NETGEAR

NETGEAR ProSafe VPN Client

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

December 2010
202-10684-02
v1.0

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10684-02	v1.0	December 2010	Reorganization and revision of the entire manual.
202-10684-01	v1.0	June 2010	First publication

Contents

Chapter 6 Configuration Panel Screen Tasks

Chapter 7 VPN Client Software Setup and Deployment

Chapter 8 Configure the VPN Client with a NETGEAR Router

Chapter 9 VPN Troubleshooting

Appendix A VPN Client Software Setup Deployment and Command-Line Interface Guide

Introduction 1

The VPN Client supports all Windows versions and allows you to establish secure connections over the Internet usually between a remote worker and the corporate Intranet. IPSec is the most secure way to connect to the enterprise as it provides strong user authentication and strong tunnel encryption with the ability to work with existing network and firewall settings. This chapter includes the following sections:

Linux Appliance Support

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

The VPN Client Features

The VPN Client has the following features.

Table 1. List of Features

Feature	Specifications
Windows versions	• Windows 2000 32-bit • Windows XP 32-bit • Windows Server 2003 32-bit • Windows Server 2008 32/64-bit • Windows Vista 32/64-bit • Windows 7 32/64-bit
Languages	Arabic, Chinese (simplified), Dutch, English, Finnish, French, German, Greek, Hindi, Italian, Japanese, Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, and Turkish

Table 1. List of Features (Continued)

Feature	Specifications
Connection modes	• Operates in a peer-to-peer VPN as well as point–to–multiple mode without a gateway or server. All connection types such as dial-up, DSL, cable, GSM/GPRS, and Wi-Fi are supported. • Allows IP range networking. • Runs in a Remote Desktop (RDP) connection session
Tunneling protocols	• Full Internet Key Exchange (IKE) support: the IKE implementation is based on the OpenBSD 3.1 implementation (ISAKMPD). This provides the best compatibility with existing IPSec routers and gateways. • Full IPSec support: - Main mode and aggressive mode - MD5 and SHA-1 hash algorithms - Change IKE port
NAT Traversal	• NAT Traversal Draft 1 (enhanced), Draft 2 and 3 (full implementation), including: - NAT OA support - NAT keepalive - NAT T aggressive mode • Forced NAT-Traversal mode.
Encryption	Provides the following encryption algorithms: • 3DES, DES and AES 128/192/256bits encryption • Support of Group 1, 2, and 5 (that is, 768, 1024, and 1536)
User authentication	Supports the following user authentication methods: • Preshared keying and X509 certificates support. Compatible with most of the currently available IPSec gateways. • Extended authentication (AUTH) • Flexible certificates: PEM, PKCS#12 certificates can be directly imported from the user interface. Ability to configure one certificate per tunnel. • Hybrid authentication method
	Certificate storage capabilities: • USB token and smart card support • Windows certificate store support • VPN configuration file
	Remote login: • Vista Credential Providers support (also known as GIna on Windows 2000 and Windows XP) to enable Windows logon via a VPN tunnel or choose to logon on a local machine.
Dead Peer Detection	Dead Peer Detection (DPD) is an IKE extension (RFC3706) for detecting a dead IKE peer.
Redundant Gateway	The Redundant Gateway feature provides a highly reliable secure connection to a corporate network. The Redundant Gateway feature allows the VPN Client to open an IPSec tunnel with an alternate gateway if the primary gateway is down or not responding.

Table 1. List of Features (Continued)

Feature	Specifications
Mode Config	Mode Config is an IKE extension that enables the VPN gateway to provide LAN configuration to the remote user's machine (that is, the VPN Client). With Mode Config, you can access all servers on the remote network by using their network name (for example, //myserver/marketing/budget) instead of their IP address.
USB dDrive	You can save VPN configurations and security elements (certificates, preshared key, and so on) to a USB drive to remove security information (for example, user authentication) from the computer. You can automatically open and close tunnels when plugging in or removing the USB drive. You can attach a VPN Configuration to a specific computer or to a specific USB drive.
Smart card and USB token	The VPN Client can read certificates from smart cards to make full use of existing corporate ID or employee cards that carry digital credentials. You can easily import smart card ATR codes to enable new smart card and USB token models that are not yet in the software.
Log console	All phase messages are logged for testing or staging purposes.
Flexible user interface	• Silent install and invisible graphical interface allow network administrators to deploy solutions while preventing user misuse of configurations. • Small Connection Panel screen and VPN Configuration Panel screen can be available to end-users separately with access control. • Drag and drop VPN configurations into the VPN Client. • Keyboard shortcuts to easily navigate the VPN Client
Scripts	Scripts or applications can be launched automatically on events (for example, before and after a tunnel opens, or before and after a tunnel is closed).
Configuration management	• User interface and command-line interface (CLI) • Password protected VPN configuration file. • Specific VPN configuration file can be provided within the setup • Embedded demo VPN configuration to test and debug with online servers • Ability to prevent software upgrade or uninstallation if protected by password
Live update	Ability to check for online updates

VPN Client Licenses

NETGEAR products can include a license for the VPN Client Lite or for a 30-day trial copy of the VPN Client Professional, or for both. The following table lists the features that are included in the VPN Client Lite and VPN Client Professional versions. When you launch the VPN Client, you are given the opportunity to purchase a license for the Professional VPN Client and to activate (register) either the VPN Client Professional or VPN Client Lite.

The following table compares the features of the VPN Client Professional and VPN Client Lite.

Table 2. Feature Comparison Between VPN Client Lite and VPN Client Professional

VPN Client Functions		Lite	Pro
Configuration	Configuration wizard	X	X
	X-Auth	X	X
	Mode Config	X	X
	DNS/WINS server manual configuration	X	X
	Hybrid mode		X
	IKE/NAT-T ports can be modified		X
Control	Connection panel/monitor	X	X
	Console logs	X	X
	Block non-ciphered connections (split tunneling)	X	X
	Dead Peer Detection	X	X
	System tray popup	X	X
	GUI protection (password)		X
	Auto Open (windows on startup/on traffic detection)		X
	Start VPN tunnel before Windows Logon		X
	Easy deployment by command-line interface (CLI)		X
Advanced Features	Multi-tunnel configurations		X
	Redundant Gateways	X	X
	Scripts		X
	USB mode		X

Installation

2

This chapter describes installation of the VPN Client and related processes. This chapter includes the following sections:

Software Installation

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

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

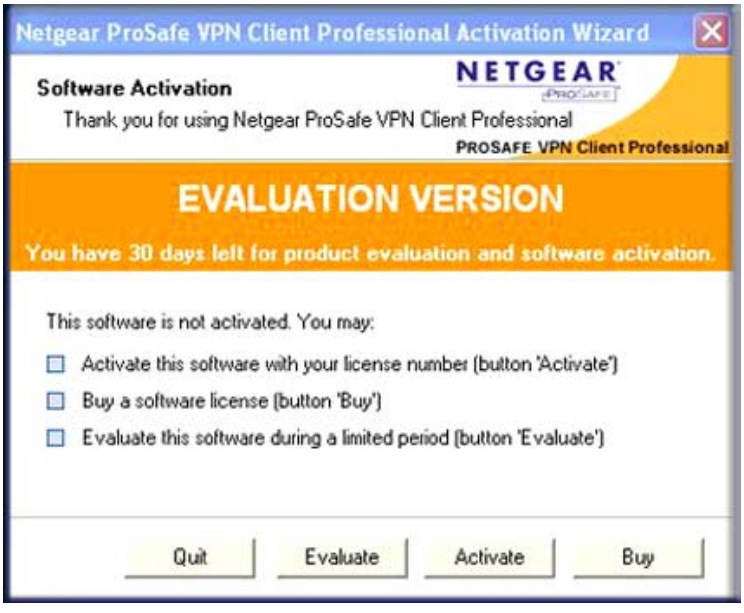


Figure 1.

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

- **Quit**. Closes the window and software.
- **Evaluate**. Lets you continue software evaluation. Evaluation time left is displayed in the orange banner.
- **Activate**. Lets you activate the software license online. This requires a license number and Internet access. When you click the Activate button, an Activation Wizard displays.
- **Buy**. Lets you go online and purchase a software license. When you purchase a software license you must activate it before using the VPN Client.

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

After software installation, there are three ways by which you can launch the VPN window:

- On your desktop, double-click the VPN shortcut.
- In the taskbar, click the VPN Client icon.
- From the Start menu, select the path to the VPN Client, for example, **Start** > **Programs** > **Netgear** > **NETGEAR VPN Client**.

Access Rights

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

Table 3. Access Rights

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

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

Table 4. Windows Firewall Rules

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

Trial Software Evaluation

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

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

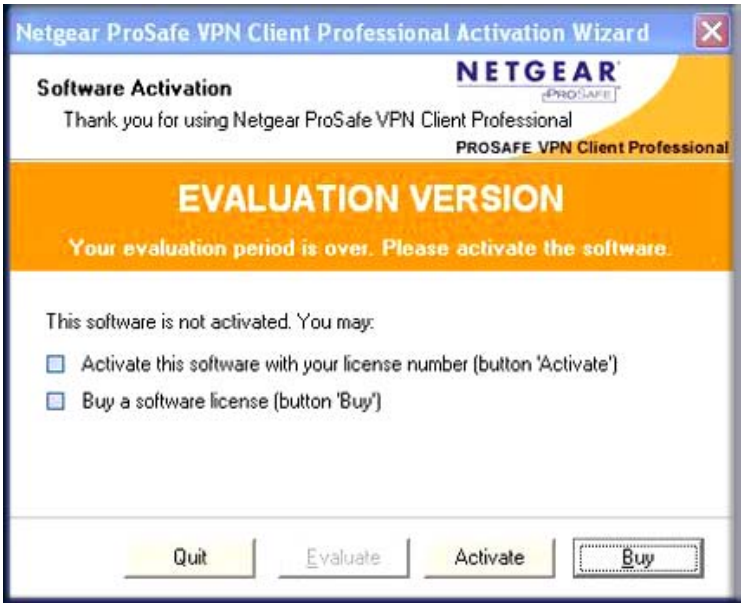


Figure 2.

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

When the temporary license expires, the **Evaluate** button is disabled. You must then click the **Buy** button to purchase a license and click the **Activate** button to activate the purchased license.

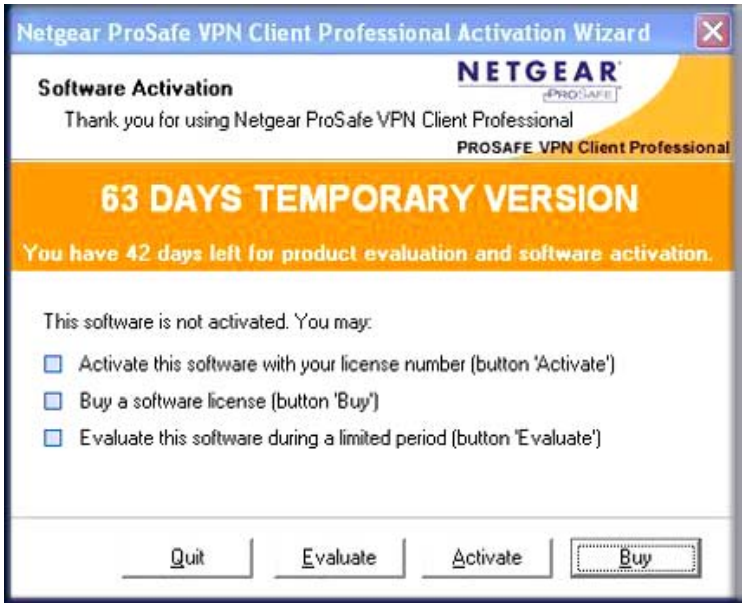


Figure 3.

Software Activation

Software Activation Wizard

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

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

To activate your software using the Activation WIzard:

1. Launch the Activation Wizard from the VPN Client by using either of the following methods:
   - Click the **Activate** button in the VPN Client startup window.
   - Click **?** on the main menu of the Connection Panel screen, then click **Activation Wizard**.

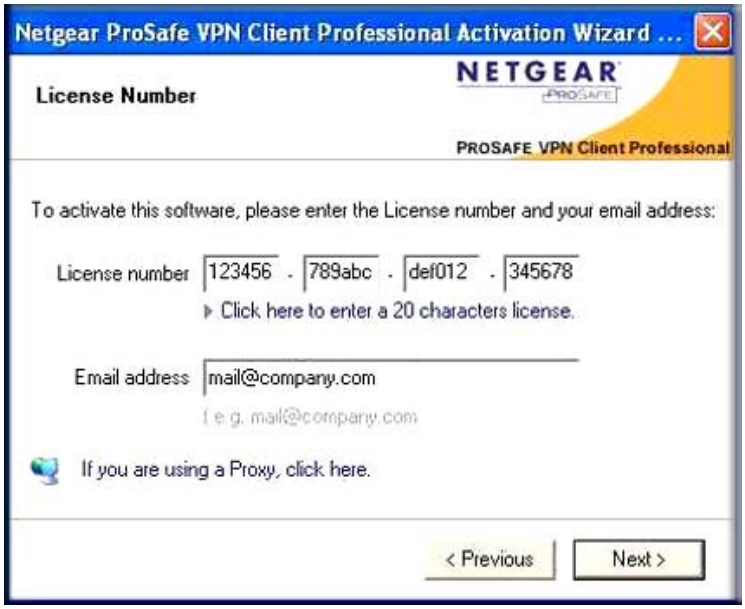


Figure 4.

2. Enter your license lumber. If you have a 20-character license lumber instead of a 24-character one, clicking on **Click here to enter a 20 character License**.
3. Enter your email address, which will be used to send you the activation confirmation.

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

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

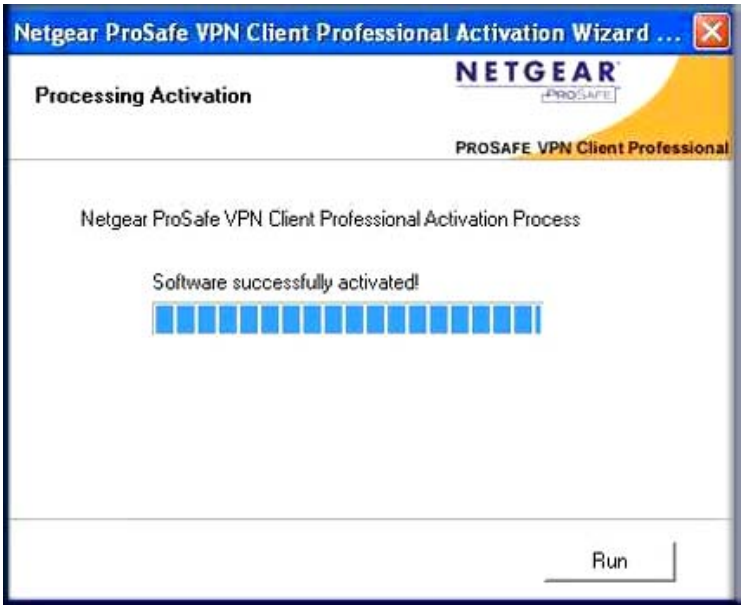


Figure 5.

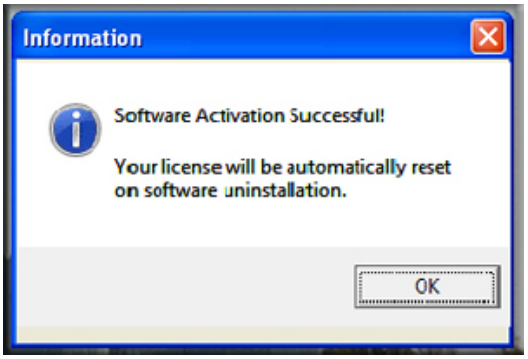


Figure 6.

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

Note: At any time you can change the license number, but you first need to uninstall the VPN Client.

Note: A license number is attached to a single computer after activation. However, you can deactivate the license number and transfer it to another computer.

Troubleshooting Activation

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

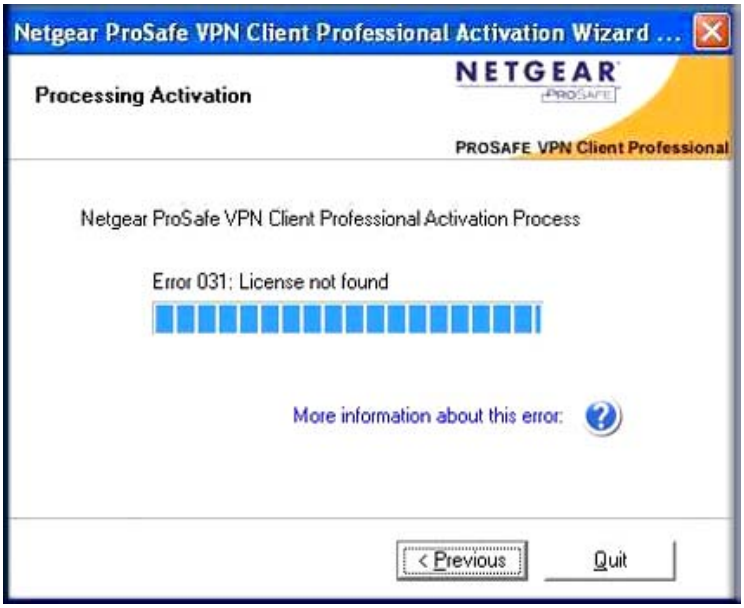


Figure 7.

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

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

All activation errors are listed at *www.netgear.com/support*.

Software Upgrade

Note: The VPN Client must be activated after each software upgrade. Depending on your maintenance contract, a software upgrade activation might be rejected. Carefully read the recommendations in this section and check the current status of your software release by clicking **?** on the main menu of the Connection Panel screen and then **Check for update**.

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

- During the maintenance period (which starts from your first activation), all software upgrades are allowed.
- If the maintenance period has expired or if you have no maintenance contract, only maintenance software upgrades are allowed. Maintenance software upgrades are identified by the last digit of a version.

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

If you want to subscribe or extend your maintenance period, please contact NETGEAR by email at *sales@netgear.com*.

Note: The VPN configuration is saved during a software upgrade and automatically reenabled within the new release.

Note: If you have specified a password in the access control Configuration screen (see *Access Control and Hidden Interface* on page 26), you must enter it to be able to upgrade the software.

Software Uninstallation

You can uninstall the VPN Client through one of the following methods:

- Open the Windows Control Panel, select **Add or Remove Programs**, then select **NETGEAR VPN Client**.
- From the Start menu, select the path to the VPN Client, for example, **Start** > **Programs** > **Netgear** > **NETGEAR VPN Client**, and then the uninstall option.

When you uninstall the VPN Client, make sure your computer is connected to the Internet. If your computer is not connected to the Internet, contact NETGEAR support by email at *support@netgear.com* or call the technical center to inactivate your license key.

Tip: After uninstallation, save the license key number. You might need it again to reactivate your software. Also, keep the CD label for technical support.

User Interface Overview

3

This chapter describes the user interface for the VPN Client. This chapter includes the following sections:

User Interface Elements

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

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

The user interface consists of several elements:

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

You can launch the VPN Client by double-clicking the application icon on the desktop or Windows start menu or by single-clicking on the application icon in the system tray. Once launched, the VPN Client displays an icon in the system tray that indicates whether or not a tunnel is opened, using a color code.

Green icon:
at least one VPN tunnel opened.

Purple icon:
no VPN tunnel opened.

Figure 8.

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

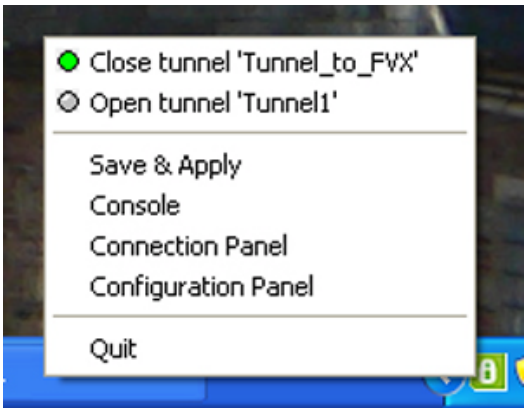


Figure 9.

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

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

System Tray Popup Screens

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

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

Figure 10.

- VPN tunnel closing.

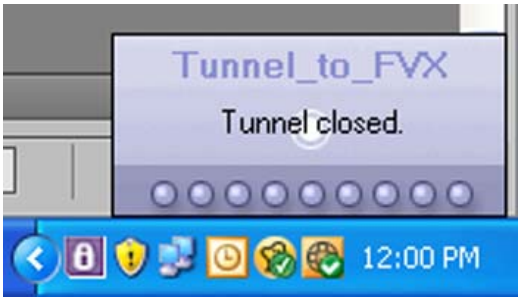


Figure 11.

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

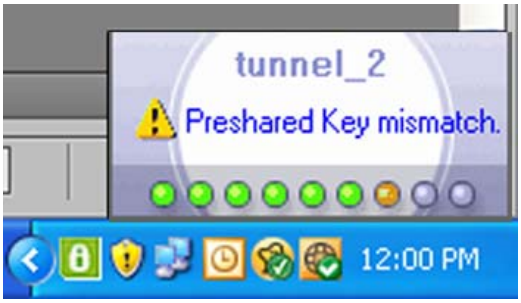


Figure 12.

Keyboard Shortcuts

The user interface supports the following keyboard shortcuts.

Table 5. Keyboard Shortcuts

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

Connection Panel Screen

The Connection Panel screen enables you to open, close, and receive clear information about every tunnel that has been configured. If an administrator has configured the VPN tunnels, the end user only needs access to the Connection Panel to open and close tunnels.

The Connection Panel screen consists of the following components:

- An animated network diagram that shows information about the current tunnel (at the top of the screen)
- A list of all configured tunnels with buttons to open and close the tunnels (below the network diagram)
- A link back to the Configuration Panel screen (at the left bottom of the screen)

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

Figure 13.

Configuration Panel Screen

The Configuration Panel screen enables you to configure VPN tunnels, and consists of the following components:

- Main menu (at the top of the screen)
- The **Console**, **Parameters**, and **Connections** buttons in the left column of the screen
- A tree list window (in the left column of the screen) that contains all the IKE and IPSec configurations
- A configuration window (in the right column of the screen) that shows the associated settings for each tree level.
- Status bar (at the bottom of the screen)

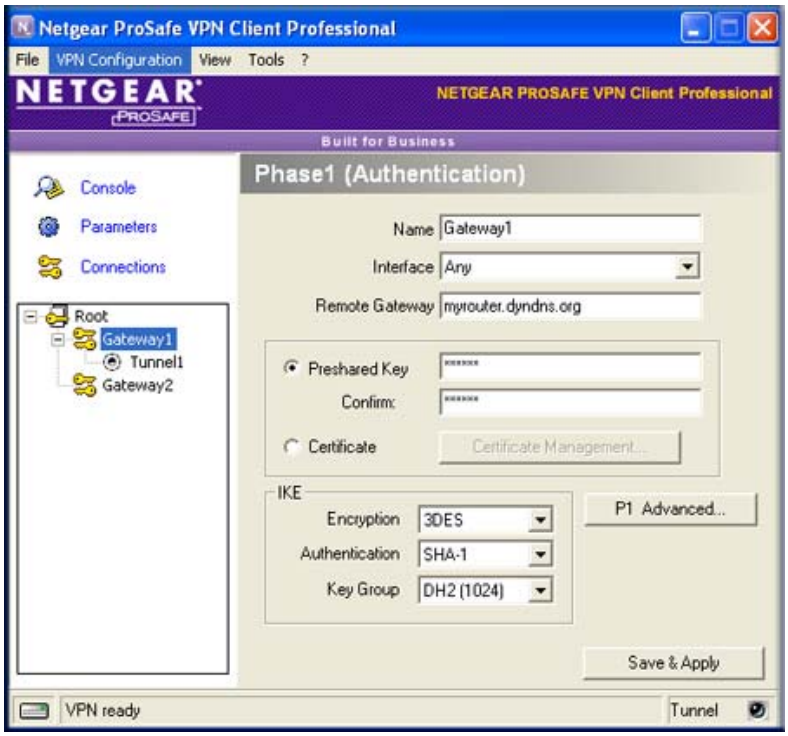


Figure 14.

You can drag and drop a VPN configuration file (that is, a file with a .tgb extension) onto the Configuration Panel screen to easily apply a new VPN configuration. If a tunnel is configured to be opened when the VPN Client starts (see *Phase 2 (IPSec) Advanced Configuration* on page 53), the tunnel is immediately opened when you click **Save & Apply** to apply the new VPN configuration.

Main Menu

The main menu lets you make the following selections:

- **File**. Lets you import and export a VPN configuration, select the location of the VPN configuration (locally stored on the computer or on a USB drive), and configure miscellaneous preferences such as the way the VPN Client starts.
- **VPN Configuration**. Lets you create and change VPN configurations and access the configuration wizard (Config. Wizard).
- **View**. Lets you access the Connection Panel screen and configure access to the user interface.
- **Tools**. Lets you access the VPN Console screen and the Connections screen and lets you reset the IKE settings..
- **?**. Lets you access online help, check for software updates, access the Activation Wizard, and access the About screen.

> **Note:** Some selections that are available from the **File** and **VPN Configuration** menus are also available by right-clicking a component of the tree list window in the Configuration Panel screen.

Status Bar

The status bar at the bottom displays the following information:

- The narrow left field lets you select the location of the VPN configuration
- The large central field provides the status of the VPN Client (for example, opening tunnel in progress, saving configuration rules in progress, and VPN Client start up in progress).
- The narrow right field provides information about tunnels: a green light indicates that at least one tunnel is open; a gray light indicates that no tunnel is open).

The About Screen

The About screen that you can access by clicking **?** on the main menu provides the VPN Client software release number and software activation information. There is also an URL to the NETGEAR website.

Figure 15.

Access Control and Hidden Interface

Access control is a feature that is intended for use by administrators. It allows you to restrict access to the Connection Panel screen and the system tray menu with a password and to lock access to the Configuration Panel screen to prevent users from modifying the VPN configuration. Only the Configuration Panel screen can be password-protected; the Connection Panel screen cannot.

When access control is enabled, you are asked for the password under the following circumstances:

- when you click (or double-click) on the VPN Client icon in the system tray.
- when you switch from the Connection Panel screen to the Configuration Panel screen.
- when you start a software upgrade.

Figure 16.

You can also configure this password as an option of the software setup (see *VPN Client Software Setup Commands* on page 80).

The access control Configuration screen that you can access by clicking **View** on the main menu also lets you configure the system tray menu items. In this way an administrator can restrict the software access from a full access to a completely hidden interface.

Figure 17.

To remove access control, clear the **Password** and **Confirm** fields, and then click **OK**.

Note: The **Quit** check box for the system tray menu is disabled in the standard version of the software. You can remove this check box during the software setup through the `menuitem` option (see *Software Setup for System Tray Menu Items* on page 82).

When access control is enabled, you cannot open the Configuration Panel screen by double-clicking on desktop icon or by using the Start menu; when you right-click on the system tray icon, the options are limited to accessing the VPN Console, opening and closing the configured tunnels, and closing the VPN Client.

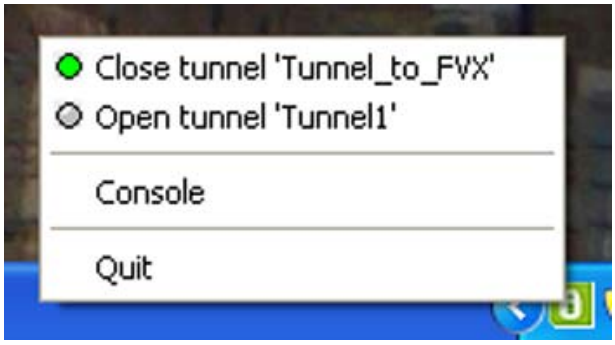


Figure 18.

Wizards

There are several wizards available:

- **VPN configuration wizard**. Access this wizard by selecting **VPN Configuration** > **Config. Wizard** from the main menu (for more information, see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 39).
- **Software activation wizard**. Access this wizard by selecting **?** > **Activation Wizard** from the main menu (for more information, see *Software Activation Wizard* on page 14).
- **USB drive mode wizard**. Access this wizard by selecting **File** > **Move VPN Configuration to USB Drive** from the main menu (for more information, see *USB Mode* on page 59).

Preferences Screen

The Preferences screen that you access by selecting **File** > **Preferences** from the main menu lets you specify the following:

- VPN Client startup modes:
  - Start the VPN Client after you have logged into Windows.
  - Do not start the VPN Client after you have logged into Windows. In this case, you need to manually start the VPN Client or use a script to start it.

Note: You can also configure these modes in the software setup (see *VPN Client Software Setup Commands* on page 80).

- Enable or disable the detection of the interface disconnection feature. When you disable the detection of interface disconnection the VPN Client keeps tunnels open when the network interface disconnects momentarily. This type of behavior occurs when the interface that is used to open tunnels is unstable such as Wi-Fi, GPRS, and 3G interfaces.

Figure 19.

VPN Console Active Screen

You can access the VPN Console Active screen from the system tray menu, from the Console **button** on the Configuration Panel screen, or by selecting **Tools** > **Console** from the main menu of the Console Panel screen. Use the VPN Console Active screen to analyze VPN tunnels, which can be useful if you are an administrator and have to set up a network.

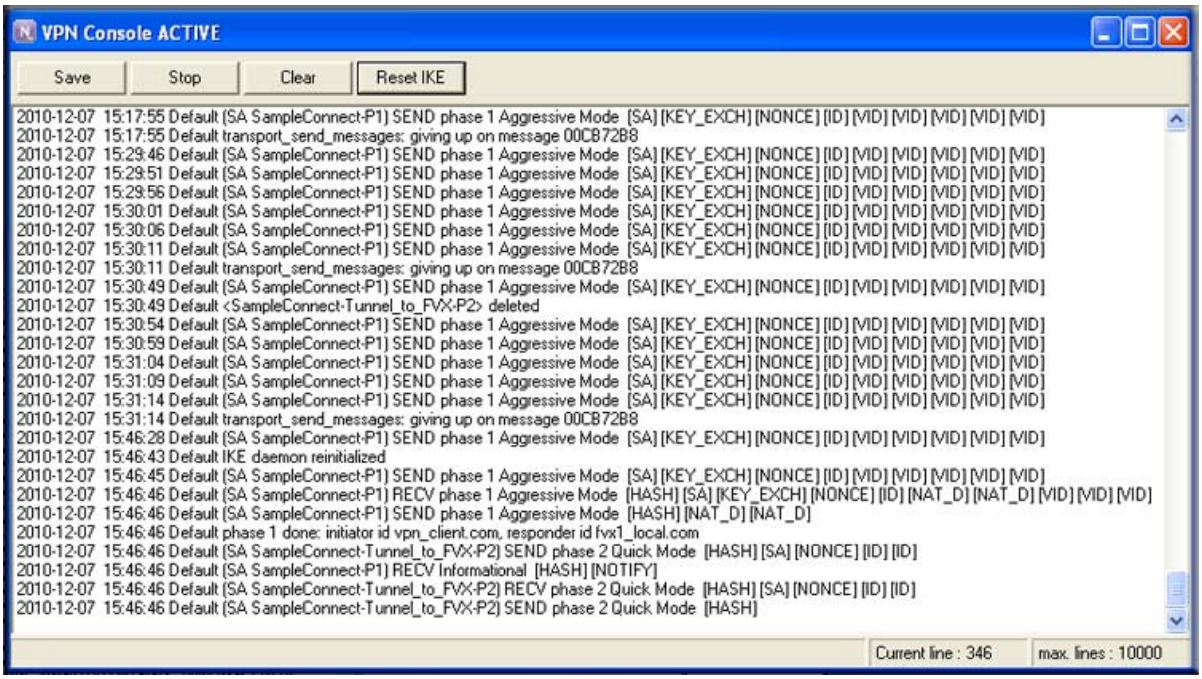


Figure 20.

The buttons on the VPN Console ACtive screen have the following functions:

- **Save**. Saves the current logs in a file without overwriting previous logs.
- **Start** or **Stop**. Starts or stops the collection of logs. Only one of these buttons is displayed on screen.
- **Clear**. Removes the content from the screen.
- **Reset IKE**. Restarts the IKE process.

Basic Tasks

4

This chapter describes some basic tasks of the VPN Client. These tasks are described in more detail in other chapters. This chapter includes the following sections:

Open a VPN Tunnel

You can open a tunnel only after the VPN configuration has been specified.

To manually open a tunnel:

- Select a tunnel on the Connection Panel screen, and click **Open** (see *Connection Panel Screen Basics* on page 36).
- Right-click on the system tray icon and select the tunnel that you want to open (see *User Interface Elements* on page 20).
- Double-click on a VPN configuration icon on your desktop or in an email attachment. (To create a VPN configuration icon, see *VPN Configuration Management* on page 73.)
- Use the command-line interface (CLI) (see *Open or Close VPN Tunnels* on page 85).

To enable a tunnel to be opened automatically:

Select one or more of the following check boxes on the Phase 2 (Authentication) window of the Configuration Panel screen:

- Automatically open this tunnel when the VPN Client starts after login
- Automatically open this tunnel when USB stick is inserted
- Automatically open this tunnel on traffic detection

(For more information, see *Phase 2 (IPSec) Advanced Configuration* on page 53.)

Easily Import a VPN Configuration

You can create various VPN configurations on the windows desktop and open a tunnel by double-clicking a VPN configuration icon (that is, a file with a .tgb extension).

To create a VPN configuration shortcut icon on the desktop:

1. Configure a tunnel on the Configuration Panel screen (see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 39 or *Manually Create a VPN Tunnel Connection* on page 42).
2. Configure the tunnel to automatically open when the VPN Client starts after login (see *Phase 2 (IPSec) Advanced Configuration* on page 53).
3. Export the VPN configuration onto your computer desktop (see *Import or Export a VPN Configuration* on page 73).

