HotBrick

Don't Get Hacked. Get HotBrick.

Official Tech Documents
The better way to get your HotBrick
product up and running

HotBrick VPN Client

User Manual

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano,100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

Table of Content

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

1   Introduction

HotBrick VPN client is a complete IPSec VPN solution for all Windows versions. It provides full IKE support (preshared keying and X509 certificates) and Nat Traversal. It is compatible with most of the currently available IPSec gateways and also operates as a peer-to-peer VPN in a "point – to – multiple" mode, without a gateway or server.

HotBrick VPN Client provides 3DES, DES and AES encryption and MD5 and SHA authentication.

* Our IPSec 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.

* Our IKE implementation is based on the OpenBSD 3.1 implementation (ISAKMPD), thus providing best compatibility with existing IPSec routers and gateways.

Our offer is specially designed to target OEM clients and System Integrators. We provide a fully functional VPN Client solution to complete existing offers. Our IPSec VPN Client can be re-branded and source code license is available on demand.

The VPN IPSec Client completes our range of network security products and like all our products is easy to use and to install.

HotBrick VPN IPSec Client is compatible with all current Windows versions: 9x, ME, NT4, 2000, XP.

2   Install

2.1   Software installation

HotBrick 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.

<u>Caution</u>: On Windows NT, 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.

After reboot and session login, a window appears for a license number request.

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

The license number is a string with hexadecimal characters as "0123456789ABCDEF0123". An error message warns user if this value is false.

If the License number is correct, HotBrick VPN Client is activated. You can then find a green/red icon in the taskbar. Right and left click give access to the configuration user interface and "Quit" command.

<u>Shortcuts</u>: After software installation, HotBrick VPN window can be launched:

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

2.2   Evaluation Period

It is possible to use HotBrick IPSec VPN Client during the evaluation period (i.e. limited to 30 days) by clicking on "Trial" button. When the IPSec VPN Client is on "Evaluation" mode, the register window appears at each boot of the client.

3   Software manipulation

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

The VPN Client configuration is defined in a configuration file. The software user interface allows creating, modifying, saving, exporting or importing the configurations.

3.1 System Tray

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


3.1.1 Color code is the following

Red icon: no VPN tunnel is established

Green icon: at least one VPN tunnel is established

Tool tips 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
- "HotBrick VPN Client" when the client is up but with no established tunnel.

A left-button click on VPN icon opens configuration user interface. A right-button click shows the following menu:
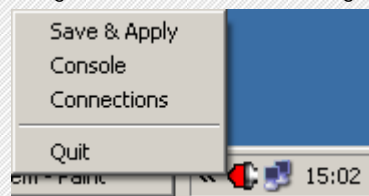
- "Quit" will close established VPN tunnels, stops the configuration user interface.
- "Save & Apply" will close established VPN tunnels and reopen all the VPN tunnels.
- "Console" shows log window.
- "Connections" opens the list of already established VPN tunnels. You can configure tunnels to open up automatically when the software starts.

3.2 Hidden User interface

The configuration 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 4.10.3 page 18.

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:

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

3.3 Main window

The main window is made of several elements:

- A tree list window (left column) that contains all the IKE and IPSec configuration

- Three buttons "Console", "Parameters" et "Connections" (left column)

