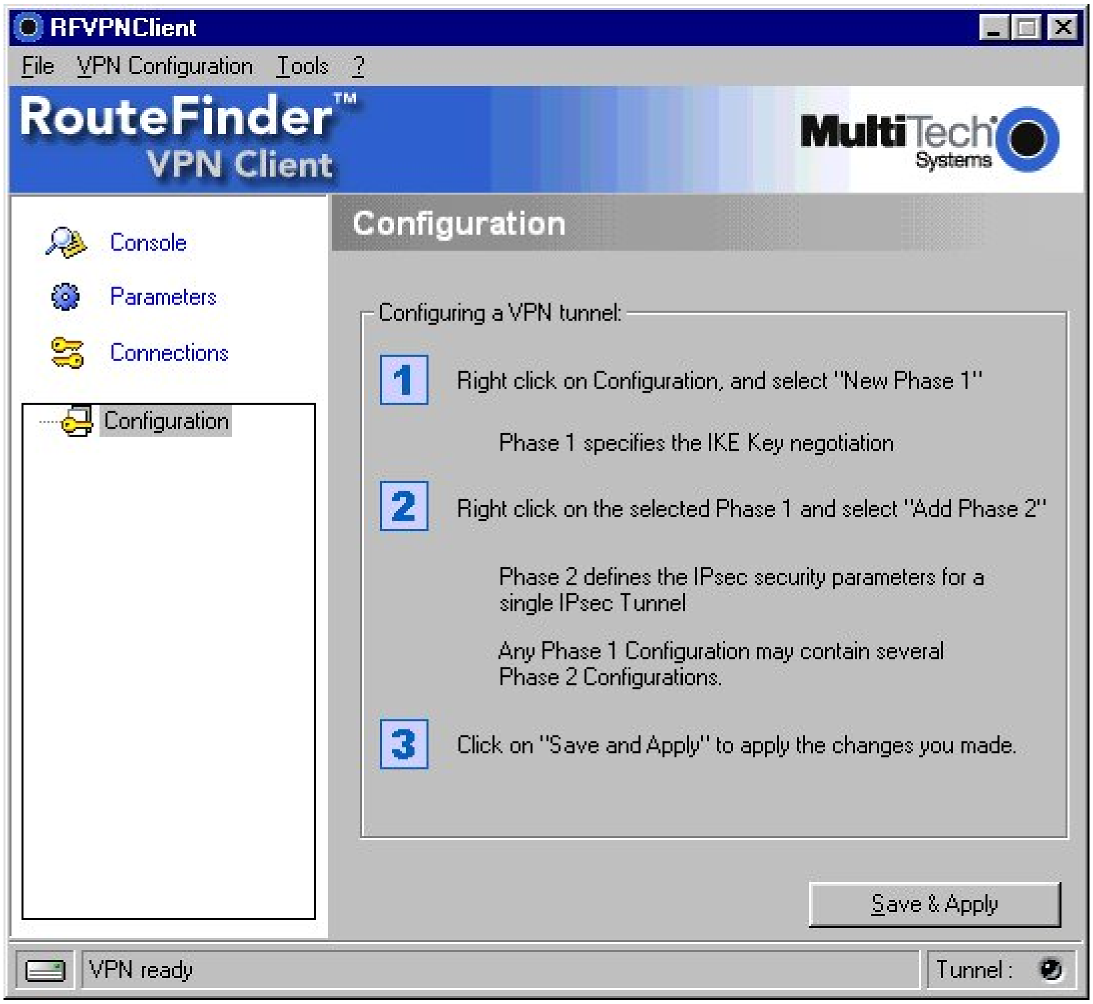
Tooltips over VPN Client icon shows the connection status of the VPN tunnel:

Tunnel Status	Description
Tunnel <tunnelname>	When one or more tunnels are established
Wait VPN ready...	When the IKE service is reinitializing
Name of VPN tunnel	When the VPN Client is up but with no opened tunnel.

Main Window

The main window is made of several elements:

Three buttons **Console, Parameters and Connections** in the left column. A tree list window in the left column that contains all the IKE and IPSec configuration. A configuration window in the right column that shows the associated tree level.



Configuring a VPN tunnel:

1 Right click on Configuration, and select "New Phase 1"

Phase 1 specifies the IKE Key negotiation

2 Right click on the selected Phase 1 and select "Add Phase 2"

Phase 2 defines the IPsec security parameters for a single IPsec Tunnel

Any Phase 1 Configuration may contain several Phase 2 Configurations.

3 Click on "Save and Apply" to apply the changes you made.

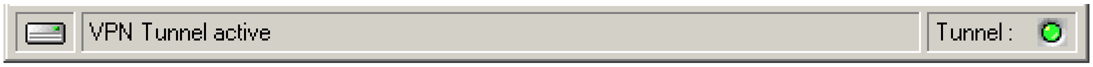
Menu Bar Buttons

There are several menus as followed:

Menu Bar Buttons	Description
File	Is used to import or export a configuration. It is also used to choose the location of the VPN Configuration: local, USB, server, or Token. It is finally used to configure miscellaneous preferences such as the way the VPN Client may start (e.g. before or after logon, ...).
Configuration	Contains all actions from tree control right-click menu. The Configuration menu gives also access to the Configuration Wizard.
Tools	Contains Console and Connections choice.
?	Gives access to online help and window About. ? menu also gives access to the Activation Wizard.

Status Bar

The status bar displays several information:



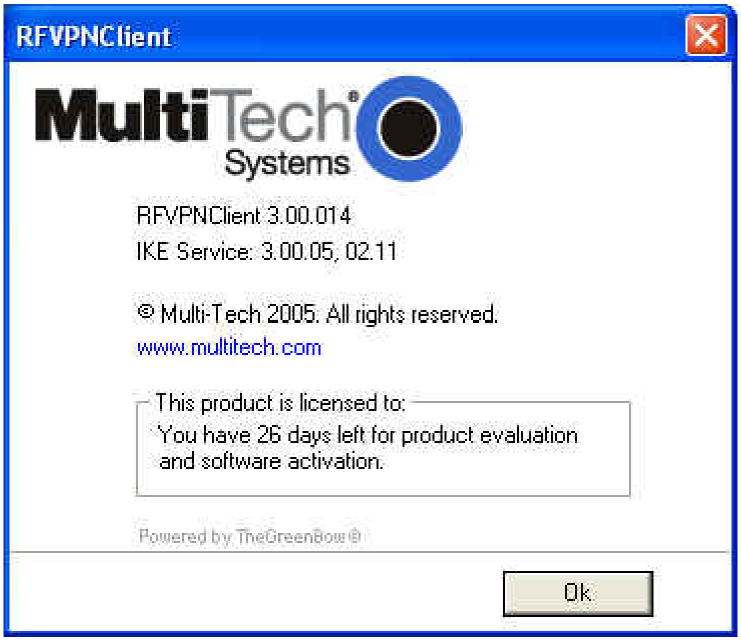
VPN Tunnel active

The left 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, or VPN client start up in progress, …)

The light box (right side) gives some information about tunnels (e.g. Green light Tunnel : 🟢 means at least one tunnel is open, Gray light Tunnel : ⚫ means no tunnel open)

Windows About

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



RFVPNClient 3.00.014
IKE Service: 3.00.05, 02.11

© Multi-Tech 2005. All rights reserved.
www.multitech.com

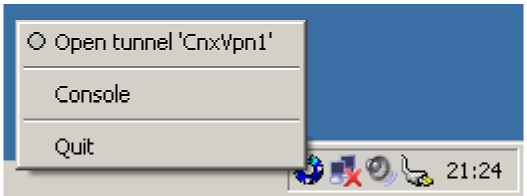
This product is licensed to:
You have 26 days left for product evaluation and software activation.

Powered by TheGreenBow ®

Hidden Interface

The graphical user interface can be hidden to the end user. We provide configuration tools for IT managers that prevent the end user from changing their configuration. Access to the configuration user interface can be restricted with configuration tool VPNHIDE. See section Configuration Tools.

In that case, the Main window can not be opened and showed by double-clicking on desktop icon, by selecting Start menu. Right-click over the icon in taskbar is limited to "Console" access, quitting the software, and opening/closing the configured tunnels:



Wizards

There are two Wizards available:

VPN Configuration Wizard can be launched from the Menu 'VPN Configuration' > 'Config Wizard'.

Software Activation Wizard can be launched from the Menu '?' > 'Activation Wizard'.