Specify a Certificate for User Authentication

To configure a new phase 1 and new phase 2, and then specify a certificate for the tunnel:

1. Create a new phase 1 configuration (see *Phase 1 (Authentication) Configuration* on page 43) and configure the advanced settings (see *Phase 1 (Authentication) Advanced Configuration* on page 45).

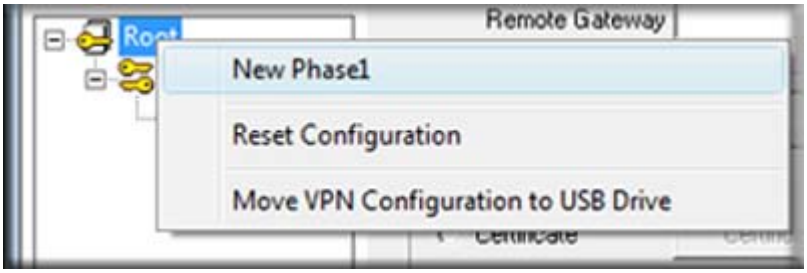


Figure 21.

2. Add a new phase 2 configuration (see *Phase 2 (IPSec) Configuration* on page 50) and configure the advanced settings (see *Phase 2 (IPSec) Advanced Configuration* on page 53).

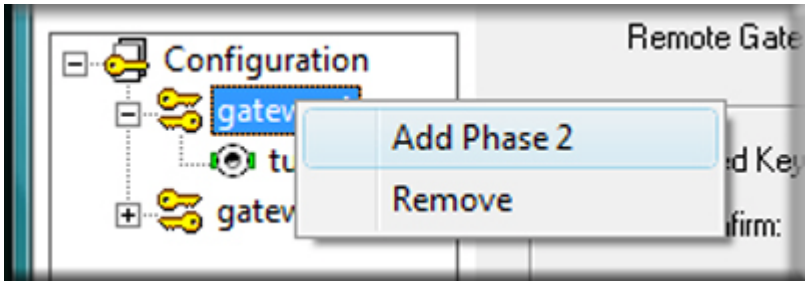


Figure 22.

3. Open the Phase 1 (Authentication) window in the Configuration Panel screen, select the **Certificate** radio button, and then click **Certificate Management** (see *Assign Certificates* on page 64).

Figure 23.

4. From the list in the Certificate for Phase 1: [*tunnel name*] screen, select one certificate or click **Import Certificate** to import a new certificate (see *Import Certificates* on page 67), and then click **OK**.

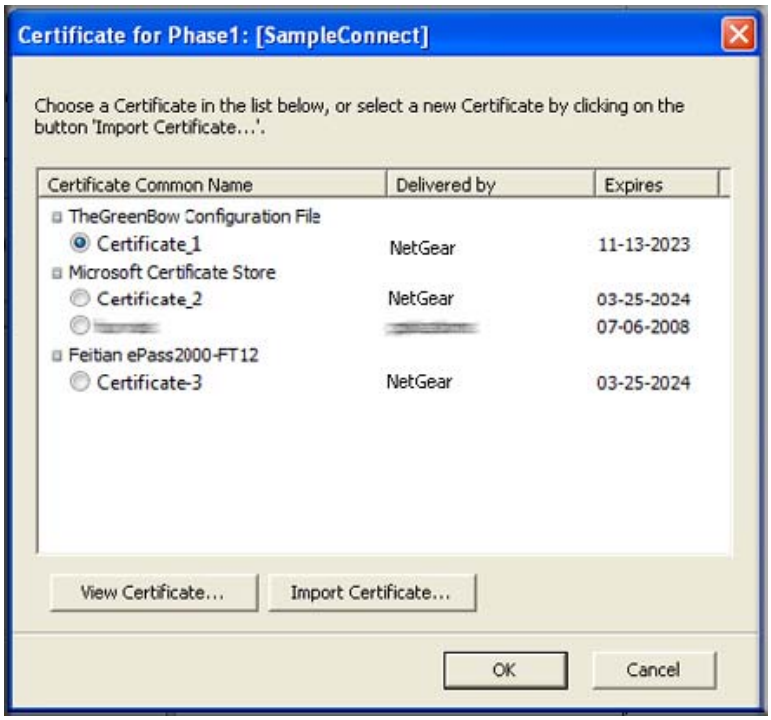
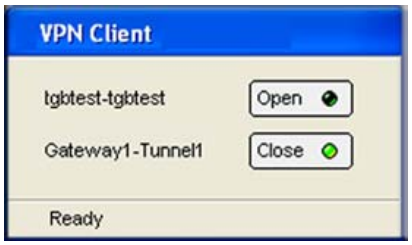


Figure 24.

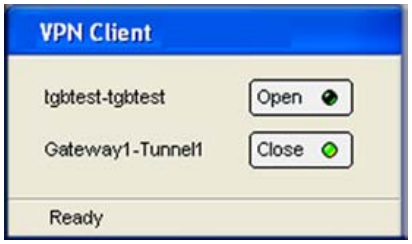
Open a VPN Tunnel Before Windows Logon

You can open manually or automatically one or more VPN tunnels before Windows logon by using a Windows logon technology that is referred to as Credential Providers on Vista and Gina mode on Windows 2000 and WIndows XP.

To manually open a VPN tunnel before Windows logon:

Settings	VPN Client Behavior
1. Open the Phase 2 Advanced screen. 2. Select the **Enable before Windows logon** check box. 3. Ensure that the **Automatically open this tunnel on traffic detection** check box is cleared. For more information, see *Phase 2 (IPSec) Advanced Configuration* on page 53.	Before Windows logon, the following popup screen appears to allow the user to the required VPN tunnel.  The popup screen lists all VPN tunnels for which you have selected the **Enable before Windows logon** check box on the Phase 2 Advanced screen.

To automatically open a VPN tunnel before Windows logon:

Settings	VPN Client Behavior
1. Open the Phase 2 Advanced screen. 2. Select the **Enable before Windows logon** check box. 3. Select the **Automatically open this tunnel on traffic detection** check box. For more information, see *Phase 2 (IPSec) Advanced Configuration* on page 53.	Before Windows logon, the following popup screen appears to display the VPN tunnels that are opened automatically.  The popup screen lists all VPN tunnels for which you have selected the **Enable before Windows logon** check box on the Phase 2 Advanced screen.

Note: To enable a VPN tunnel to automatically open on traffic detection *after* windows logon, select the **Automatically open this tunnel on traffic detection** check box and ensure that the **Enable before Windows logon** check box is cleared.

The following information applies to tunnels for which you have selected the **Enable before Windows logon** check box on the Phase 2 Advanced screen:

- You cannot hide the popup screen that appears before Windows logon.
- If two tunnels have been configured to automatically open on traffic detection but only one tunnel is configured to be enabled before Windows logon, both tunnels might open automatically before Windows logon when the IKE services is running.
- Scripts that you might have configured are disabled.
- The VPN Client cannot function in USB mode (see *USB Mode* on page 59).
- The Mode Config feature is disabled, so you might have to specify DNS or WINS server addresses (see *Phase 2 (IPSec) Advanced Configuration* on page 53).
- When extended authentication (XAUTH) is enabled (see *Extended Authentication* on page 48), a popup screen appears when tunnels open to enable you to enter the login name and password.
- When you use a USB token or SmartCard, a popup screen appears when tunnels open to enable you to enter the PIN code.

Connection Panel Screen Tasks

5

This chapter describes the Connection Panel screen. This chapter includes the following sections:

Connection Panel Screen Basics

The Connection Panel screen enables you to open, close, and receive clear information about every tunnel that has been configured. If an administrator has configured the VPN tunnels, the end user only needs access to the Connection Panel to open and close tunnels.

To open the Connection Panel screen, select **View** > **Connection Panel** from the main menu on the Configuration Panel screen or right-click on the system tray icon and select **Connection Panel**.

Figure 25.

The Connection Panel screen consists of the following components:

- An animated network diagram that shows information about the current tunnel (at the top of the screen)
- A list of all configured tunnels with buttons to open and close the tunnels (below the network diagram)
- A link back to the Configuration Panel screen (at the left bottom of the screen)

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

To open a selected tunnel, click on its **Open** button. The **Open** button automatically switches to a **Close** button when the tunnel is opened.

When you click on the name of the tunnel, the Configuration Panel screen automatically opens, enabling you to change the tunnel configuration. This feature is disabled when the Configuration Panel screen is protected with a password (see *Access Control and Hidden Interface* on page 26).

You can drag and drop a VPN configuration file (that is, a file with a .tgb extension) onto the Connection Panel screen to easily apply a new VPN configuration. If a tunnel is configured to be opened when the VPN Client starts (see *Phase 2 (IPSec) Advanced Configuration* on page 53), the tunnel is immediately opened when you click **Save & Apply** to apply the new VPN configuration.

Tunnel Connection Problems

If problems occur during the tunnel opening process, a warning is shown to the right of the tunnel, as is shown in the right screen in the following figure.

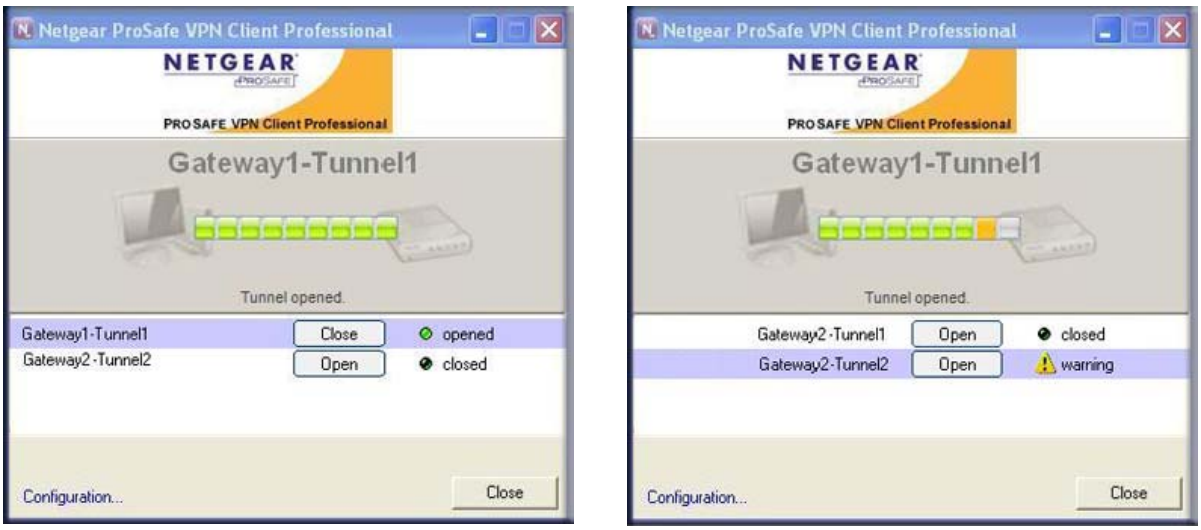


Figure 26.

When you click on the link that is associated with the warning, a popup screen displays a detailed message about the problem. Click on **More information about this error** to open an online help Web page that provides more details and suggestions for troubleshooting.

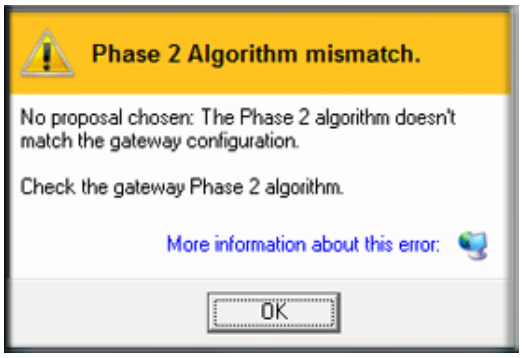


Figure 27.

Configuration Panel Screen Tasks

6

This chapter describes the Configuration Panel screen. This chapter includes the following sections:

Use the Configuration Wizard to Create a VPN Tunnel Connection

The VPN Client provides a Configuration Wizard that lets you create a VPN configuration in three easy steps. This Configuration Wizard is designed for remote computers that need to be connected to a corporate LAN through a VPN gateway and for peer-to-peer connections.

The configuration in *Figure 28* has the following characteristics:

- The remote computer has a dynamically provided public IP address.
- The remote computer connects to the corporate LAN behind a VPN gateway that has a DNS address with the name gateway.mydomain.com.
- The corporate LAN address is 192.168.1.xxx, that is, the remote computer must reach a server with the IP address 192.168.1.100.

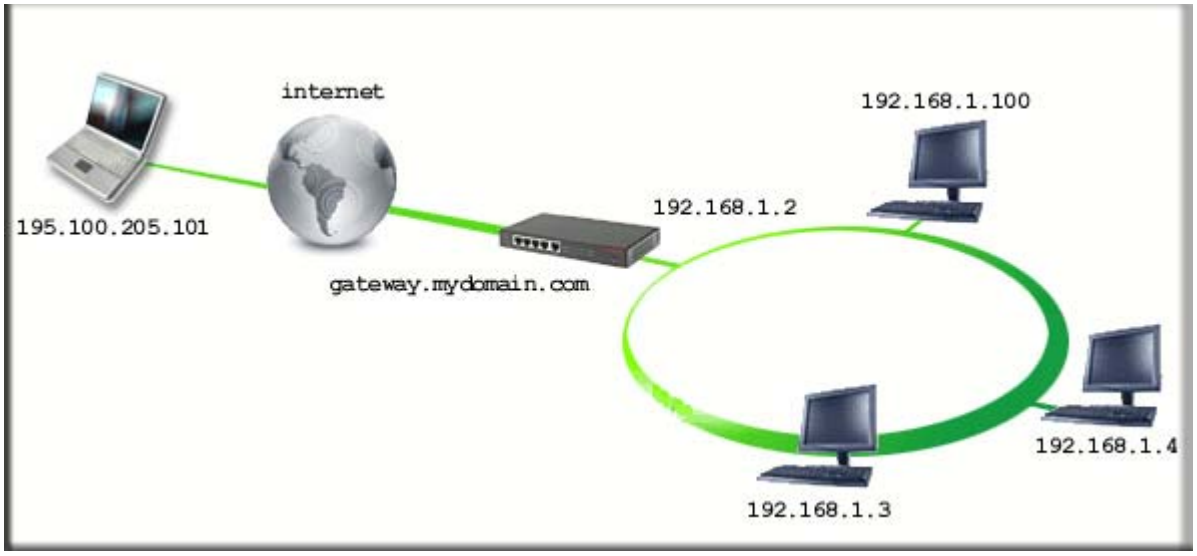


Figure 28.

To create a VPN tunnel connection between the remote computer and the corporate LAN:

1. From the main menu on the Configuration Panel screen, select **VPN Configuration** > **Config. Wizard**. The VPN Client Configuration Wizard Step 1 of 3 screen displays.

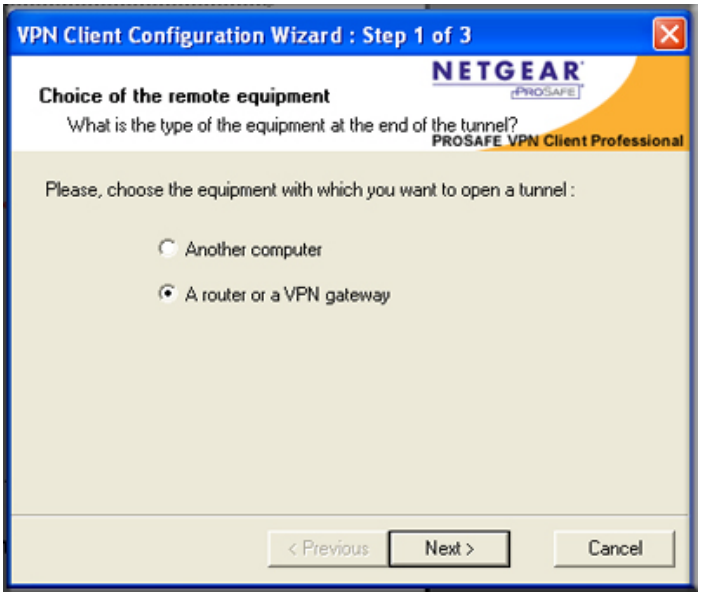


Figure 29.

2. Select the equipment to connect to. The options are **Another Computer** and **a router or a VPN gateway**. In this configuration, select the **a router or a VPN gateway** radio button.
3. Click **Next**. The VPN Client Configuration Wizard Step 2 of 3 screen displays.

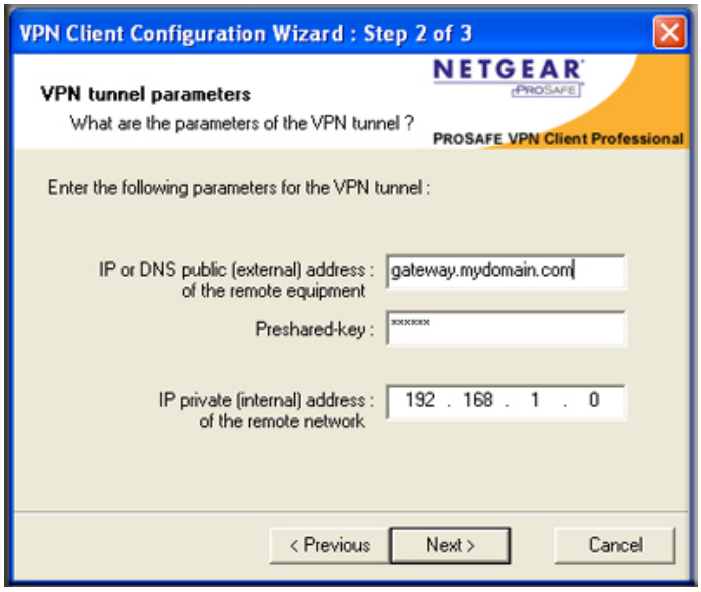


Figure 30.

4. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. The public (WAN) IP address of the remote gateway. In this example, enter **gateway.mydomain.com**.
   - **Preshared key**. The preshared key that must also be defined on the remote gateway.
   - **IP private (internal) address of the remote network**. The IP address of the remote network. In this example, enter **192.168.1.0**.
5. Click **Next**. The VPN Client Configuration Wizard Step 3 of 3 screen displays.

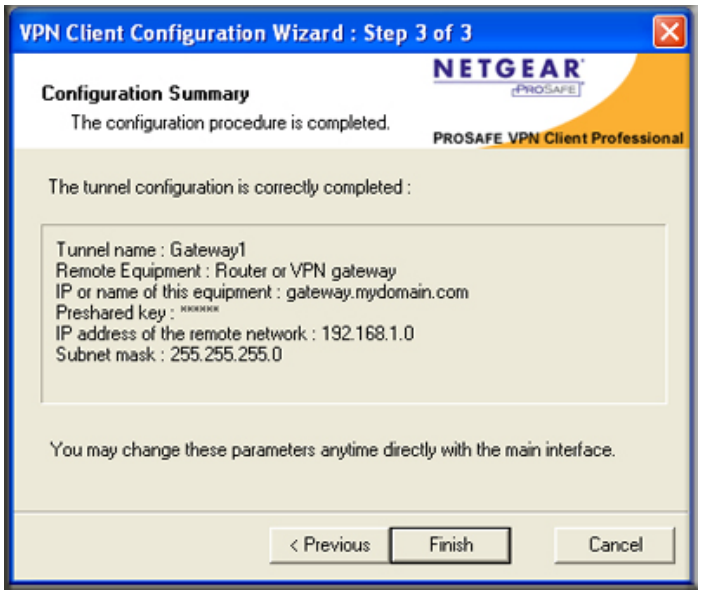


Figure 31.

This screen is a summary screen of the new VPN configuration. If required, you can specify other settings such as certificates and virtual IP addresses on the Configuration Panel screen.

6. Click **Finish**.

To open the newly created tunnel:

1. From the main menu on the Configuration Panel screen, select **View** > **Connection Panel**.
2. Next to the newly created tunnel (Gateway1-Tunnel1), click **Open**.

Manually Create a VPN Tunnel Connection

To manually create a VPN tunnel from the Configuration Panel screen:

1. In the tree list window of the Configuration Panel screen, right-click on **Root** and select **Reset Configuration**.

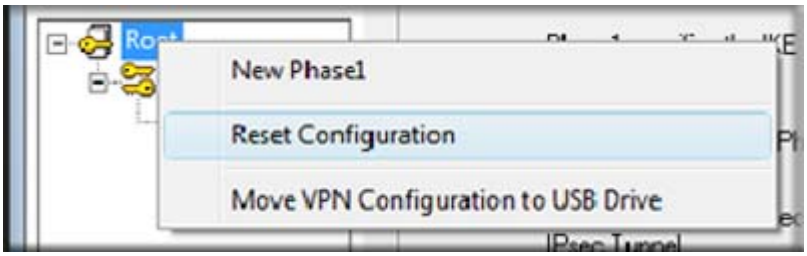


Figure 32.

2. In the tree list window of the Configuration Panel screen, right-click on **Root** and select **New Phase 1**.

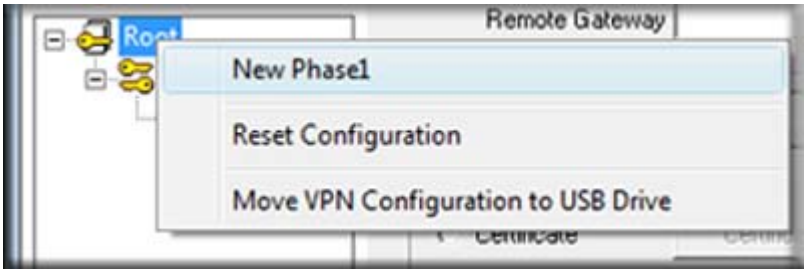


Figure 33.

3. The Phase 1 (Authentication) screen displays in the right column of the Configuration Panel screen. Configure the authentication that enables you to connect to the remote gateway or computer as explained in *Phase 1 or Authentication* on page 43.
4. In the tree list window of the Configuration Panel screen, right-click on **Gateway1** and select **Add Phase 2**.

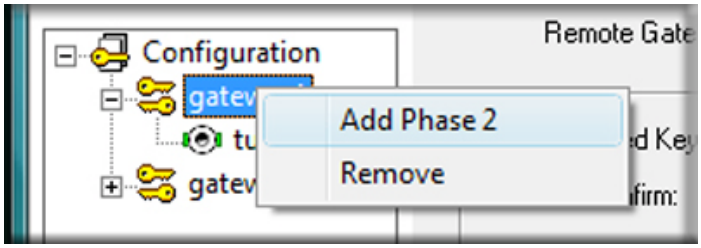


Figure 34.

5. The Phase 2 (IPSec Configuration) window displays in the right column of the Configuration Panel screen. Configure the IPSec configuration that enables to communicate securely with the remote gateway or computer as explained in *Phase 2 or IPSec Configuration* on page 50.
6. Click **Save & Apply** to save the new configuration.
7. Click **Open Tunnel** to open the new VPN tunnel.

Phase 1 or Authentication

The Phase 1 (Authentication) window that opens in the Configuration Panel screen lets you specify the settings for the authentication phase, which is also referred to as phase 1 or as the Internet Key Exchange (IKE) negotiation phase. Phase 1's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of phase 1, each end system must identify and authenticate itself to the other.

You can specify several authentication phases, enabling one computer to establish IPSec VPN connections with several gateways or other computers (peer-to-peer connections).

Phase 1 (Authentication) Configuration

To configure a new phase 1 or edit a existing phase 1 configuration:

1. Take one of the following actions:
   - To create a new phase 1 configuration:
     a. Click on **Root** in the tree list window of the Configuration Panel screen.
     b. Select **VPN Configuration** > **New Phase 1** from the main menu.
   - To edit an existing phase 1 configuration, click on an existing phase 1 name in the tree list window of the Configuration Panel screen.

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

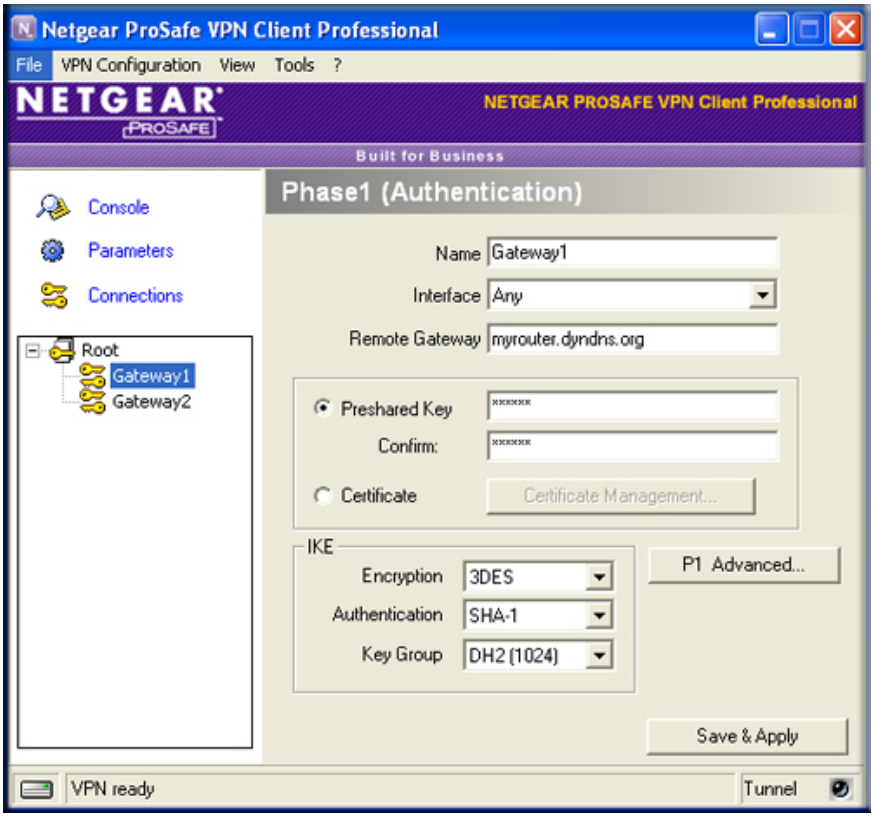


Figure 35.

2. Configure the settings as explained in the following table.

Table 6. Phase 1 Authentication Settings

Setting	Description
Name	The label for the authentication phase that is used only for the VPN Client, not during IKE negotiation. You can view and change this name in the tree control window. This name must be a unique name.
Interface	The 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 from an ISP or router), select **Any**. **Note:** If this refers to an IP address that does not exist on the computer, **Any** is automatically used
Remote Gateway	The IP address or DNS address of the remote gateway (in the example on screen, myrouter.dyndns.org). This field is mandatory.
Preshared Key	The password or key that is shared with the remote gateway. You must enter the same key in the **Confirm** field.

Table 6. Phase 1 Authentication Settings (Continued)

Setting	Description	
Certificate	This selection is optional. The X509 certificate that is used by the VPN Client. Click on **Certificate Management** to open the Certificate screen that lets you select the certificate source. You can use a PEM file, PKCS#21 file, SmartCard, or token, or a certificate from the Windows Certificate Store. Specify only one certificate per tunnel. For information about certificates, see *Certificate Management* on page 64.	
IKE	Encryption	The encryption algorithm that is used during the authentication phase. Select one of the following from the drop-down list: • **DES**. • **3DES**. This is the default setting. • **AES 128**. • **AES 192**. • **AES 256**.
	Authentication	The authentication algorithm that is used during the authentication phase. Select one of the following from the drop-down list: • **MD5**. • **SHA-1**. This is the default setting
	Key Group	The Diffie-Hellman key length that is used during the authentication phase. Select one of the following from the drop-down list: • **DH1 (768)**. • **DH2 (1024)**. This is the default setting. • **DH5 (1536)**.

3. As an optional step, click **P1 Advanced ...**. to open the Phase 1 Advanced screen and configure the advanced settings (for more information, see the following section).
4. Click **Save & Apply** to save and apply the new settings.

Phase 1 (Authentication) Advanced Configuration

Note: For each phase 1 configuration that you create, the advanced phase 1 settings apply to all its phase 2 (IPSec configuration) settings.

To configure phase 1 advanced settings:

1. Click **P1 Advanced ...** in the Phase 1 (Authentication) window of the Configuration Panel screen. The Phase 1 Advanced screen displays.

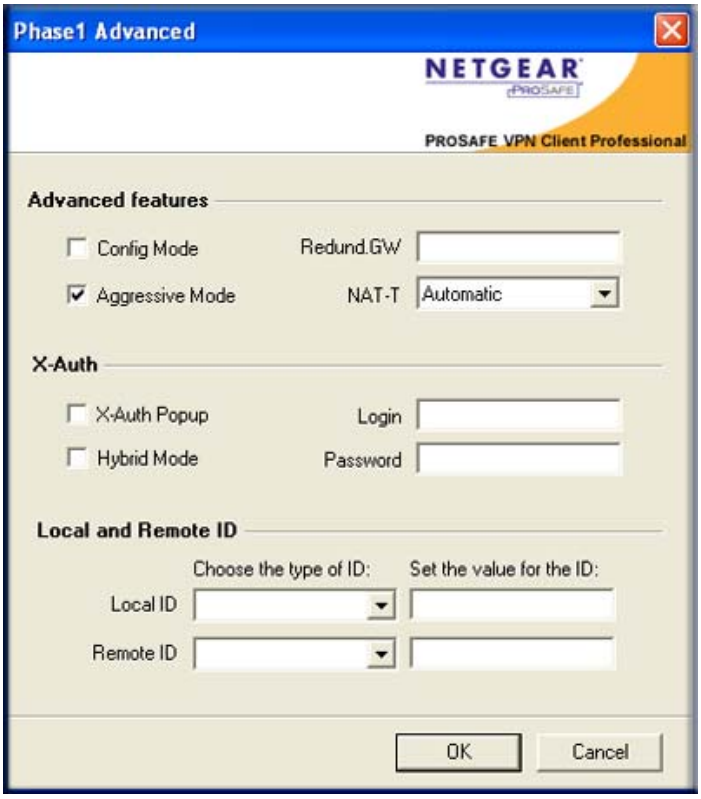


Figure 36.

2. Configure the settings as explained in the following table.

Table 7. Phase 1 Advanced Authentication Settings

Setting	Description
Advanced features	
Config Mode	Select the **Config Mode** check box to enable the Mode Config feature that allows the VPN Client to receive VPN configuration information from the remote VPN gateway. (The remote VPN gateway must support the Mode Config feature.) When the Mode Config feature is enabled, the following information is negotiated between the VPN Client and the remote VPN gateway during the authentication phase: • Virtual IP address of the VPN Client • DNS server address (optional) • WINS server address (optional) **Note:** If the Mode Config feature is not available or not supported on the remote VPN gateway, see the information in *Phase 2 (IPSec) Advanced Configuration* on page 53 to manually specify the DNS and WINS server addresses on the VPN Client.
Aggressive Mode	The **Aggressive Mode** check box is selected by default to enable the VPN Client to use aggressive mode as the negotiation mode with the remote VPN gateway. Clear the check box to disable aggressive mode.

Table 7. Phase 1 Advanced Authentication Settings (Continued)

Setting	Description
Redund.GW	Enter the IP address or URL of an alternate VPN gateway in the **Redund.GW** field to enable the VPN Client to open an IPSec tunnel with an alternate gateway when the primary VPN gateway is down, goes down, or stops responding. An alternate gateway is used under the following circumstances: • If the VPN Client cannot contact the primary gateway to establish a tunnel. After several attempts (determined by the value in the Retransmission field—the default is 5 attempts—in the Parameters window of the Configuration Panel screen (see *Global Parameters* on page 56), the VPN Client usus the alternate gateway as the new tunnel endpoint. The interval between two attempts is about 10 seconds. • If a tunnel is successfully established with the primary gateway with the Dead Pear Detection (DPD) feature (see *Global Parameters* on page 56) but the primary gateway stops responding to DPD messages. **Note:** The same connection rules apply if the alternate gateway goes down or stops responding. This means that the VPN Client could switch between the primary and alternate gateways until you click **Save & Apply** or close and exit the VPN Client. **Note:** If the primary gateway can be reached but tunnel establishment fails (that is, there are VPN configuration errors), the VPN Client does not attempt to establish a tunnel with the alternate gateway. In this case you must first resolve the configuration errors.
NAT-T	From the **NAT-T** drop-down list, select one of the following NAT Traversal (NAT-T) modes: • **Automatic**. Enables the VPN Client and VPN gateway to negotiate NAT-T. This is the default setting. • **Forced**. Enables the VPN Client to force NAT-T by encapsulating IPSec packets into UDP frames, thereby allowing packet traversal through intermediate NAT routers. • **Disabled**. Prevents the VPN Client and VPN gateway from negotiating NAT-T.
X-Auth	
X-Auth Popup	Extended authentication (XAUTH) is an extension to the IKE protocol. To enable XAUTH, enter a name in the **Login** field and a password in the **Password** field. Select the **X-Auth Popup** check box to enable a popup window in which the login name and password can be entered during the authentication phase. This popup window displays each time when authentication is required to open a tunnel with a remote VPN gateway. If XAUTH authentication fails, the tunnel establishment fails too. For more information, see *Extended Authentication* on page 48.