- A configuration window (right column) that shows the associated tree level.
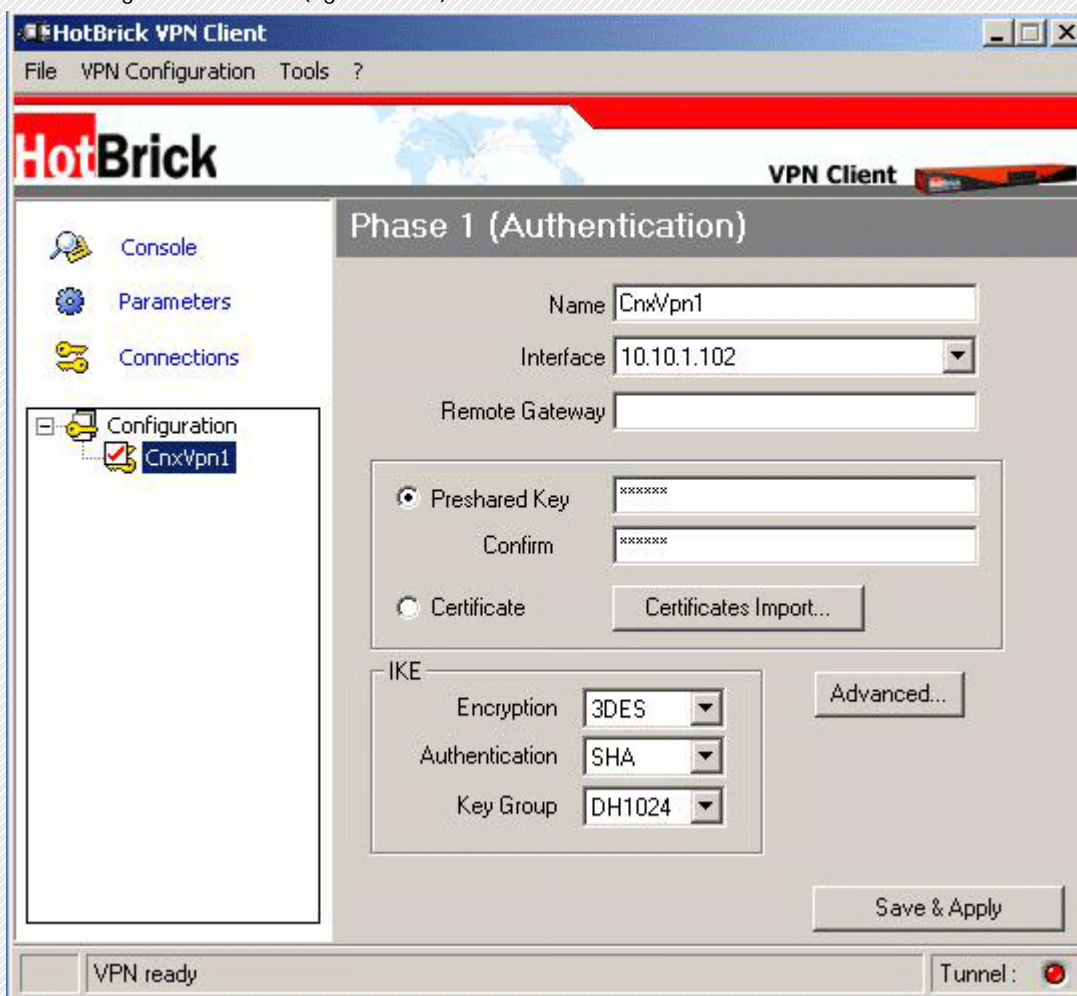
3.3.1 Main menus

- "File" menu is used for saving and loading a configuration. With this menu, you can import or export VPN configuration.

- 'Configuration' menu contains all actions from tree control right-click menu

- 'Configuration' menu gives also access to the configuration wizard.

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

- '?' menu gives access to online help and window 'About'.

3.3.2 Status bar

The status bar displays several information:

- The "USB Token box" (left side) indicates whether the "USB mode" is set "On" or "Off" (see also section 4.1 page 7). In case it is set "On", "USB" will appear.

- The "central box" gives some information about VPN Client Software status (e.g. "opening tunnel in progress", "saving configuration rules in progress", "VPN client start up in progress", …)

- The "light box" (right side) gives some information about tunnels (e.g. red light means at least one tunnels is open, green light means no tunnel open, gray light means VPN Client restart pending)

3.3.3 Window 'About'

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

4 Configuration

You'll find a set of useful VPN Client configuration documents available for each of the VPN Client gateway we support. Please go to our knowledge base on our website: http://www.hotbrick.com.br/vpnclient_list.htm

4.1 USB Mode

The VPN Client 2.5 brings the capability to secure tunnel security elements by the use of a USB Stick.

Once 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. In that mode, no tunnel can be opened.

