NETGEAR®

NETGEAR ProSAFE VPN Client

Version 5.5 and Earlier Versions

User Manual

April 2013
202-10684-05

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

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

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx.*

Trademarks

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10684-05	–	April 2013	• Entirely reorganized and rewrote the manual as a task-based manual. • Described new features in the following sections: - *VPN Client Features* - *Configure PKI Options* - *Software Setup Command Reference* - *Customize How the VPN Client Handles Readers and Certificates* • Described changes in the global parameters defaults (see *Configure the Global VPN Parameters*).
202-10684-04	v1.0	April 2012	Minor new features and improvements such as the Remote Sharing pane.
202-10684-03	v1.0	May 30, 2011	Major revision to document the new format of the user interface and some new features such as the enhanced capability to change languages.
202-10684-02	v1.1	December 2010	Minor editorial changes and addition of an index.
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 5 Advanced Configuration Options

Chapter 6 VPN Client Software Setup and Network Deployment

Index

Introduction

1

The VPN Client supports all Windows versions and allows you to establish secure connections over the Internet, for example, between a remote worker and the corporate Intranet. IPSec is the most secure way to connect to the enterprise because 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:

Note: For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

Note: Firmware updates with new features and bug fixes are made available from time to time on *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product do not match what is described in this guide, you might need to update your firmware.

How to Use This Manual

This manual is primarily intended for network administrators who need to implement the VPN Client for end users.

The manual explains how to use the user interface to configure the VPN Client. An exception is *Chapter 6, VPN Client Software Setup and Network Deployment*. That chapter describes how to use software setup commands, how to use CLI commands, and how to configure initialization files to preconfigure the VPN Client software setup before deployment to end users, to remotely install or upgrade the VPN Client, and to centrally manage VPN configurations.

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 SP3 • Windows Server 2003 32-bit • Windows Server 2008 32/64-bit • Windows Vista 32/64-bit • Windows 7 32/64-bit • Windows 8 32/64-bit
Languages	Arabic, Chinese (simplified), Czech, Danish, Dutch, English, Farsi, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, and Turkish.
Connection modes	• Supports peer-to-peer connections (point-to-point connections between two computers that have the VPN Client installed). • Supports peer-to-gateway connections, for example, between a computer that has the VPN Client installed and NETGEAR platform that supports VPN. • Supports connection types such as dial-up, DSL, cable, GSM/GPRS, 3G, 4G, and WiFi. • Allows IP range networking. • Runs in a Remote Desktop Protocol (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, SHA-1, and SHA-256 hash algorithms - Change IKE port

Table 1. List of features (continued)

Feature	Specifications
NAT Traversal	• NAT Traversal Draft 1 (enhanced), Draft 2, and Draft 3 (full implementation), including: - NAT OA support - NAT keep-alive - NAT-T aggressive mode • Forced NAT-Traversal mode
SIP/VoIP support	Support for Session Initiation Protocol (SIP) and Voice over IP (VoIP) traffic in a VPN tunnel on Window Vista, Windows 7, and Windows 8.
Encryption	Provides the following encryption algorithms: • 3DES, DES, and AES 128/192/256-bit encryption • Support for Diffie-Hellman group 1 (768 bits), group 2 (1024 bits), group 5 (1536 bits), and group 14 (2048 bits)
User authentication	Supports the following user authentication methods: • Pre-shared keying and X509 certificate 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 • Personal Certificate Store support • VPN configuration file
	Remote login: • Gina mode supported on Windows 2000 and Windows XP to enable Windows logon using a VPN tunnel or enable to log in on a local machine. • Credential providers supported on Windows Vista and Windows 7 to enable Windows logon using a VPN tunnel or enable to log in 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.
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 drive	You can save VPN configurations and security elements (certificates, pre-shared 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.