Table 7. Phase 1 Advanced Authentication Settings (Continued)

Setting	Description
Hybrid Mode	Select the **Hybrid Mode** check box to enable this mode, and enter a name in the **Login** field and a password in the **Password** field. Hybrid mode is an authentication method that is used within the phase 1 authentication. Hybrid mode assumes an asymmetry between the authenticating entities. One entity, typically an edge device (for example, a firewall), authenticates using standard public key techniques (in signature mode), while the other entity, typically a remote user, authenticates using challenge response techniques. At the end of the phase 1 authentication, these authentication methods are used to establish an IKE SA that is unidirectionally authenticated. To ensure that the IKE is bidirectionally authenticated, the phase 1 authentication is immediately followed by an extended authentication (XAUTH) to authenticate the remote user. The use of these authentication methods is referred to as hybrid authentication mode. **Note:** The VPN Client implements the RFC draft-ietf-ipsec-isakmp-hybrid-auth-05.txt.
Local and Remote ID	
Local ID	The local ID is the identity that the VPN Client transmits to the VPN gateway during the authentication phase . From the **Local ID** drop-down list, select one of the following types of IDs, and enter the associated value for the ID in the field to the right: • **IP Address**. Enter a standard IP address (for example, 195.100.205.101). • **DNS**. Enter a fully qualified domain name (FQDN) (for example, mydomain.com). This is the default selection. • **DER ASN1 DN**. Enter a certificate issuer (for more information, see *Certificate Management* on page 64) If you do not enter a certificate, the IP address of the VPN Client is used. • **Subject from X509**. These fields are automatically set when you import a certificate (see *Import Certificates* on page 67).
Remote ID	The remote ID is the identity that the VPN Client receives from the VPN gateway during the authentication phase . From the **Remote ID** drop-down list, select one of the following types of IDs, and enter the associated value for the ID in the field to the right: • **IP Address**. Enter a standard IP address (for example, 80.2.3.4). • **DNS**. Enter a fully qualified domain name (FQDN) (for example, gateway.mydomain.com). This is the default selection. • **DER ASN1 DN**. Enter a certificate issuer (for more information, see *Certificate Management* on page 64) If you do not enter a certificate, the IP address of the VPN gateway is used.

3. Click **OK** to save the settings.

Extended Authentication

IKE is an important element of the Public Key Infrastructure (PKI) that defines how security credentials are exchanged over the IPSec tunneling protocol. For extended authentication (XAUTH), IPSec negotiation requires the definition of a login name and password.

To use XAUTH:

1. Specify the XAUTH credentials on the Phase 1 Advanced screen by entering a name in the **Login** field and a password in the **Password** field (see the previous section and table). These credential are used each time that a VPN tunnel is opened.
2. For a user other than the administrator: enter credentials in the XAUTH popup window. This step applies only if the **X-Auth Popup** check box is selected to enable a popup window in which the login name and password can be entered during the authentication phase. This popup window displays each time when authentication is required to open a tunnel with a remote VPN gateway. If XAUTH authentication fails, the tunnel establishment fails too.

Note: In a multiple VPN tunnel configuration, the name of the VPN tunnel appears an the popup window.

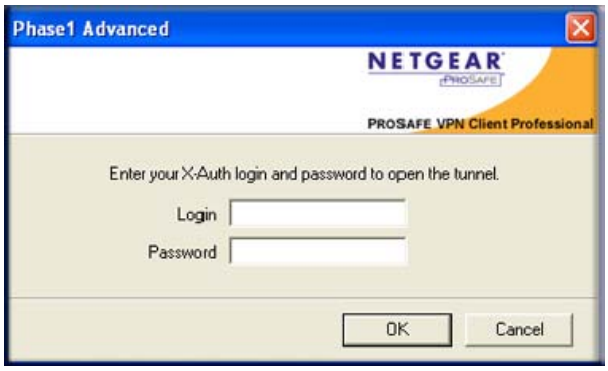


Figure 37.

The user has some times to enter the credentials. If the time allowed to enter XAUTH credentials expires, a window warning appears and the user has to reopen the VPN tunnel. The expiration time depends on the settings of the **X-Auth timeout** field on the Parameters window of the Connection Panel screen (see *Global Parameters* on page 56).

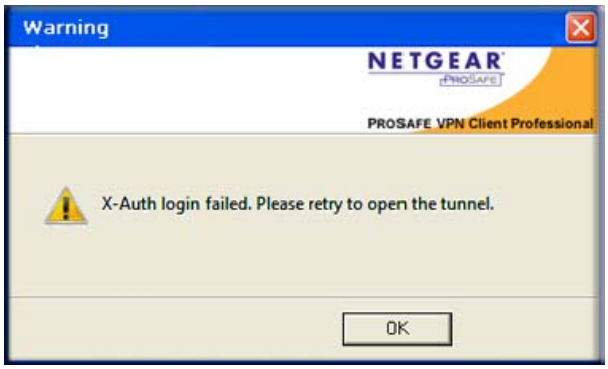


Figure 38.

The way that credentials are verified depends on the VPN gateway. When a VPN gateway detects an incorrect login name or password, one of the following actions can occur:

- The XAUTH window is displayed again.
- A popup warning similar to *Figure 39* alerts the user to try to open the VPN tunnel again.

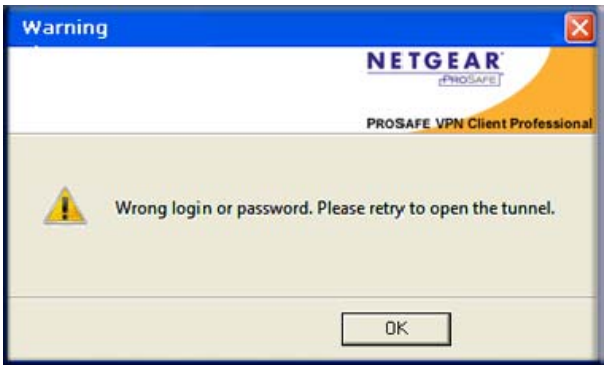


Figure 39.

Phase 2 or IPSec Configuration

The purpose of phase 2 is to negotiate the IPSec security settings that are applied to the traffic that goes through the tunnels.

Note: You can create several IPSec configurations for the same authentication phase (that is, phase 1).

Phase 2 (IPSec) Configuration

To configure a new phase 2 or edit an existing phase 2 configuration:

1. Take one of the following actions:
   - To create a new phase 2 configuration:
     a. Click on an existing phase 1 name in the tree list window of the Configuration Panel screen.
     b. Select **VPN Configuration** > **Add Phase 2** from the main menu.
   - To edit an existing phase 2 configuration, click on an existing phase 2 name in the tree list window of the Configuration Panel screen.

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

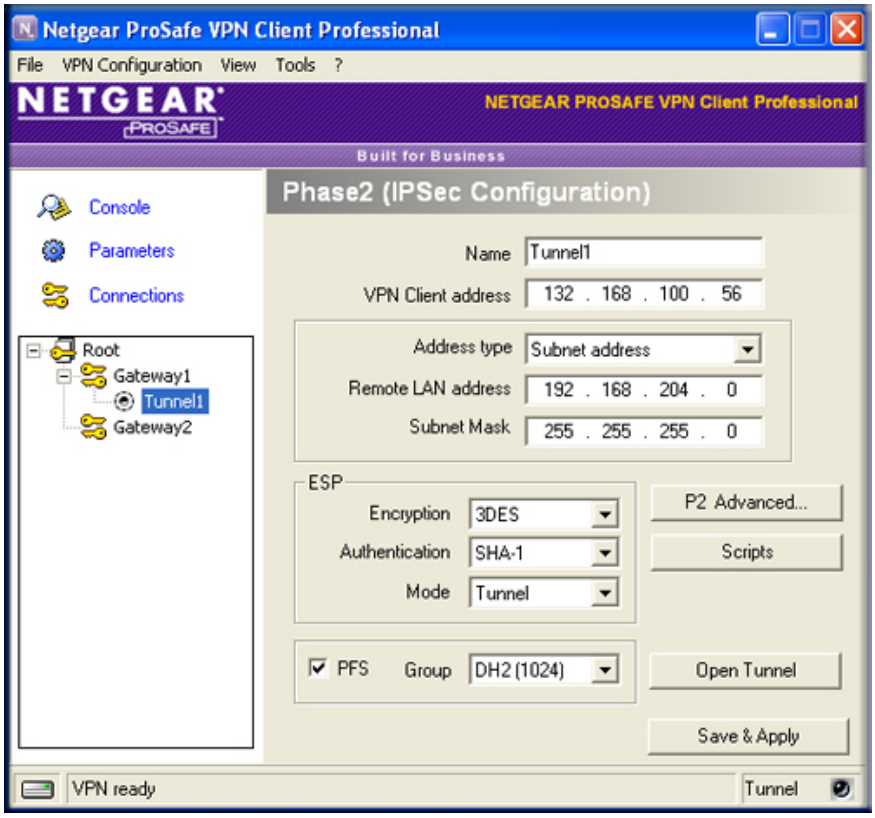


Figure 40.

2. Configure the settings as explained in the following table.

Table 8. Phase 2 IPSec Configuration Settings

Setting	Description
Name	The label for the IPSec configuration that is used only by the VPN Client, not during IPSec negotiation. You can view and change this name in the tree control window. This name must be a unique name.
VPN Client address	The virtual IP address that is used by the VPN Client in the remote LAN; the computer (for which the VPN Client opened a tunnel) appears in the LAN with this IP address. This IP address can belong to the remote LAN subnet. You might be able to forgo using an IP address and enter **0.0.0.0**. Both the local IP address of your computer and the remote LAN address can be part of the same subnet. To enable such a configuration, select the **Automatically open this tunnel on traffic detection** check box on the Phase 2 Advanced screen (see *Phase 2 (IPSec) Advanced Configuration* on page 53). When the VPN tunnel is opened in this configuration, all traffic with the remote LAN is allowed but communication with the local network becomes impossible.

Table 8. Phase 2 IPSec Configuration Settings (Continued)

<table>
<tr><th>Setting</th><th colspan="3">Description</th></tr>
<tr><td>Address type</td><td colspan="3">From the Address type drop-down list, select the remote endpoint's type of address that the VPN Client can communicate with after the VPN tunnel has been established. Depending on your selection, the screen adjusts to display the associated address fields:
• Single address. The remote endpoint is a single computer. Specify the Remote host address and Subnet Mask fields.
• Subnet address. The remote endpoint is a LAN. Specify the Remote LAN address and Subnet Mask fields.
• Range address. The remote endpoint is a LAN that consists of a range of addresses. Specify the Start address and End address fields.

Note: When you select Range address from the drop-down list and the Automatically open this tunnel on traffic detection check box on the Phase 2 Advanced screen (see Phase 2 (IPSec) Advanced Configuration on page 53), the tunnel automatically opens when traffic is detected for a specific range of IP addresses. However, this range of IP addresses must be specified in the configuration of VPN gateway.</td></tr>
<tr><td rowspan="6"></td><td rowspan="2">Single address</td><td>Remote host address</td><td rowspan="6">Enter the addresses.</td></tr>
<tr><td>Subnet Mask</td></tr>
<tr><td rowspan="2">Subnet address</td><td>Remote LAN address</td></tr>
<tr><td>Subnet Mask</td></tr>
<tr><td rowspan="2">Range address</td><td>Start address</td></tr>
<tr><td>End address</td></tr>
<tr><td>ESP</td><td>Encryption</td><td colspan="2">The encryption algorithm that is used during the IPSec configuration phase. Select one of the following from the drop-down list:
• DES.
• 3DES. This is the default setting.
• AES 128.
• AES 192.
• AES 256.</td></tr>
<tr><td></td><td>Authentication</td><td colspan="2">The authentication algorithm that is used during the IPSec configuration phase. Select one of the following from the drop-down list:
• MD5.
• SHA-1. This is the default setting</td></tr>
<tr><td></td><td>Mode</td><td colspan="2">IPSec encapsulation mode. Select one of the following from the drop-down list:
• Tunnel. The mode that is commonly used when either end of a security association (SA) is a security gateway or when both ends of an SA are security gateways that function as proxies for the hosts behind them. Tunnel mode encrypts both the payload and the entire header (UDP/TCP and IP). This is the default setting.
• Transport. The mode in which traffic is destined for a security gateway that functions as a host. (For example, you could use transport mode for SNMP commands.) Transport mode encrypts only the payload, not the IP header.</td></tr>
</table>

Table 8. Phase 2 IPSec Configuration Settings (Continued)

Setting	Description	
PFS	Select the **PFS** check box to specify a Perfect Forward Secrecy (PFS) key length that is used during the IPSec configuration phase. Then, specify a group. By default, the **PFS** check box is selected.	
	Group	Select one of the following from the drop-down list: • **DH1 (768)**. • **DH2 (1024)**. This is the default setting. • **DH5 (1536)**.

3. As an optional step, click **P2 Advanced ...**. to open the Phase 2 Advanced screen and configure the advanced settings (for more information, see the following section).
4. As an optional step, click **Scripts** to open the Script Configuration screen. For information, see *Phase 2 Script Configuration* on page 55.
5. Click **Save & Apply** to save and apply the new settings.
6. As an optional step, click **Open Tunnel** to open the (newly configured) tunnel. When the tunnel is opened, the button changes to **Close Tunnel**.

Phase 2 (IPSec) Advanced Configuration

Note: The advanced phase 2 settings apply only to the associated phase 2 (IPSec configuration) settings.

To configure phase 2 advanced settings:

1. Click **P2 Advanced ...** in the Phase 2 (Authentication) window of the Configuration Panel screen. The Phase 2 Advanced screen displays.

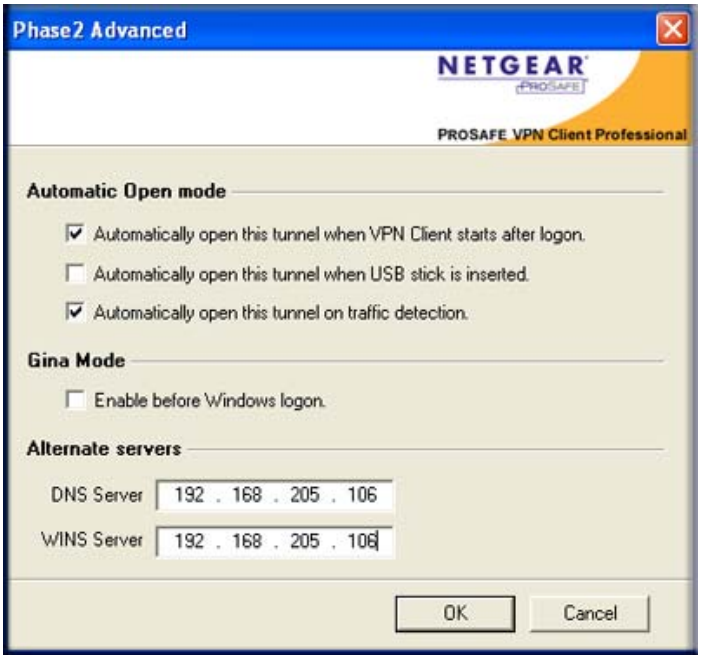


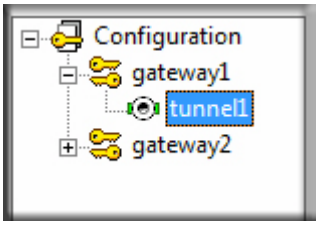
Figure 41.

2. Configure the settings as explained in the following table.

Figure 42. Phase 2 Advanced IPSec Configuration Settings

Settings	Description
Automatic Open mode **Note:** When you select any of these check boxes, the VPN Client automatically opens the tunnel to which these advanced setting apply.	
Automatically open this tunnel when the VPN Client starts after login	Select this check box to automatically open the tunnel when the VPN Client starts after you have logged in.
Automatically open this tunnel when USB stick is inserted	Select this check box to automatically open the tunnel when you insert an external USB drive in to the computer. (For more information, see *USB Mode* on page 59). **Note:** This check box is disabled before Windows logon.

Figure 42. Phase 2 Advanced IPSec Configuration Settings (Continued)

Settings	Description
Automatically open this tunnel on traffic detection	Select this check box to automatically open the tunnel when the VPN Client detects traffic. The phase 2 icon for the tunnel in the tree list window of the Configuration Panel screen changes its shape and color to reflect that this feature is now active. 
Gina Mode	
Enable before Windows logon	Select this check box to enable Gina mode, which is a mode that allows the tunnel to be used by Vista Credential Providers (also referred to as Gina mode on Windows 2000 and Windows XP) to process Windows logon. This mode can be useful when a corporate employee database is used for logon and the remote computer need to connect to the corporate network before processing the Windows logon. For more information, see *Open a VPN Tunnel Before Windows Logon* on page 34.
Alternate servers **Note:** When the Mode Config feature is enabled (see *Phase 1 (Authentication) Configuration* on page 43), you do not need to use a DNS or WINS server.	
DNS Server	Enter the IP address of the DNS server of the remote LAN. The DNS server is used to resolve Intranet addressing while the tunnel is open.
WINS Server	Enter the IP address of the WINS server of the remote LAN. The WINS server is used to resolve Intranet addressing while the tunnel is open.

3. Click **OK** to save the settings.

Phase 2 Script Configuration

This feature enables you to specify and execute scripts (including batches and applications) at each step of a tunnel connection for a variety of purposes; for example, to detect the current software release, to detect the database availability before launching a backup application, to configure the network, to detect whether or not a software application is running or a logon procedure is specified, and so on.

You can specify and execute several scripts for each step of a VPN tunnel opening and closing process:

- before tunnel is opened
- after the tunnel is opened
- before the tunnel closes
- after the tunnel is closed

To configure scripts:

1. Click **Scripts** in the Phase 2 (IPSec Configuration) window of the Configuration Panel screen. The Script Configuration screen displays.

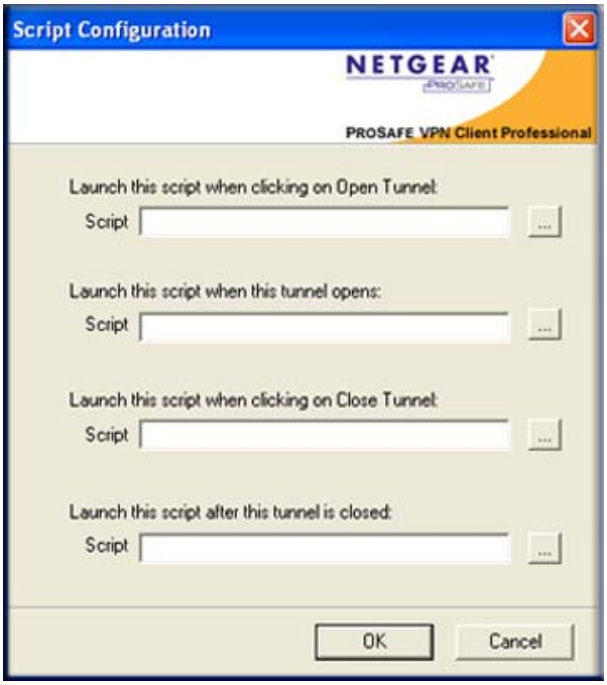


Figure 43.

2. Click **...** to navigate to a script file and open it. You can open up to four script files in the Script Configuration screen:
   - Launch this script when clicking on Open Tunnel.
   - Launch this script when this tunnel opens.
   - Launch this script when clicking on Close Tunnel.
   - Launch this script after this tunnel is closed.
3. Click **OK** to save the settings.

Global Parameters

Global parameters are generic settings that apply to all VPN tunnels that you create.

To configure global parameters:

1. Click **Parameters** in the left column of the Configuration Panel screen or select **VPN Configuration** > **Parameters** from the main menu. The Parameters window displays in the Configuration Panel screen.

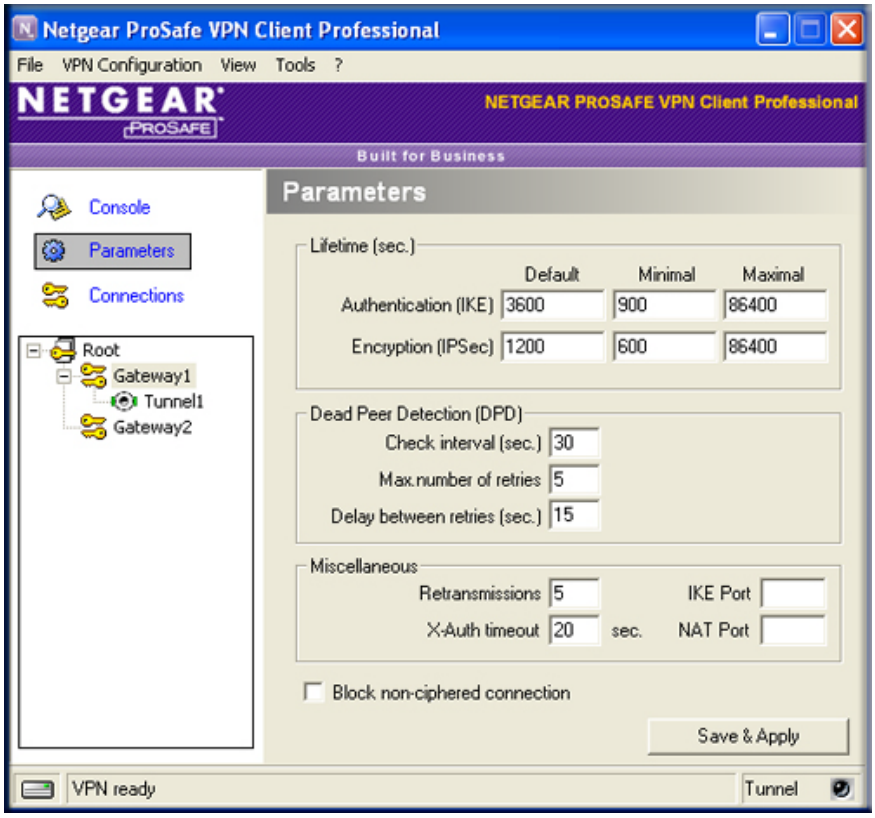


Figure 44.

2. Configure the settings as explained in the following table.

Table 9. Global Parameters

Setting		Description
Lifetime (sec.)		
Authentication (IKE)	Default	Enter the default lifetime for IKE rekeying. The default is 3600 sec.
	Minimal	Enter the minimum lifetime for IKE rekeying. The default is 900 sec.
	Maximal	Enter the maximum lifetime for IKE rekeying. The default is 86400 sec.
Encryption (IPSec)	Default	Enter the default lifetime for IPSec rekeying. The default is 1200 sec.
	Minimal	Enter the maximum lifetime for IPSec rekeying. The default is 600 sec.
	Maximal	Enter the minimum lifetime for IPSec rekeying. The default is 86400 sec.
Dead Peer Detection (DPD) DPD is an Internet Key Exchange (IKE) extension (RFC3706) for detecting a dead IKE peer. The IPSec VPN Client uses DPD under the following circumstances: • to detect a dead peer and to delete the associated open SA in the VPN Client. • to restart IKE negotiations with an alternate gateway, if you have configured one (see *Phase 2 (IPSec) Advanced Configuration* on page 53).		

Table 9. Global Parameters (Continued)

Setting	Description
Check interval (sec.)	Enter the interval between DPD messages. The default is 30 sec.
Max.number of retries	Enter the number of times that DPD messages are sent when no reply is received from the peer. The default number is 5 times.
Delay between retries (sec.)	Enter the interval between DPD messages when no reply is received from the peer. The default is 15 sec.
Miscellaneous	
Retransmissions	Enter the number of times that a message should be retransmitted before the attempts are stopped. The default number is 5 times.
X-Auth timeout	Enter the time that is allowed to a user to enter their XAUTH credentials. The default is 20 sec.
IKE Port	Enter the default UDP port that is used during phase 1 IKE negotiation. The default port is 500 (which is not displayed in the **IKE Port** field). **Note:** Some firewalls do not allow IKE port 500 or outgoing traffic on port 500 might not be allowed. If you change the IKE port number, the remote gateway must be able to reroute the incoming traffic that is associated with a port other than IKE port 500.
NAT Port	Enter the default NAT port that is used during phase 2 IPSec negotiation. The default port is 4500 (which is not displayed in the **NAT Port** field). **Note:** Some firewalls do not allow NAT port 4500 or outgoing traffic on port 4500 might not be allowed. If you change the NAT port number, the remote gateway must be able to reroute the incoming traffic that is associated with a port other than NAT port 4500.
Block non-ciphered connection	Select this check box to limit traffic to encrypted traffic and forcing all traffic to go through the VPN tunnel.

3. Click **Save & Apply** to save and apply the new settings.

VPN Tunnel View

The Tunnel View screen displays all VPN tunnels that are open and lets you close open tunnels.

To display the Tunnel View window in the Configuration Panel screen and close a tunnel:

1. Click **Connections** in the left column of the Configuration Panel screen.

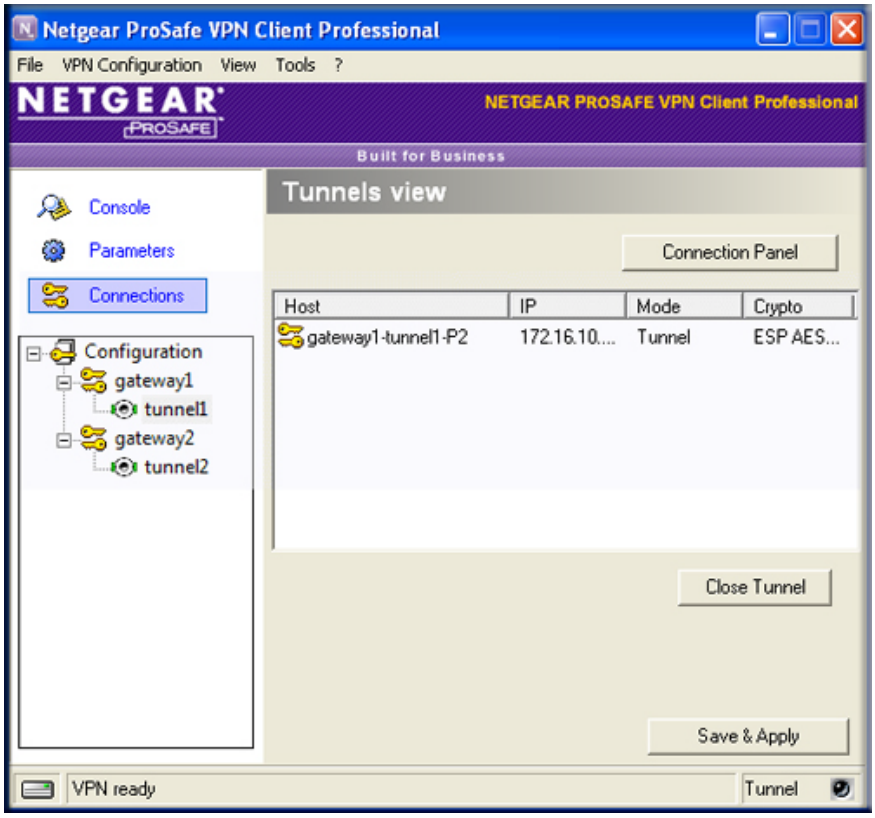


Figure 45.

2. Select a tunnel from the list.
3. Click **Close Tunnel**.
4. Click **Save & Apply** to save and apply the new settings.

You can also view, open, and close tunnels by clicking **Connection Panel** and opening the Connection Panel screen, or by right-clicking on the system tray icon and making a menu selection.

USB Mode

The VPN Client lets you save VPN configurations and VPN security elements such as preshared keys and certificates onto a USB drive to allow you to do the following:

- Limit a VPN configuration to a specific computer. VPN tunnels that are defined in the VPN configuration can be used only on a specific computer.
- Limit a VPN configuration to a specific USB drive. VPN tunnels that are defined in the VPN configuration can be used only with a specific USB drive.

After you have moved a VPN configuration and its security elements onto a USB drive and removed the USB drive, you then just need to insert the USB drive into a computer to automatically open the tunnels. When you remove the USB drive from the computer, all open tunnels are automatically closed.

Enable a New USB Drive with a VPN Configuration

You can enable a new USB drive by copying a VPN configuration and its security elements onto it in one of the following ways:

- Select **File** > **Export VPN Configuration** from the main menu of the Configuration Panel screen, and then copy the VPN configuration file onto the USB drive
- Use the USB mode wizard

To start the USB mode wizard and copy VPN configuration onto a USB drive:

1. Select **File** > **Move VPN Configuration to USB Drive** from the main menu of the Configuration Panel screen. The USB Mode Wizard 1/4 screen displays.

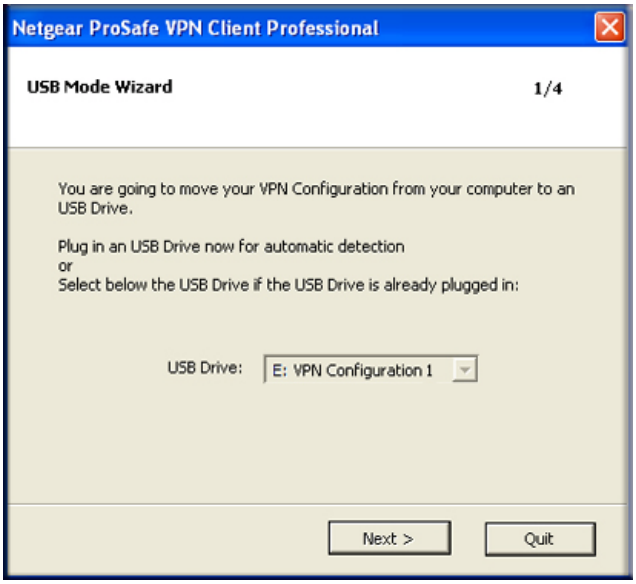


Figure 46.

If one or more USB drives are already inserted, the VPN Client detects and displays them, as shown in *Figure 46* in which a single drive is displayed.

Note: If you insert a USB drive with a VPN configuration while the USB Mode Wizard 1/4 screen is displayed, and the VPN Client detects that the USB drive is the only one in the computer, the VPN Client automatically displays the next screen, USB Mode Wizard 2/4.

Note: If you insert a USB drive with a VPN configuration while another USB drive with another VPN configuration is already inserted, a warning message asks you to remove one of the USB drives.

2. Click **Next**. The USB Mode Wizard 2/4 screen displays.

Figure 47.

3. Select one of the following security options:
   - **With this computer only**. The VPN tunnels that are defined in the VPN configuration can be used only on this specific computer.
   - **On any computer**. The VPN tunnels that are defined in the VPN configuration can be used with this USB drive only, but on any computer.
4. As an optional step, protect the VPN configuration with a password that you must enter in the **Password field**. Select the **Hide password** check box to make the passport invisible.

> **Note:** At this step in the wizard, if you remove the USB drive, the wizard automatically returns to the USB Mode Wizard 1/4 screen.

5. Click **Next**. The USB Mode Wizard 3/4 screen displays.

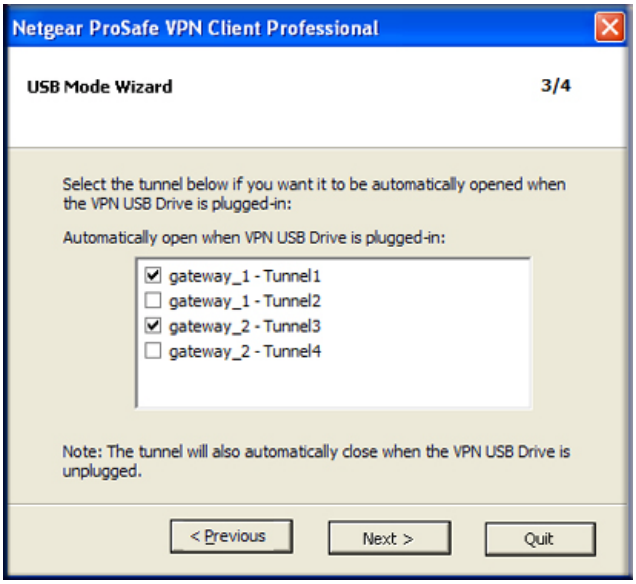


Figure 48.

6. Specify the tunnels that you want to be opened automatically by selecting the associated check boxes.

Note: If there is only one tunnel configured, it is sufficient to select the **Automatically open this tunnel when USB stick is inserted** check box on the Phase 2 Advanced screen for the tunnel to be opened (see *Phase 2 (IPSec) Advanced Configuration* on page 53). If there is more than one tunnel configured, you must select on the USB Mode Wizard 3/4 screen which tunnel or tunnels should be opened.

7. Click **Next**. USB Mode Wizard 4/4 screen displays. This screen is a summary screen.

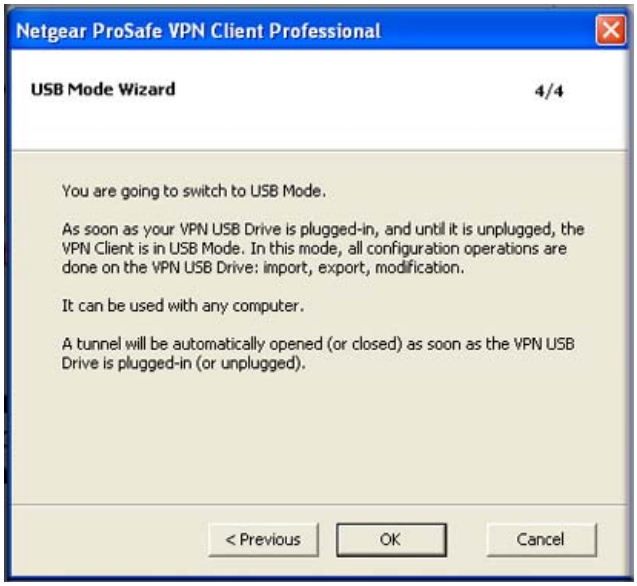


Figure 49.

8. Click **OK** to save the settings. The VPN configuration and its associated security information is now removed from the computer and copied onto the USB drive; the VPN Client is now functioning in USB mode.