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

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

4.1.1   How to set "USB mode" on?

- Select menu File > Configuration Mode

- Select USB Stick

- Optional: indicates the drive of the USB stick if you've plugged it in
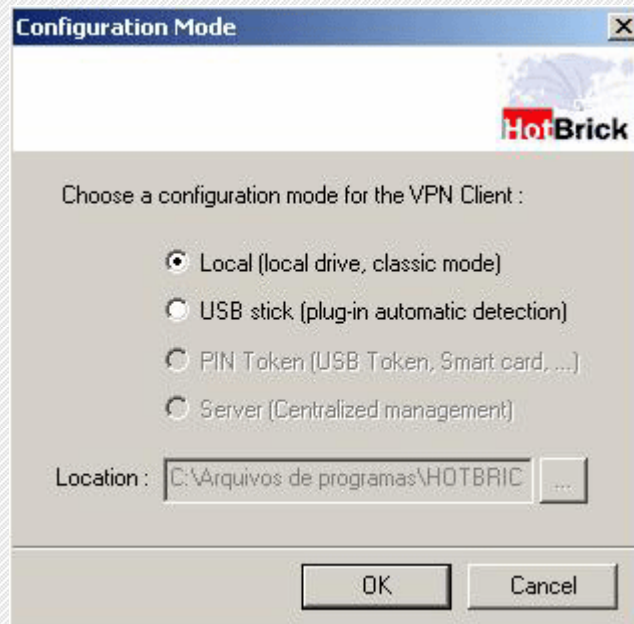
Note: At this stage, if an USB stick containing a VPN configuration with tunnel security elements is already plugged in, the associated drive will be automatically recognized. Please note also that this is not necessary to insert a USB Stick during this step. In case no USB Stick is plugged in, the following pop window will inform the user:
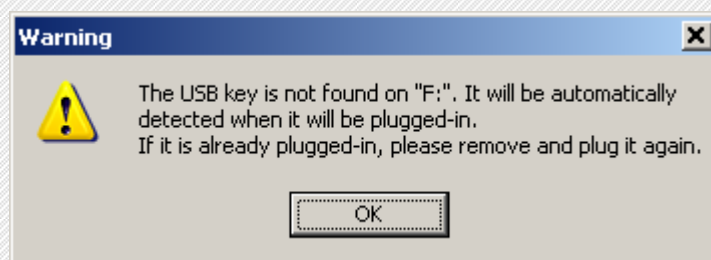
Once USB mode is set on, the "USB token box" (status bar) shows "USB". The text is gray (i.e. see below) if no USB stick is plugged in. The text is plain when a USB Stick is plugged in.
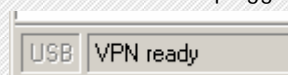
4.1.2   How to enable the USB Stick?

When you insert a new USB stick, the IPSec VPN Client automatically propose to enable the USB stick through the following options:

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

- **Copying** the configuration onto the USB stick: the VPN client will copy the configuration onto the USB Stick and leave a copy in the computer. This is used by IT managers to enable multiple USB Sticks for multiple users.

- **Moving** the configuration onto the USB stick: the VPN client will copy the configuration onto the USB Stick and remove all configuration information from the computer. This method is used to secure a computer once VPN configuration completed setup.

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

Each and every tunnel must be configured individually:

- Select one tunnel by clicking on IPSec Configuration (Phase 2) in the tree list window (see section 4.5)

- Set the mode "Auto open when USB stick plugged in" on

4.2 Configuration Wizard

HotBrick IPSec VPN client integrates a Configuration Wizard that allows the creation of VPN configuration in three easy steps.

This wizard is designed for remote computers that need to get connected to a corporate LAN through a VPN gateway. Let take the following example:

- The remote computer has a dynamically provided public IP address.

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

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

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br
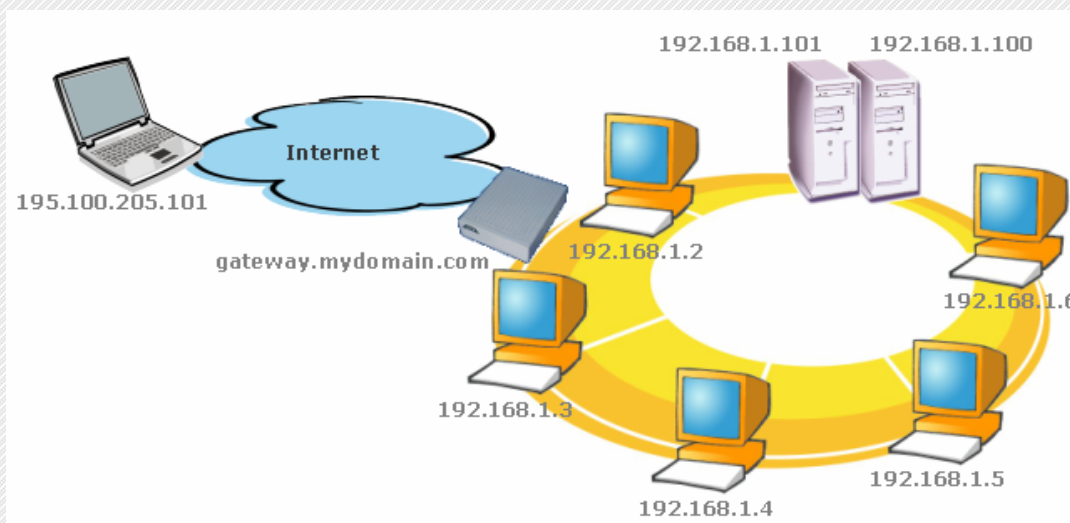
For configuring this connection, open wizard's window by selecting menu "Configuration > Wizard"