Table 1. List of features (continued)

Feature	Specifications
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 (Lite and Professional) and Supported Features

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 can purchase a license for the VPN Client and 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-Auth	✓	✓
	Mode Config	✓	✓
	DNS/WINS server manual configuration	✓	✓
	Hybrid mode	–	✓
	IKE/NAT-T ports can be modified	–	✓
Control	Connection Panel	✓	✓
	Console logs	✓	✓
	Disable split tunneling	✓	✓
	Dead Peer Detection	✓	✓
	System tray popup	✓	✓
	GUI protection (password)	–	✓
	Auto Open (Windows on startup on traffic detection)	–	✓
	Start VPN tunnel before Windows logon	–	✓
	Easy deployment by command-line interface (CLI)	–	✓
Advanced Features	Multitunnel configurations	–	✓
	Redundant Gateways	✓	✓
	Scripts	–	✓
	USB mode	–	✓

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 and appliances that are based on those Linux implementations.

References and Useful Websites

These references and websites are for the ProSAFE VPN Client Lite and ProSAFE VPN Client Professional, both of which are developed by TheGreenBow.

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

  http://support.netgear.com/product/VPNG01L

- Access to VPNG05L product information and a 30-day trial software version:

  http://support.netgear.com/product/VPNG05L

- 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

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

Note: For documentation about the *legacy* ProSAFE VPN Client that was developed by SafeNet, see the following NETGEAR sites:
http://support.netgear.com/product/VPN01L
http://support.netgear.com/product/VPN05L

2. Install the Software

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

- *Software Installation*
- *Launch the VPN Client*
- *Trial Software Evaluation*
- *Software Activation*
- *Software Upgrade Concepts*
- *Software Uninstallation*

Software Installation

The VPN Client software installation does not require specific information and is self-explanatory. After completing the installation, you are asked to reboot your computer. However, if your operating system is Windows 8, Windows 7, or Windows Vista, you can install the VPN Client software without rebooting your computer.

After you have rebooted and logged in to your computer, the VPN Client Activation Wizard screen displays. The information about how to proceed depends on whether you want to use a trial license or activate a permanent license:

- If you downloaded a free trial software version, see *Trial Software Evaluation* on page 14.
- If you purchased a permanent license, see *Software Activation* on page 17.

Launch the VPN Client

After you have installed the VPN Client software, there are three methods to launch the VPN Client:

- On your desktop, double-click the VPN Client shortcut.
- In the taskbar, click the VPN Client icon.
- From the Start menu, select the path to the VPN Client, for example:

  Start > All Programs > NETGEAR > NETGEAR VPN Client.

  Note: *If your operating system is Windows 8, Windows 7 or Windows Vista, you can select a check box to automatically run the VPN Client after software installation.*

The VPN Client creates new rules in the Windows firewall (Vista and later operating systems) so that VPN traffic is enabled: UDP ports 500 and 4500 are authorized both for authentication (phase 1) traffic and for IPSec (phase 2) traffic.

If you use an earlier Windows operating system or another firewall, you might have to create firewall rules to enable the VPN Client. For information, see *Resolve Firewall Interference* on page 133.

Trial Software Evaluation

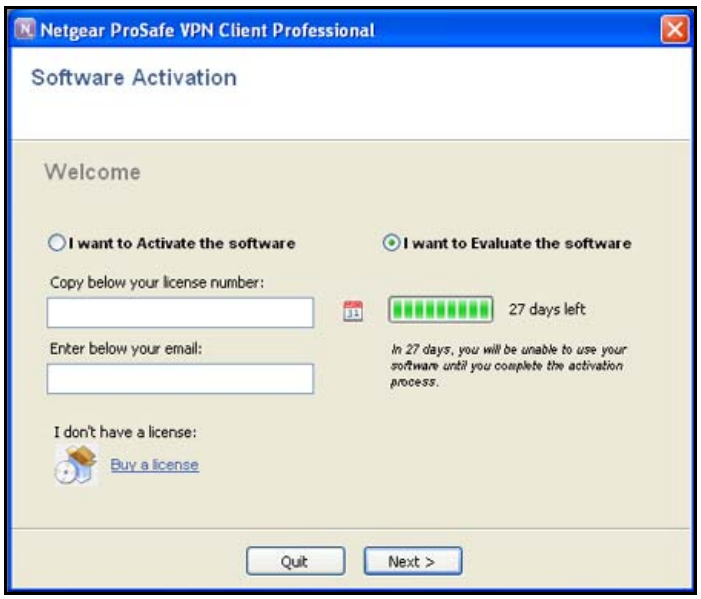
The VPN Client is available as a free trial version. The evaluation period is limited to 30 days. After the evaluation period has expired, the VPN Client becomes disabled. By purchasing and activating a permanent license, you can transfer the trial version to a permanent version and access the VPN Client indefinitely. For more information, see *License Number Concepts* on page 17 and *Software Activation* on page 17.