Note: When you remove the USB drive from the computer, the VPN configuration is reset, that is, an empty configuration displays in the Configuration Panel screen. The next time that the VPN Client starts without the USB drive that contains the VPN configuration inserted, the VPN configuration is not present in the VPN Client.

Note: The VPN Client does not let you change the password or computer association that is on the USB drive. However, you can export the VPN configuration to a local disk, remove the USB drive, import the VPN configuration in the VPN Client, and start the USB mode wizard again to specify a new password or a new association with a computer. For information about importing and exporting, see *Import or Export a VPN Configuration* on page 73.

Automatic Opening of Tunnels

The following is required for a tunnel to be opened automatically:

1. If there is only one tunnel configured, select the **Automatically open this tunnel when USB stick is inserted** check box on the Phase 2 Advanced screen for the tunnel to be opened (see *Phase 2 (IPSec) Advanced Configuration* on page 53).
2. If there is more than one tunnel configured, you must select on the USB Mode Wizard 3/4 screen which tunnel or tunnels should be opened (see *USB Mode* on page 59).
3. A USB drive that contains a VPN configuration must be inserted.

If a USB drive without a VPN configuration is inserted, or if no USB drive is inserted, the VPN Client starts in local mode and uses a VPN configuration that is available on the local disk.

Certificate Management

The VPN Client can use certificates from various sources:

- PEM format files
- PKCS#12 format file
- Microsoft Certificate Store
- USB token or SmartCard

The Certificate screen displays these certificate sources and lets you select a certificate for a particular tunnel. One certificate is bound to one tunnel. You can easily export the configuration to another computer.

Certificates can be stored on a USB token or SmartCard for which access is protected by a PIN code; the VPN Client uses these certificates dynamically while establishing a tunnel.

The VPN Client does not create certificates. You can create certificates by using third-party software such as Microsoft Certificates Server or OpenSSL (see *Appendix B, Generating Certificates With Microsoft Certificates Services and OpenSSL*) or purchase certificates from the Microsoft Certificate Store. You can store certificates on USB tokens and SmartCards.

Assign Certificates

To assign a certificate to a tunnel:

1. Click on an existing phase 1 name in the tree list window of the Configuration Panel screen. The Phase 1 (Authentication) window displays in the Configuration Panel screen.
2. Select the **Certificate** radio button, and then click **Certificate Management**. The Certificate for Phase 1: [*tunnel name*] screen displays.

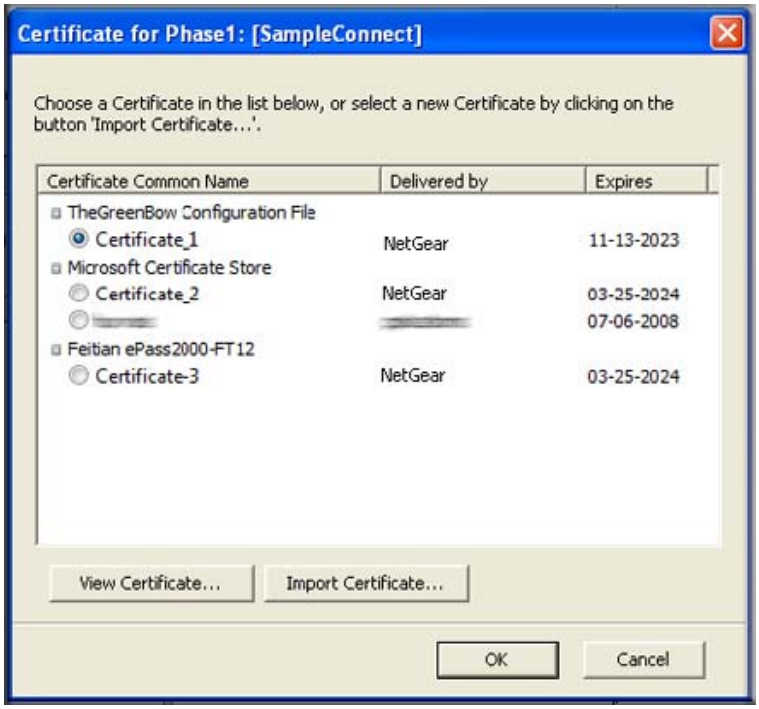


Figure 50.

Figure 50 shows several sources that you can select certificates from. These sources are explained in the following table.

Table 10. Sources of Certificates

Source	Description
NETGEAR Configuration File	Certificates are located in the VPN configuration file that is used by the VPN Client. These certificates have been imported previously from another source such as a certificate file or the Microsoft Certificate Store.
Microsoft Certificate Store	Certificates are located in the Microsoft Certificate Store. To be visible and usable, certificates must be certified and in the correct location: • Certificates must be certified by a certificate authority (CA) and the certificate status must be *Ok* (see also *Certificate Troubleshooting* on page 72). • Certificates must be located in the Personal Certificate Store to represent the personal identity of the user attempting to connect to a corporate network.
USB token or SmartCard (such as Feitian ePass2000-FT21)	Certificates are located on one ore more USB tokens and SmartCards that are inserted in the computer and are therefore displayed on the Certificates screen.

Note: To import a certificate, see *Import Certificates* on page 67.

3. Select one certificate from the list by selecting its associated radio button. You can select and assign only one certificate to a tunnel.
4. Click **OK** to save the settings.

View Certificate Details

To view the details of a certificate:

1. Click on an existing phase 1 name in the tree list window of the Configuration Panel screen. The Phase 1 (Authentication) window displays in the Configuration Panel screen.
2. Select the **Certificate** radio button, and then click **Certificate Management**. The Certificate for Phase 1: [*tunnel name*] screen displays.
3. Select a certificate from the certificate list.
4. Click **View Certificate**. The Certificate (details) screen displays (this might take up to 30 seconds).

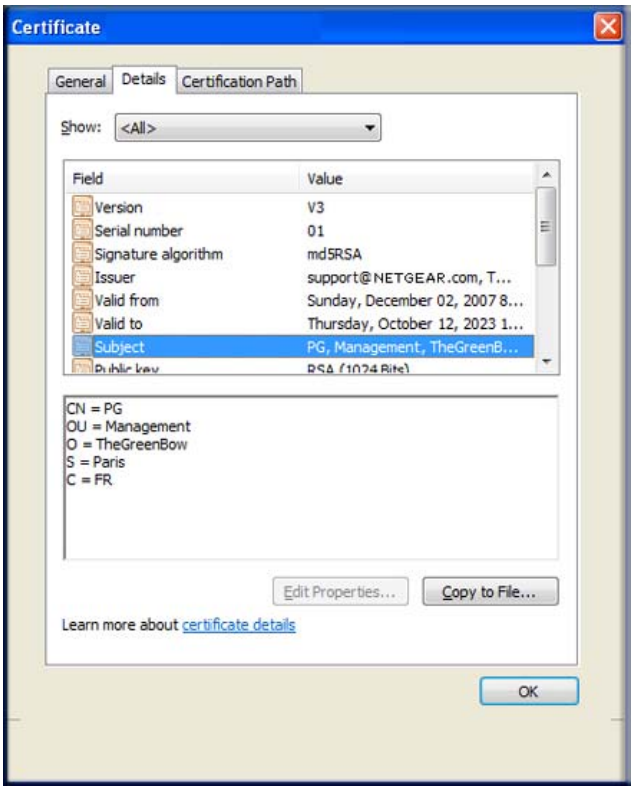


Figure 51.

You can display the details of a certificate properties by clicking on fields such as **Issuer**, **Valid from**, **Valid to**, **Subject**, and so on.

5. As an optional step, click **Copy to File** to open the Certificate Export Wizard that enables you to export the certificate to a file.
6. Click **OK** to close the Certificate (details) screen.

Import Certificates

You can import several certificates and assign each certificate to a different tunnel to enable the VPN Client to connect to various gateways that are part of different a Public Key Infrastructure (PKI).

You import and specify one PEM format and one P12 format per tunnel.

Note: After you have imported a PEM or P12 certificate, the **Local ID** fields of the associated Phase 1 Advanced screen are automatically set: the left field is set to **Subject from X509** and the right field contains values from the certificate. For more information, see *Phase 1 (Authentication) Advanced Configuration* on page 45.

PEM Certificates

To import a PEM certificate in a tunnel configuration:

1. Click on an existing phase 1 name in the tree list window of the Configuration Panel screen. The Phase 1 (Authentication) window displays in the Configuration Panel screen.
2. Select the **Certificate** radio button, and then click **Certificate Management**. The Certificate for Phase 1: [*tunnel name*] screen displays.
3. Click **Import Certificate**. The Import Certificate screen displays.

Figure 52.

4. Select the **PEM Format** radio button.
5. Click **Next**. The (PEM) Import Certificate screen displays.

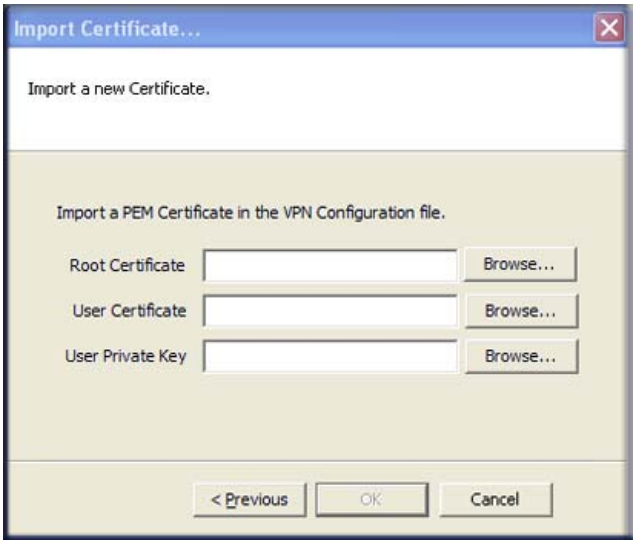


Figure 53.

6. Import the three PEM certificate files:
   - Next to the **Root Certificate** field, click **Browse**. Locate the root certificate file that you want to import. This file has either a .pem or a .crt extension.
   - Next to the **User Certificate** field, click **Browse**. Locate the user certificate file that you want to import. This file has either a .pem or a .crt extension.
   - Next to the **User Private Key** field, click **Browse**. Locate the user private key file that you want to import. This file has a .key extension.

> **Note:** A PEM certificate file that includes a user private key must not be encrypted or protected with a password.

7. Click **OK** to import the certificate. The Certificate for Phase 1: [*tunnel name*] screen now displays the imported certificate (see *Figure 50* on page 65).
8. Click **OK** to close the Certificate for Phase 1: [*tunnel name*] screen.

P12 Certificates

To import a P12 certificate in a tunnel configuration:

1. Click on an existing phase 1 name in the tree list window of the Configuration Panel screen. The Phase 1 (Authentication) window displays in the Configuration Panel screen.
2. Select the **Certificate** radio button, and then click **Certificate Management**. The Certificate for Phase 1: [*tunnel name*] screen displays.
3. Click **Import Certificate**. The Import Certificate screen displays.

Figure 54.

4. Select the **P12 Format** radio button.
5. Click **Next**. The (P12) Import Certificate screen displays.

Figure 55.

6. Click **Browse**, and then locate and open the certificate file that you want to import. This file can have either a .p12 or a .pfx extension.
7. Click **OK** to import the certificate. The PKCS12 password file screen displays.

Figure 56.

8. Enter the password, and click **OK**. The Certificate for Phase 1: [*tunnel name*] screen now displays the imported certificate (see *Figure 50* on page 65).
9. Click **OK** to close the Certificate for Phase 1: [*tunnel name*] screen.

Use Certificates From USB Tokens and SmartCards

The VPN Client can read certificates from USB tokens and Smart Cards. Smart Cards can contain X509 certificates that can be protected by a PIN code.

To configure a tunnel with a certificate from a USB token or SmartCard:

1. Insert a USB token or SmartCard in the computer.
2. If requested as part of USB token or SmartCard reader identification process, enter the PIN code and click **OK**.
3. Click on an existing phase 1 name in the tree list window of the Configuration Panel screen. The Phase 1 (Authentication) window displays in the Configuration Panel screen.
4. Select the **Certificate** radio button, and then click **Certificate Management**. The Certificate for Phase 1: [*tunnel name*] screen displays.

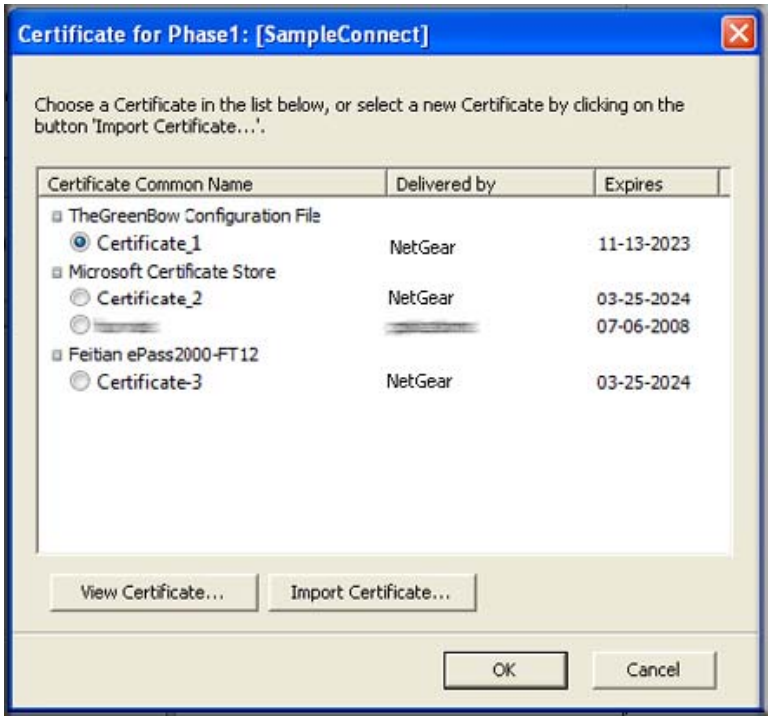


Figure 57.

The certificates from the USB token or SmartCard have been automatically imported and display in the certificates list.

5. Select a certificate by selecting its radio button.
6. Click **OK** to close the Certificate for Phase 1: [*tunnel name*] screen.

Open a Tunnel with Certificates From a USB Token or SmartCard

When you have configured a tunnel to use a certificate from a USB token or SmartCard, you must enter the PIN code that is associated with the USB token or SmartCard each time that the tunnel is opened (except for automatic VPN renegotiations).

To open a tunnel with a certificates from a USB token or SmartCard:

1. Ensure that either the SmartCard reader is inserted in the computer and contains a SmartCard or the USB token is inserted in the computer.
2. Enter the PIN code that is associated with the USB token or SmartCard
3. Right-click the system tray icon, and click **Open tunnel *<tunnel name>***.

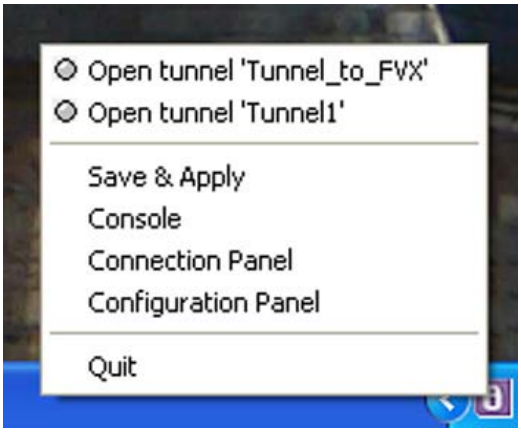


Figure 58.

Certificate Troubleshooting

Troubleshooting USB Tokens and SmartCards

When an error occurs while you use a USB token or SmartCard, a small warning icon appears next to the token name. Click on this warning icon to open a popup window that provides more information about the error. One of the following errors might occur:

- **Error**: Token not found: previously plugged in but not at this time.

  Resolution: Reinsert the USB token or SmartCard.

- **Error**: Token found but no middleware to access it (often required when using SmartCard readers).

  Resolution: Install the software (middleware) that enables your computer to read the SmartCard, and restart the computer.

- **Error**: Token and store found but no certificate found.

  Resolution: Ensure that the certificate is located in the Personal Certificate Store to represent the personal identity of the user.

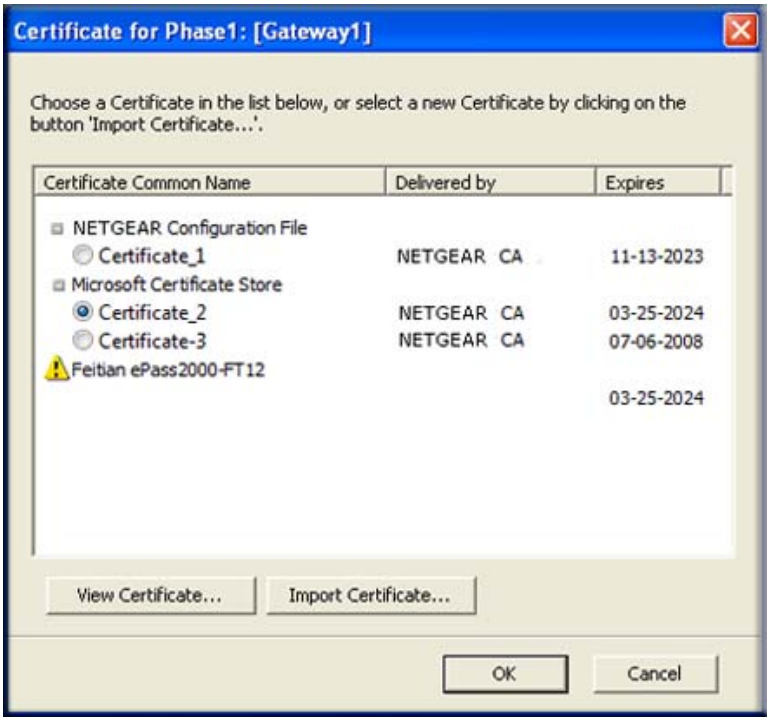


Figure 59.

Troubleshooting the Microsoft Certificate Store

To prevent error, ensure the following:

- Certificates must be certified by a certificate authority (CA) and the certificate status must be *Ok*.
- Certificates must be located in the Personal Certificate Store to represent the personal identity of the user.

Windows provides a Certificate Management tool you can use to troubleshot certificate issues. To open this tool, select **Start** > **Run** > **certmgr.msc**.

VPN Configuration Management

Import or Export a VPN Configuration

The VPN Client can import or export a VPN configuration. This capability would be typically used by an administrator to prepare a configuration and deliver it to other users.

To import a VPN configuration:

1. Select **File** > **Import VPN Configuration** from the main menu on the Configuration Panel screen.

2. Navigate to the location of the VPN configuration file that you want to import, and click **Open**. An Information screens displays.

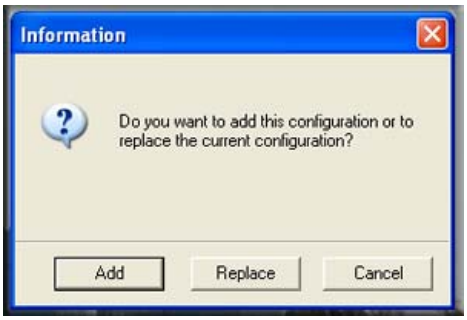


Figure 60.

3. Select one of the following buttons:
   - **Add**. Adds the imported VPN configuration to the existing VPN configuration.
   - **Replace**. Replaces the existing VPN configuration with the imported VPN configuration.

   The imported VPN configuration displays in the tree list window of the Configuration Panel screen.

Note: When you import a VPN configuration while the VPN Client is functioning in USB mode with a USB drive inserted in the computer, the file is automatically saved on the USB drive. If the VPN Client is functioning in USB mode but no USB drive is inserted in the computer, you cannot import or export a VPN configuration.

Note: To use the command-line interface (CLI) to import a VPN configuration file, see the following section and *Import, Export, Add, or Replace the VPN Configuration* on page 86.

To export a VPN configuration:

1. Select **File** > **Export VPN Configuration** from the main menu on the Configuration Panel screen. The Export Protection screen displays.

Figure 61.

As a security measure, you have the option to specify a password for the exported file.

2. Select one of the following radio buttons:
   - **Don’t protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. Enter a password in the field. The VPN configuration file can be opened with this password.
3. Click **OK**.
4. Navigate to the location where you want to save the VPN configuration file, and click **Save**. An exported VPN configuration file has a .tgb extension.

You can now forward the VPN configuration or double-click on the VPN configuration shortcut icon to start the VPN Client.

Note: When you export a phase 2 configuration, the associated phase 1 configuration is also exported, including certificates that might have been defined in the phase 1 configuration, and global parameters.

Merge VPN Configurations

You can import one or several tunnels into an existing VPN configuration. This capability would be typically used by an administrator to merge a new VPN configuration with new gateways into an existing VPN configuration and deliver it to other users.

You can merge VPN configurations in several ways:

- Select **File** > **Import VPN Configuration** from the main menu on the Configuration Panel screen, and then select **Add** instead of **Replace**, as explained in the previous section (see *To import a VPN configuration:* on page 73).
- Drag and drop a new VPN configuration onto the tree list window software of the Configuration Panel screen, and then select **Add** instead of **Replace**.
- Import new VPN Configuration via the CLI by entering **`[path]\vpnconf.exe /add:[file.tgb]`**, in which `[path]` is the VPN Client installation directory, and `[file.tgb]` is the VPN configuration file. This command does not process relative paths such as `..\..\file.tgb`. For more information, see *Import, Export, Add, or Replace the VPN Configuration* on page 86.

Irrespective of the way that you import a VPN configuration, the following rules apply:

- Global parameters are *not* imported if at least one tunnel is already configured before you import and add the VPN configuration.
- Global parameters *are* imported if you import and replace the VPN configuration, or if no tunnel is configured when you import and add the VPN configuration.
- A tunnel name conflict between an existing and an imported VPN configuration is automatically resolved by adding an increment between brackets—for example, tunnel_office(1)—to the imported tunnel name.

Split a VPN Configuration

You can export a single tunnel from an existing VPN configuration. This capability would be typically used by an administrator to split an existing large VPN configuration into a smaller VPN configuration and deliver it to other users.

To export a single tunnel:

1. In the tree list window of the Configuration Panel screen, right-click on a tunnel that is part of a phase 2 configuration, and select **Export Tunnel**.

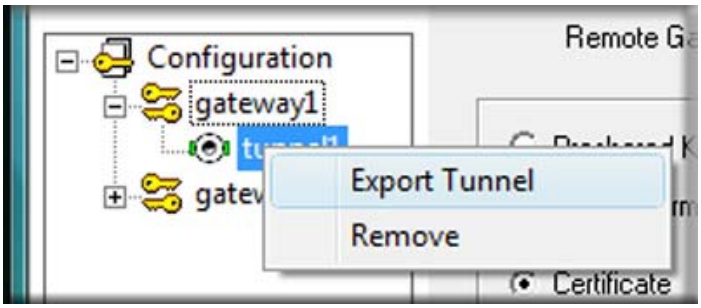


Figure 62.

The Export Protection screen displays.

Figure 63.

As a security measure, you have the option to specify a password for the exported file.

2. Select one of the following radio buttons:
   - **Don't protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. Enter a password in the field. The VPN configuration file can be opened with this password.
3. Click **OK** to save the settings.
4. Navigate to the location where you want to save the VPN configuration file, and click **Save**. An exported VPN configuration file has a .tgb extension.

You can now forward the VPN configuration or double-click on the VPN configuration shortcut icon to start the VPN Client.

Note: When you export a phase 2 configuration, the associated phase 1 configuration is also exported, including certificates that might have been defined in the phase 1 configuration, and global parameters.

Embed Your Own VPN Configuration in a VPN Client Software Setup

You can include a preconfigured VPN configuration in the VPN Client software setup. This capability would be typically used by an administrator to deploy a preconfigured VPN Client in

a single package to other users. For information, see *Embedded VPN Configuration* on page 79.

Demo VPN Configuration

The VPN Client software setup embeds a demo VPN configuration. This demo VPN configuration enables you to open a tunnel to a demo server after the VPN Client is installed.

Using the demo VPN configuration and demo server, you can check for testing and debugging purposes if a tunnel can be opened from your computer to an operational remote network. You can also find this demo VPN configuration at *http://www.thegreenbow.fr/doc/tgbvpn_demo.tgb*.

VPN Client Software Setup and Deployment

7

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

Note: The information in this chapter is typically used by network administrators.

Note: Enter software setup commands and command-line interface (CLI commands in a command window.

Note: For more information about software setup and the CLI, see *Appendix A, VPN Client Software Setup Deployment and Command-Line Interface Guide*.

Embedded VPN Configuration

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

To create a VPN Client software setup with a VPN configuration:

1. Create the VPN configuration that you want to embed in the software setup. You do this by exporting the VPN configuration (that is, a .tgb file) from a formerly installed VPN Client and by importing the VPN configuration into the software setup.
2. Create a silent software setup (see *Create a Silent VPN Client Software Setup* on page 122) or unzip the VPN Client software setup file (NETGEARVPNClientPro_Setup.exe).
3. Add the VPN configuration file (that is, the .tgb file) to the unzipped setup directory.
4. Deploy the package to the user. The VPN configuration will be used during the software setup.

Note: The software setup cannot import and process an encrypted (protected) VPN configuration. When you create your VPN configuration, make sure that it is exported without being encrypted or without being protected with a password.

VPN Client Software Setup Commands

Several commands are available for the VPN Client software setup. These commands are described in the following sections:

- *Software Setup for GUI Mode* on page 81
- *Software Setup for GUI Mode With Access Control* on page 81
- *Software Setup for System Tray Menu Items* on page 82
- *Other Software Setup Options* on page 83

The following is a syntax example of a software setup:

```
NETGEARVPNClientPro_Setup.exe /S --license=0123456789ABCDEF0123 --activmail=
smith@smith.com
```

Note that you can use the following software setup commands only when the `/S` switch (silent mode installation, case-sensitive) is active:

```
--guidefs
--menuitem
--license|
--start
--activmail
--password
--autoactiv
--noactiv
--lang
```

Software Setup for GUI Mode

Enter the **`--guidefs=full`**, **`--guidefs=user`**, or **`--guidefs=hidden`** software setup command to define the user interface appearance when the VPN Client starts. These are the options:

- **`full`**. The Configuration Panel screen is displayed. This is the default setting.
- **`user`**. The Connection Panel screen is displayed.
- **`hidden`**. Neither the Configuration Panel screen nor the Connection Panel screen are displayed. Only the system tray menu can be opened. Tunnels can be opened from the system tray menu.

The following figure shows the system tray menu after you have entered the **`--guidefs=hidden`** software setup command.

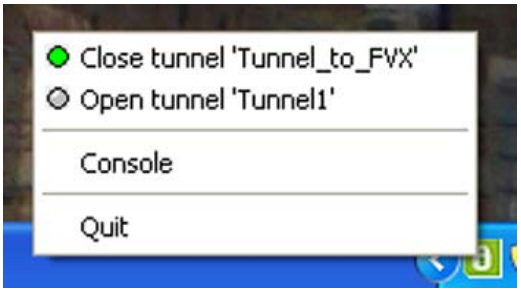


Figure 64.

Software Setup for GUI Mode With Access Control

Enter the **`--password=[password]`** software setup command to enable to control access to the Configuration Panel screen with a password.

`[password]` is the specified password.

For more information, see *Access Control and Hidden Interface* on page 26.

After implementation, you are asked for the password under the following circumstances:

- when you click or double-click on the VPN system tray icon
- when you want to switch from the Connection Panel screen to the Configuration Panel screen

Figure 65.

The following is a syntax example of this software setup:

```
--guidefs=user --password=admin01
```

This example locks the VPN Client in the Connection Panel screen, while access to the Configuration Panel screen is protected with a password.

Software Setup for System Tray Menu Items

Enter the **`--menuitem=[0...31]`** software setup command to specify the items of the system tray menu that you want to keep visible.

The value is a bit field:

1. Quit menu item displays.

2. Connection Panel menu item displays.

4. Console menu item displays.

5. Quit and Console menu items display.

8. Save & Apply menu item displays.

16. Configuration Panel menu item displays.

31. All menus display. This is the default setting.

The following is a syntax example of this software setup:

```
--menuitem=5
```

This example configures a system tray menu with the Quit and Console menu items.

> **Note:** Tunnels are always shown in the system tray menu and can always be opened and closed from the system tray menu.

Note: By default, --guidefs=hidden sets the system tray menu item list to Quit and Console (that is, the Save & Apply and Connection Panel menu items are not visible). However, --menuitem overrides --guidefs. That means that when you enter **--guidefs=hidden --menuitem=1**, the system tray menu shows the Quit menu item only.

Other Software Setup Options

Note: For more information about software setup commands , see *Software Setup Command Reference* on page 129.

You can enter the following commands in the software setup:

- **/S** to enable a silent installation (no dialogs are displayed during the installation). S must be preceded by only one slash and is case-sensitive. The following is an example:

  ```
  NETGEARVPNClientPro_Setup.exe /S
  ```

- **/D=[install path]** in which [install path] is the path where the VPN Client must be installed. D must be preceded by only one slash and is case-sensitive. Quotation marks are not allowed, even if there is a space in the path. You must place this option at the end of the command line, as the last option, and you muse it with the /S option (silent mode).
- **--license=[license_number]** to configure and automatically enter the license number, which consists of 20 or 24 hexadecimal characters.
- **--start=[1|2]** to configure the start mode for the VPN Client. These are the options:
  - **1**. The VPN Client starts after Windows login. This is the default setting.
  - **2**. The VPN Client must be started manually.
- **--activmail=[activation_email]** to configure and automatically enter the email that is used for activation confirmation. During the activation process, the field that is used to enter the email is disabled.
- **--autoactiv=1** to activate the VPN Client automatically when the network is available during startup or when there is a request to open a tunnel. This option requires that the license number and activation email have already been entered in a previous installation.
- **--noactiv=1** to prevent the Trial screen from displaying when the VPN Client starts until the trial period ends. A user other than the administrator does not know about the trial period and the VPN Client is disabled at the end of the trial period. If a user attempts to launch the VPN Client after the end of trial period, the VPN Client starts and opens the Trial screen but the **Evaluate** button is disabled.

- **`--lang=[language code]`** to specify the language for the software setup and for the VPN Client. The available languages are shown in the following table.

Table 11. Available Languages

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

The following is an example of a software setup that includes several options that are described in this section:

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

Command-Line Interface Commands

> **Note:** For more information about command-line interface (CLI) commands, see *Command-Line Interface Command Reference* on page 133.

Several CLI commands are available to administrators to adapt the VPN Client behavior to a specific environment and help integrate the VPN Client with other applications.

Open or Close VPN Tunnels

You can open or close a VPN tunnel through a CLI command, also when the VPN Client is running.

- To open a VPN tunnel, enter the following CLI command:

  `[path]\vpnconf.exe /open:[NamePhase1-NamePhase2]` in which `[path]` is the VPN Client installation directory, and `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

  If the specified tunnel is already open, the CLI command has no effect.

- To close a VPN tunnel, enter the following CLI command:

  `[path]\vpnconf.exe /close:[NamePhase1-NamePhase2]` in which `[path]` is the VPN Client installation directory, and `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

  If the specified tunnel is already closed, the CLI command has no effect.

The `open` and `close` commands are mutually exclusive.

> **Note:** When you enter the `open` or `close` command, the user interface opens. This restriction will be removed in a future software release.

Stop the VPN Client

To stop the VPN Client, enter the following CLI command:

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

This CLI command closes all active tunnels.

Use this CLI command, for example, in a script that starts the VPN Client after establishing a dial-up connection and closes it just before disconnecting the dial-up connection.

Import, Export, Add, or Replace the VPN Configuration

To enable the VPN Client to import a specific configuration file, enter the following CLI command:

`[path]\vpnconf.exe /import:[ConfigFileName]` in which `[path]` is the VPN Client installation directory, and `[ConfigFileName]` is the VPN configuration file that has a .tgb extension. This CLI command does not handle relative paths such as `"..\..\file.tgb"`. Use double-quotes to specify paths that contain spaces.

You can enter **`/import:`** whether or not the VPN Client is running. If the VPN Client is already running, it dynamically imports the new configuration and automatically applies it (that is, it restarts the IKE service). If the VPN Client is not running, it is starts with the new configuration.

Instead of entering **`/import:`**, you can also enter one of the following commands to export, add, or replace a specific configuration file:

- **`/importonce:`** to import a VPN configuration file when the VPN Client is not running. This command is useful in installation scripts: it allows you to run a silent installation and to automatically import a VPN configuration file.
- **`/export:`** to export the current VPN configuration (including certificates) to the specified file and to start the VPN Client if it is not already running. This command also requires a password (for information, see the paragraph following this list).
- **`/exportonce:`** to export the current VPN configuration (including certificates) to the specified file. This command does not start the VPN Client if it is not running. This command also requires a password (for information, see the paragraph following this list).
- **`/add:`** to import a new VPN configuration into an existing VPN configuration and merge both into a single VPN configuration, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running. You can use this command instead of the `/importonce:` command to import a VPN configuration file when the VPN Client is not running.
- **`/replace:`** to replace the current configuration with a new VPN configuration, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running . You can use this command instead of the `/importonce:` command to import a VPN configuration file when the VPN Client is not running.

All six commands, `/import:`, `/importonce:`, `/export:`, `/exportonce:`, `/add:`, and `/replace:` are mutually exclusive.

In addition, in combination with any of these commands, you can set a password by entering the **`/pwd:[password]`** CLI command, placing it after the other command. The `/export:` and `/exportonce:` commands require a password.

Support for ATR Code (SmartCard)

Each new software release of the VPN Client includes the latest list of Answer to Reset (ATR) code that are available from token and SmardCard vendors. Because new ATR code appear every day, you have the option to manually add one or more new ATR codes to the VPN Client without waiting for a new software release.