4.2.1   Step 1 of 3

You specify the type of the equipment at the end of the tunnel: VPN gateway.
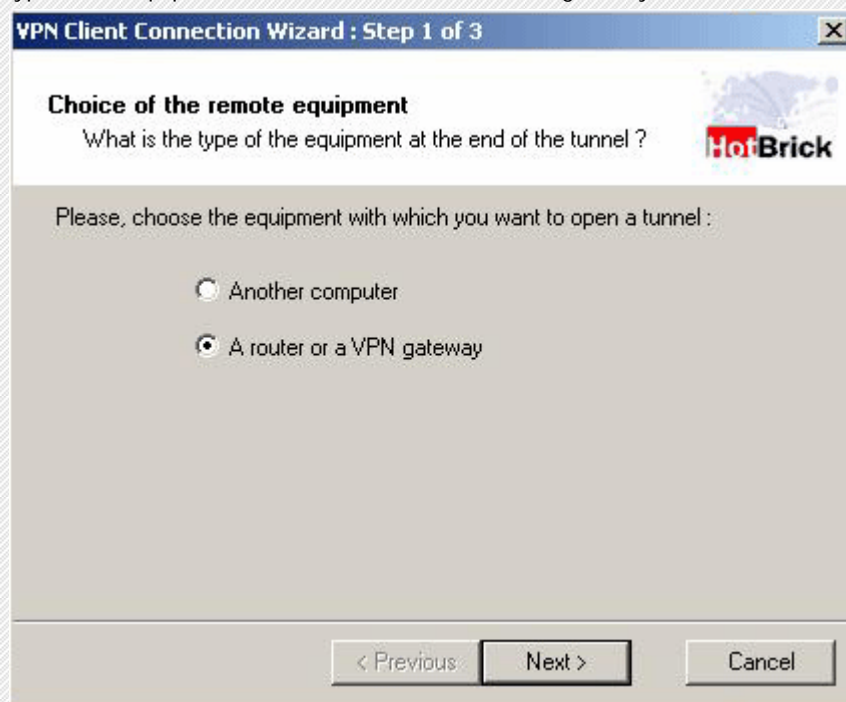
4.2.2   Step 2 of 3

You must specify the following information:

- the public (network side) address of the 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)

4.2.3 Step 3 of 3

The third step summaries your configuration. Other parameters may be further configured directly via the main interface (e.g. Certificates, virtual IP address, etc...)

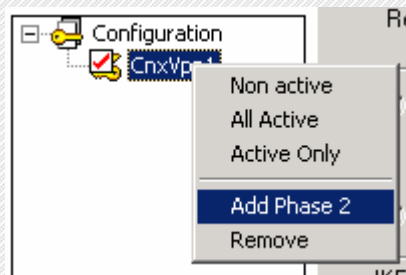## 4.3 Tunnel configuration (main window)

4.3.1 How to create a tunnel?

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

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

2. Configure Authentication Phase (Phase 1)

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

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

4. Configure IPSec Phase (Phase 2)

5. Once the parameters are set, click on "Save & Apply" to take into account the new configuration. That way the IKE service will run with the new parameters

6. Click on "Open Tunnel" for establishing the IPSec VPN tunnel (only in "IPSec Configuration" window)

4.3.2 Several Authentication or IPSec Configuration Phases

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

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

4.3.3 Active or Non Active phase

A phase can be either "active" or "non active". If a phase is "non active", its settings will not be applied. This feature can be used with a configuration composed of several VPN tunnels that do not need to be enabled simultaneously.

Changing "active" to "non-activate" state for a specific Phase can be achieved by a right-click on the phase name:

- Active (or Non active)   Enable or disable the phase

- All active   Enable all phases

- Active Only   Disable every phase except the phase selected with the mouse.