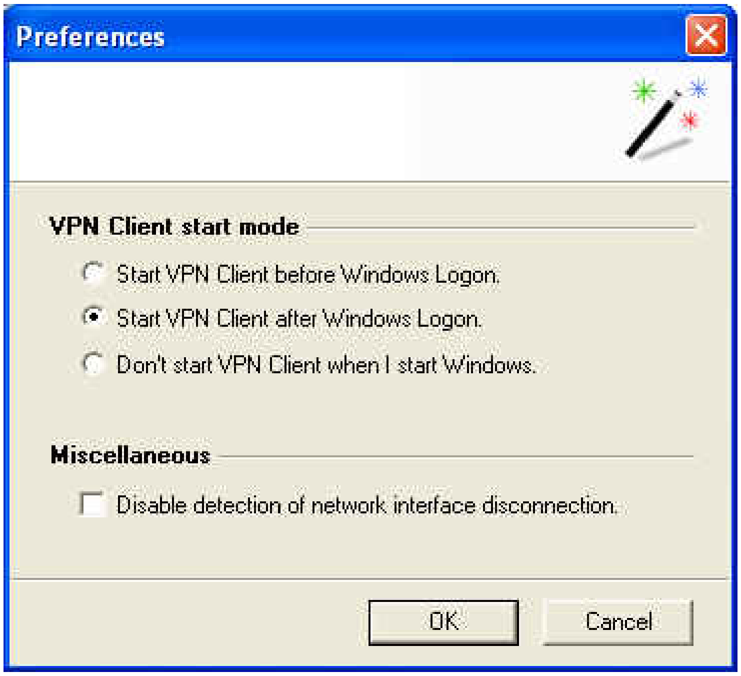
Preferences

Preferences window allows you to define:

Start up mode of the software

Enable/Disable the detection of network interface disconnect feature.

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



VPN Client start mode

○ Start VPN Client before Windows Logon.

● Start VPN Client after Windows Logon.

○ Don't start VPN Client when I start Windows.

Miscellaneous

□ Disable detection of network interface disconnection.

VPN Client start mode

The RouteFinder VPN Client software has several start up modes, such as: Client can start with 3 different modes:

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

Start VPN Client after MS Windows logon.

Don't start VPN Client when I start MS Windows: VPN Client is launched by user or from a script (manual mode)

Miscellaneous

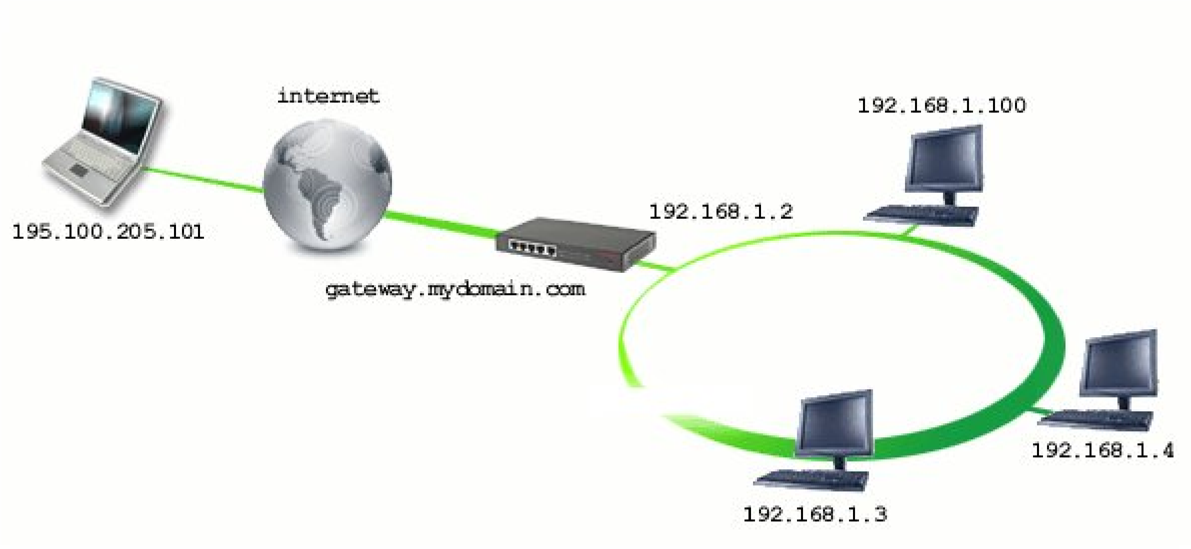
Disable detection of interface disconnect allows the VPN Client to maintain tunnels opened while the network interface disconnects momentarely, but very often. This type of behavior occurs when the interface used to open tunnels is unstable such as WiFi, GPRS and all 3G interfaces.

Chapter 4 - VPN Configuration

The RouteFinder VPN client provides a Configuration Wizard that allows the creation of a VPN configuration in three easy steps. This Configuration Wizard is designed for remote computers that need to get connected to a corporate LAN through a VPN gateway.

Lets look at the following example:

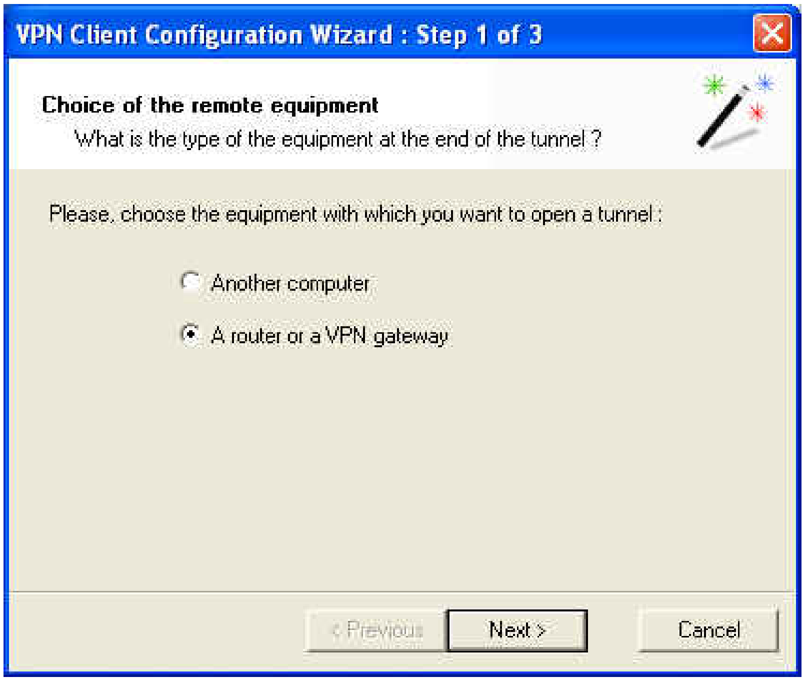
- The remote computer has a dynamic public IP address.
- It tries to connect the Corporate LAN behind a VPN gateway that has a DNS address "gateway.mydomain.com".
- The Corporate LAN address is 192.168.1.xxx. e.g. the remote computer wants to reach a server with the IP address: 192.168.1.100.



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

Step 1 of 3: Choice of remote equipment

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



VPN Client Configuration Wizard : Step 1 of 3

Choice of the remote equipment

What is the type of the equipment at the end of the tunnel ?

Please, choose the equipment with which you want to open a tunnel :

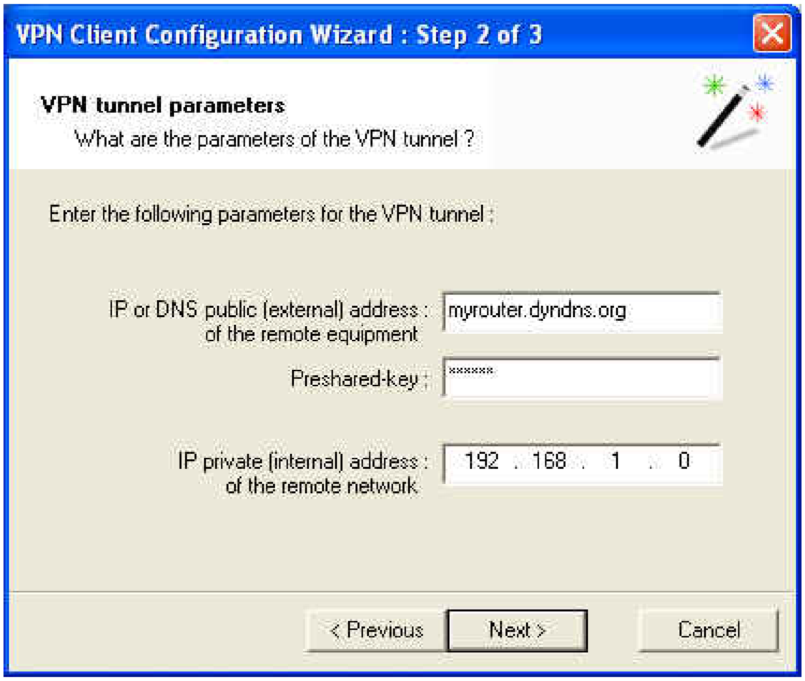
○ Another computer

● A router or a VPN gateway

Step 2 of 3: VPN tunnel parameters

You must specify the following information:

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



VPN Client Configuration Wizard : Step 2 of 3

VPN tunnel parameters

What are the parameters of the VPN tunnel ?