Include the ATR code in an initialization file that you must name vpnconf.ini. This file must be a text file and must be placed in the same installation folder as the tgbike.exe file.

The syntax for the vpnconf.ini file is as follows:

```
[3B:65:00:00:9C:02:02:07:02]
mask="FF:FF:00:00:FF:FF:FF:FF:FF"
scname="My token"
manufacturer="Token Manufacturer"
pkcs11DllName="pkcs11.dll"
registry="HKEY_LOCAL_MACHINE:SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\App
Paths\\TgbIke.exe:DllPath"

[3B:65:00:00:9C:02:02:07:03]
mask="FF:FF:00:00:FF:FF:FF:FF:FF"
scname="My token2"
manufacturer="Token Manufacturer"
pkcs11DllName="pkcs11.dll"
registry="HKEY_LOCAL_MACHINE:SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\App
Paths\\TgbIke.exe:DllPath"
```

The parameters are as follows:

Table 12. Parameters for the vpnconf.ini File

Parameter	Description
[atr]	Token ATR code. This the delimiter to separate several ATR codes.
mask	Token mask code.
scname	Token name.
manufacturer	Token manufacturer’s name.

Table 12. Parameters for the vpnconf.ini File (Continued)

Parameter	Description
pkcs11DllName	PKCS#11 middleware file.

registry	Value in the registry that points to the complete path of the DLL.
	
	Note: If the PKCS#11 DLL (shown in the example as pkcs11.dll) is not in c:\windows\system32\, then the registry parameter must be set.
	
	The syntax is as follows:
	`HKEY_LOCAL_MACHINE:<registry key>:<value in the registry key>.`
	`For example, if a value "DllPath" with content:`
	`C:\Program Files\Netgear\Netgear VPN\pkcs11.dll`
	`is created in:`
	`HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\AppPaths\\TgbIke.exe,`
	`the registry line is:`
	`HKEY_LOCAL_MACHINE:SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\AppPaths\\TgbIke.exe:DllPath`

Configure the VPN Client with a NETGEAR Router

8

This chapter describes how to configure the VPN Client with a NETGEAR ProSafe FVX538 VPN router. This chapter includes the following sections:

Introduction

In addition to the NETGEAR ProSafe FVX538 VPN router, you can also apply the information in this chapter to the following NETGEAR ProSafe routers and ProSecure UTM appliances. The information in this chapter has been tested with the VPN Client firmware version 4.66.012 and the firmware releases that are listed in the following table.

Table 13. Routers, Appliances, and Firmware Versions

Routers	Firmware Version
FVS318G	3.0.5-27 or later
FVG318	2.1.2-67 or later
FVS338	3.0.6-25 or later
DGFV338	3.0.5-24 or later
SRXN3205	3.0.6-25 or later
FVS336G	3.0.6-25 or later
FVX538	3.0.6-25 or later
SRX5308	3.0.6-9 or later

Table 13. Routers, Appliances, and Firmware Versions (Continued)

Routers	Firmware Version
UTM5	1.0.26-0 or later
UTM10	
UTM25	

Example VPN Network Topology

In the VPN network example that is shown in *Figure 66*, the FVX538 VPN router functions as a gateway for a main office. The Windows PC VPN Client is installed on a remote laptop that runs Windows 7 and that connects to the Internet through a DSL modem. The Windows PC VPN Client connects to the FVX538 VPN router and establishes a secure IPSec VPN connection with the router so the laptop user can gain access to a fileserver or any other resources at the main office.

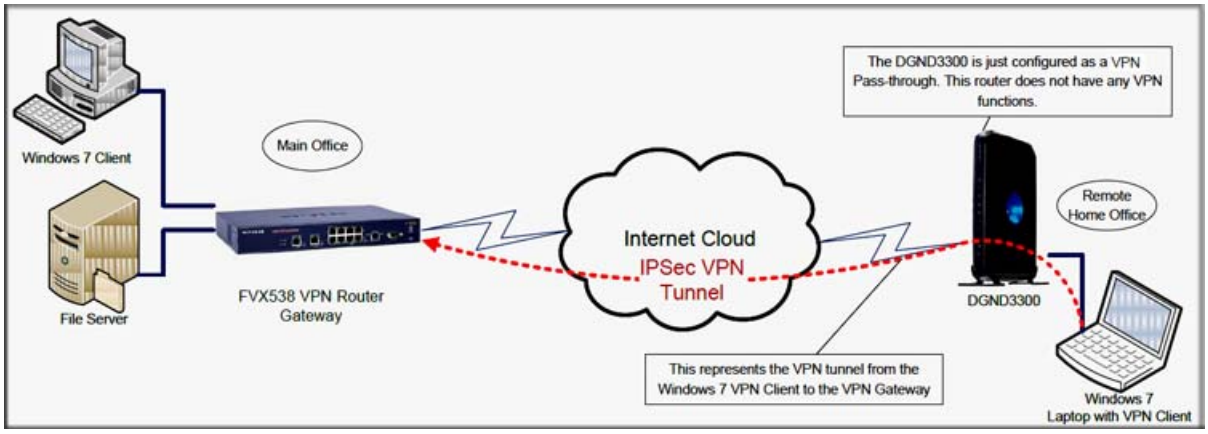


Figure 66.

The following table shows the IP addresses that are usee in the VPN network example that is shown in *Figure 66*.

Main Office	Remote Home Office
Main office router: WAN IP: myrouter.dyndns.org or 110.200.13.18 FVX538 IP address: 192.168.30.1 Subnet mask: 255.255.255.0 File server IP: 192.168.30.2 Subnet mask: 255.255.255.0 Default gateway: 192.168.30.1 Windows 7 client IP: 192.168.30.3 Subnet mask: 255.255.255.0 Default gateway: 192.168.30.1	**Home office router:** DGND3300 IP address: 192.168.0.1 Subnet mask: 255.255.255.0 Windows 7 laptop with VPN Client: 192.168.0.2 Subnet mask: 255.255.255.0 Default gateway: 192.168.0.1 **VPN Client settings:** Pre-shared key: N3tg4ar12 Router identifier: fvx_router.com VPN Client identifier: fvx_client.com

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

While you configure the FVX538 VPN router, there is information that you add and that will later be used in the configuration of the VPN Client. This information is marked with a number in between brackets in red bold font in the text (for example **(3)**) or with a number in white font in a red circle in the figures (for example ❸). You can print the following table to help you keep track of this information.

(1)	**Pre-Shared Key**	
(2)	**Remote Identifier Information**	
(3)	**Local Identifier Information**	
(4)	**Router's LAN Network IP Address**	
(5)	**Router's LAN Network Mask**	
(6)	**Router's WAN IP Address**	

Configure the FVX538 VPN Router

The router lets you to set up the VPN connection manually or with the integrated VPN Wizard, which is the easier and preferred method. The VPN Wizard configures the default settings and provides basic interoperability so that the VPN router can easily communicate with NETGEAR or third-party VPN devices.

Use the VPN Wizard to Configure a Client-to-Router VPN Connection

To use the VPN Wizard to set up a VPN connection between the VPN router and a client:

1. Access the router's Web management interface, select **VPN** from the main menu, and **VPN Wizard** from the submenu. The VPN Wizard screen displays.

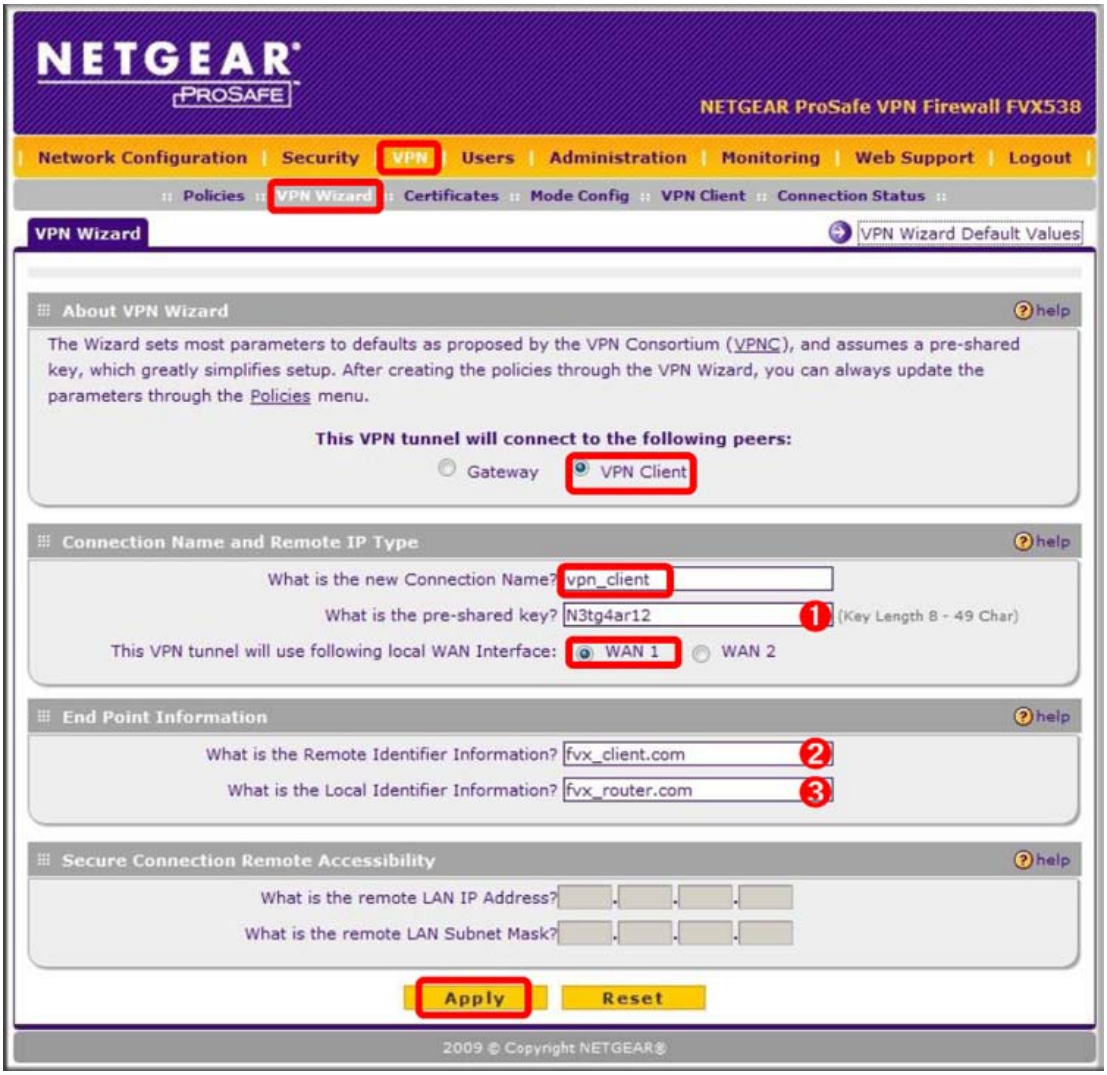


Figure 67.

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

Table 14. FVX538 VPN Wizard Settings

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **VPN Client** radio button.
Connection Name and Remote IP Type	
What is the new Connection Name	Enter **vpn_client**.
What is the pre-shared key	Enter the pre-shared key **N3tg4ear12**. **(1)** **Note:** This key must be at least 8 characters long and should not be easy to guess.
This VPN Tunnel will use the following WAN Interface	Select the **WAN1** radio button. **Note:** This option is not available for platforms with a single WAN port.
End Point Information	
What is the Remote Identifier Information	Enter **fvx_client.com**. **(2)** The default setting is **fvx_remote.com**.
What is the Local Identifier Information	Enter **fvx_router.com**. **(3)** The default setting is **fvx_local.com**.

3. Click **Apply** to save the settings.
4. Review the policies by selecting **VPN** from the main menu, **Policies** from the sub menu, and then click the **VPN Polices** tab. The VPN Policies screen displays. Take note of the local LAN IP address **(4)** and subnet mask **(5)**, both of which you will later use in the configuration of the VPN Client.

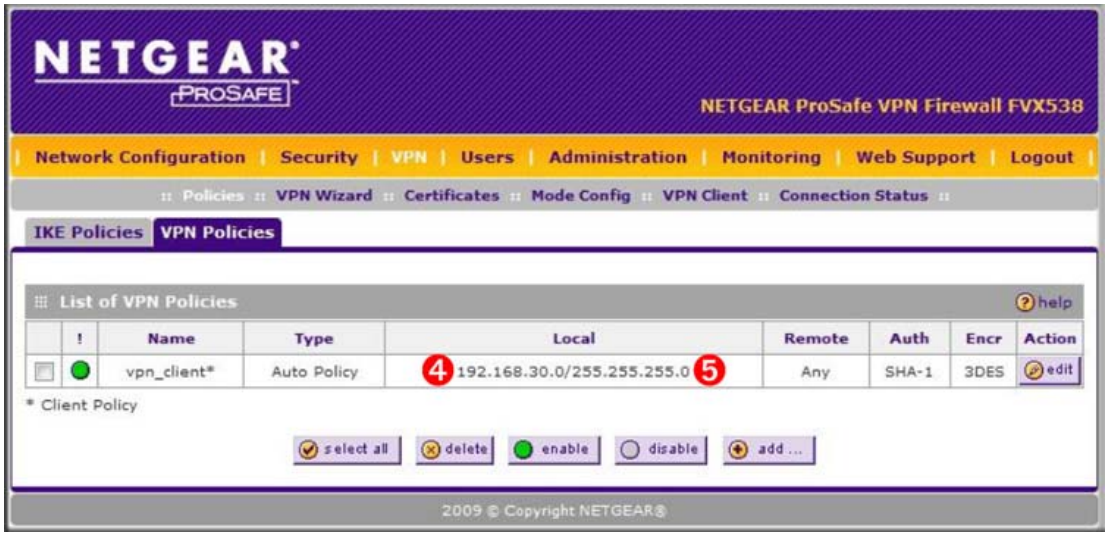


Figure 68.

5. Optional step. Review or edit the VPN policy. To edit the VPN policy:
   a. Disable the VPN policy by selecting the check box that is associated with the policy and then clicking **disable**.
   b. Click **edit** in the Action column of the VPN Policies screen to open the Edit VPN Policy screen.

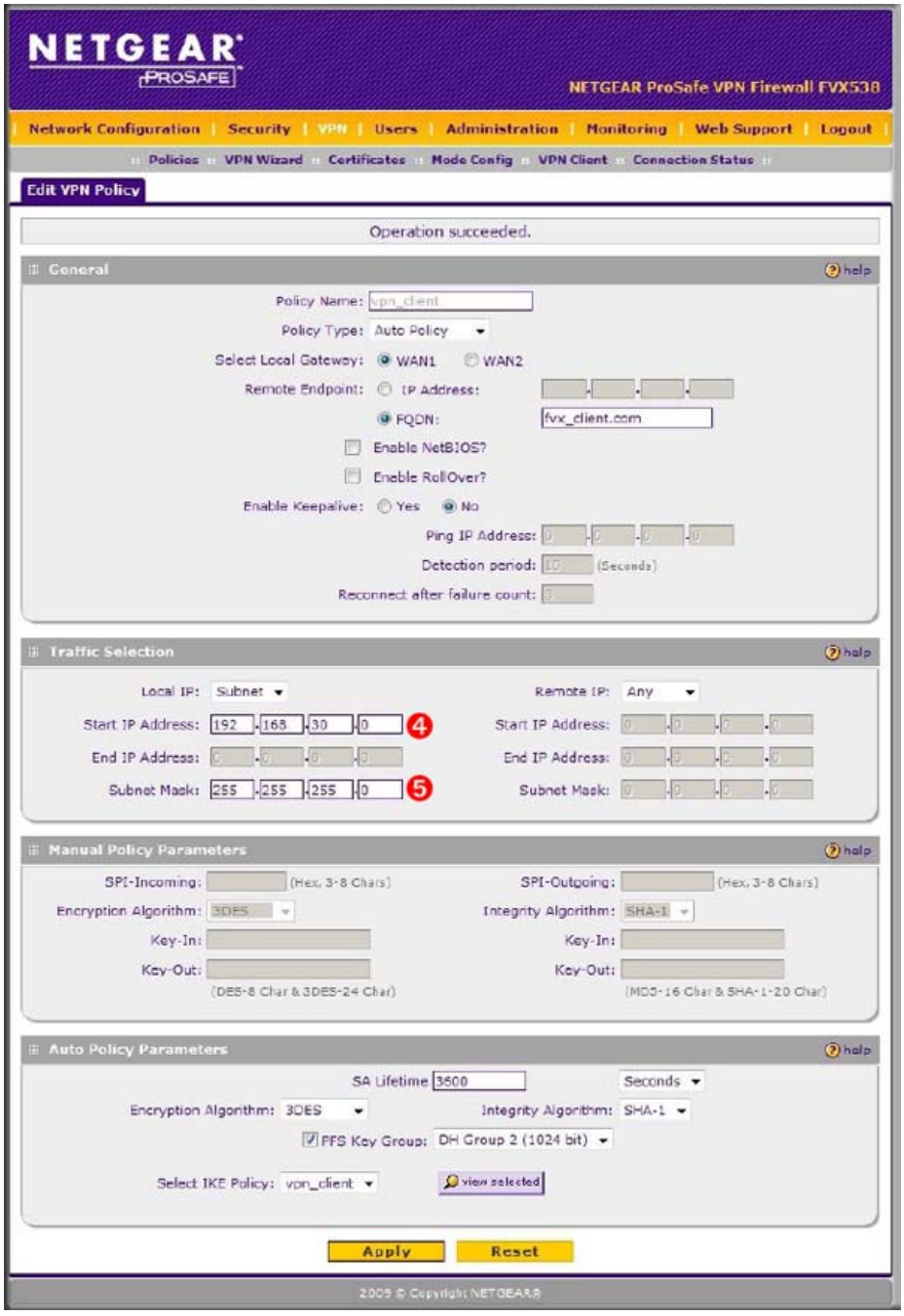


Figure 69.

c. Make your changes to the VPN policy, and click **Apply**. The VPN Policies screen displays again.

d. Reenable the VPN policy by selecting the check box that is associated with the policy and then clicking **enable**.

6. Optional step. Review or edit the IKE policy. To edit the IKE policy:

a. You cannot edit the IKE policy without disabling the associated VPN policy. On the VPN Policies screen, disable the associated VPN policy by selecting the check box that is associated with the policy and then clicking **disable**.

b. Click the **IKE Policies** tab. The IKE Policies screen displays. Take note of the remote ID **(2)** and local ID **(3)**, both of which you will later use in the configuration of the VPN Client.

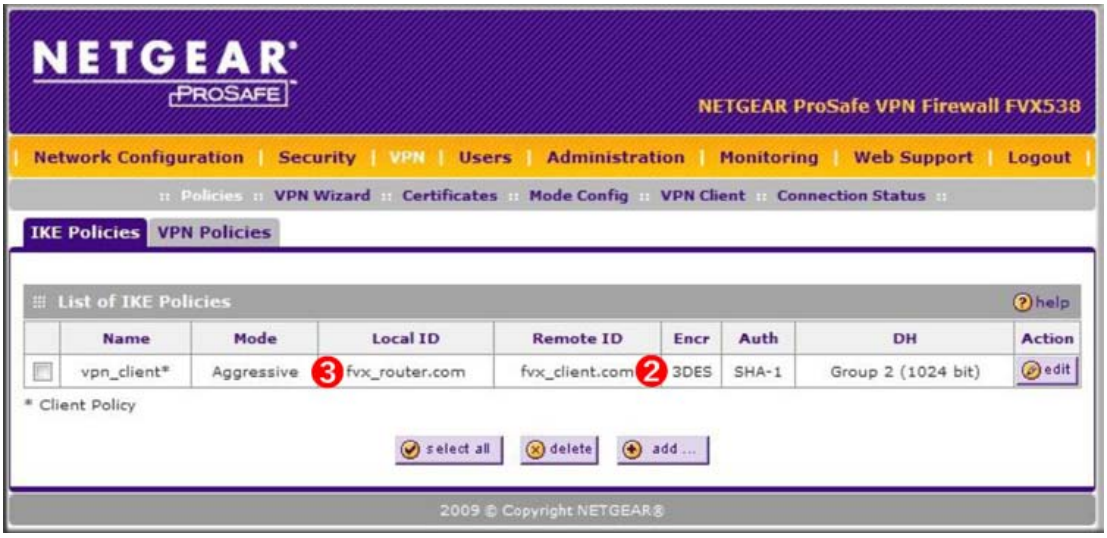


Figure 70.

c. Click **edit** in the Action column of the IKE Policies screen to open the Edit IKE Policy screen. Take note of the pre-shared key **(1)**, which you will later use in the configuration of the VPN Client.

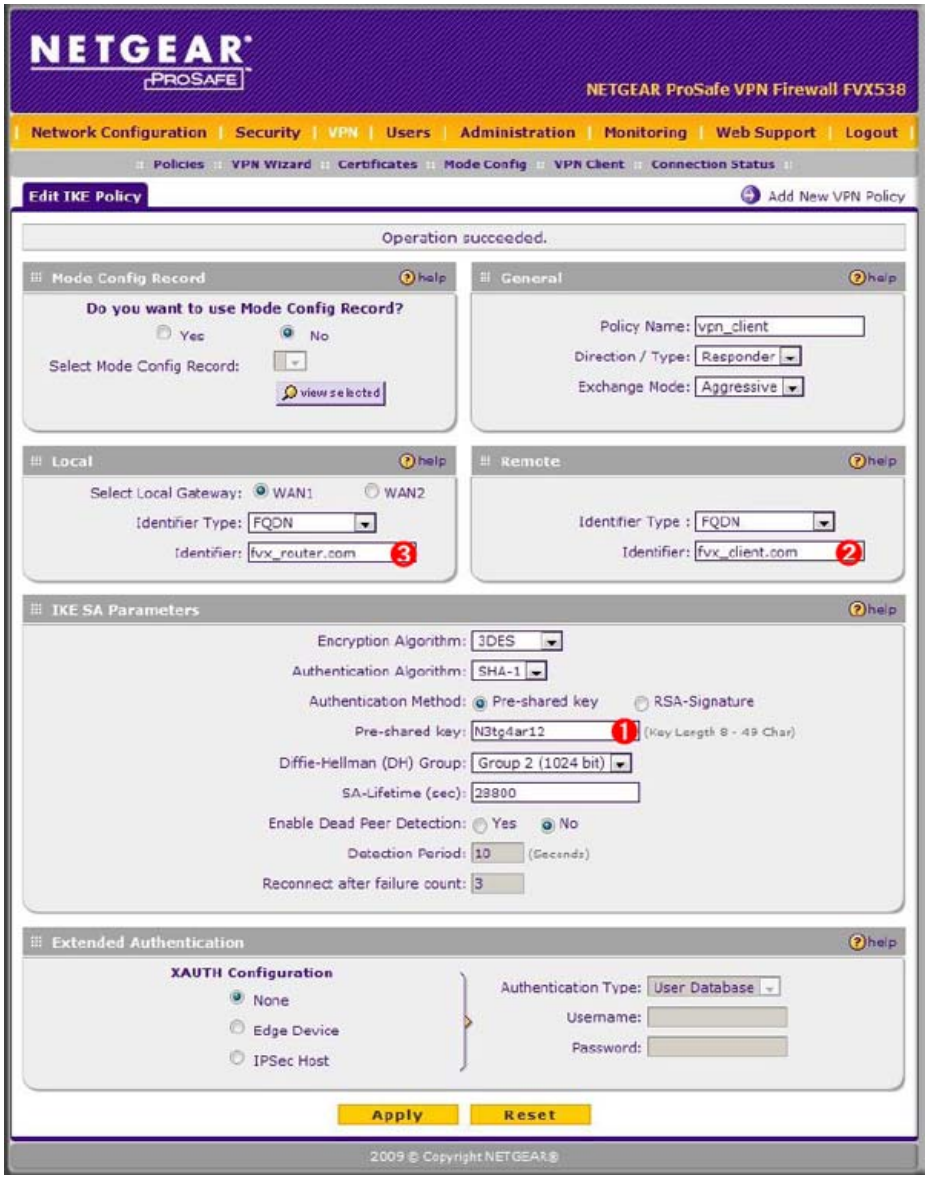


Figure 71.

d. Make your changes to the IKE policy, and click **Apply**. The IKE Policies screen displays again.

e. Reenable the VPN policy by clicking the **VPN Policies** tab to open the VPN Policies screen, selecting the check box that is associated with the policy, and then clicking **enable**.

To configure the VPN Client, see *Configure the VPN Client* on page 101.

Manually Configure a Client-to-Router VPN Connection

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

IKE Policy

To set up an IKE policy:

1. Select **VPN** from the main menu, **Policies** from the submenu, and then click the **IKE Polices** tab. The IKE Policies screen displays.
2. Click **add**. The Add IKE Policy screen displays. (This screen has the same fields and menus as the Edit IKE Policy screen that is shown in the following figure).

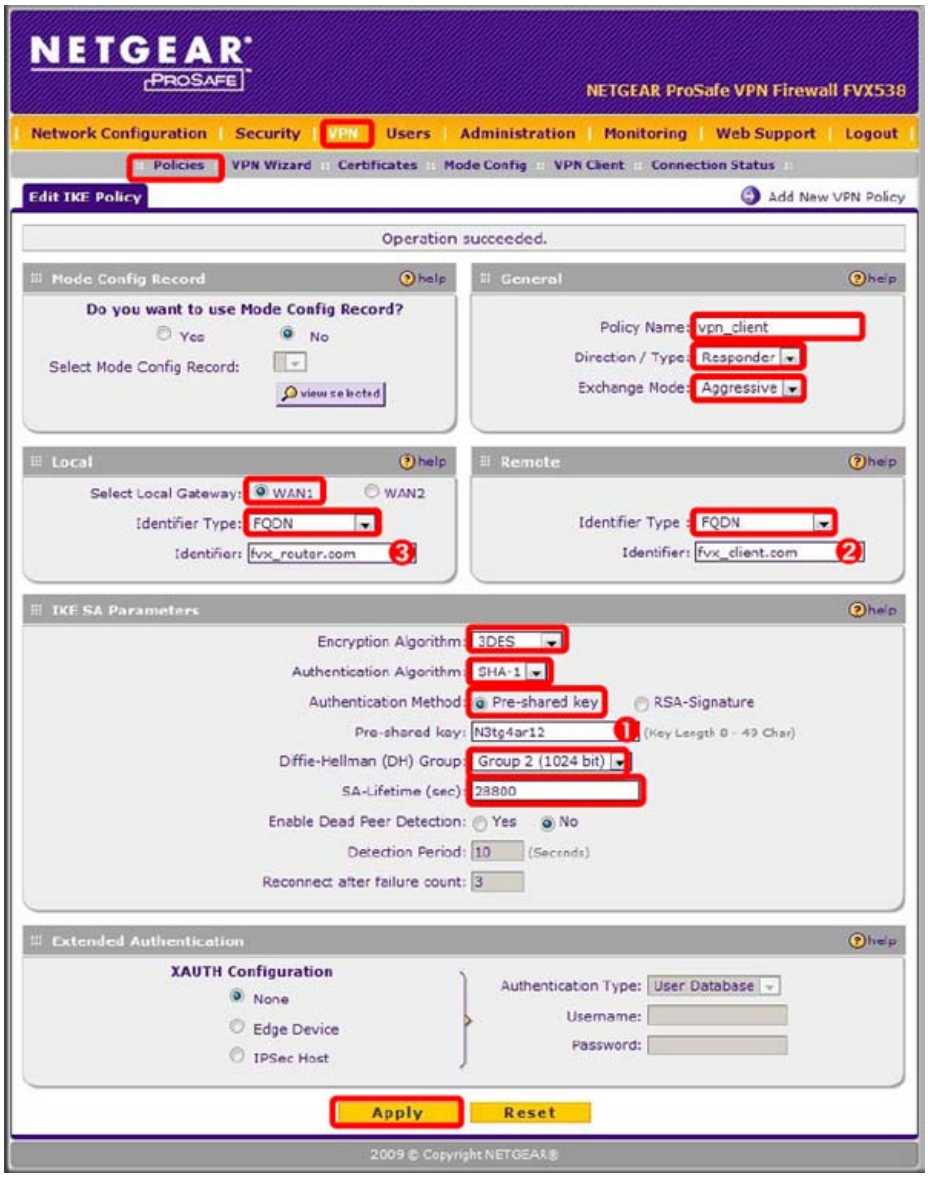


Figure 72.

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

Table 15. FVX538 Add IKE Policy Settings

Setting	Description
General	
Policy Name	Enter **vpn_client**.
Direction / Type	Select **Responder** from the drop-down list (the router will be responding to the client).
Exchange Mode	Select **Aggressive** (mode) from the drop-down list.
Local	
Select Local Gateway	Select the **WAN1** radio button. **Note:** This option is not available for platforms with a single WAN port.
Identifier Type	Select **FQDN** from the drop-down list.
Identifier	Enter **fvx_router.com**. **(3)**
Remote	
Identifier Type	Select **FQDN** from the drop-down list.
Identifier	Enter **fvx_client.com**. **(2)**
IKE SA Parameters	
Encryption Algorithm	Select **3DES** from the drop-down list.
Authentication Algorithm	Select **SHA-1** from the drop-down list.
Authentication Method	Select the **Pre-Shared Key** radio button.
Pre-shared key	Enter the pre-shared key **N3tg4ear12**. **(1)** **Note:** This key must be at least 8 characters long and should not be easy to guess.
Diffie-Hellman (DH) Group	Select **Group 2 (1024bit)** from the drop-down list.
SA-Life Time (sec)	Enter **28800**.
Enable Dead Peer Detection	Select the **No** radio button. (This is the default setting.)
Extended Authentication	
Extended Authentication	Select the **No** radio button. (This is the default setting.)

4. Click **Apply**. The IKE Policies screen displays.

VPN Policy

To set up a VPN policy:

1. Select **VPN** from the main menu, **Policies** from the submenu, and then click the **VPN Polices** tab. The VPN Policies screen displays.
2. Click add. The Add VPN Policy screen displays. (This screen has the same fields and menus as the Edit VPN Policy screen that is shown in the following figure).

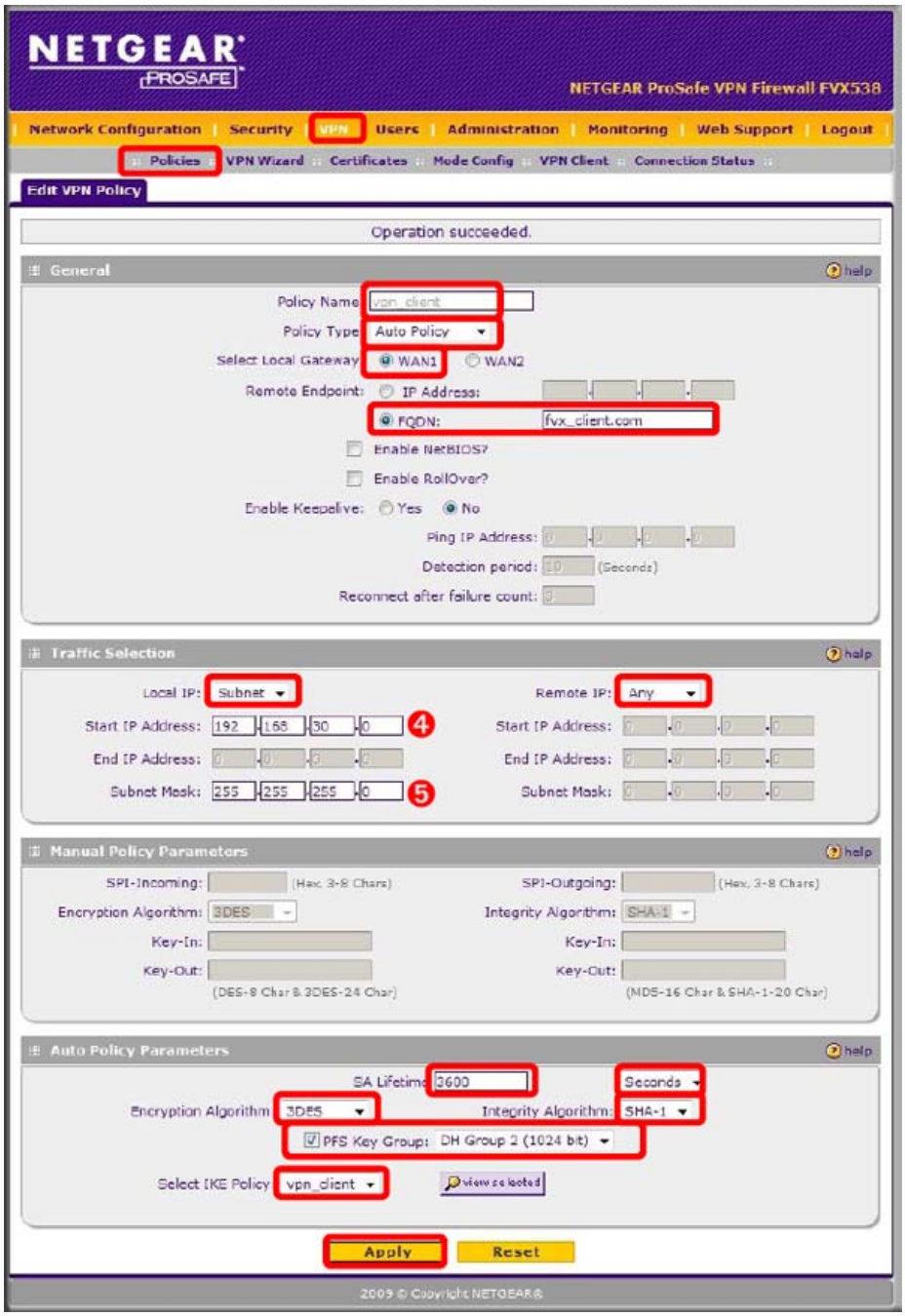


Figure 73.