4.4   Authentication or Phase 1

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

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano,100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br
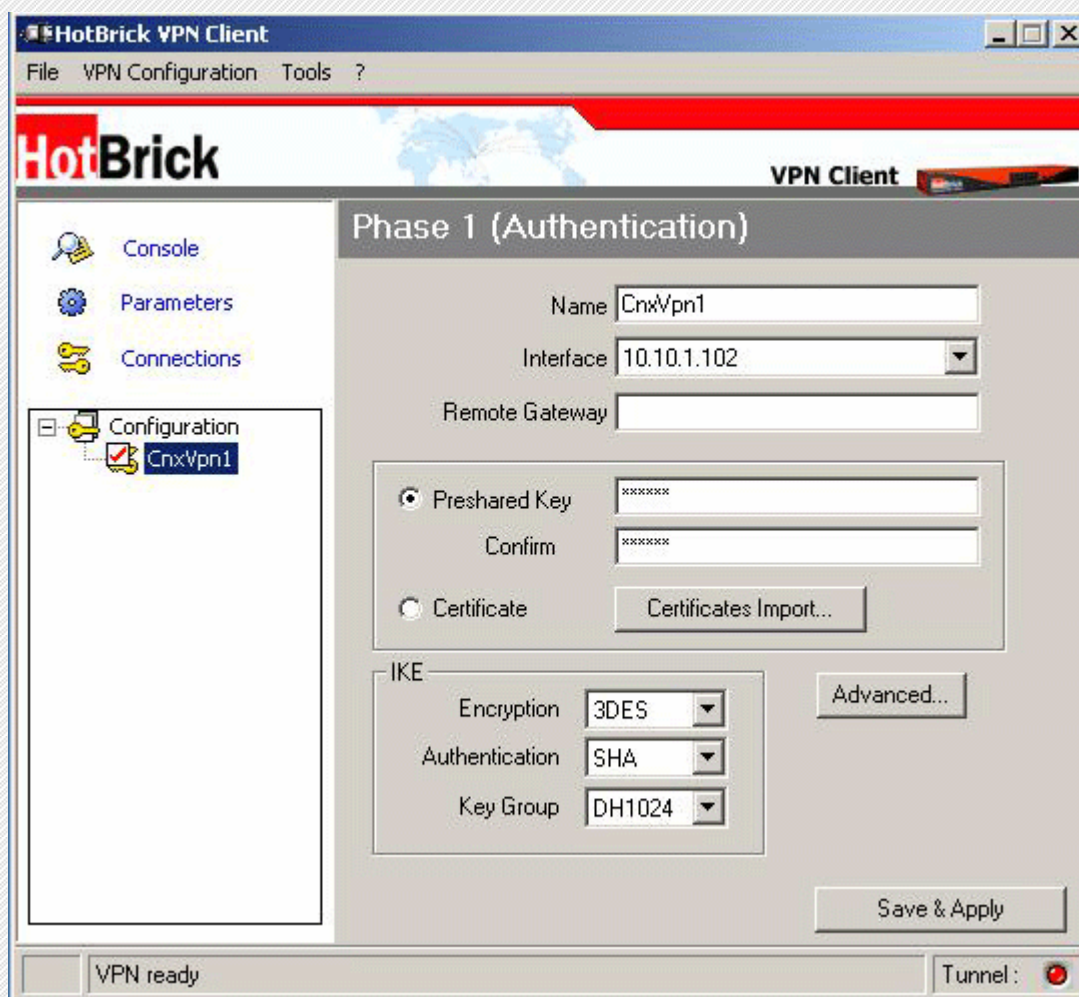
4.4.1 Settings description

Name	Label for Authentication phase used only the configuration 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 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 may change (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 with 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.

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

4.4.2 Advanced configuration ("Advanced" Button)

4.4.3   Settings description

Aggressive Mode	If checked, the VPN client will used aggressive mode as negotiation mode with the remote gateway
Nat port	Negotiation port for IKE. Default value is 500.
Local ID	Local ID is the identity the VPN client is sending during Phase 1 to VPN gateway.

This identity can be:

- 1   an IP address (type = IP address), for example: 195.100.205.101
- 2   an domain name (type = DNS), e.g. mydomain.com
- 3   an email address (type = Email), e.g. support@HotBrick.com
- 4   a string (type = KEY ID), e.g. 123456
- 5   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:

- 6   an IP address (type = IP address), for example: 80.2.3.4
- 7   an domain name (type = DNS), e.g. gateway.mydomain.com
- 8   an email address (type = Email), e.g. admin@mydomain.com
- 9   a string (type = KEY ID), e.g. 123456
- 10 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	Here are specified the login and password of an X-AUTH IPSec negotiation.

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

4.5   IPSec Configuration or Phase 2

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

4.5.1 Settings 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 in the LAN with this IP address. **It is important this IP address not to belong to the 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.
Auto open when Client starts	If checked, this option allows a tunnel to be automatically opened when the VPN Client starts. **Note: as the VPN Client may also start during the boot (see section VPN Tools), tunnels can be configured to be opened automatically during the boot of the computer.**
Auto open when USB stick plugged in	If checked, this option allows a tunnel to be automatically opened when a USB stick is inserted (see chapter "USB mode").
Open Tunnel	This button allows opening directly the tunnel without using a ping for example.

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

4.6   Certificate management

HotBrick IPSec VPN Client uses X509 certificates with PEM format. This kind of certificates is created with OpenSSL, not with HotBrick VPN Client.

In order to use X509 Certificates with HotBrick IPSec VPN client, you must have the following items:

- Root certificate
- User certificate
- Private key of the user certificate

The private key must not be encrypted. X509 certificates are used during Phase 1.