Enter the following parameters for the VPN tunnel :

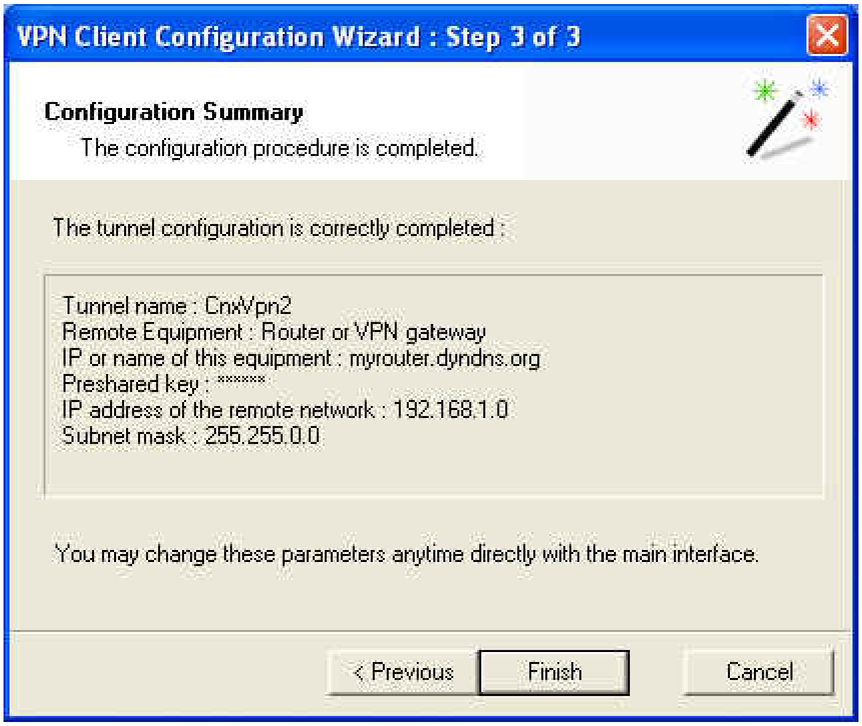
IP or DNS public (external) address of the remote equipment : myrouter.dyndns.org

Preshared-key : ******

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

Step 3 of 3: Summary

The third step summaries your new VPN configuration. Other parameters can be changed via the main interface (e.g. Certificates, virtual IP address, etc..).



Configuration Summary

The configuration procedure is completed.

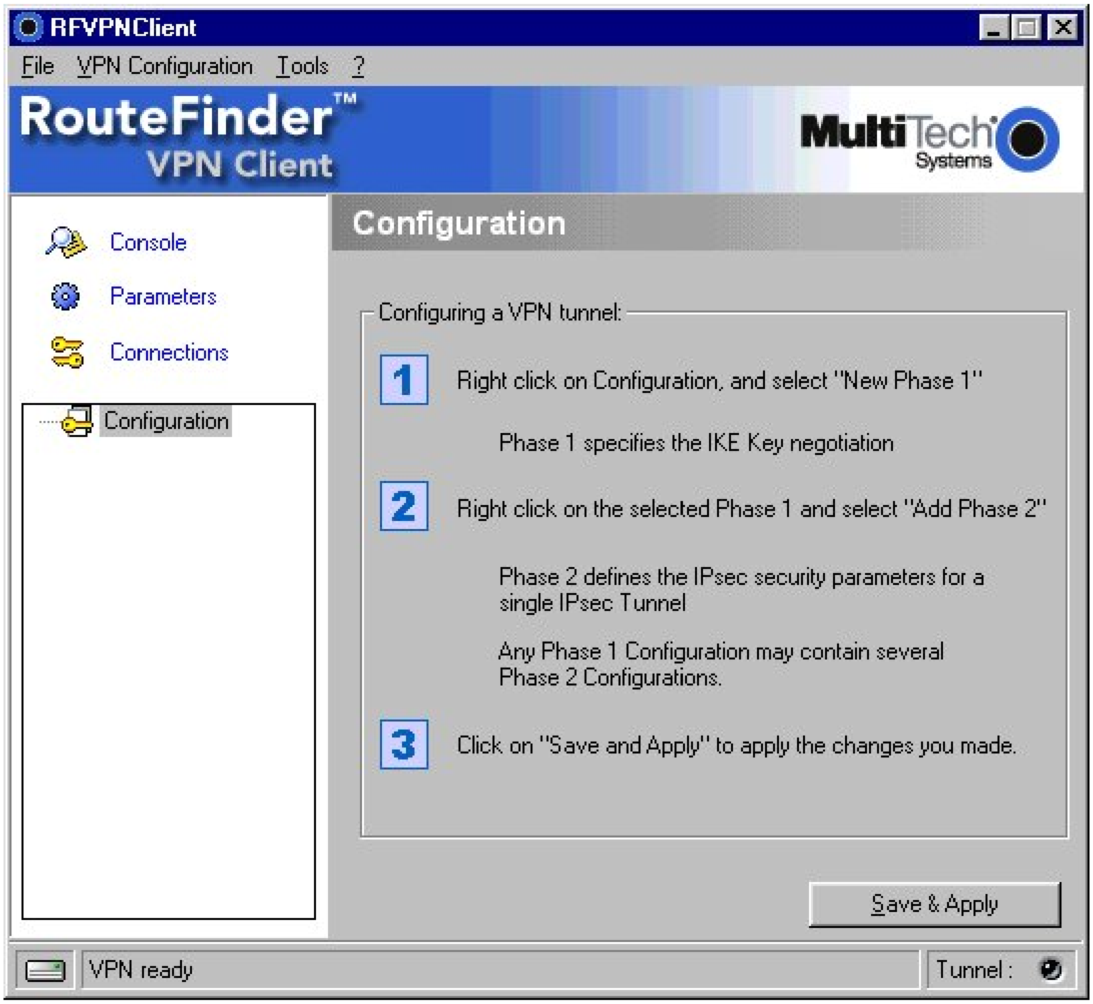
The tunnel configuration is correctly completed :

Tunnel name : CnxVpn2
Remote Equipment : Router or VPN gateway
IP or name of this equipment : myrouter.dyndns.org
Preshared key : ******
IP address of the remote network : 192.168.1.0
Subnet mask : 255.255.0.0

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

Tunnel Configuration

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



Configuration

Configuring a VPN tunnel:

1 Right click on Configuration, and select "New Phase 1"

Phase 1 specifies the IKE Key negotiation

2 Right click on the selected Phase 1 and select "Add Phase 2"

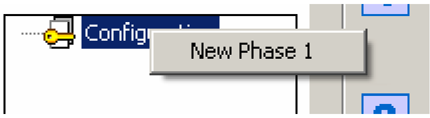
Phase 2 defines the IPsec security parameters for a single IPsec Tunnel

Any Phase 1 Configuration may contain several Phase 2 Configurations.

3 Click on "Save and Apply" to apply the changes you made.

VPN ready

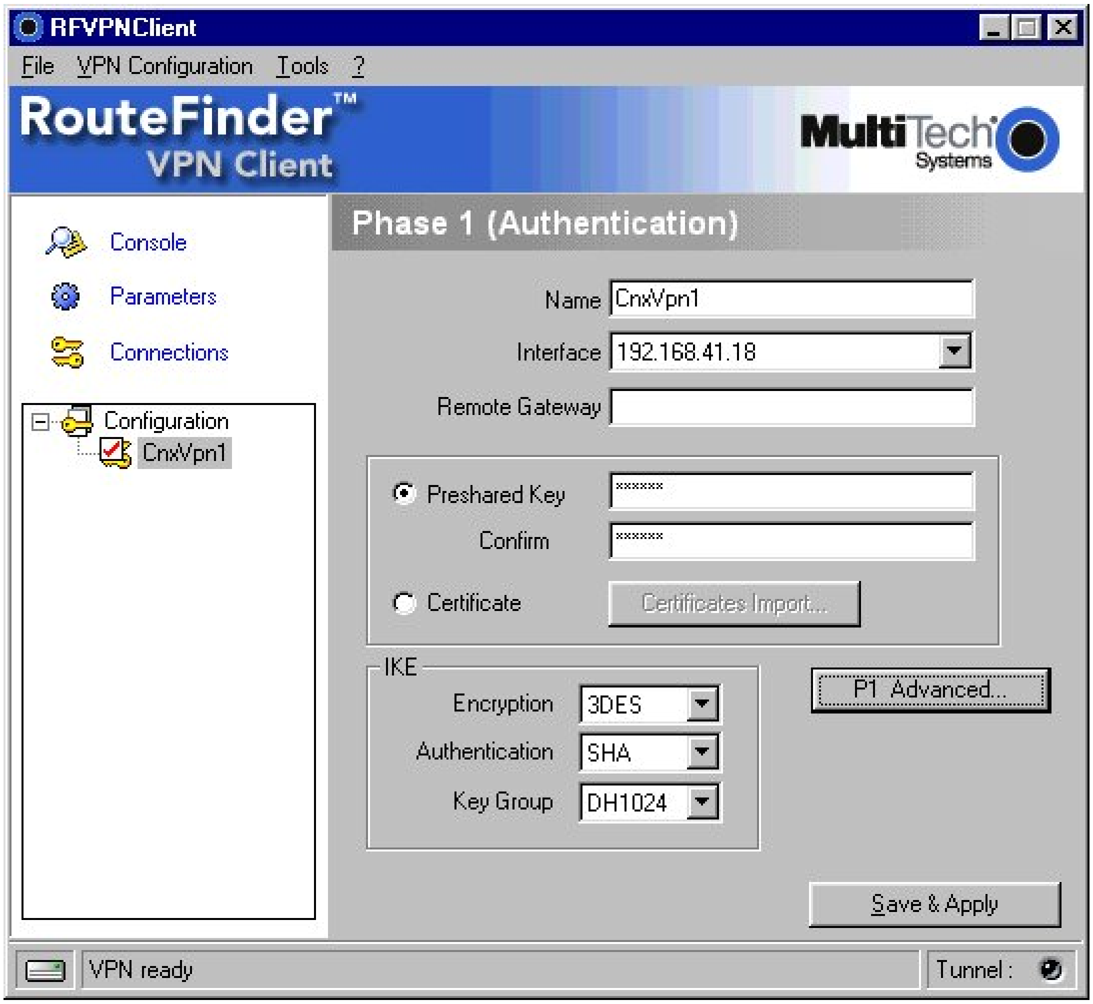
1. Right-click on 'Configuration' in the tree list window and select 'New Phase 1'