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

Table 16. FVX538 Add VPN Policy Settings

Setting	Description
General	
Remote Endpoint	Enter **vpn_client**. (Keep the policy name the same as the IKE policy name.)
Policy Type	Select **Auto Policy** from the drop-down list.
Select Local Gateway	Select the **WAN1** radio button. **Note:** This option is not available for platforms with a single WAN port.
Remote Endpoint	Select the **FQDN** radio button, and enter **fvx_client.com** in the field to the right .
Enable NetBIOS	Do not enable NetBIOS; leave this check box cleared. (This is the default setting.) **Note:** Because you are creating a client-to-router configuration, the remote IP addresses are likely unknown.
Enable RollOver	Do not enable rollover; leave this check box cleared. (This is the default setting.) **Note:** This option is not available for platforms with a single WAN port.
Enable Keepalive	Do not enable keepalives; select the **No** radio button. (This is the default setting.)
Traffic Selection	
Local IP	Select **Subnet** from the drop-down list.
Start IP Address	Enter **192.168.30.0**. **(4)**
Subnet Mask	Enter **255.255.255.0**. **(5)**
Remote IP	Select **Any** from the drop-down list.
Auto Policy Parameters **Note:** If you select **Manual Policy** from the **Policy Type** drop-down list (See the General section on the screen), the Manual Policy Parameters section is enabled on screen. Because you selected **Auto Policy** the Auto Policy Parameters section is enabled.	
SA Lifetime	Enter **3600** and select **Seconds** from the drop-down list.
Encryption Algorithm	Select **3DES** from the drop-down list.
Integrity Algorithm	Select **SHA-1** from the drop-down list.

Table 16. FVX538 Add VPN Policy Settings (Continued)

Setting	Description
PFS Key Group	Select the **PFS Key Group** check box, and then **DH Group 2 (1024 bit)** from the drop-down list.
Select IKE Policy	Select **vpn_client** from the drop-down list. This is the IKE policy that you created in the previous section.

4. Click **Apply**. The VPN Policies screen displays.

To configure the VPN Client, see the following section.

Configure the VPN Client

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

Use the Configuration Wizard to Configure the VPN Client

Note: For another example of how to use the Configuration Wizard, see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 39.

To use the Configuration Wizard to set up a VPN connection between the VPN Client and a router:

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

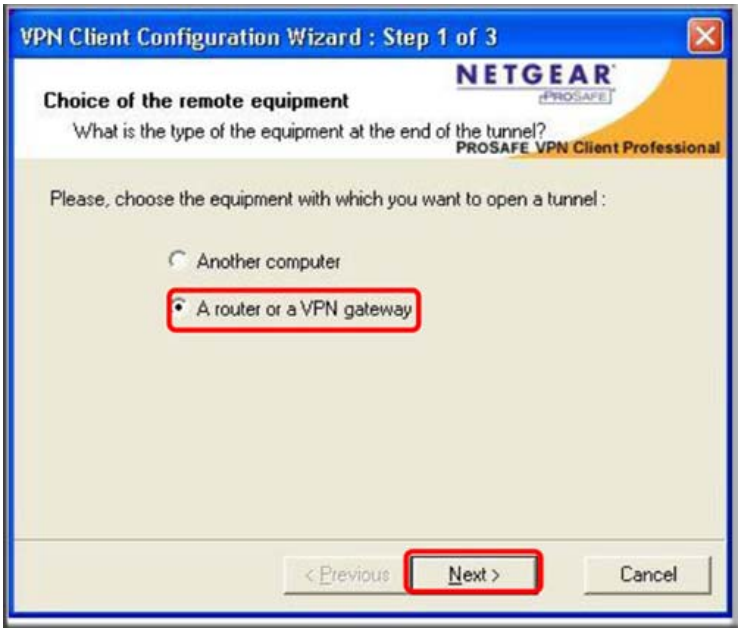


Figure 74.

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

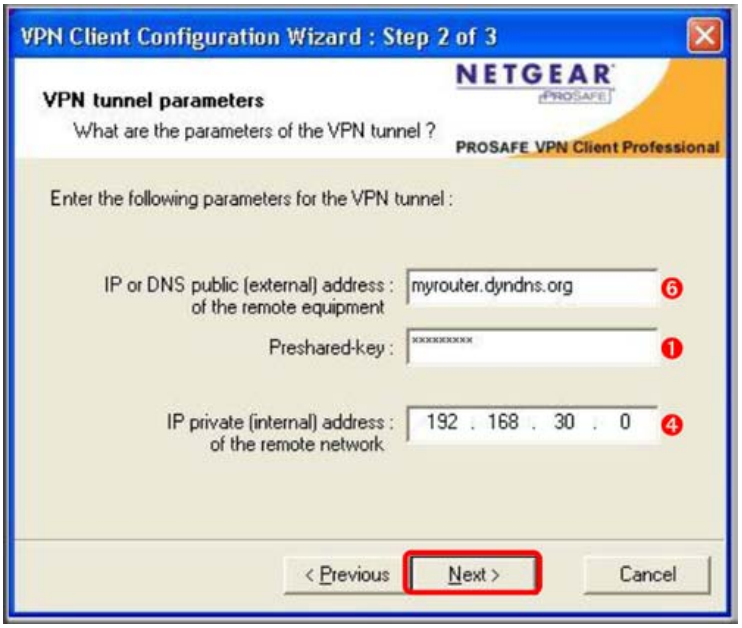


Figure 75.

3. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the VPN router. For example **myrouter.dyndns.org** or **110.200.13.18**. **(6)**

- **Preshared key**. Enter **N3tg3ar12**, which is the preshared key that you already specified on the VPN router. **(1)**
- **IP private (internal) address of the remote network**. Enter **192.168.30.0**, which is the remote private IP address of the remote VPN router. This IP address enables communication with the entire 192.168.30.x subnet. **(4)**

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

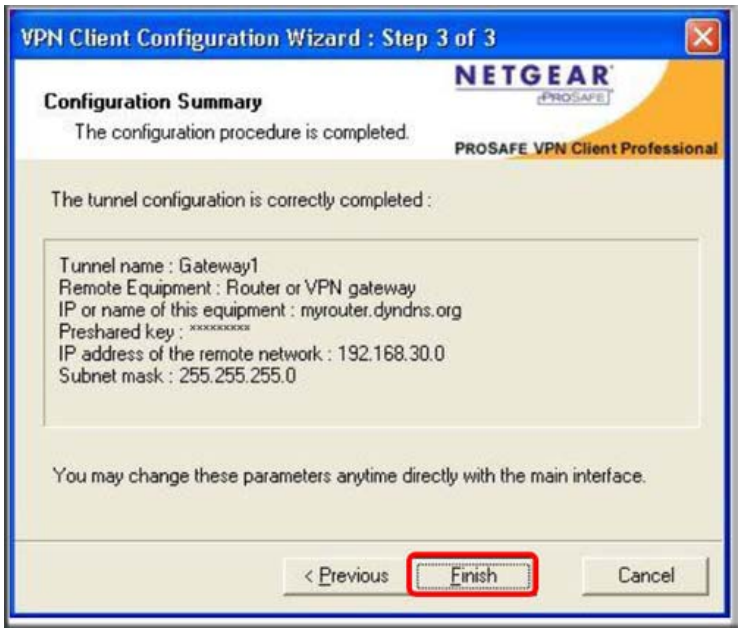


Figure 76.

5. This screen is a summary screen of the new VPN configuration. Click **Finish**.
6. Specify the local and remote IDs:
   a. Click on **vpn_client** (or the default name **Gateway1**) in the tree list window of the Configuration Panel screen. The Phase 1 (Authentication) window displays in the Configuration Panel screen.
   b. Click **P1 Advanced...**. The Phase 1 Advanced screen displays.

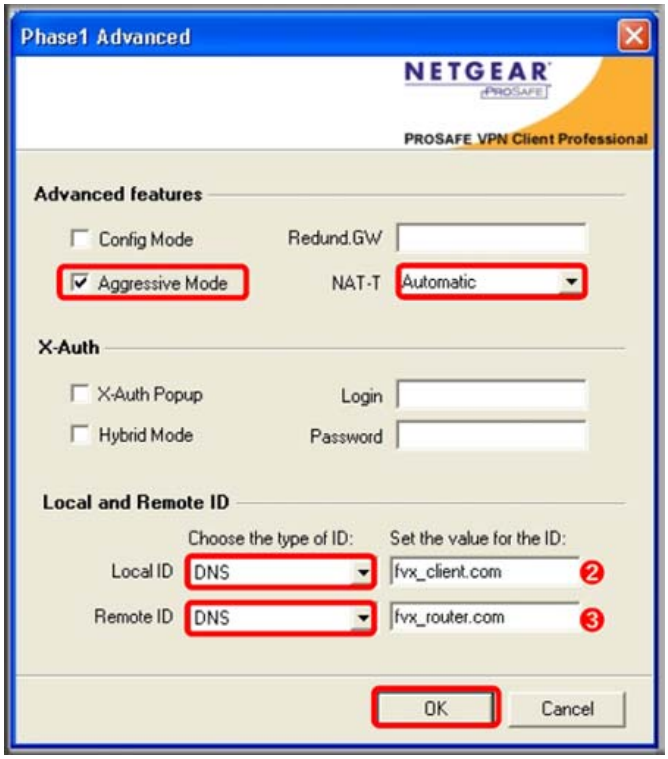


Figure 77.

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

Table 17. VPN Client Phase 1 Advanced Settings

Setting	Description
Advanced Features	
Aggressive Mode	Select this check box to enable aggressive mode as the negotiation mode with the VPN router.
NAT-T	Select **Automatic** from the drop-down list to enables the VPN Client and VPN router to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the **Local ID** drop-down list because you specified **FQDN** in the VPN router configuration. **(2)** As the value of the ID, enter **fvx_client.com** as the local ID for the VPN Client.
Remote ID	As the type of ID, select **DNS** from the **Remote ID** drop-down list because you specified **FQDN** in the VPN router configuration. **(3)** As the value of the ID, enter **fvx_router.com** as the remote ID for the VPN router.

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

7. Specify the global parameters:

   a. Click **Parameters** in the left column of the Configuration Panel screen or select **VPN Configuration** > **Parameters** from the main menu. The Parameters window displays in the Configuration Panel screen.

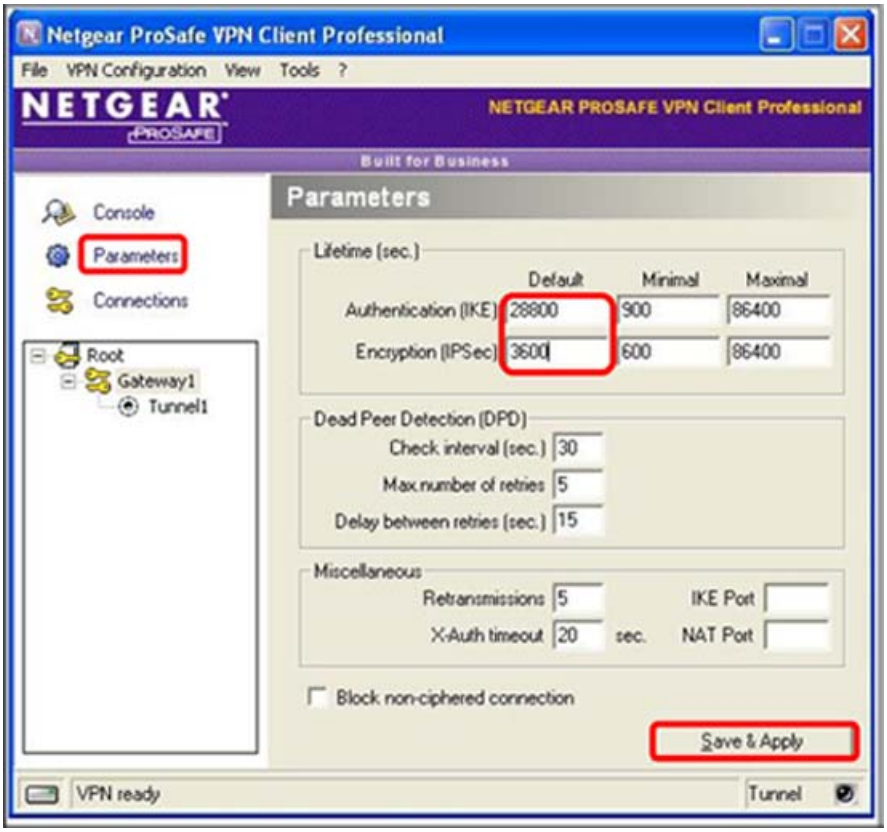


Figure 78.

   b. Specify the default lifetimes in seconds:

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

   c. Click **Save & Apply**.

The VPN Client configuration is now complete.

To connect the VPN Client to the VPN router, see *Establish a VPN connection* on page 111.

Manually Configure the VPN Client

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

IKE Phase 1

To set up an IKE phase 1 configuration:

1. In the tree list window of the Configuration Panel screen, click on **Root**.

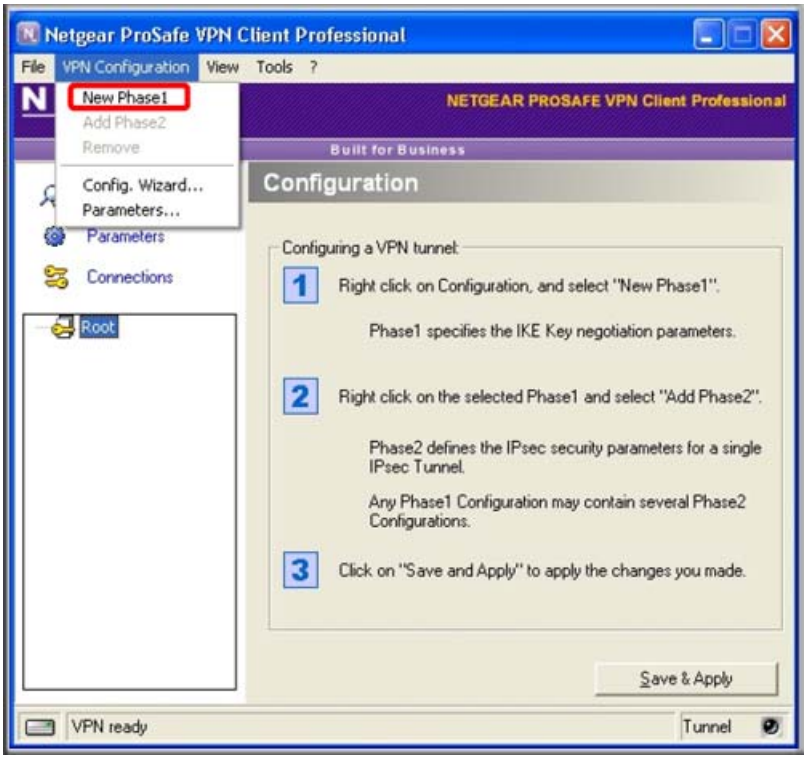


Figure 79.

2. Select **VPN Configuration** > **New Phase 1** from the main menu. The Phase 1 (Authentication) window displays in the Configuration Panel screen.

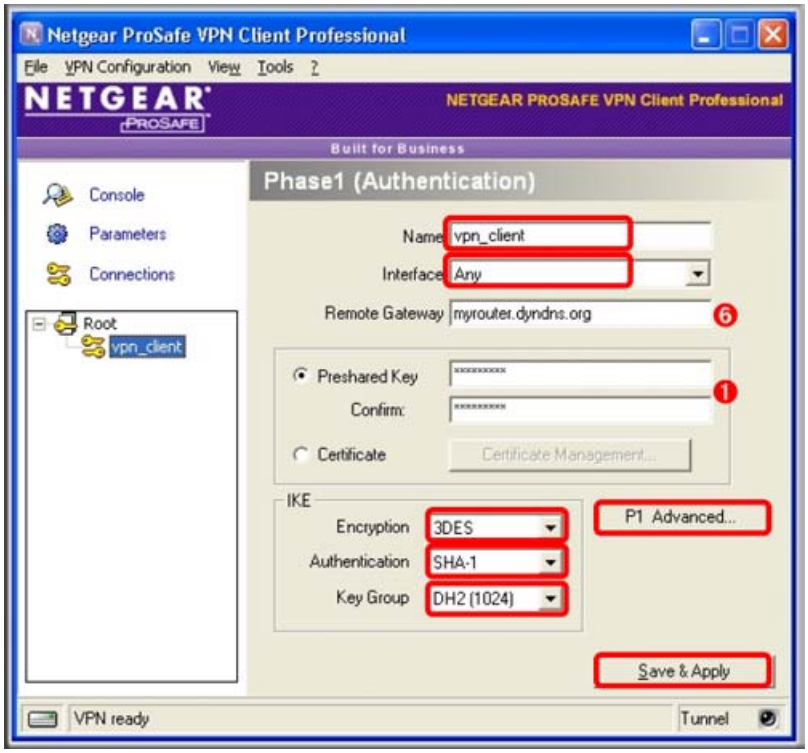


Figure 80.

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

Table 18. VPN Client Phase 1 Authentication Settings

Setting	Description	
Name	Enter **vpn_client**. This is the label for the authentication phase that is used only for the VPN Client, not during IKE negotiation. You can view and change this name in the tree control window. This name must be a unique name.	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN router. For example **myrouter.dyndns.org** or **110.200.13.18**. **(6)**	
Preshared Key	Select the **Preshared Key** radio button. Enter **N3tg3ar12**, which is the preshared key that you already specified on the VPN router. **(1)** Confirm the key in the **Confirm** field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On NETGEAR routers, this key group is referred to as Diffie-Hellman Group 2 (1024bit).

4. **Click Save & Apply** to save the settings.

5. On the same screen, click **P1 Advanced...**. The Phase 1 Advanced screen displays.

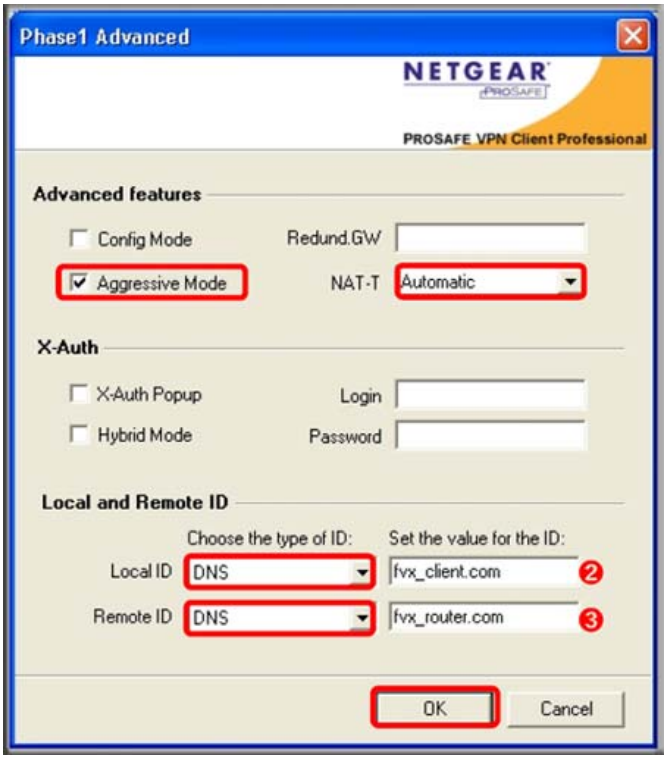


Figure 81.

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

Table 19. VPN Client Phase 1 Advanced Settings

Setting	Description
Advanced Features	
Aggressive Mode	Select this check box to enable aggressive mode as the negotiation mode with the VPN router.
NAT-T	Select **Automatic** from the drop-down list to enables the VPN Client and VPN router to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the **Local ID** drop-down list because you specified **FQDN** in the VPN router configuration. **(2)** As the value of the ID, enter **fvx_client.com** as the local ID for the VPN Client.
Remote ID	As the type of ID, select **DNS** from the **Remote ID** drop-down list because you specified **FQDN** in the VPN router configuration. **(3)** As the value of the ID, enter **fvx_router.com** as the remote ID for the VPN router.

7. Click **OK** to save the settings.

IPSec Phase 2

Note: On NETGEAR routers, the IPSec phase 2 configuration is referred to as the VPN settings.

To set up an IPSec phase 2 configuration:

1. Click on the **vpn_client** phase 1 name in the tree list window of the Configuration Panel screen. Select **VPN Configuration** > **Add Phase 2** from the main menu. The Phase 2 (IPSec Configuration) screen displays.

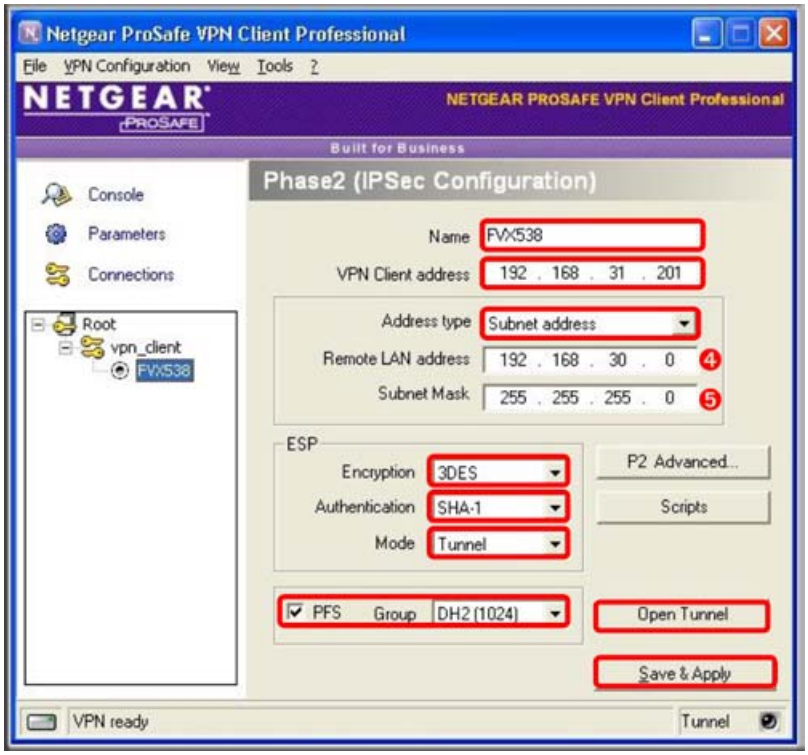


Figure 82.

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

Table 20. VPN Client Phase 2 IPSec Configuration Settings

Setting	Description
Name	Enter **FVX538**. This is the label for the IPSec configuration that is used only for the VPN Client, not during IPSec negotiation. You can view and change this name in the tree control window. This name must be a unique name.
VPN Client address	Enter **192.168.31.201**. This is the virtual IP address that is used by the VPN Client in the VPN router's LAN; the computer (for which the VPN Client opened a tunnel) appears in the LAN with this IP address. You might be able to forgo using an IP address and enter **0.0.0.0**.

Table 20. VPN Client Phase 2 IPSec Configuration Settings (Continued)

Setting	Description	
Address Type	Select **Subnet address** from the drop-down list. This selection defines what the VPN Client can communicate with after the VPN tunnel is established.	
Remote LAN address	Enter **192.168.30.0** as the remote IP address, or LAN network address, of the gateway that opens the VPN tunnel. **(4)**	
Subnet Mask	Enter **255.255.255.0** as the remote subnet mask of the gateway that opens the VPN tunnel. **(5)**	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On NETGEAR routers, this key group is referred to as Diffie-Hellman Group 2 (1024bit).	

3. Tick **PFS** and select the Diffie-Hellman key group, select **DH2 (1024).** This is also called Diffie-Hellman Group 2 (1024bit) on the NETGEAR Routers.
4. Click on **Save & Apply.**

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

Global Parameters

To specify the global parameters:

1. Click **Parameters** in the left column of the Configuration Panel screen or select **VPN Configuration** > **Parameters** from the main menu. The Parameters window displays in the Configuration Panel screen.

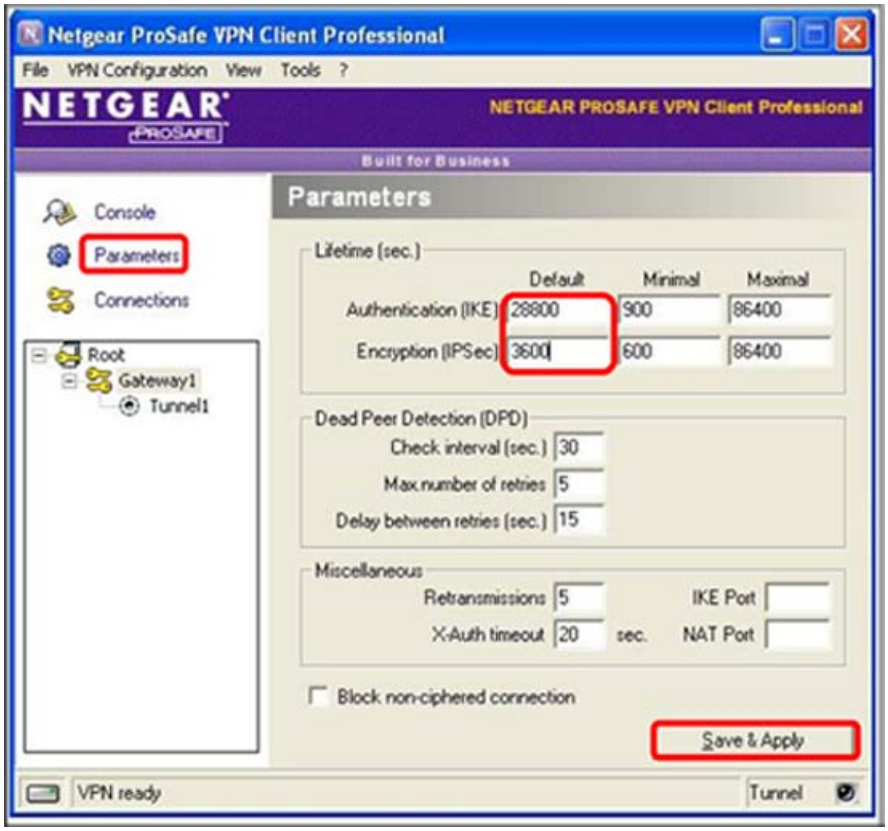


Figure 83.

2. Specify the default lifetimes in seconds:
   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Replace this setting to 28800 seconds to match the configuration of the VPN router.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Replace this setting to 3600 seconds to match the configuration of the VPN router.
3. Click **Save & Apply**.

The VPN Client configuration is now complete.

To connect the VPN Client to the VPN router, see the next section.

Establish a VPN connection

There are several ways to establish a connection.

- On the Phase 2 (IPSec Configuration) screen, click **Open Tunnel**.
- Right-click on the system tray icon, then click
- On the **Configuration** Panel screen:
  a. Click **View** on the main menu, and then click **Connection Panel**. The Connection Panel screen opens.

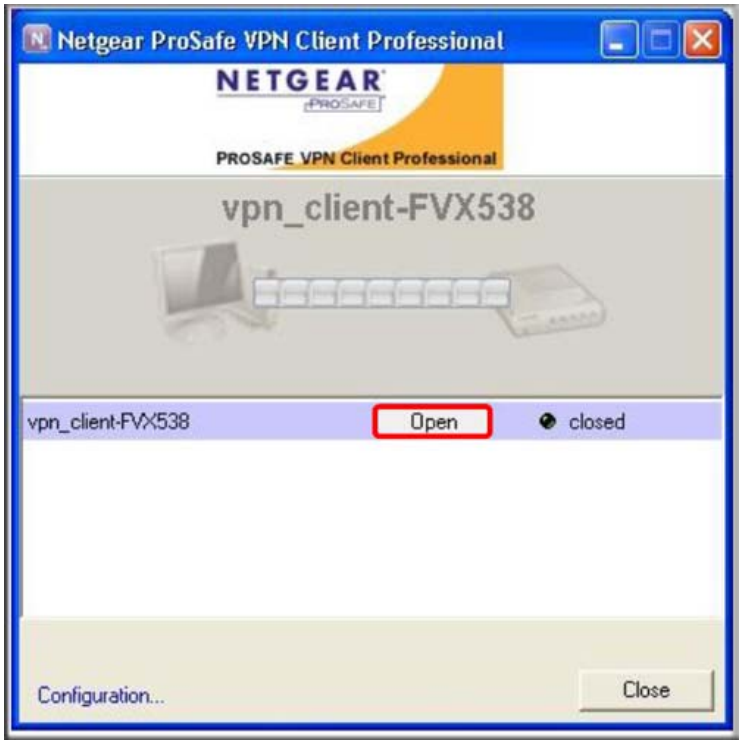


Figure 84.

b. Next to vpn_client-FVX538, click **Open**.

VPN Troubleshooting

9

This chapter contains troubleshooting procedures for the VPN Client. This chapter includes the following sections:

Overview

You can find information about the VPN connection state, VPN traces, and VPN Logs on the Console screen (see *VPN Console Active Screen* on page 29).

Be careful when configuring an IPSec VPN tunnel. One missing parameter can prevent a VPN connection from being established. Some tools are available to find the source of VPN connection problems. For example, *Etherea* is a good and free network analysis software tool (see *http://www.ethereal.com*) that shows IP or TCP packets that are received on a network card. You can use this tool for packet and traffic analysis, and to follow the protocol exchange between two devices.

Note: For difficulties with certificates, see *Certificate Troubleshooting* on page 72.

Typical Errors

The following typical errors might occur on the VPN Client:

"PAYLOAD MALFORMED" Error (Wrong Phase 1 [SA])

VPN Console Log:

```
114915 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
114915 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
114915 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
114920 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA Cnx-P1) RECV phase 1 Main Mode [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification type
PAYLOAD_MALFORMED
114920 Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error
```

Explanation: The phase 1 [SA] configuration might be incorrect.

Resolution: Ensure that the encryption algorithms are the same on each side of the VPN tunnel.

"INVALID COOKIE" Error

VPN Console Log:

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification type
INVALID_COOKIE
115933 Default SEND Informational [NOTIFY] with INVALID_COOKIE error
```

Explanation: One of the endpoints attempts to use an SA that is no longer alive.

Resolution. Reset the VPN connection on each side of the VPN tunnel.

"no keystate" Error

VPN Console Log:

```
115305 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
115305 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
115305 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
115315 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
115319 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Explanation: The preshared key or local ID might be incorrect. The logs of the remote endpoint might provide additional information.

Resolution. Ensure that you use the same preshared key on each side of the VPN tunnel and that the local IDs are correctly defined. For the VPN Client, see *Phase 1 (Authentication) Advanced Configuration* on page 45.

."received remote ID other than expected" Error

VPN Console Log:

```
120343 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
120343 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
120343 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
120348 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
```

Explanation: The value of the **Remote ID** field does not match the value that the remote endpoint is expecting.

Resolution. Ensure that you use the correct value in the **Remote ID** field on the VPN Client (see *Phase 1 (Authentication) Advanced Configuration* on page 45).