➢ **To use the VPN Client during the evaluation period:**

1. In the taskbar, click the VPN Client icon.

   For other methods to launch the VPN Client, see *Launch the VPN Client* on page 14.

   The Software Activation screen displays:



2. Select the **I want to Evaluate the software** radio button.

   You do not need to enter a license number and email address to activate the trial software.

3. Click **Next**.

   The Configuration screen displays, and the user interface is accessible.

During the evaluation period, the Software Activation screen displays each time that you start the VPN Client. The remaining days of the evaluation period are displayed next to the calendar icon on the right of the screen. You can also see the remaining time of the evaluation period on the About screen (see *About Screen* on page 26).

When the evaluation period expires, the following occurs:

- The **I want to Activate the software radio** button is automatically selected.
- The **I want to Evaluate the software** radio button is masked out.
- The message *Evaluation period expired* is displayed.
- The software is disabled.

When the evaluation period has expired, in order for you to use the VPN Client, you need to purchase and activate a permanent license. You can purchase and activate a permanent license while you are still in the evaluation period or after the evaluation period has expired.

- **To view the remaining time of the evaluation period from VPN Client's user interface:**

  From the main menu of the Connection Panel screen, select **? > About**.

  (When you launch the VPN Client, the Configuration Panel screen displays by default.)

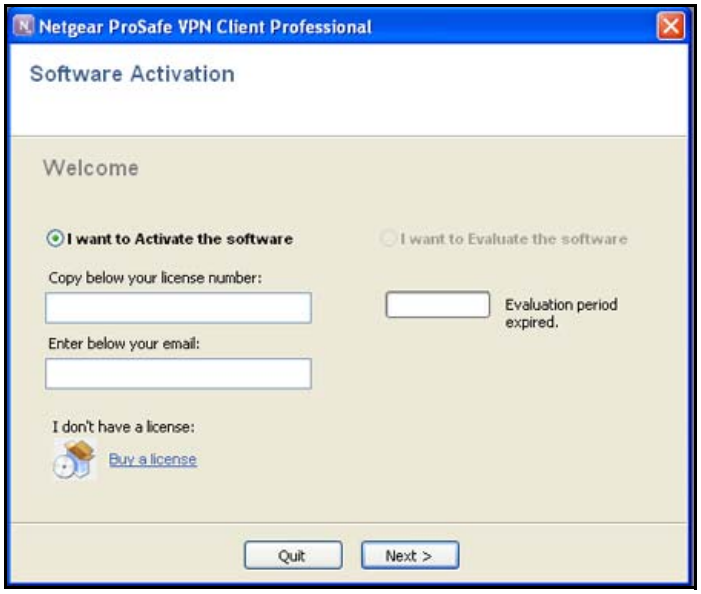
  The About screen displays, showing the number of days that remain in the evaluation period:

- **To buy a permanent license:**

  1. In the taskbar, click the VPN Client icon.

     For other methods to launch the VPN Client, see *Launch the VPN Client* on page 14.

The Software Activation screen displays. The following figure shows the Software Activation screen after the evaluation period has expired:



2. Click the **Buy a license** link.

   The NETGEAR website displays. Follow the instructions onscreen to purchase a permanent license.

3. After you have purchased a license, follow the procedure in *Software Activation*, to activate the permanent license.

License Number Concepts

A license number is attached to a single computer after activation. However, you can deactivate the license number (see *Software Uninstallation* on page 22) and transfer it to another computer.