2. Configure Authentication Phase (Phase 1)

Phase 1 (Authentication)

Phase 1 (Authentication) window provides settings for Authentication Phase or Phase 1. It is also called IKE Negotiation Phase. Phase 1's purpose is to negotiate IKE policy sets, authenticate 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.



Phase 1 (Authentication)

Name: CnxVpn1

Interface: 192.168.41.18

Remote Gateway:

● Preshared Key: ******

Confirm: ******

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA

Key Group: DH1024

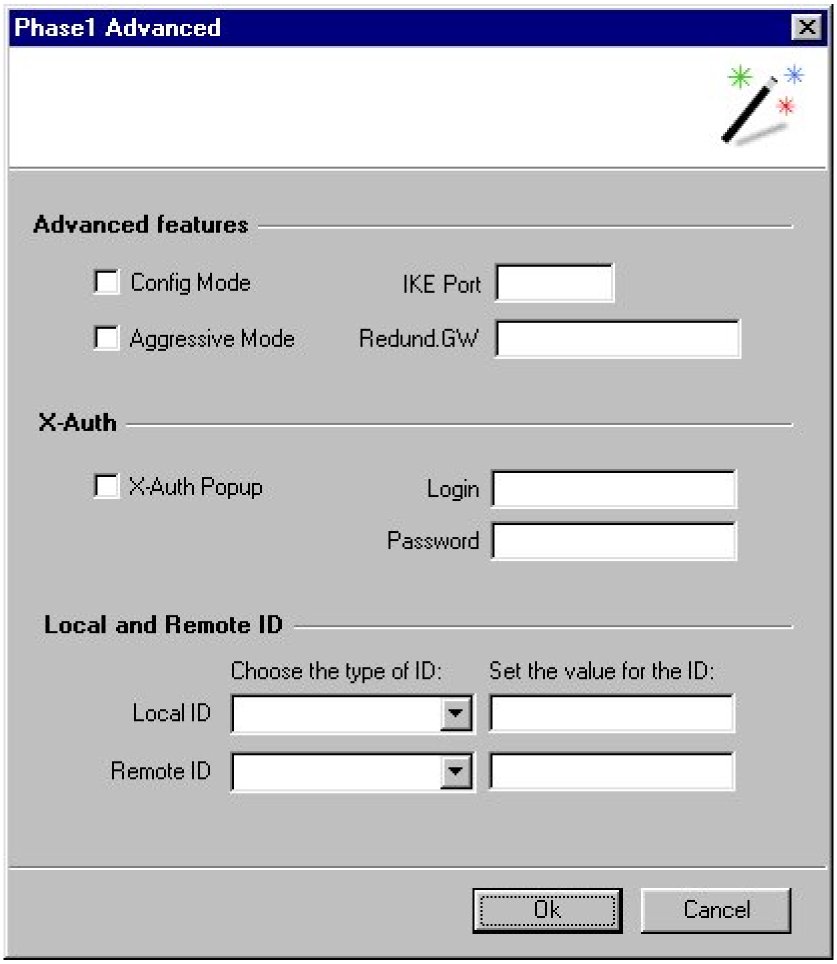
VPN ready

Tunnel :

Field	Description
Name	Label for Authentication phase used only to configure the user interface. This value is never used during IKE negotiation. It is possible to change this name at any time and read it in the tree control. Two Phase 1's can not 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 (when it is received dynamically by an ISP), select "*".
Remote Gateway	IP address or DNS address of the remote gateway (in our example: gateway.mydomain.com). This field is mandatory.
Pre-shared key	Password or key shared of the remote gateway.
Certificate	X509 certificate used by the VPN client (see certificate configuration).
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.

Phase1 Advanced

For advanced settings, click on the **P1 Advanced** button in the Phase 1 Authentication window.

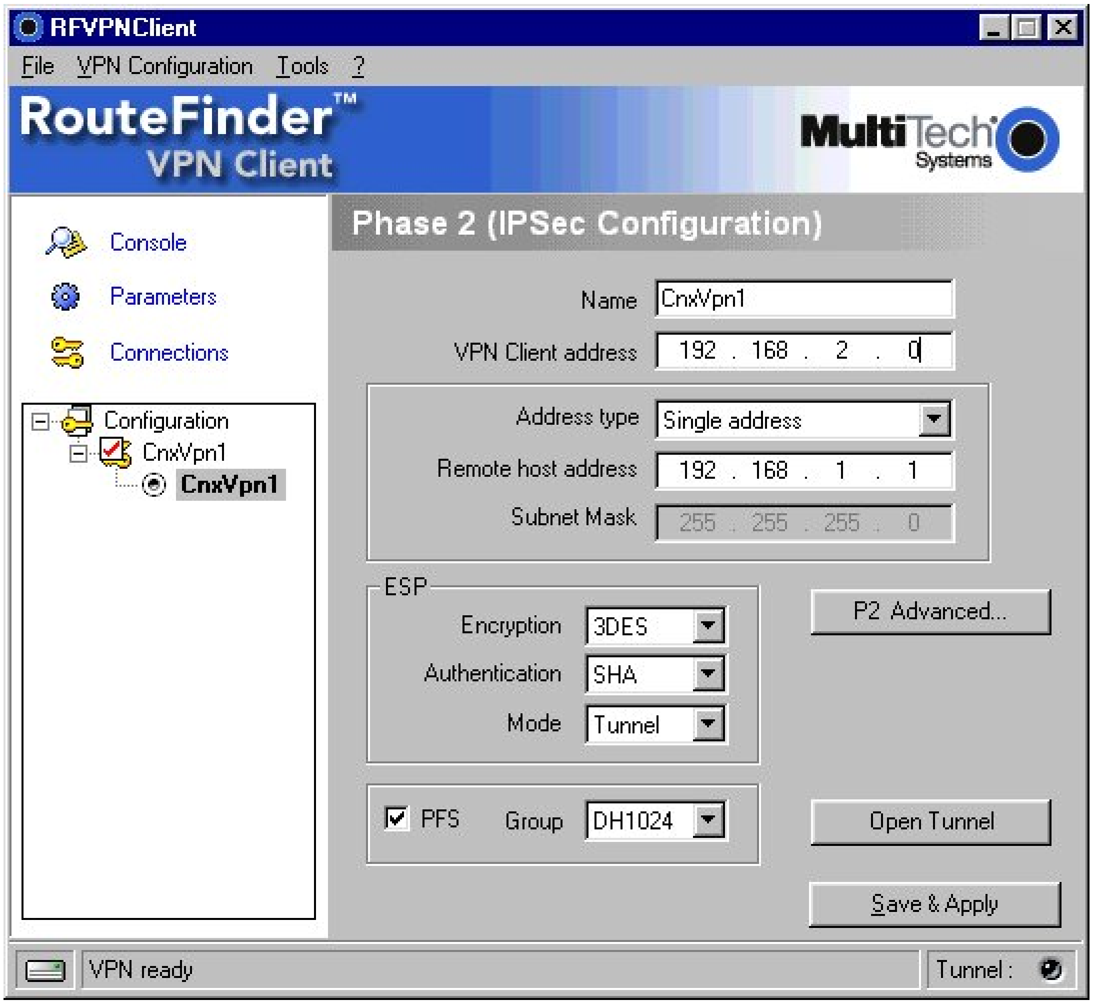


Feature	Description
Config-Mode	If checked, the VPN Client will activate Config-Mode for this tunnel. Configuration Mode allows the VPN Client to retrieve some VPN Configuration information from the VPN gateway, like DNS/WINS server IP addresses. In case Config-Mode is not available on the remote gateway, please refer to section 'Phase2 Advanced' settings to manually set DNS/WINS server addresses.
Aggressive Mode	If checked, the VPN client will used aggressive mode as negociation 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). The VPN Client will contact the primary gateway to establish a tunnel. If it fails after several tries (default is 5 tries, it can be changed in the 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. Tunnel configuration needs to change. 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 behaviour 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 clicks on 'Save & Apply'.
IKE Port	Negociation port for IKE. Default value is 500.
Local ID	Local ID identifies the VPN client during Phase 1 which is sent to the 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@multitech.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 of the VPN client which is expected to be received 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 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.