4.6.1   How configuring IPSec VPN Client with certificates?

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

2. Click on "Browse" and select the appropriate files.
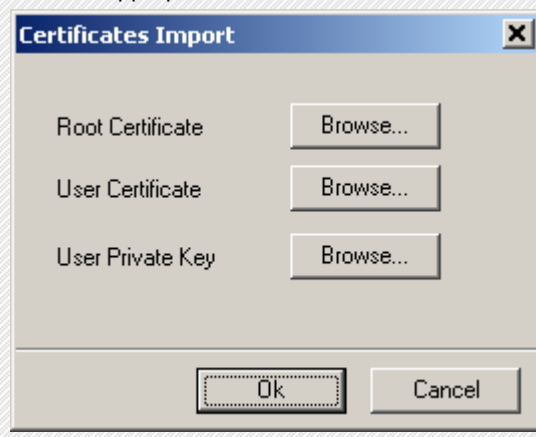
3. Open "Advanced button" and fill Local ID with:

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

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

4.7   Global Parameters

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano,100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br
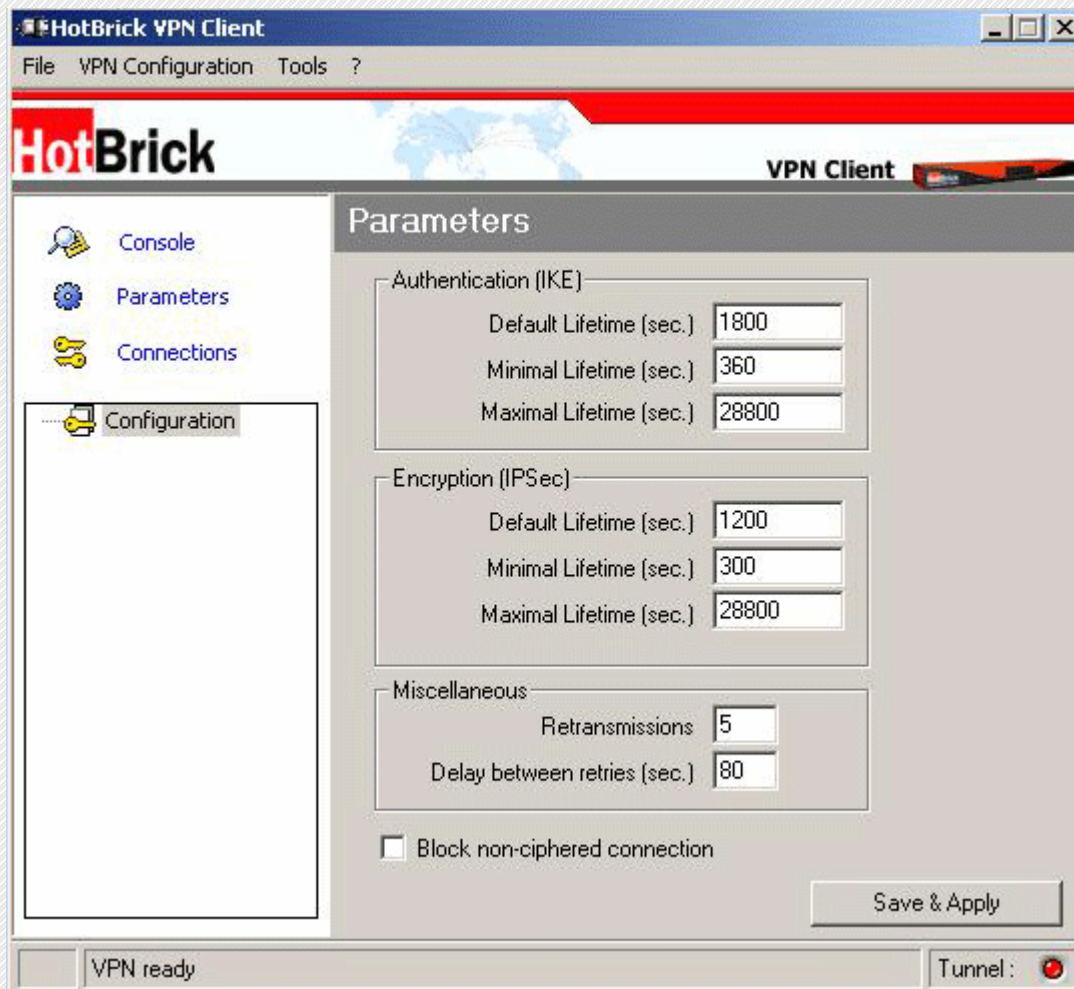
4.7.1   Settings description

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.
Retransmissions	How many times a message should be retransmitted before giving up.
Delay between retries	Waiting time in an exchange before giving up a negotiation
Block non-ciphered connection	When this option is checked, only encrypted traffic is authorized.