"NO PROPOSAL CHOSEN" Error (Phase 1)

```
115905 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
115905 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
115905 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
115911 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

Explanation: The phase 1 encryption algorithms might mismatch on the tunnel endpoints.

Resolution. Ensure that the phase 1 IKE encryption algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Phase 1 (Authentication) Configuration* on page 43.

"NO PROPOSAL CHOSEN" Error (Phase 2)

```
115905 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
115905 Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
115905 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
115911 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
115913 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
```

```
115915 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational [HASH][DEL]
115915 Default Cnx-P1 deleted
```

Explanation: The phase 2 encryption algorithms might mismatch on the tunnel endpoints.

Resolution. Ensure that the phase 2 ESP encryption algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Phase 2 (IPSec) Configuration* on page 50.

"INVALID ID INFORMATION" Error

```
122609 Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
122609 Default sysdep_app_open: IPV4_SUBNET Network 192.168.3.1
122609 Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
122623 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72:
195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational [HASH][DEL]
122626 Default Cnx-P1 deleted
```

Explanation: An address might mismatch on the tunnel endpoints, or an SA might no longer be alive.

Resolution. Ensure that both the phase 2 address types and phase 2 address values (see *Phase 2 (IPSec) Configuration* on page 50) match with the remote endpoint's address configuration. Ensure that no old SA is still alive on the VPN router.

Other Common Problems

There is No Response to a Phase 1 Request

VPN Console Log:

```
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID]
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID]
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID]
114920 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID]
```

Explanation: The remote gateway does not answer because some phase 1 settings mismatch on the tunnel endpoints.

Resolution. Ensure that the algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Phase 1 (Authentication) Configuration* on page 43.

Also ensure that the local and remote IDs are correctly specified on each side of the VPN tunnel. For the VPN Client, see *Phase 1 (Authentication) Advanced Configuration* on page 45.

The Console Shows Only “SEND” and “RECV”

VPN Console Log:

```
115315 Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID]
115317 Default (SA CnxVpn1-P1) RECV phase 1 Aggressive Mode [HASH][SA][KEY_EXCH][NONCE] [ID]
[VID]
```

Explanation: The preshared key might mismatch on the tunnel endpoints.

Resolution. Ensure that you use the same preshared key on each side of the VPN tunnel, and there is not a second VPN tunnel to the VPN Client on the VPN router.

There is No Response to a Phase 2 Requests

VPN Console Log:

```
120348 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID] [ID]
120349 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID] [ID]
120351 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID] [ID]
120351 Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID] [ID]
```

Explanation: The phase 2 encryption algorithms or phase 2 addresses might mismatch on the tunnel endpoints.

Resolution. Ensure that the phase 2 ESP encryption algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Phase 2 (IPSec) Configuration* on page 50.

Ensure that both the phase 2 address types and phase 2 address values (see *Phase 2 (IPSec) Configuration* on page 50) match with the remote endpoint’s address configuration.

A Tunnel No Longer Opens

Resolution. Read the logs for each VPN tunnel endpoint. IKE requests can have been dropped by firewalls. The VPN Client must be able to use UDP port 500 and ESP port 50.

A VPN Tunnel is Up but You Cannot Ping the Remote Endpoint

If a VPN tunnel is up but you cannot ping the remote endpoint, check the following:

1. Verify that the phase 2 settings are correct, in particular that the VPN Client address and the remote LAN address are correct. Normally the VPN Client address should not belong to the remote LAN subnet.
2. When a VPN tunnel is up, packets are sent with the Encapsulating Security Payload (ESP) protocol that could be blocked by a firewall. Verify that all devices between the VPN Client and the VPN router accept the ESP protocol.
3. Look at the VPN router logs. Packets might have been dropped by one of its firewall rules.
4. Verify hat your ISP support ESP.
5. Use a network analysis software tool (such as the free *Etherea tool, see http://www.ethereal.com*) to analyze ICMP traffic on the LAN interface of the VPN router and on the LAN interface of the computer to see if encryption functions correctly.
6. Verify that the VPN router's LAN default gateway is correctly specified. A target on the remote LAN might receive pings but might not answer because there is a no default gateway specified.
7. Verify that the computers in the LAN are specified by their IP address and not by their FQDN
8. Use a network analysis software tool (such as the free *Etherea tool, see http://www.ethereal.com*) on one of the target computers to verify that the ping arrives inside the LAN.

View the Logs

To view the VPN logs on the VPN Client, see *VPN Console Active Screen* on page 29.

The following figure shows an example of VPN logs on a NETGEAR ProSafe VPN Firewall FVX538 router.

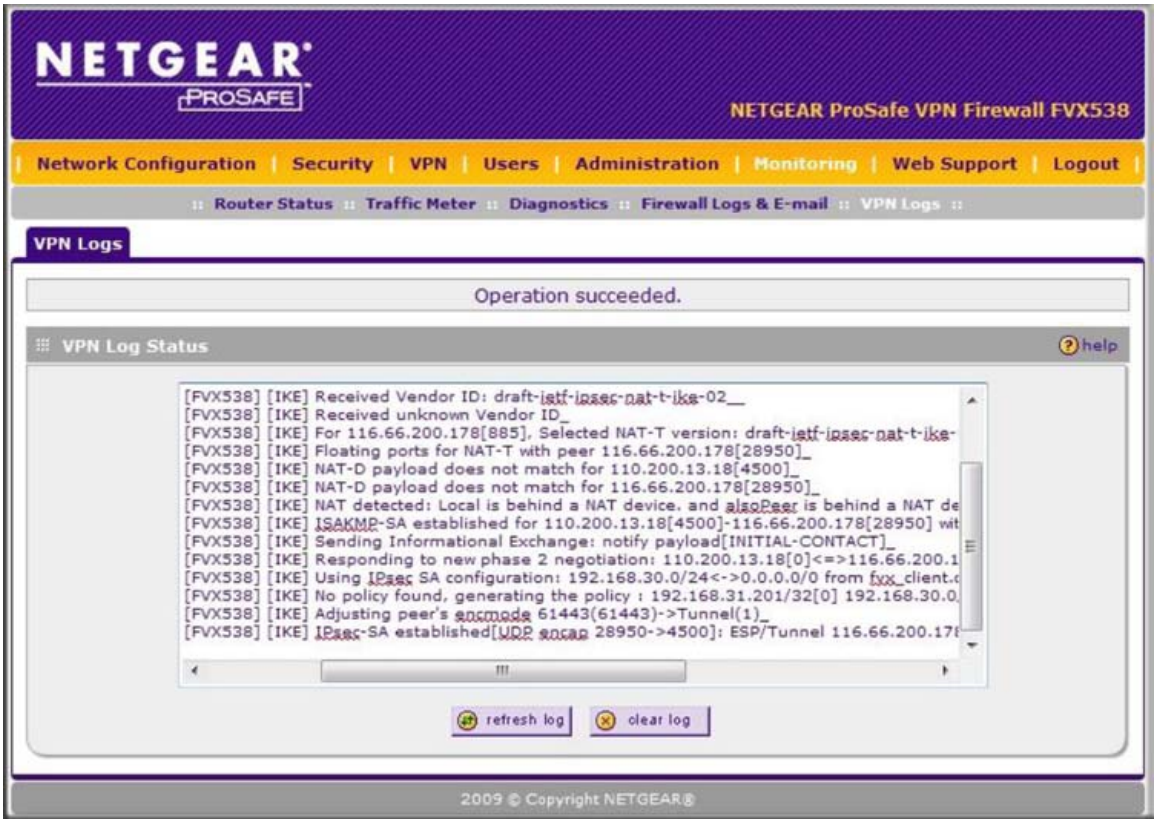


Figure 85.

Following is an example of a VPN log on the VPN router after a VPN Client successfully has established a VPN connection with the VPN router.

```
[FVX538] [IKE] Remote configuration for identifier "fvx_client.com" found_
[FVX538] [IKE] Received request for new phase 1 negotiation: 110.200.13.18[500]<=
>116.66.200.178[885]_
[FVX538] [IKE] Beginning Aggressive mode._
[FVX538] [IKE] Received unknown Vendor ID_
[FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02__
[FVX538] [IKE] Received unknown Vendor ID_
[FVX538] [IKE] For 116.66.200.178[885], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
[FVX538] [IKE] Floating ports for NAT-T with peer 116.66.200.178[28950]_
[FVX538] [IKE] NAT-D payload does not match for 110.200.13.18[4500]_
[FVX538] [IKE] NAT-D payload does not match for 116.66.200.178[28950]_
[FVX538] [IKE] NAT detected: Local is behind a NAT device. and alsoPeer is behind a NAT
device_
[FVX538] [IKE] ISAKMP-SA established for 110.200.13.18[4500]-116.66.200.178[28950] with
spi:14e465c525b13972:87ea734ec64e1c97_
[FVX538] [IKE] Sending Informational Exchange: notify payload[INITIAL-CONTACT]_
[FVX538] [IKE] Responding to new phase 2 negotiation: 110.200.13.18[0]<=>116.66.200.178[0]_
[FVX538] [IKE] Using IPsec SA configuration: 192.168.30.0/24<->0.0.0.0/0 from fvx_client.com_
```

```
[FVX538] [IKE] No policy found, generating the policy : 192.168.31.201/32[0]
192.168.30.0/24[0] proto=any dir=in_
[FVX538] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1)_
[FVX538] [IKE] IPsec-SA established [UDP encap 28950->4500]: ESP/Tunnel
116.66.200.178->110.200.13.18 with spi=8414587(0x80657b)_
```

VPN Client Software Setup Deployment and Command-Line Interface Guide

A

This appendix is an extension of the *VPN Client Software Setup and Deployment* chapter and duplicates some information that is also presented in the chapter. This appendix describes further management and software setup configuration options for the VPN Client as well as provides examples that illustrate how to manage the software; it includes the following sections:

Note: The information in this appendix is typically used by network administrators.

Overview

The following are some of the options that you can integrate in the installation process of the VPN Client:

- The license number for activation
- The email address for activation
- The mode in which the VPN Client starts
- Whether or not the user interface is hidden, and if so, to which degree

The following are some of the options that you can specify to be automatically configured after the VPN Client has been installed:

- If and how the VPN configuration is imported
- If and how a VPN tunnel starts and stops automatically
- If and how the VPN Client starts and quits automatically

You can deploy the VPN Client software setup installation package via several media:

- **Network drive**. Enables users to download and install the VPN Client with a simple double-click on an icon .
- **CD-ROM disk**. Enables users can insert and VPN Client installation will run automatically (AutoPlay)
- **USB drive**. Enables you to carry the installation package with you, insert the USB drive into a user's computer, and let the installation will automatically.

VPN Client Software Setup Deployment

Silent Installation

The VPN Client software deployment mainly uses the capability of the software setup to be run silently. A silent VPN Client software setup is an installation that is automatically processed without user input through the use of software setup commands. The VPN Client software setup is specifically designed to be installed silently.

A silent installation uses installation parameters (software setup commands) that are delivered via the CLI.

To improve the transparency of the installation, the VPN Client software setup also lets you add specific CLI commands to customize the software setup installation. For more information, see *Software Setup Command Reference* on page 129.

Create a Silent VPN Client Software Setup

1. Download the vpn_client.exe setup file or copy it from the installation CD.
2. Open a command window, and enter the following software setup commands:

```
[software path]setup.exe /S --lang=1036 --license=123456789 --start=1 /D=[install
path] [CLI commands]
```

`[software path]` is the path to the setup software file.

`[install path]` is the path to the directory where the setup software file is installed.

`[CLI commands]` are the optional CLI commands that you can add.

The following is a syntax example of this software setup:

```
C:\Users\bob\Downloads\NETGEARVPNClientPro_Setup.exe /S --lang=1036 --license=
123456789 --start=1 /D=c:\Program Files\NETGEAR\NETGEAR VPN Client Professional
```

Note: The directory that is specified after the `/D` switch must specify the path entirely. This switch does not recognize a relative directory. The `/D` switch must be the last switch in the command line.

Note: You must specify a software setup command that requires a parameter without a space between the command and the parameter. Quotation marks are required if the parameter contains spaces. However, if there are spaces in the installation path `[install path]`, quotation marks are not required.

Deploy a VPN Client Setup Software From a CD-ROM

1. Create a silent VPN Client software setup.
2. Create an autorun file by creating a text file and saving it as **autorun.inf**. Upon CD-ROM insertion, this autorun file is used by the operating system to automatically run the VPN Client software installation.
3. Place the following content in the autorun.inf file:

```
[autorun]
OPEN=[cdpath\]VPN_Client.exe /S /D=[install path] [optional CLI commands]
ICON=[cdpath\]VPN_Client.exe
```

   `[install path]` is the path to the directory where the setup software file is installed.

   `[CLI commands]` are the optional CLI commands that you can add.

4. Copy the content of the setup directory and the autorun.inf file to the root directory of the CD-ROM.

The following is a syntax example of this software setup:

```
[autorun]
OPEN=VPN_Client.exe /S --start=1 --lang=1036 --license=123456789 /D=c:\Program
Files\NETGEAR\NETGEAR VPN Client Professional
ICON=VPN_Client.exe
```

Run a VPN Client Software Setup From a Shortcut (Double-Click on an Icon)

1. Create a silent VPN Client software setup.
2. Right-click on the **setup.exe** file in the setup directory, and from the pop-up menu, select **Create Shortcut**. A shortcut to the setup.exe file in the setup directory is created.
3. Right-click on the new shortcut, and from the pop-up menu select **Properties**. In the **Target** field, add the following software setup commands to the command line:

```
/S --start=1 --lang=1036 --license=123456789 /D=[install path]
```

   `[install path]` is the path to the directory where the setup software file is installed.

The following is a syntax example of this software setup:

```
C:\Users\bob\Downloads\NETGEARVPNClientPro_Setup.exe /S --lang=1036 --license=
123456789 --start=1 /D=C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
```

IMPORTANT:

Place space characters between each command as is shown in the example.

4. Move the shortcut to a location where it can be easily clicked by the user (for example, on the desktop).

Deploy a VPN Client Software Setup Using a Batch Script

1. Create a silent VPN Client software setup.
2. Create a text file with a **.bat** extension, for example VPN Client Setup.bat.
3. Edit this file (that is, right-click on the file and select **modify**) with the commands that you want to be processed, for example:

```
cd .\setup
setup.exe /S –-lang=1036
cd ..
copy myvpnconfig.tgb C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
cd C:\Program Files\VPN
vpnconf.exe /importance:myvpnconfig.tgb
```

In this example, the setup directory is called *setup* and is located under the directory that contains the batch file; a VPN configuration is imported at the end of the installation.

4. Deploy this file from a server or on an USB stick together with the setup directory to the users.

Deploy a VPN Client Software Setup From a Network Drive

1. Create a silent VPN Client software setup on a network drive.
2. Right-click on the **setup.exe** file in the setup directory, and from the pop-up menu, select **Create Shortcut**. A shortcut to the setup.exe file in the setup directory is created.
3. Right-click on the new shortcut, and from the pop-up menu, select **Properties**. In the Target field, add the following software setup commands to the command line:

```
/S --start=1 --lang=1036 --license=123456789 /D=[install path]
```

`[install path]` is the path to the directory where the setup software file is installed.

The following is a syntax example of this software setup:

```
F:\NETGEARVPNClientPro_Setup.exe /S --start=1 --lang=1036 --license=123456789 /D=
C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
```

IMPORTANT:

Place space characters between each command as is shown in the example.

4. Move the shortcut to a location where it can be easily clicked by the user (for example, on the desktop).

Deploy a VPN Client Software Update

To deploy a VPN Client software update, you only need to launch the silent installation for the new software release. The entire uninstallation of the old software release and installation of the new software release is silent; no user action is required.

Customize VPN Client Software for End Users

End users can access the VPN Client in three ways:

- By opening the Configuration Panel screen. This screen is typically used by network administrators and can be hidden or protected by a password.
- By opening the Connection Panel screen. This screen lets the end user open and close tunnels and view simple warning messages about VPN connection problems. You can hide this screen,
- By right-clicking the system tray menu. With the exception of the tunnels (these are always show), you can hide most menu items of the system tray menu.

These access methods enable the administrator to hide the configuration options from the end user to prevent misuse of the VPN configuration, and to present the end user with simple access to the VPN Client and VPN tunnels.

Note: The VPN configuration is signed and encrypted. Manual editing of the file disables the VPN configuration.

The VPN Client software setup options that enable you to limit access to the VPN Client's configuration options are described in the following sections.

Limit Usage of the VPN Client to the Connection Panel

1. Open the VPN Client's user interface.
2. On the Configuration Panel screen, select **View** > **Configuration** from the main menu. The Configuration screen displays.
3. In the **Password** and **Confirm** fields, enter and then confirm a password.
4. As an option, you can limit the number of items that display in the system tray menu.
5. Enter **Ctrl + Enter** to switch to the Connection Panel screen.
6. As an option, close the Connection Panel screen.

Now, only the Connection Panel screen is displayed when you open the software (that is, when you click on the system tray icon). If an end user wants to open the Configuration Panel

screen by entering **Ctrl + Enter** or by clicking the **Configuration** link on the Connection Panel screen, the password is automatically requested.

For more information, see *Access Control and Hidden Interface* on page 26

Specify Display of the Connection Panel Screen in a VPN Client Software Setup

To specify display of the Connection Panel screen, add the **`--guidefs=user`** software setup command to the command line.

The following is a syntax example of this software setup:

```
NETGEARVPNClientPro_Setup.exe /S --guidefs=user /D=C:\Program Files\NETGEAR\NETGEAR VPN
Client Professional
```

After you have installed the VPN Client and rebooted the computer, the VPN Client starts up and displays the Connection Panel screen.

Limit Usage to the Connection Panel Screen in a VPN Client Software Setup

To limit usage to the Connection Panel screen and protect access to the Configuration Panel screen with a password, add the **`--guidefs=user --password=mypassword`** software setup commands to the command line.

`mypassword` is the specified password.

The following is a syntax example of this software setup:

```
NETGEARVPNClientPro_Setup.exe /S --guidefs=user --password=group2 /D=C:\Program
Files\NETGEAR\NETGEAR VPN Client Professional
```

After you have installed the VPN Client and rebooted the computer, the VPN Client starts up and displays the Connection Panel screen, and access to the Configuration Panel screen is protected by a password.

Limit Usage of the VPN Client to the System Tray Icon Menu in a VPN Client Software Setup

To limit usage to the system tray icon menu and protect access to both the Connection Panel screen and Configuration Panel screen with a password, add the **`--guidefs=hidden --password=mypassword`** software setup commands to the command line.

`mypassword` is the specified password.

The following is a syntax example of this software setup:

```
NETGEARVPNClientPro_Setup.exe /S --guidefs=user --password=group2 /D=C:\Program
Files\TheGreenBow\TheGreenBow VPN
```

After you have installed the VPN Client and rebooted the computer, the VPN Client starts up with access to the system tray menu only, and access to both the Connection Panel screen and Configuration Panel screen is protected by a password. You can open and close tunnels from the system tray menu.

VPN Configuration Deployment

The VPN Client software setup lets you embed a preconfigured VPN configuration that is automatically used by the VPN Client during the installation process.

Embed a VPN Configuration in the VPN Client Software Setup

1. Create a VPN configuration. You can do this any computer on which the VPN Client is installed.
2. Export the VPN configuration (by selecting **File** > **Export VPN Configuration** from the main menu on the Configuration Panel screen), and rename your configuration, for example to **conf.tgb**.

> **Note:** Do not protect the exported VPN configuration with a password.

3. Add the VPN configuration (that is, the conf.tgb file) to the directory in which you intend to place the software setup file on the target computer. If you intend to use the software setup files on a USB drive, copy the VPN configuration onto the USB drive together with the software setup file.
4. Deploy the package to the user and execute the setup. The VPN configuration (that is, the conf.tgb file) is automatically imported during the software setup process.

Export and Deploy a New VPN Configuration

To create a VPN Client software setups with an embedded VPN configuration

1. Create a VPN configuration. You can do this any computer on which the VPN Client is installed.
2. Export the VPN configuration (by selecting **File** > **Export VPN Configuration** from the main menu on the Configuration Panel screen), and rename your configuration, for example to **conf.tgb**. You *can* protect this exported VPN configuration with a password.
3. Forward the VPN configuration to the end user, either by email or through file-sharing.

   When the end user opens the VPN configuration (for example, the end user opens the email attachment), the VPN configuration is automatically imported and applied by the VPN Client. If you have specified a password, it is automatically requested and must be entered by the end user before the VPN configuration is processed.

VPN Automations

Create a Batch or Script That Automatically Opens or Closes a Tunnel

You can open or close a VPN tunnel through a CLI command, also when the VPN Client is running.

- To open a VPN tunnel, enter the following CLI command:

  `[path]\vpnconf.exe /open:[NamePhase1-NamePhase2]` in which `[path]` is the VPN Client installation directory, and `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

  If the specified tunnel is already open, the CLI command has no effect.

- To close a VPN tunnel, enter the following CLI command:

  `[path]\vpnconf.exe /close:[NamePhase1-NamePhase2]` in which `[path]` is the VPN Client installation directory, and `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

  If the specified tunnel is already closed, the CLI command has no effect.

The `open` and `close` commands are mutually exclusive.

Note: When you enter the `open` or `close` command, the user interface opens. This restriction will be removed in a future software release.

Automatically Open a Web Page When a VPN Tunnel Opens

1. Create a VPN configuration.
2. In the Phase 2 (IPSec Configuration) window of the Configuration Panel screen, click **Scripts**. The Script Configuration screen displays (see *Figure 43* on page 56).
3. In the **Launch this script when this tunnel opens** field, enter the URL of the Web page that you want to be opened, for example, **http://kb.netgear.com/app/products/list/p3/315**.
4. Click **OK** to save the settings.

When the tunnel for which the script is defined opens, the Web page is opened.

Open a Tunnel With a Double-Click on a Desktop Icon

1. Create a VPN configuration.
2. In the Phase 2 (Authentication) window of the Configuration Panel screen, click **P2 Advanced ...**.The Phase 2 Advanced screen displays (*Figure 41* on page 54).

3. Select the **Automatically open this tunnel when the VPN Client starts after login** check box.
4. Export the VPN configuration to a file by selecting **File** > **Export VPN Configuration** from the main menu on the Configuration Panel screen.
5. Place a shortcut of the VPN configuration file on the desktop.

When you double-click (open) desktop icon, the VPN Client opens with the specified VPN configuration, and the tunnel is then automatically opened.

Software Setup Command Reference

The following table lists the software setup switches and commands that are available to customize the VPN Client software setup.

Note: The software setup command that are described in this section must be used together with the `/S` switch (silent mode installation, case-sensitive).

Note: You must specify a software setup command that requires a parameter without a space between the command and the parameter. Quotation marks are required if the parameter contains spaces. However, if there are spaces in the installation path `[install path]`, quotation marks are not required.

Table 21. Software Setup Switches and Commands

Switch or Command	Description
`/D=[install path]`	`[install path]` is the path where the VPN Client must be installed. **Note:** `D` must be preceded by only one slash and is case-sensitive. Quotation marks are not allowed, even if there is a space in the path. **Note:** `/D` must be placed at the end of the command line, as the last option, and you muse it with the `/S` option (silent mode).
`/S`	Enables a silent installation (no dialogs are displayed during the installation). **Note:** `S` must be preceded by only one slash and is case-sensitive. **Example**: `NETGEARVPNClientPro_Setup.exe /S`

Table 21. Software Setup Switches and Commands (Continued)

Switch or Command	Description
`--activmail=[activation_email]`	Lets you configure and automatically enter the email that is used for activation confirmation. During the activation process, the field that is used to enter the email is disabled. `[activation_email]` is the email that is required for activation. **Note:** `activmail` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --activmail= salesgroup@company.com`
`--autoactiv=1`	Activates the VPN Client automatically when the network is available during startup or when there is a request to open a tunnel. This option requires that the license number and activation email have already been entered in a previous installation. **Note:** `--autoactiv=1` must be the last command in the command line. **Note:** `autoactiv=1` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --autoactiv=1`
`--guidefs=[full|user|hidden]`	Configures the user interface appearance when the VPN Client starts. • **full**. The Configuration Panel screen is displayed. This is the default setting. • **user**. The Connection Panel screen is displayed. • **hidden**. Neither the Configuration Panel screen nor the Connection Panel screen are displayed. Only the system tray menu can be opened. Tunnels can be opened from the system tray menu. **Note:** `guidefs` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --guidefs=hidden`

Table 21. Software Setup Switches and Commands (Continued)

<table>
<tr><th>Switch or Command</th><th colspan="3">Description</th></tr>
<tr><td rowspan="23"><code>--lang=[language code]</code></td><td colspan="3">Specifies the language for the software setup and for the VPN Client.
<code>[language code]</code> is the code for the language. The codes are shown in the following roes in this table.

Note: <code>lang</code> must be preceded by two dashes (<code>--</code>).

Example:
<code>NETGEARVPNClientPro_Setup.exe --lang=1040</code></td></tr>
<tr><td>ISO 639-2 Code</td><td>Language Code</td><td>English Name</td></tr>
<tr><td>EN</td><td>1033 (default)</td><td>English</td></tr>
<tr><td>FR</td><td>1036</td><td>French</td></tr>
<tr><td>ES</td><td>1034</td><td>Spanish</td></tr>
<tr><td>PT</td><td>2070</td><td>Portuguese</td></tr>
<tr><td>DE</td><td>1031</td><td>German</td></tr>
<tr><td>NL</td><td>1043</td><td>Dutch</td></tr>
<tr><td>IT</td><td>1040</td><td>Italian</td></tr>
<tr><td>ZH</td><td>2052</td><td>Chinese simplified</td></tr>
<tr><td>SL</td><td>1060</td><td>Slovenian</td></tr>
<tr><td>TR</td><td>1055</td><td>Turkish</td></tr>
<tr><td>PL</td><td>1045</td><td>Polish</td></tr>
<tr><td>EL</td><td>1032</td><td>Greek</td></tr>
<tr><td>RU</td><td>1049</td><td>Russian</td></tr>
<tr><td>JA</td><td>1041</td><td>Japanese</td></tr>
<tr><td>FI</td><td>1035</td><td>Finnish</td></tr>
<tr><td>SR</td><td>2074</td><td>Serbian</td></tr>
<tr><td>TH</td><td>1054</td><td>Thai</td></tr>
<tr><td>AR</td><td>1025</td><td>Arabic</td></tr>
<tr><td>HI</td><td>1081</td><td>Hindi</td></tr>
</table>

Table 21. Software Setup Switches and Commands (Continued)

Switch or Command	Description
`--license=[license_number]`	Lets you configure and automatically enter the license number that is used for activation. `[license_number]` is the license number that consists of 24 hexadecimal characters. **Note:** `license` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --license= 1234567890ABCDEF12345678`
`--menuitem=[0...31]`	Specifies the items of the system tray menu that are visible. The value is a bit field: • **1**. Quit menu item displays. • **2**. Connection Panel menu item displays. • **3**. Quit and Connection Panel menu items display. • **4**. Console menu item displays. • **5**. Quit and Console menu items display. • **8**. Save & Apply menu item displays. • **16**. Configuration Panel menu item displays. • **31**. All menus display. This is the default setting. **Note:** Tunnels are always shown in the system tray menu and can always be opened and closed from the system tray menu. **Note:** By default, `--guidefs=hidden` sets the system tray menu item list to Quit and Console (that is, the Save & Apply and Connection Panel menu items are not visible). However, `--menuitem` overrides `--guidefs`. That means that when you enter **`--guidefs=hidden --menuitem=1`**, the system tray menu shows the Quit menu item only. **Note:** `menuitem` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --menuitem=3`
`--noactiv=1`	Prevents the Trial screen from displaying when the VPN Client starts until the trial period ends. A user other than the administrator does not know about the trial period and the VPN Client is disabled at the end of the trial period. If a user attempts to launch the VPN Client after the end of trial period, the VPN Client starts and opens the Trial screen but the **Evaluate** button is disabled. **Note:** `noactiv=1` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --noactiv=1`

Table 21. Software Setup Switches and Commands (Continued)

Switch or Command	Description
`--password=[password]`	Protects the user interface or a protected screen of the user interface. `[password]` is the password that you must enter to gain access under the following circumstances. • when you click or double-click on the VPN system tray icon. • when you want to switch from the Connection Panel screen to the Configuration Panel screen. **Note:** `password` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --password=adm253q`
`--start=[1|2]`	Configures the start mode for the VPN Client. These are the options: • **1**. The VPN Client starts after Windows login. This is the default setting. • **2**. THe VPN Client must be started manually. **Note:** `start` must be preceded by two dashes (`--`). **Example**: `NETGEARVPNClientPro_Setup.exe --start=2`

Command-Line Interface Command Reference

The following table lists the command-line interface (CLI) commands that are available to customize the VPN Client software setup.

You can use command-line interface (CLI) commands to customize the VPN Client software setup. Use CLI commands in batch files, in scripts, or in software setup autorun.inf files.

The following is the standard syntax for CLI commands:

```
[install_directory]\vpnconf.exe [/option[:value]]
```

`[install_directory]` is the installation directory of the VPN Client software files.

`[/option[:value]]` are the CLI command and argument. If the argument contains space characters, place the argument between double quotes.

The following table lists the CLI commands that are available to customize the VPN Client software setup.

Table 22. CLI Commands

Command	Description
`/add:[ConfigFileName]`	Imports a new VPN configuration into an existing VPN configuration and merges both into a single VPN configuration, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running. `[ConfigFileName]` is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** This command can replace the `/importonce:` command. **Example**: `vpnconf.exe /add:"c:\my documents\myvpnconf.tgb"`
`/close:[NamePhase1-NamePhase2]`	Closes a specified VPN tunnel. `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file. **Example**: vpnconf.exe /close:"Home gateway-cnx1" **Note:** In the example, the `Home gateway-cnx1` VPN configuration is placed in between double quotes because there is a space character in the name.
`/export:[ConfigFileName]`	Exports the current VPN configuration (including certificates) to the specified file and starts the VPN Client if it is not already running. If the VPN Client is running, the VPN configuration is exported without stopping VPN Client. `[ConfigFileName]` is the file name of file to which the VPN configuration is exported. Enclose this name in double quotes if it contains space characters. This command requires you to also specify a password with the `/pwd:` command. **Example**: `vpnconf.exe /export:"c:\my documents\myvpnconf.tgb"`
`/exportonce:[ConfigFileName]`	Exports the current VPN configuration (including certificates) to the specified file when the VPN Client is not running and does not start the VPN Client. If the VPN Client is running, the VPN configuration is exported without stopping VPN Client. `[ConfigFileName]` is the file name of file to which the VPN configuration is exported. Enclose this name in double quotes if it contains space characters. This command requires you to also specify a password with the `/pwd:` command. **Example**: `vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb"`

Table 22. CLI Commands (Continued)

Command	Description
`/import:[ConfigFileName]`	Enables the VPN Client to import a VPN Configuration. If the VPN Client is not running, the VPN configuration is imported and the VPN Client is automatically started. If the VPN Client is running, the VPN configuration is imported without stopping VPN Client. `[ConfigFileName]` is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** To prevent the end user from being asked if the new VPN configuration should be added to or replace the existing VPN configuration, enter the **`/add:`** or **`/replace:`** command instead of the **`/import:`** command. **Example**: `vpnconf.exe /import:"c:\my documents\myvpnconf.tgb"`
`/importonce:[ConfigFileName]`	Imports a VPN configuration file when the VPN Client is *not* running and does not start the VPN Client. If the VPN Client is running, the VPN configuration is imported without stopping VPN Client. This command is useful in installation scripts: it allows you to run a silent installation and to automatically import a VPN configuration file without starting the VPN Client. `[ConfigFileName]` is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** To prevent the end user from being asked if the new VPN configuration should be added to or replace the existing VPN configuration, enter the **`/add:`** or **`/replace:`** command instead of the **`/importonce:`** command. **Example**: `vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb"`
`/open:[NamePhase1-NamePhase2]`	Opens a specified VPN tunnel. `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file. **Example**: `vpnconf.exe /open:Corporate-gateway1`

Table 22. CLI Commands (Continued)

Command	Description
`/pwd:[Password]`	Enables you to set a password for import and export operations. `[Password]` is the password that you must enter to enable the command with which the `/pwd:` command is combined. The `/exportonce:` and `/exportonce:` commands require you to set a password. A password is optional for the `/import:`, `/importonce:`, `/add:`, and `/replace:` commands. **Note:** You must place the `/pwd:` command *after* the other command that you combine the `/pwd:` command with. **Example**: `vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd=mypwd`
`/replace:[ConfigFileName]`	Imports a new VPN configuration into an existing VPN configuration and replaces the old configuration with the new one, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running. `[ConfigFileName]` is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** This command can replace the `/importonce:` command. **Example**: `vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb"`
`/stop:`	Closes all active tunnels and closes the VPN Client. Use this command, for example, in a script that starts the VPN Client after establishing a dial-up connection and closes it just before disconnecting the dial-up connection. **Example**: `vpnconf.exe /stop`

Generating Certificates With Microsoft Certificates Services and OpenSSL

B

This appendix is an extension *Certificate Management* on page 64. This appendix includes the following sections:

- *Microsoft Certificates Services* on this page
- *OpenSSL* on page 146

Note: The information in this chapter is typically used by network administrators.

Note: For information about how to import and display certificates, see *Certificate Management* on page 64.

Microsoft Certificates Services

This section describes how to generate a user certificate, sign a certificate signing request (CSR), and export a certificates using Microsoft certificates services.

Install Microsoft Certificate Services

Microsoft certificate services comes as a part of the Windows NT, Windows 2000, and WIndows 2003 server option pack and requires Microsoft Internet Information server (IIS) and Microsoft Internet Explorer (IE).

The enrollment Web pages that are provided by the certificate cervices let you connect to the services with a Web browser and perform common tasks such as requesting the certification authority (CA) and processing a CSR file or Smart Card enrollment file. The Web pages are located at http://ServerName/CertSrv, in which ServerName is the name of the CA.

The following Microsoft Web pages provide information about certificate services:

- Windows 2000 server:
  http://technet.microsoft.com/en-us/library/cc961642.aspx
- Windows 2003 server:
  http://technet.microsoft.com/en-us/library/cc780742(WS.10).aspx
- Windows 2008 server (Active Directory certificate services):
  http://technet.microsoft.com/en-us/library/cc770357(WS.10).aspx

To install the Internet Information Server (IIS 6.0):

1. In Windows, select **Start** > **Control Panel** > **Add or Remove Programs** > **Add/Remove Windows Components** (in the left column of the Add or Remove Programs screen).
2. Select **Application Server**, and click **Details**.
3. Select **Internet Information Services (IIS)**, and click **Details**.
4. Select the **World Wide Web Service** check box, and click **OK**.
5. Click **OK** on the Application Server screen.
6. Click **Next** on the Windows Components Wizard screen.
7. Click **Finish** on the Completing the Windows Components Wizard screen.

To install the Microsoft Certificate Server with a standalone root CA on a Windows 2003 server:

1. In Windows, select **Start** > **Control Panel** > **Add or Remove Programs** > **Add/Remove Windows Components** (in the left column of the Add or Remove Programs screen).
2. Select **Certificate Services**, and click **Details**.
3. Select both the **Certificate Services CA** and **Certificate Services Web Enrollment Support** check boxes, and click **OK**.
4. Click **Next** on the Windows Components Wizard screen.
5. Configure the CA type by selecting the **Stand-alone root CA** radio button and the **Use custom settings to generate the key pair and CA certificate** check box as shown in the following figure, and then click **Next**.

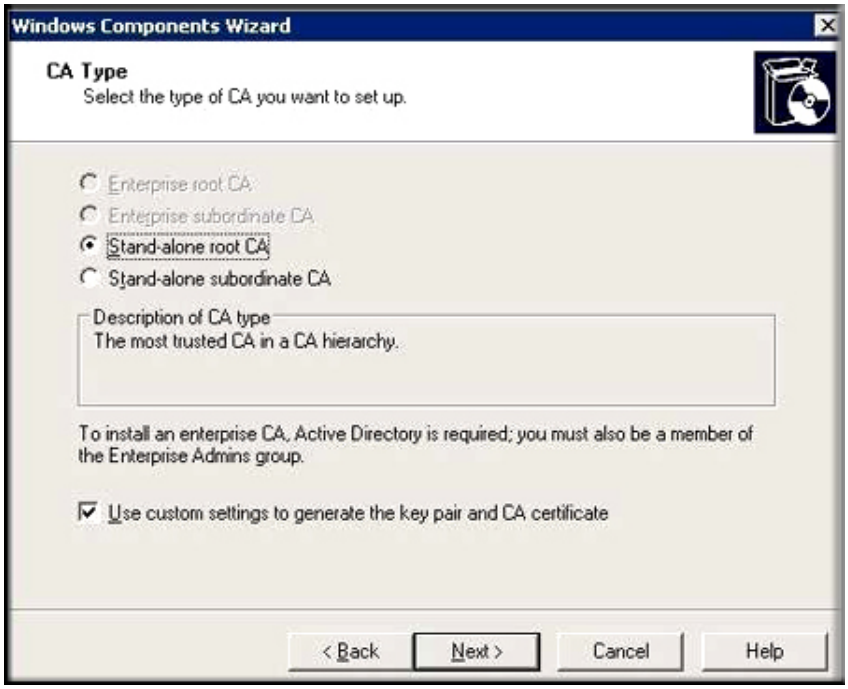


Figure 86.

6. Configure the public and private key pair by selecting **Microsoft Strong Cryptographic Provider** from the **CSP** drop-down list, **SHA-1** from the **Hash algorithm** drop-down list, and **1024** from the **Key length** drop-down list as shown in the following figure, and then click **Next**.

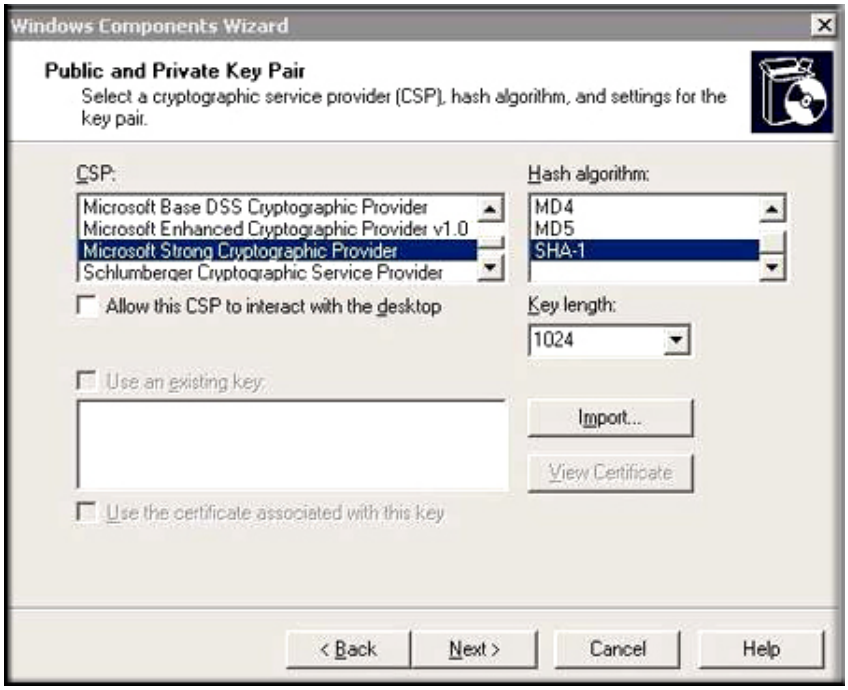


Figure 87.

7. Configure the CA identifying information by entering a common name (**TgbCA** in the example) and distinguished name suffix (**DC=TheGreenBow,DC-fr** in the example) and by selecting a validity period (**10 Years** in the example) as shown in the following figure, and then click **Next**.

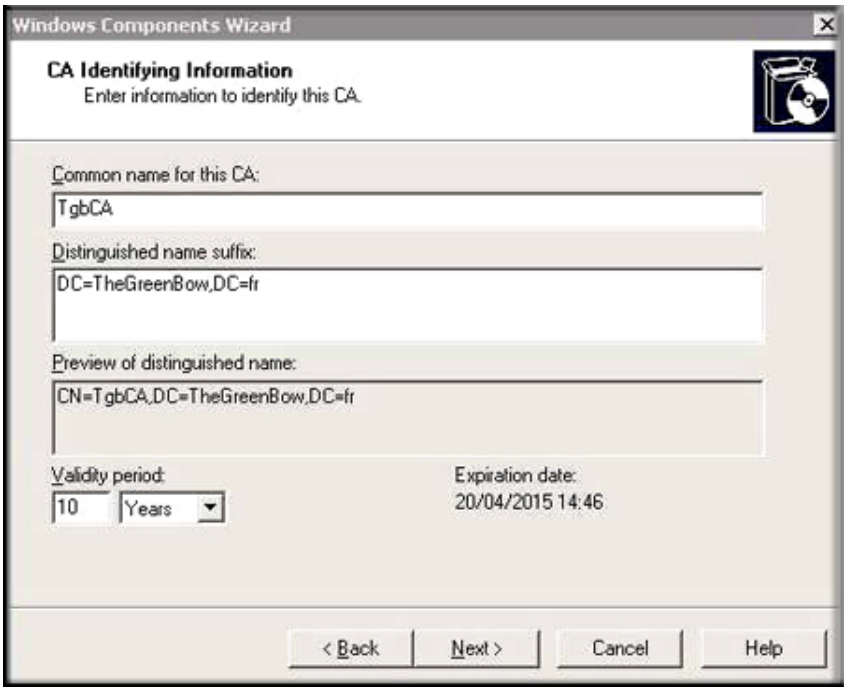


Figure 88.

8. On the Certificate Database Settings screen, use the default locations for the **Certificate Database** and **Certificate Database Log**. You do not need to specify a shared folder to store configuration information because this information is stored in the Active Directory. Click **Next**.
9. Click **Yes** on the Microsoft Certificate Services warning screen to confirm that Internet information services can be stopped temporarily.
10. Click **Yes** on the Microsoft Certificate Services warning screen to confirm that Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) if you want to use the certificate services Web enrollment site.
11. Click **Finish** on the Completing the Windows Components Wizard screen.
12. Close the Add or Remove Programs screen.

Generate a User Certificate With Microsoft Certificates Services

This section describes how to generate a user certificate for the VPN Client but also can be applied to any other VPN IPSec endpoint such as a VPN router.

To generate and install a user certificate:

1. Connect to your certificate server (http://ServerName/CertSrv in which ServerName is the name of the CA server).
2. Select **Request a Certificate** on the Welcome screen.
3. Select **Advanced Certificate Request** on the Request a Certificate screen.
4. Select **Create and submit a request to this CA** on the Advanced Certificate Request screen.
5. Fill in the fields of the Advanced Certificate Request screen, and select the **Mark keys as exportable** check box in the Key Options section because the VPN Client needs the certificate's private key to establish a tunnel. The following figure shows examples.

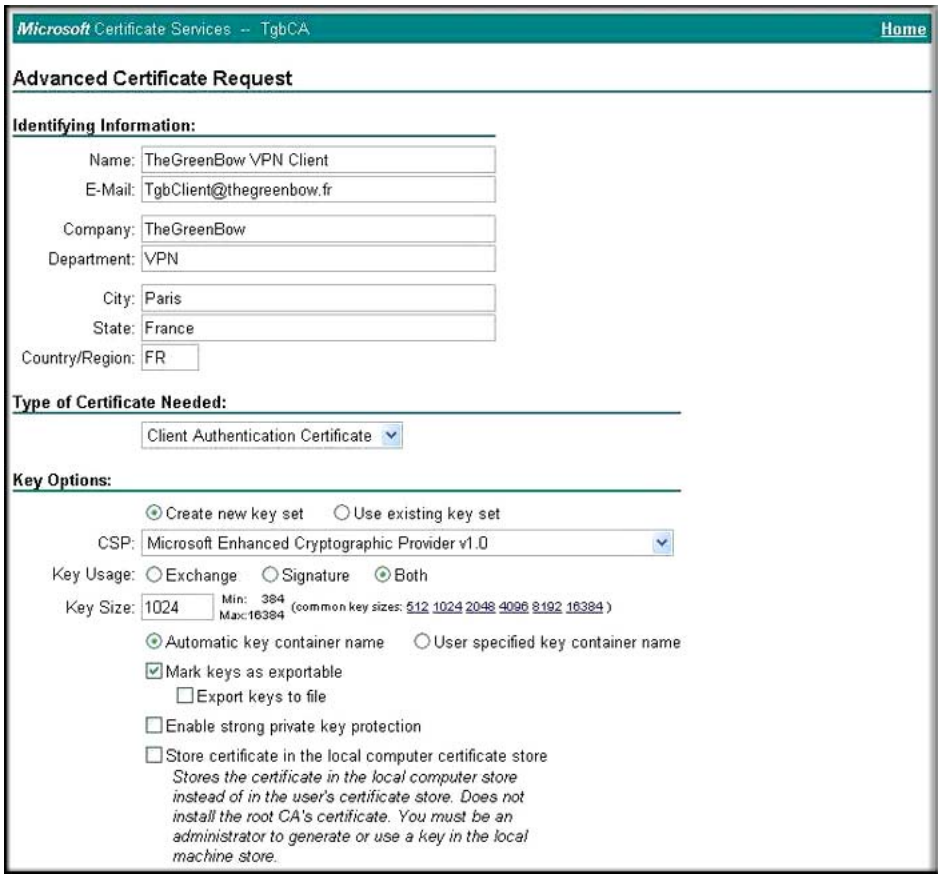


Figure 89.

6. Still on the Advanced Certificate Request screen, configure the additional options, for example, by selecting the **CMC** radio button and **SHA-1** from the **Hash Algorithm** drop-down list as shown in the following figure.

Figure 90.

7. Click **Submit**.

   After processing, the Certificate Pending screen displays. Wait until your request is accepted and validated by your Microsoft certificate services administrator.

   After the request has been validated and returned to you, you can view it on the Certificate Authority screen.

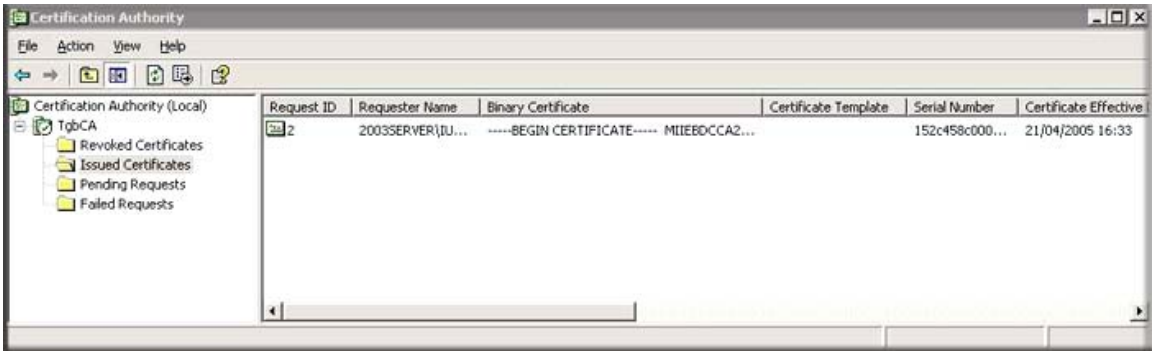


Figure 91.

8. To retrieve the certificate, return to the Microsoft Certificate Services screen, and click **View the status of a pending Certificate Request**.
9. On the View the Status of a Pending Certificate Request screen, select the certificate request that you want to view. The Certificate Issued screen displays.

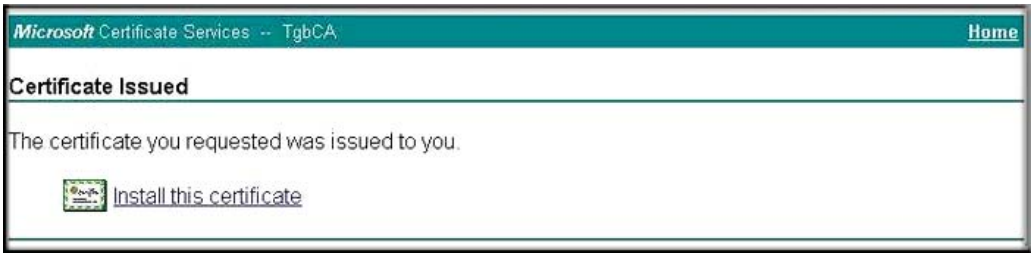


Figure 92.

10. Click **Install this certificate** to add the certificate to your local certificates stores, and click **Yes** on the Root Certificate Store warning screen.

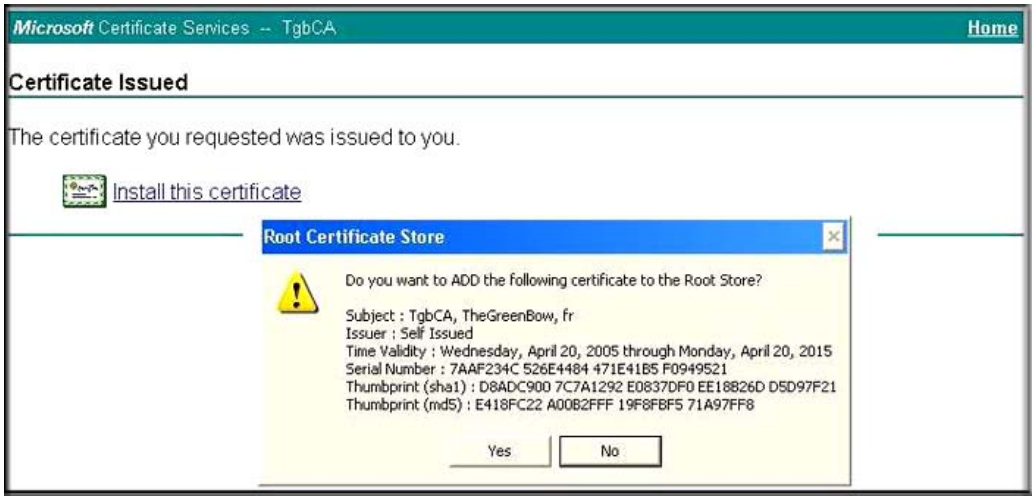


Figure 93.

11. After processing the **Certificate Installed** page appears confirming the Certificate successful installation in the Internet Explorer Certificate store.

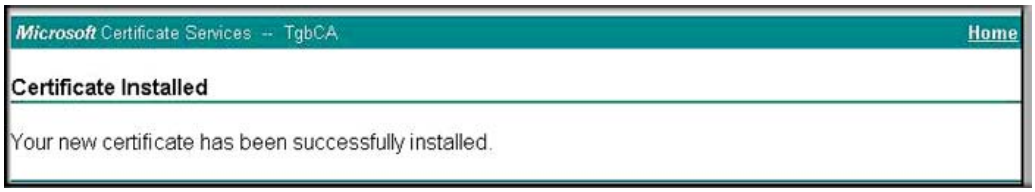


Figure 94.

To export a certificate from the Internet Explorer certificate store, see *Export Certificates* on page 144.

Sign a Certificate Request

To sign a certificate request using Microsoft Certificate Services:

1. Connect to your certificate server (http://ServerName/CertSrv in which ServerName is the name of the CA server).
2. Select **Request a Certificate** on the Welcome screen.
3. Select **Advanced Certificate Request** on the Request a Certificate screen.
4. Select **Submit a Certificate Request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7** file.
5. Click **Browse for a file to insert**, locate the certificate request file, and then click **Read!**. The Submit a Certificate Request or Renewal Request screen displays.

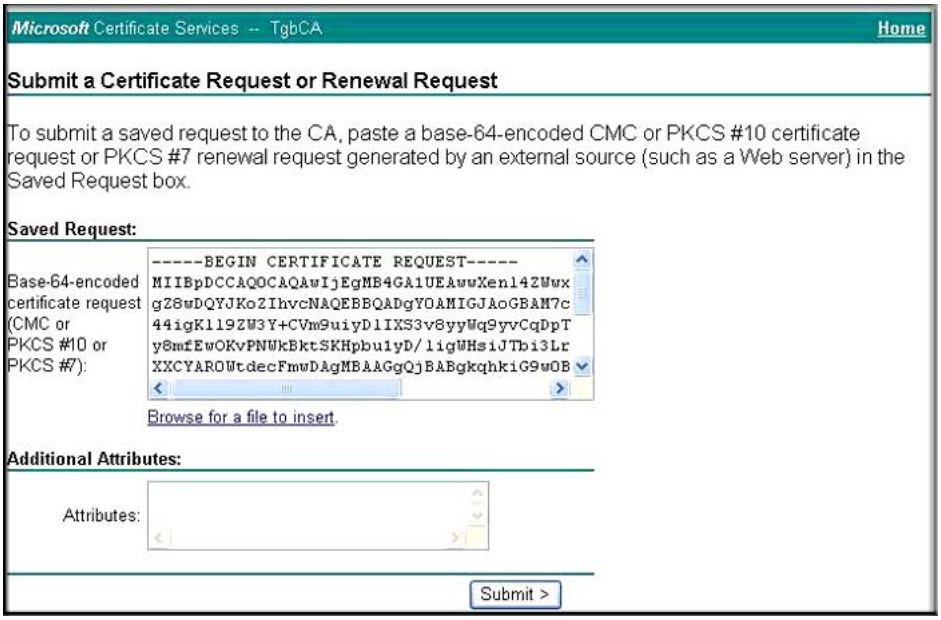


Figure 95.

6. Click **Submit**. After processing, the Certificate Pending screen displays. Wait until your request is accepted and validated by your Microsoft certificate services administrator.
7. To retrieve the certificate, return to the Microsoft Certificate Services screen, and click **View the status of a pending Certificate Request**.
8. On the View the Status of a Pending Certificate Request screen, select the certificate request that you want to view. The Certificate Issued screen displays.

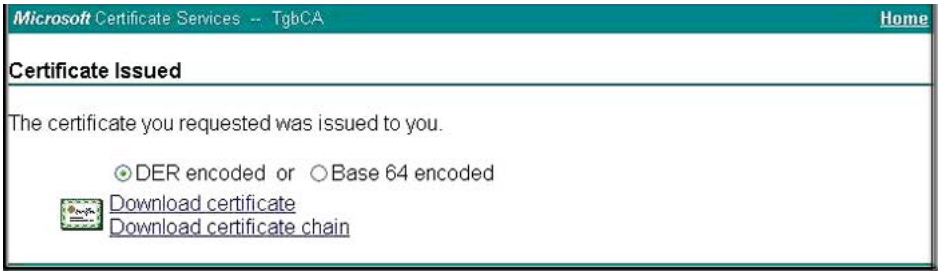


Figure 96.

9. Click **Download certificate**. A file download screen displays. Click **Save** to save the file. The default file name is certnew.cer.

Export Certificates

After a certificate has been installed in the Internet Explorer Certificate Store, you can export it in the PKCS12 file format.

To export a certificate from the Internet Explorer Certificate Store:

1. Open Internet Explorer.

2. Select **Tools** > **Internet Options** from the menu.
3. Select the **Content** tab, and then click **Certificates**.
4. On the Certificates screen, click the **Personal** tab, and select the certificate that you want to export.

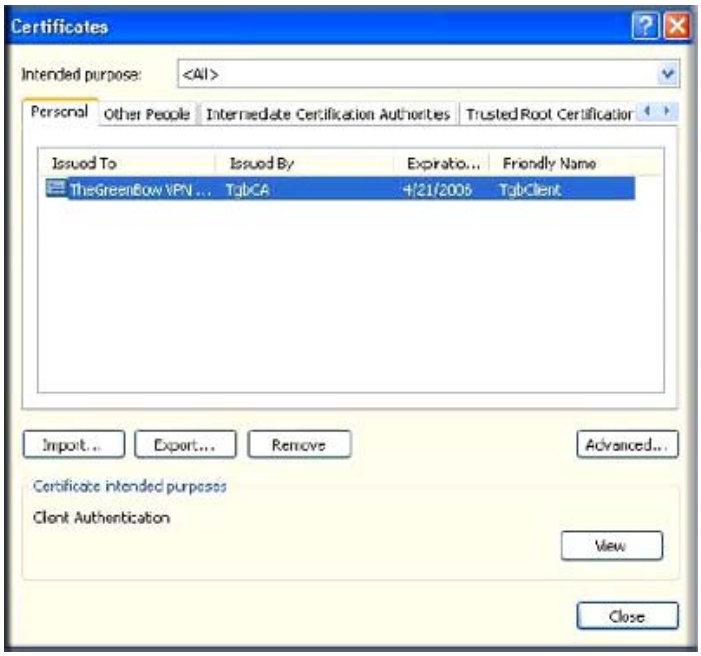


Figure 97.

5. Click **Export…**. The Certificate Export Wizard displays.
6. Click **Next**.
7. Select the **Yes, export the private key** radio button.

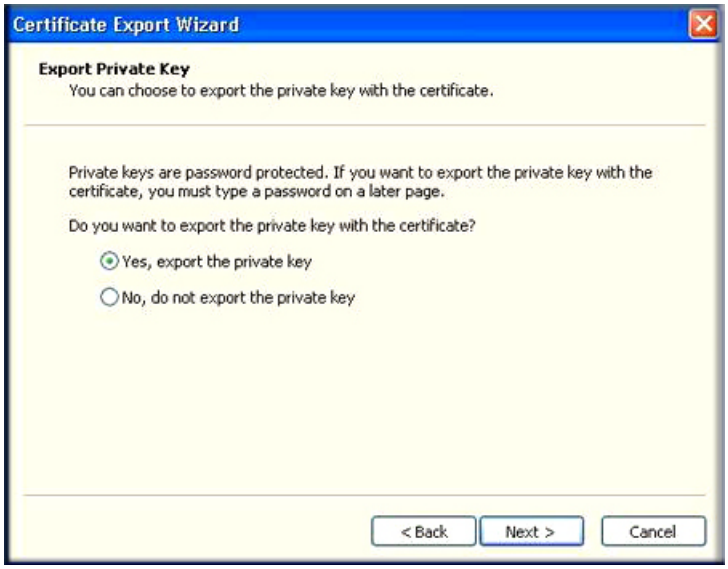


Figure 98.

8. Click **Next**.
9. Select the **Personal Information Exchange - PKCS #12 (.PFX)** radio button and the **Include all certificates in the certification path if possible** check box. The root CA is also exported.

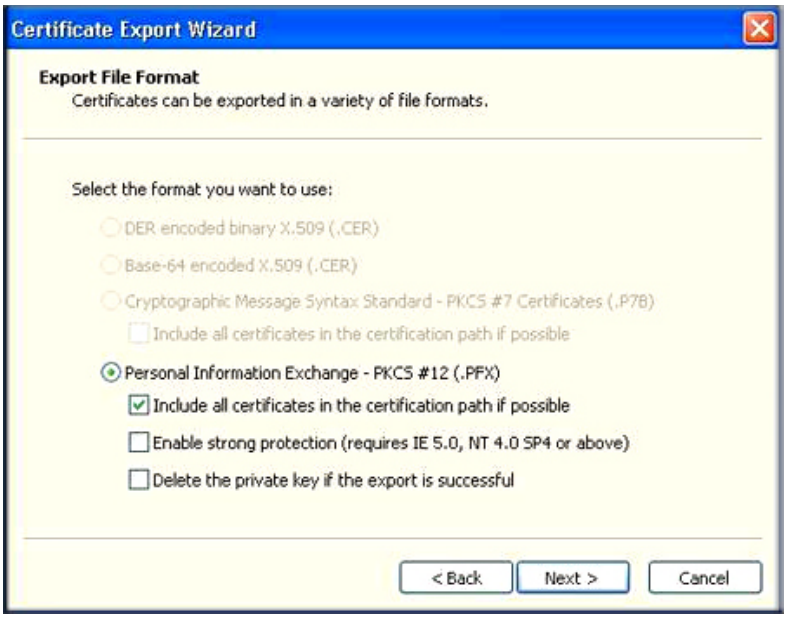


Figure 99.

10. Click **Next**.
11. On the Password screen, enter and confirm your password, and then click **Next**.
12. On the File to Export screen, specify the destination file path, and then click **Next**.
13. On the Completing the Certificate Export Wizard screen, click **Finish**.

OpenSSL

OpenSSL is a free noncommercial toolkit that provides a wide range of cryptographic operations. It also includes utilities for certificate management. You can find information about building and using OpenSSL at *http://www.openssl.org*.

The OpenSSL program is a command-line tool. You can download several batch scripts for certificate generation and management by downloading the TgbSmallPKI.zip file at *http://www.thegreenbow.fr/bin/tgbvpn_smallpki.zip*. Unzip this file, for example to the root of your hard drive. After unzipping, the TgbSmallPKI folder contains the following batch scripts a Bin folder, and readme text file:

- **RootCA.bat**. Generates a self-signed root certificate.
- **UserCA.bat**. Generates a user certificate signed by the root certificate.
- **Pkcs12.bat**. Converts a P12 file into PEM files.
- **CAinfo.bat**. Displays PEM certificate information.

- **CAsign.bat**. Signs a certificate request.
- The \Bin folder contains:
  - **openssl.cnf**. A large part of the information that is included in a certificate depends on the contents of this configuration file. This file is divided into sections to help you to make the configuration more modular. You can customize this file depending on your needs. For more information, see the OpenSSL documentation at *http://www.openssl.org*.
  - **openssl.exe**, **libeay32.dll**, and **ssleay32.dll** make up the core toolkit for Windows platforms.
- **ReadME.txt**. A documentation file.

Generate a Certificate With OpenSSL

This section explains how to generate a self-signed root certificate and user certificate, and how to sign a certificate request using OpenSSL for Windows.

Generate a Self-Signed Certificate

A self-signed certificate is a certificate that is not signed by a recognized certificate authority (CA). You can use a self-signed certificate to function as a CA that issues, renews, and revokes certificates.

To create a self-signed certificate, run the RootCA.bat batch script. The following is a sample output:

```
*
! Creating Root CA folders
*
Root CA folder set to .\RootCA
Root CA key length is 1024 bits
Root CA validity is 3650 days
The system cannot find the file specified.
*
! Creating CA private key (1024 bits, 3650 days)
*
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.........++++++++++++
e is 65537 (0x10001)
*
! CA autosigning (1024 bits, 3650 days)
*
Using configuration from .\Bin\openssl.cnf
You are about to be asked to enter information
that will be incorporated into your Certificate Request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:FR
State or Province Name (full name) [France]:France
```

```
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [TheGreenBow]:TheGreenBow
Organizational Unit Name (eg, section) []:Authority Certificate
Common Name (eg, YOUR name) []:TheGreenBow CA
Email Address []:TgbCA@thegreenbow.fr
Please enter the following 'extra' attributes
to be sent with your Certificate Request
A challenge password []:capassword
An optional company name []:TheGreenBow
Loading 'screen' into random state - done
Signature ok
subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=Authority Certificate/CN=TheGreenBow
CA/Email=TgbCA
@thegreenbow.fr
Getting Private key
"----------------------------"
"----------------------------"
Root Certificate at .\RootCA\RootCA.pem
Root Private Key at .\RootCA\CAKey.key
```

Note: The root certificate RootCA.pem and its private key CAKey.key are located in RootCA folder.

Generate a User Certificate

When you select X.509 certificate authentication in the phase 1 configuration (see *Phase 1 (Authentication) Configuration* on page 43), a user certificate is used to identify a VPN IPSec endpoint and to perform signature verification operations.

The UserCA.bat batch script generates a user certificate, its private key, and a PKCS12 file. It requires an intermediate folder as a parameter. You can use this script to generate a certificates for any VPN IPSec endpoint.

To generate all required files for the VPN Client, run the UserCA.bat batch script by entering **`UserCA TgbClient`**.

The following is a sample output:

```
*
! Creating User CA folder
*
Creating User Certificate folder at .\TgbClient
User CA key length is 1024 bits
User CA validity is 3650 days
*
! Creating User CA private key (1024 bits)
*
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.......++++++
...................++++++
e is 65537 (0x10001)
*
! Signing User CA
```

```
*
Using configuration from .\Bin\openssl.cnf
You are about to be asked to enter information that will be
incorporated into your Certificate Request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:FR
State or Province Name (full name) [France]:France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [TheGreenBow]:TheGreenBow
Organizational Unit Name (eg, section) []:VPN
Common Name (eg, YOUR name) []:TheGreenBow VPN Client
Email Address []:TgbClient@thegreenbow.fr
Please enter the following 'extra' attributes
to be sent with your Certificate Request
A challenge password []:tgbcapwd
An optional company name []:TheGreenBow
Loading 'screen' into random state - done
Signature ok
subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN
Client/Email=TgbClient@thegreenbow.fr
Getting CA Private Key
*
! User CA in P12 Format
*
Loading 'screen' into random state - done
Enter Export Password:
Verifying password - Enter Export Password:
TgbClient.p12 created in .\TgbClient.p12
"---------------------------"
"---------------------------"
User Certificate at .\TgbClient\TgbClient.pem
User Private Key at .\TgbClient\local.key
User Certificate Subject is:
subject= /C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN
Client/Email=TgbClient@thegreenbow.fr
```

After you have run the script, the following files are the most important ones in the TgbClient folder:

- **TgbClient.pem**. The user certificate.
- **Local.key**. The private key of the user certificate .
- **Subject.txt**. The subject of the user certificate.
- **TgbClient.p12**. A file in the PKCS12 format that contains the user and root certificates, and the private key of the user certificate.

Displaying Certificate Information Using TgbSmallPKI Tools

This section explains how to display certificate information and how to extract certificates and private keys from a file in PKCS12 file by using the following batch script files:

- **Pkcs12.bat**. Converts a P12 file into PEM files.
- **CAinfo.bat**. Displays PEM certificate information.

Displaying certificate information can be useful to retrieve information from several fields such as the Issuer, the Validity date, and the Subject fields.

The CAinfo.bat batch script displays the user certificate information. It requires a certificate file as a parameter.

To display more information about the TgbClient.pem file (which is the user certificate that was created in *Generate a User Certificate With Microsoft Certificates Services* on page 140), run the CAinfo.bat batch script by entering **`CAinfo TgbClient\TgbClient.pem`**.

The following is a sample output:

```
*
! Certificate TgbClient\TgbClient.pem information
*
Certificate:
  Data:
  Version: 1 (0x0)
  Serial Number: 1 (0x1)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=Authority Certificate, CN=
TheGreenBow CA
/Email=TgbCA@thegreenbow.fr
    Validity
      Not Before: Apr 19 12:44:03 2005 GMT
      Not After: Apr 17 12:44:03 2015 GMT
    Subject: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=VPN, CN=TheGreenBow VPN
Client/Email=TgbClient@thegreenbow.fr
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:ac:00:2c:1b:82:6d:32:2e:17:09:9f:13:8d:b9:
          9f:9b:db:d7:3f:f7:45:9b:f2:73:6d:8b:3d:9b:b1:
          14:99:25:22:fb:a8:56:30:9d:68:43:e9:14:84:6f:
          4c:24:fa:e2:36:84:56:2d:b2:5c:11:fd:be:b9:9e:
          ed:49:c8:c1:08:29:d0:17:ca:b8:12:41:41:55:4d:
          48:01:57:bc:22:9a:c9:48:ca:e2:c2:59:2c:78:8d:
          6d:cc:89:09:3a:97:f5:f4:b7:96:ea:da:82:0e:8c:
          87:49:a7:45:a4:74:45:31:8e:ac:be:9a:a2:8c:a1:
          16:be:f7:46:4a:94:78:31:73
        Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
  b2:ba:7c:92:9c:eb:59:c2:7e:d9:95:af:71:8b:06:2f:b8:44:
  b3:b5:2a:b7:98:0b:1e:08:97:85:c7:bc:21:1c:cf:df:15:97:
  d9:4f:e5:ec:31:14:6f:9e:b1:8a:47:37:ad:6b:4b:c8:15:bf:
  cd:8a:1b:ed:a5:f7:3e:ac:72:73:b9:bc:f6:22:b3:05:f5:26:
  40:dd:f8:4c:83:3f:25:da:68:32:8b:bd:1b:68:24:e8:df:31:
```

```
83:5b:74:91:10:1f:6a:d0:b9:3c:f3:04:50:4c:6e:ce:c9:de:
3a:38:fe:2d:ad:6c:6b:e6:74:38:51:0c:5b:c5:bb:6b:05:25:
44:d9
```

References and Useful Websites

C

These references and websites are for the ProSafe VPN Client Professional / Lite that is powered by TheGreenBow.

> **Note:** For documentation about the *legacy* ProSafe VPN Client that is powered by SafeNet, see the following NETGEAR knowledge base links.
> *http://kb.netgear.com/app/products/model/a_id/2543*
> *http://kb.netgear.com/app/products/model/a_id/2544*

- Access to VPNG01L product Information and a 30-day trial software version:

  http://kb.netgear.com/app/products/model/a_id/14552
- Access to VPNG05L product Information and a 30-day trial software version:

  http://kb.netgear.com/app/products/model/a_id/14554
- VPNG01L/VPNG05L FAQs:

  http://kb.netgear.com/app/answers/detail/a_id/14903
- TheGreenBow IPSec VPN Client:

  http://www.thegreenbow.com/vpn.html
- TheGreenBow VPN Documentation and manuals

  http://www.thegreenbow.com/vpn_doc.html
- TheGreenBow VPN documentation for various VPN gateways

  http://www.thegreenbow.com/vpn_gateway.html

  The documents that you can access from this link are based on TheGreenBow VPN Client. The NETGEAR ProSafe VPN Client Professional / Lite is powered by TheGreenBow, so configuration is likely identical or very similar.