Phase 2 (IPSec Configuration)

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.



Name: CnxVpn1

VPN Client address: 192 . 168 . 2 . 0

Address type: Single address

Remote host address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

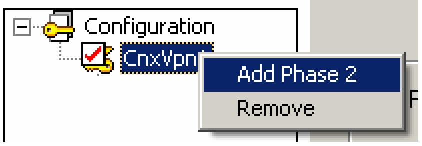
Authentication: SHA

Mode: Tunnel

☑ PFS Group: DH1024

VPN ready

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



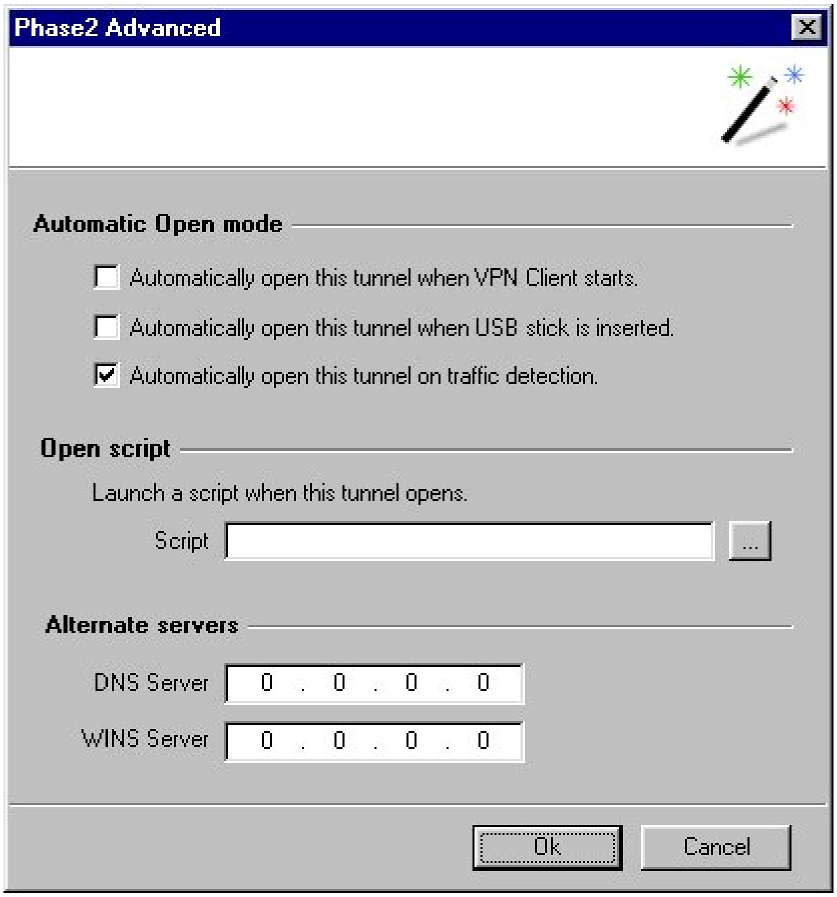
4. Configure IPSec Phase (Phase 2)

Field	Description
Name	Label for IPSec Configuration only used by the VPN client. This parameter is never transmitted during IPSec Negotiation. It is possible to change this name at any time and read it in the tree list window. Two Phases can not have the same name.
VPN Client address	Virtual IP address used by the client inside the remote LAN. The computer will appear on the LAN with this IP address. It is important that this IP address does not belong to a remote LAN (e.g., in the example, you should avoid an IP address like 192.168.1.10).

Address type	The remote endpoint may be a LAN or a single computer. In the first case choose Subnet address. Choose Single address otherwise. When choosing Subnet address, the two fields Remote LAN address and Subnet mask became available. When choosing Single address, only the field Remote host address is available.
Remote 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.
Open Tunnel	This button opens the tunnel. This button changes to Close Tunnel as soon as the tunnel is opened.

Phase2 Advanced

For advanced features & parameters, click on the P2 Advanced button in the Phase2 panel.



Phase2 Advanced

Automatic Open mode

□ Automatically open this tunnel when VPN Client starts.

□ Automatically open this tunnel when USB stick is inserted.

☑ Automatically open this tunnel on traffic detection.

Open script

Launch a script when this tunnel opens.

Script:

Alternate servers

DNS Server: 0 . 0 . 0 . 0

WINS Server: 0 . 0 . 0 . 0

Field	Description
Automatic Open Mode	The VPN Client can automatically open the specified tunnel (Phase2) 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.
Open Script	A specific script or application (e.g. Outlook, CRM apps, ..) can be launched when this tunnel opens. Script or application can be selected by browsing using '...' button.
Alternate Servers	DNS and WINS server IP addresses of the remote LAN can be entered here, to help users to 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.

5. Once the parameters are set, click on **Save & Apply** button to take into account the new configuration. Then the IKE service will run with the new parameters.
6. Click on **Open Tunnel** button to establish the IPSec VPN tunnel (only in IPSec Configuration window)

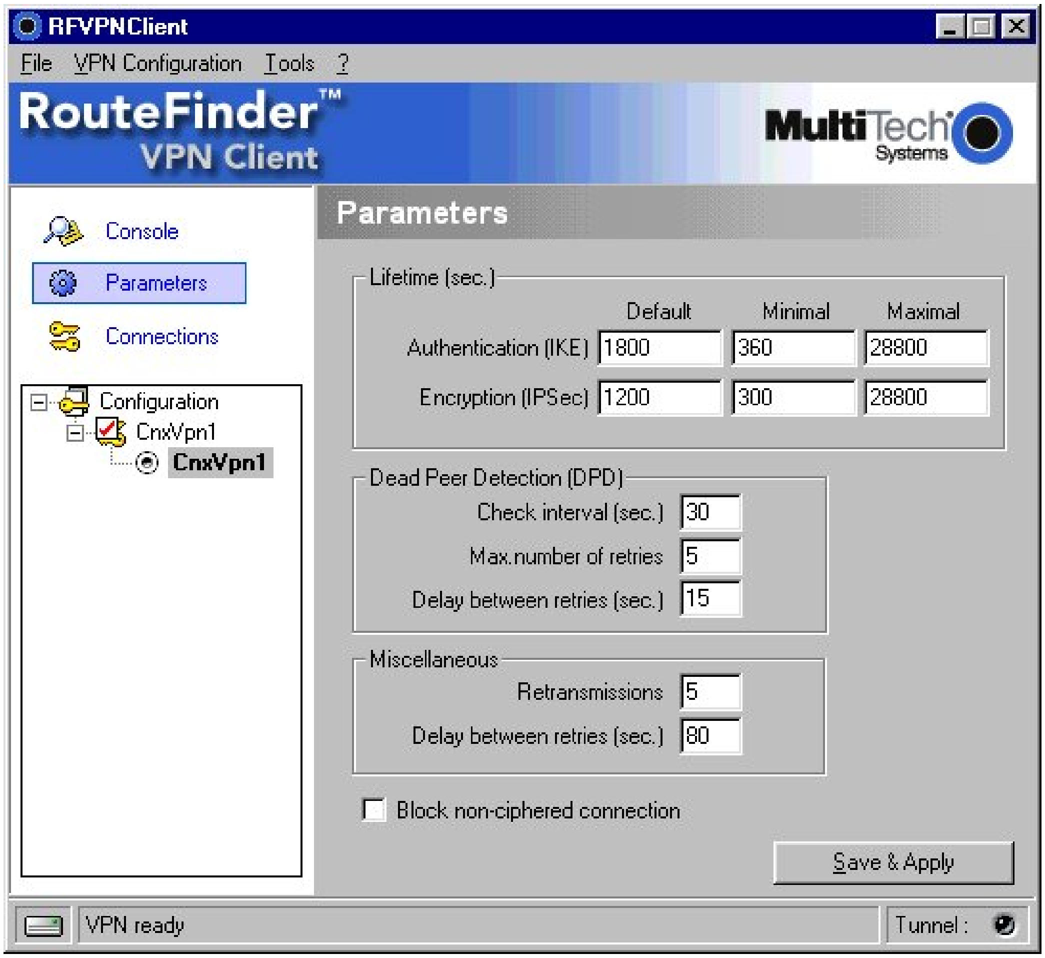
Global Parameters

Global Parameters are generic settings that apply to all created VPN tunnels. Dead Peer Detection (i.e. DPD) is an Internet Key Exchange (IKE) extension (i.e. RFC3706) for detecting a dead IKE peer.