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

4.8   Configuration management

4.8.1   How to Import or Export an IPSec VPN configuration

HotBrick 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 "File > Load configuration".
- Exporting a configuration, select "File > Save 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 re import it again. This is other way for IT managers to customize VPN configurations before dispatching to end users.

4.9   Tunnel management (Connections)

"Connections" screen shows opened VPN tunnels and this interface can be used to close them.

To close a tunnel, select one tunnel in the tunnel list and click on "Close tunnel".

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br
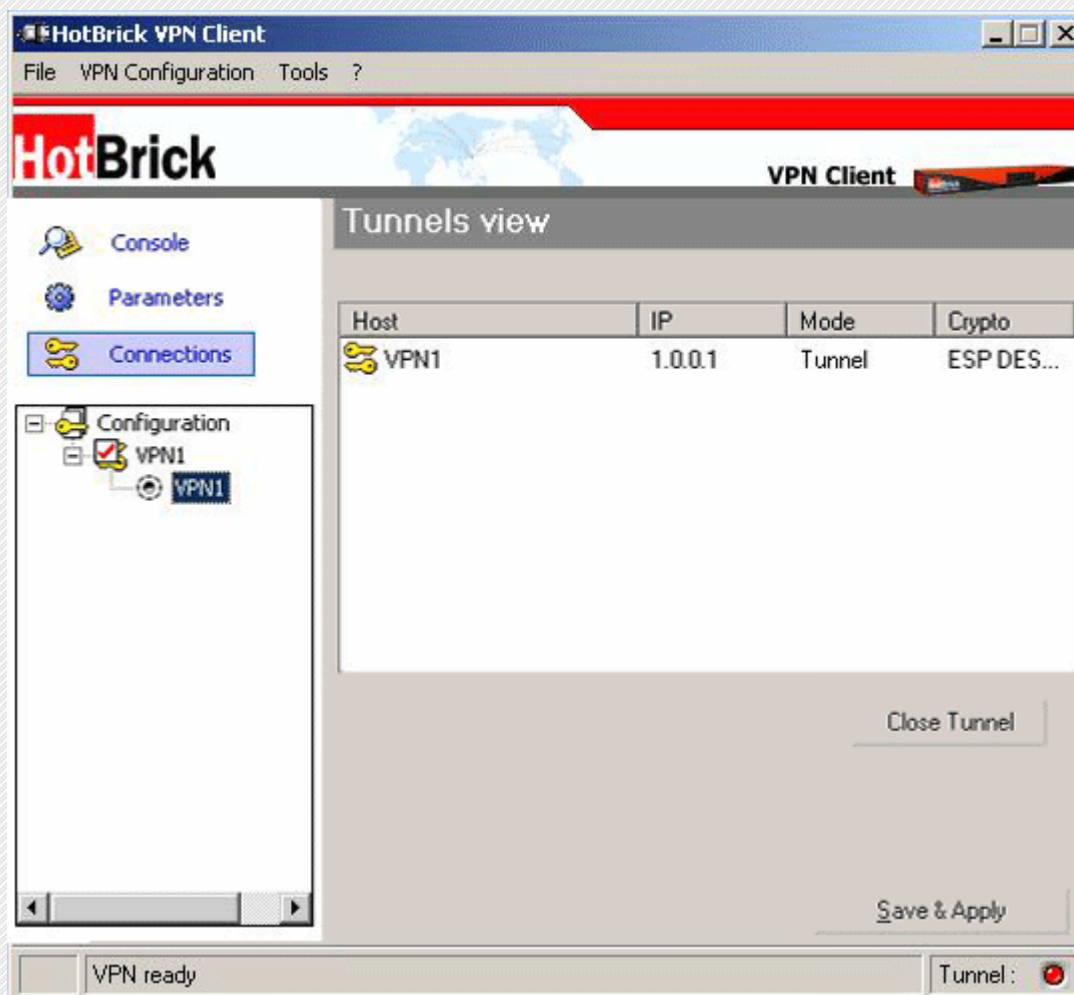
4.10   Configuration tools

4.10.1   Stopping IPSec VPN Client: option "/stop"

HotBrick 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.

4.10.2   IPSec VPN Client Startup mode: VPNSTART

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

HotBrick 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)

4.10.3 Hiding IPSec VPN Client configuration user interface: VPNHIDE

VpnHide.exe is a configuration tool that hides HotBrick 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.

4.11 Console

The "Console" window is available from icon menu that can be found in the taskbar 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.