VPN Client uses DPD:

To delete opened SA in the VPN Client when peer has been detected as dead.

To re-start IKE negotiations with the Redundant Gateway, if activated in the Phase1 Advanced VPN configuration panel.



Parameters

Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	1800	360	28800
Encryption (IPSec)	1200	300	28800

Dead Peer Detection (DPD)

Check interval (sec.) 30

Max.number of retries 5

Delay between retries (sec.) 15

Miscellaneous

Retransmissions 5

Delay between retries (sec.) 80

□ Block non-ciphered connection

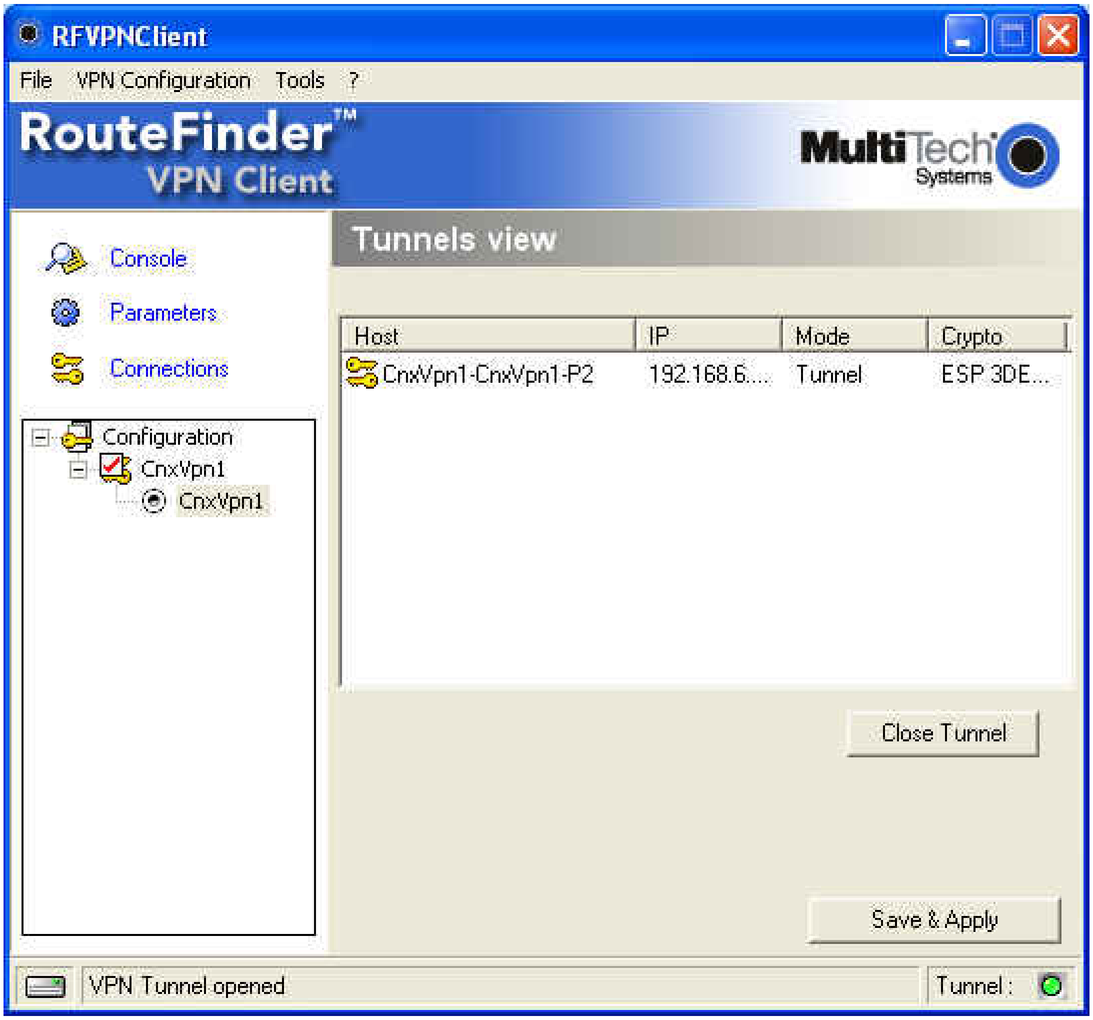
Group	Setting	Description
Lifetime (sec.)	IKE default lifetime	Default lifetime for IKE rekeying.
	IKE minimal lifetime	Minimal lifetime for IKE rekeying.
	IKE maximal lifetime	Maximal lifetime for IKE rekeying.
	IPSec default lifetime	Default lifetime for IPSec rekeying.
	IPSec maximal lifetime	Maximal 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 attemps by user to restart IKE negotiation.
	Block non-ciphered connection	When this option is checked, only encrypted traffic is authorized.

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

Tunnel View

The Tunnels view screen shows VPN tunnels currently opened. To open the Tunnels view screen, click on the **Connections** button in the left panel. 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** button. Tunnels may also be viewed, opened and closed directly from the context menu of the system tray icon.



Host	IP	Mode	Crypto
CnxVpn1-CnxVpn1-P2	192.168.6....	Tunnel	ESP 3DE...

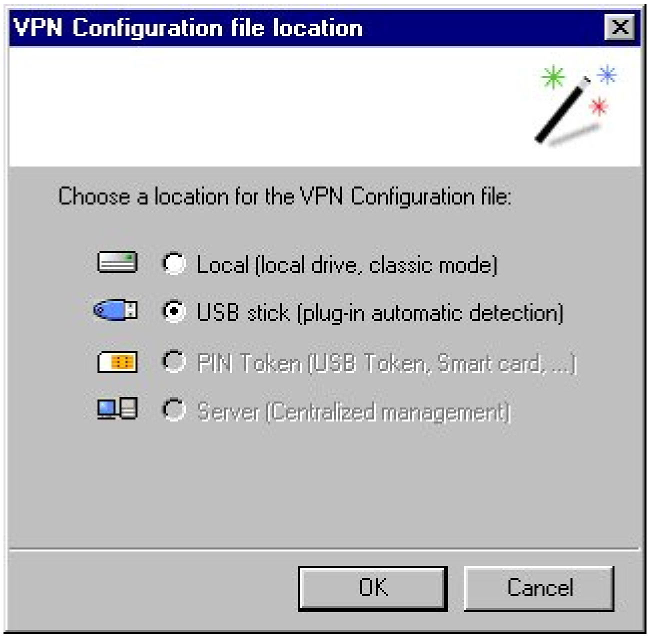
VPN Tunnel opened

Tunnel : ●

USB Mode

The VPN Client provides the capability to secure the VPN configurations and VPN security elements (e.g. PreShared key, Certificates, …) on an USB Stick.

To select the USB mode, click on the left box in the status bar at the bottom of the screen. The VPN Configuration file location window opens. Choose the USB stick (plug-in automatic detection) option and click on the OK button.

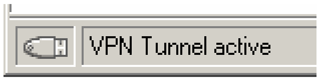


VPN Configuration file location

Choose a location for the VPN Configuration file:

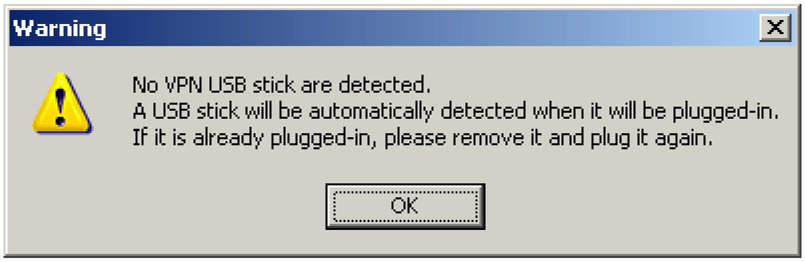
○ Local (local drive, classic mode)
● USB stick (plug-in automatic detection)
○ PIN Token (USB Token, Smart card, ...)
○ Server (Centralized management)

When you select "USB mode", the VPN configuration and security elements contained in the configuration are stored on the USB Stick the first time you plug it in. Once done and the "USB mode" is set "On", 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.



VPN Tunnel active

Note: At this stage, if an USB Stick containing a VPN configuration with VPN security elements is already plugged in, the associated drive will automatically be recognized. If no USB Stick is plugged in, the following pop window informs the user:

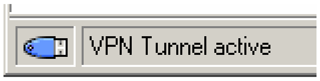


Warning

No VPN USB stick are detected.
A USB stick will be automatically detected when it will be plugged-in.
If it is already plugged-in, please remove it and plug it again.

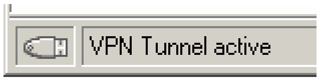
Once USB mode is set on, the left side box in the status bar shows an USB stick icon.

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



VPN Tunnel active

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



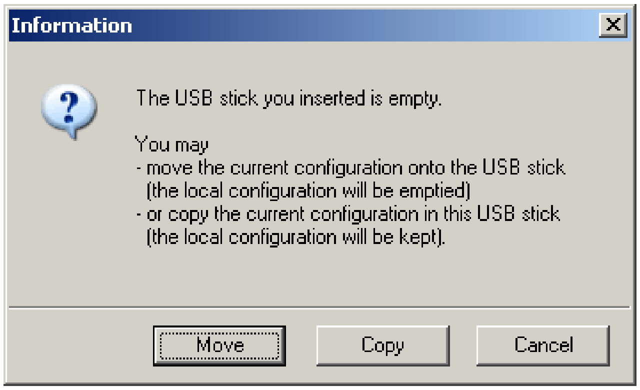
VPN Tunnel active

How to enable a new USB Stick

A new USB Stick (no data) is enabled by copying the VPN configuration and security elements onto it.

When you insert a new USB Stick, the VPN Client automatically enables 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 on the computer. This is used by IT managers to enable multiple USB Sticks for multiple users in no time.
- **Moving** the configuration onto the USB Stick: the 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 VPN configuration is setup.

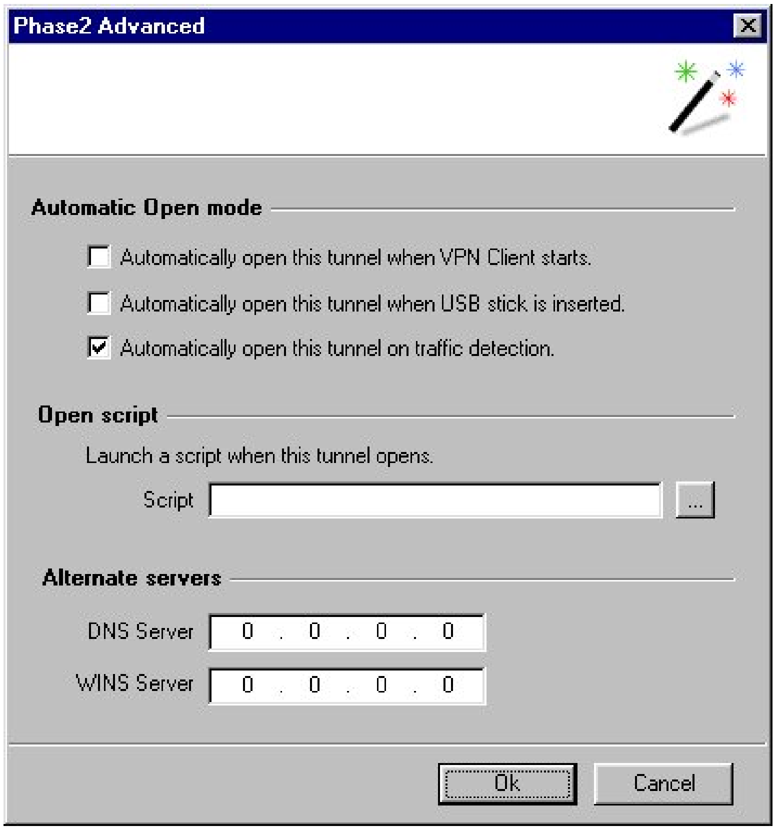


The USB stick you inserted is empty.

You may
- move the current configuration onto the USB stick
  (the local configuration will be emptied)
- or copy the current configuration in this USB stick
  (the local configuration will be kept).

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

Select a tunnel by clicking on the configuration in the tree control and then click on the P2 Advaced button. The Phase2 Advanced window is opened. Click on Automatically open this tunnel when USB stick is inserted.



Automatic Open mode

□ Automatically open this tunnel when VPN Client starts.

□ Automatically open this tunnel when USB stick is inserted.

☑ Automatically open this tunnel on traffic detection.

Open script

Launch a script when this tunnel opens.

Script

Alternate servers

DNS Server 0 . 0 . 0 . 0

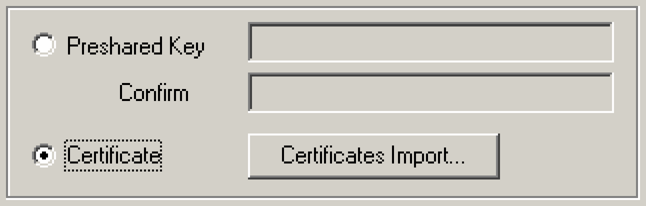
WINS Server 0 . 0 . 0 . 0

Certificate Management

The RouteFinder IPSec VPN Client uses X509 certificates with PEM format. This kind of certificate is created the RouteFinderVPN Gateway, not with the RouteFinder VPN Client.

How to configure IPSec VPN Client with Certificates

1. Select radio button 'Certificate' in the 'Authentication' window and click on 'Certificates Mgt'



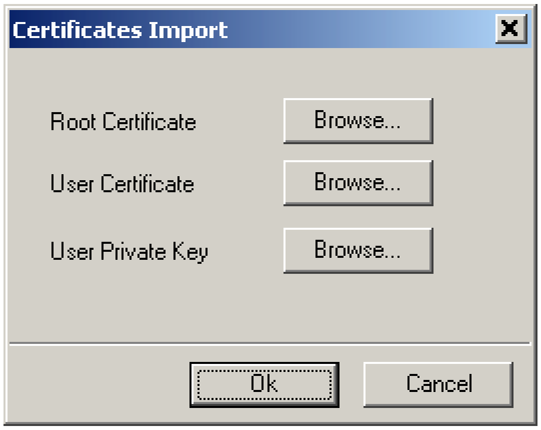
○ Preshared Key

Confirm

● Certificate

2. Click on 'Browse' and select the appropriate files.

Root certificate is copied into directory " [install_path]\ca\".
User certificate is copied into directory " [install_path]\cert\".
User certificate private key is copied to " [install_path]\private\local.key".



Certificates Import

3. Open 'P1 Advanced' button and fill Local ID with:

Type = "DER_ASN1_DN".
Value = subject user certificate ("Subject:") content like "C=FR, ST=Paris, L=Paris, O= Multi-tech Systems, OU=Internal OpenSSL CA, CN=exemple/Email=support@multitech.com".

Configuration Management

The RouteFinder 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".

All configuration files will have a ".tgb" extension.

You can open and modify an exported configuration file (extension .tgb) with any word processing e.g. Notepad and reimport it again. This is another way for IT managers to customize VPN configurations before dispatching to end users.

Configuration Tools

Stopping IPSec VPN Client: option "/stop"

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

" **[path]\vpnconf.exe /stop** " where [path] is the client installation directory.

If there are 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 exit it just before the disconnection.

You'll be able to find the latest version of those tools on our website.

Import VPN Configuration: option "/import" and "/importonce"

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

" **[path]\vpnconf.exe /import:[file.tgb]** " where [path] is the client installation directory, and [file.tgb] is the VPN Configuration file.

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

IPSec VPN Client Startup mode: VPNSTART

VpnStart.exe is a configuration tool that sets up the client startup mode.

The RouteFinder VPN Client can start with 3 different modes:

During PC boot: this mode can be used for secure remote action
At Windows login ("login" mode)
Launched by user or from a script ("manual" mode)

The RouteFinder IPSec VPN Client 3.0 and later includes this feature into the VPN Client itself.