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br
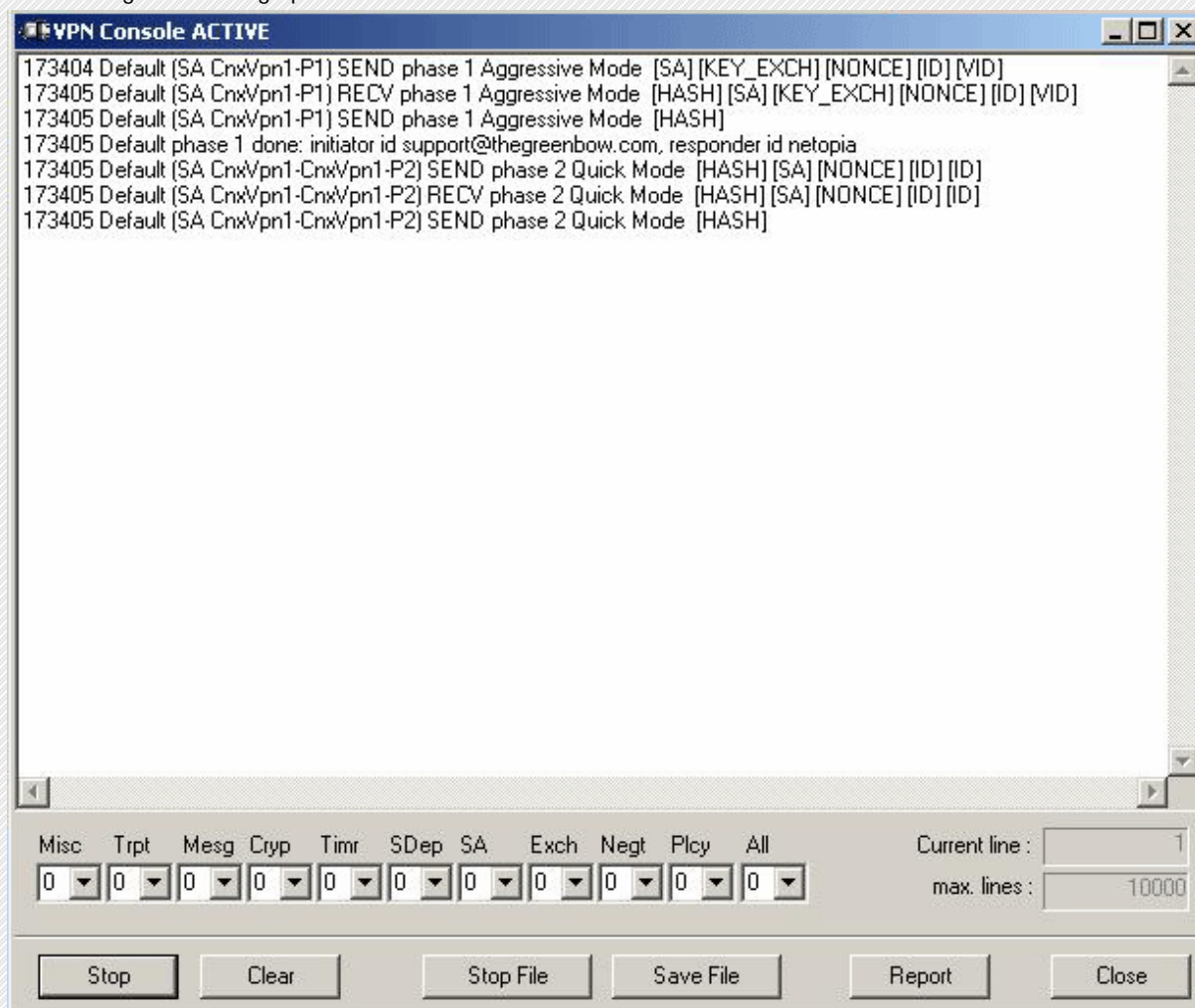
Button	Description
Start / Stop	Start / Stop printing log
Clear	Clear console window content
Save File	Save logs in a file
Stop File	Stop saving logs in a file
Report	Print VPN configuration and IKE internal state.

Label	Name	Description
Misc	Misc	log level for configuration reading or dump of low level messages
Trpt	Transport	log level for UDP transport mode
Msg	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 management
Exch	Exchange	log level about IKE exchanges (very useful)
Nego	Negotiation	log level about phase 1 and phase 2 negotiation
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.

5 Uninstall

5.1 Software uninstall

HotBrick IPSec VPN Client can be uninstalled:

- from Windows Control Panel by selecting "Add/Remove de programs"

6 Troubleshooting

You will be able to find all troubleshooting issues, listed in a Troubleshooting Document on our website. Please have a look at: http://www.hotbrick.com/support_detail.asp?tipo=2.

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

7   Contacts

Information and update are available at: www.HotBrick.com.

Technical support is available by email: support@HotBrick.com .

End of Document

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com