Hiding IPSec VPN Client configuration user interface: VPNHIDE

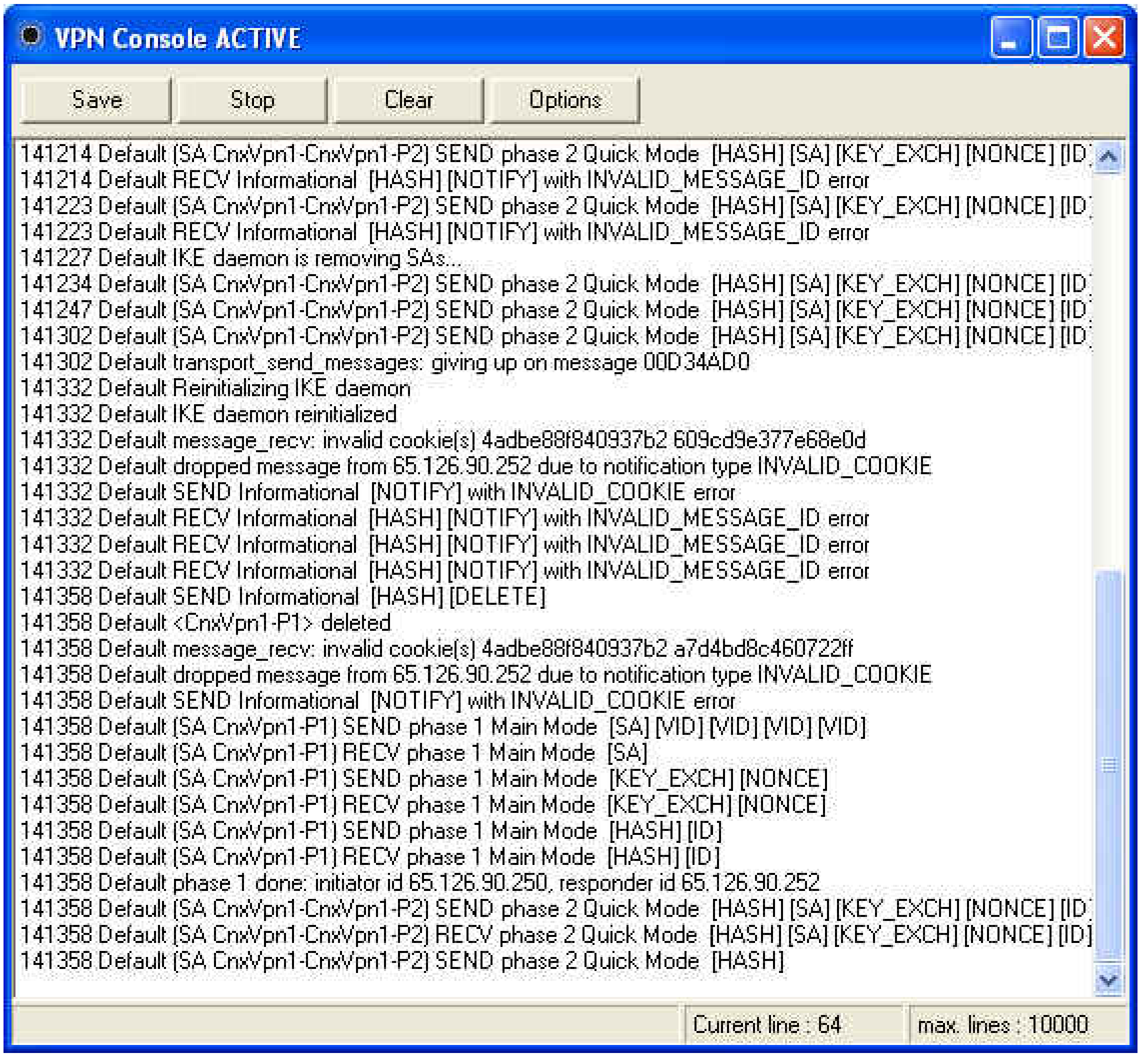
VpnHide.exe is a configuration tool that hides the Client VPN interface. It can be used by IT managers for preventing end-user from modifying configuration settings.

In "invisible" mode, the window interface is never shown.

You'll be able to find the latest version of those tools on our website.

Chapter 5 - Console and Logs

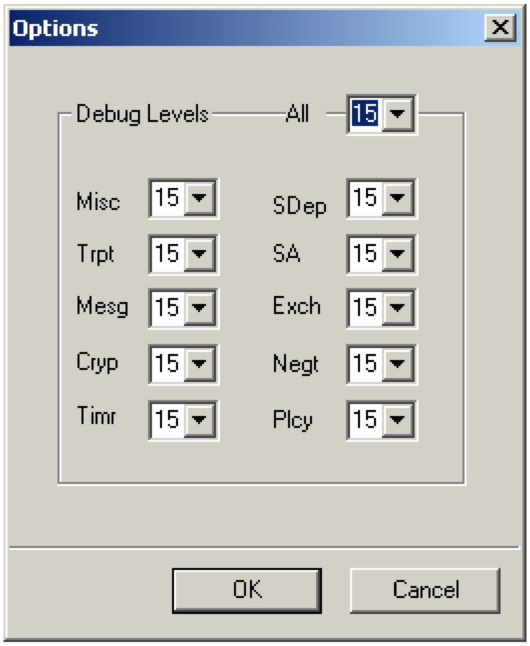
The Console window is available from the context menu of the system tray icon or from **Console** button in the configuration user interface. This window can be used to analyze VPN tunnels. This tool is particularly useful for IT managers in setting up their network.



```
141214 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID]
141214 Default RECV Informational  [HASH] [NOTIFY] with INVALID_MESSAGE_ID error
141223 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID]
141223 Default RECV Informational  [HASH] [NOTIFY] with INVALID_MESSAGE_ID error
141227 Default IKE daemon is removing SAs...
141234 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID]
141247 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID]
141302 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID]
141302 Default transport_send_messages: giving up on message 00D34AD0
141332 Default Reinitializing IKE daemon
141332 Default IKE daemon reinitialized
141332 Default message_recv: invalid cookie(s) 4adbe88f840937b2 609cd9e377e68e0d
141332 Default dropped message from 65.126.90.252 due to notification type INVALID_COOKIE
141332 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
141332 Default RECV Informational  [HASH] [NOTIFY] with INVALID_MESSAGE_ID error
141332 Default RECV Informational  [HASH] [NOTIFY] with INVALID_MESSAGE_ID error
141332 Default RECV Informational  [HASH] [NOTIFY] with INVALID_MESSAGE_ID error
141358 Default SEND Informational  [HASH] [DELETE]
141358 Default <CnxVpn1-P1> deleted
141358 Default message_recv: invalid cookie(s) 4adbe88f840937b2 a7d4bd8c460722ff
141358 Default dropped message from 65.126.90.252 due to notification type INVALID_COOKIE
141358 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
141358 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID]
141358 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode  [SA]
141358 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE]
141358 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE]
141358 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode  [HASH] [ID]
141358 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode  [HASH] [ID]
141358 Default phase 1 done: initiator id 65.126.90.250, responder id 65.126.90.252
141358 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID]
141358 Default (SA CnxVpn1-CnxVpn1-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID]
141358 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode  [HASH]
```

Button	Description
Clear	Clear console window content
Save	Save logs in a file
Stop	Stop saving logs in a file
Options	Set level of log filtering

Console Filters



Debug Levels

All 15

Misc 15

Trpt 15

Mesg 15

Cryp 15

Timr 15

SDep 15

SA 15

Exch 15

Negt 15

Plcy 15

Label	Name	Description
Misc	Misc	log level for configuration reading or dump of low level messages
Trpt	Transport	log level for UDP transport mode
Mesg	Message	log level for IKE decode
Cryp	Crypto	log level and dump for crypto material exchanged
Timr	Timer	log level about timers
SDep	Sysdep	log level about IKE interface from/to IPSec
SA	SA	log level for SA managment
Exch	Exchange	log level about IKE exchanges (very useful)
Negt	Negotiation	log level about phase 1 and phase 2 negociation
Plcy	Policy	not used
All	All	Apply the same log level to all subsystems

Most of the time log level set to 0 is largely enough for resolving configuration issues.

Appendix A – Technical Support

When contacting Multi-Tech, be sure to have your RouteFinder information and details about the functioning of the software.

Contacting Technical Support

Country	Using email	By phone
France	Support@multitech.fr	+(33) 1-64 61 09 81
India	Support@multitechindia.com	+(91) 124-340778
U.K.	Support@multitech.co.uk	+(44) 118 959 7774
Rest of World	Support@multitech.com	800-972-2439 (U.S. & Canada) or +763-785-3500

Recording RouteFinder Information

Before placing a call to our Technical Support staff, record the following information about your Multi-Tech RouteFinder.

Model no.: ____

Serial no.: ____

Firmware version: ____

List information that indicates the status of your RouteFinder in the space provided before calling tech support. Include screen messages, diagnostic test results, problems with a specific application, etc.

____

____

Appendix B – VPN Client CD

A CD is provided with your purchase of the RouteFinder IPSec VPN Client software. The CD contains the VPN Client software, this Install User Guide, and the software license agreement.

When you insert the CD into your computer's CD-ROM drive, the RouteFinder IPSec VPN Client Welcome to... screen appears.

Some of the CD selections are described below:

Click on the **Load Software** button to load the VPN Client software onto your computer's hard disk drive.

Click on the **Install User Guide** button to view and/or print the RouteFinder IPSec VPN Client Install User Guide. This is an Adobe Acrobat file – if you don't have the Acrobat Reader, download it from http://www.adobe.com.

Click on the **Client License** button to view the Multi-Tech Multi-User Software License Agreement. Note that the Software License Agreement is also provided in this manual.

Click on the **Setup Examples** Guide to view and/or print the RouteFinder IPSec VPN Client Setup Examples Reference Guide. This is an Adobe Acrobat file - if you don't have the Acrobat Reader, download it from http://www.adobe.com.