You can also change the license number at any time, but you first need to uninstall the VPN Client before you can reinstall the VPN Client with another license number.

After activation, save the license key number. You might need it again to reactivate your software if a problem has occurred. Also, keep the CD label for technical support.

Software Activation

When you purchase a permanent license, you are required to activate it before you can use the VPN Client.

Software Activation Wizard

In order for you to use the VPN Client beyond the evaluation period, you need to activate the VPN Client license on your computer. You need the license number or key and an email address.

➢ **To activate your software using the Activation Wizard:**

1. Make sure that your computer is connected to the Internet.
2. Do one of the following:
   - **If you did not yet launch the VPN Client:**

     In the taskbar, click the VPN Client icon.

     For other methods to launch the VPN Client, see *Launch the VPN Client* on page 14.
   - **If you already launched the VPN Client and the user interface is accessible:**

     From the main menu on the Configuration Panel screen, select **? > Activation Wizard**.

   The Software Activation screen displays. The following figure shows the Software Activation screen when the evaluation period has not yet expired:

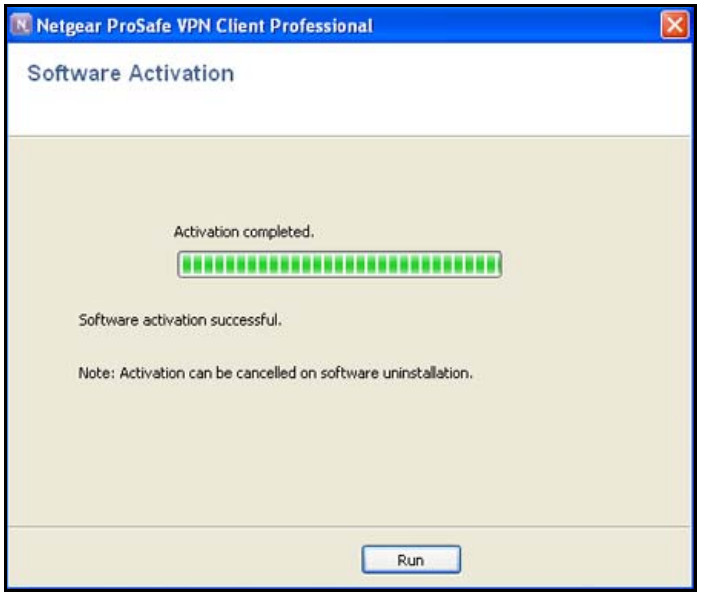
3. Select the **I want to Activate the software** radio button.
4. Enter your permanent license number.
5. Enter your email address.

   Your email address is used to send you the activation confirmation.

Note: The email address might not be required. If the network administrator suppresses display of the Email address field during the software setup, the Software Activation Wizard does not display the Email address field. Suppression can be used to centralize all software activation confirmation emails to a single email address.

6. Click **Next**.

   The Activation Wizard attempts to automatically connect to the activation server to activate the VPN Client software. The progress bar shows the activation progress.



   When the activation is complete, the screen shows whether the activation was successful and displays messages associated with the outcome (see also *Troubleshoot Software Activation* on page 20).

7. (Optional, and only if an error occurs) Click the **More information about this error** link.

   For troubleshooting information, see the following section, *Troubleshoot Software Activation*.

8. Click **Run**.

   The VPN Client relaunches with the new license. The Configuration screen displays and the user interface is accessible.

Troubleshoot Software Activation

Errors can occur during the activation process. Each activation error type is displayed on the Software Activation screen.

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

- Verify that you entered the correct license number. (Error 031 indicates that the license number was not found.)
- Your license number could already be activated (Error 033). Contact NETGEAR support.
- Your license number cannot be used for activation (Error 034). Contact NETGEAR support.
- A firewall might block communication with the activation server (Error 053 or Error 054). Find out if a personal or corporate firewall is blocking communications.
- The activation server might be temporarily unreachable. Wait a few minutes and try again.

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

The following two figures show examples of activation errors.

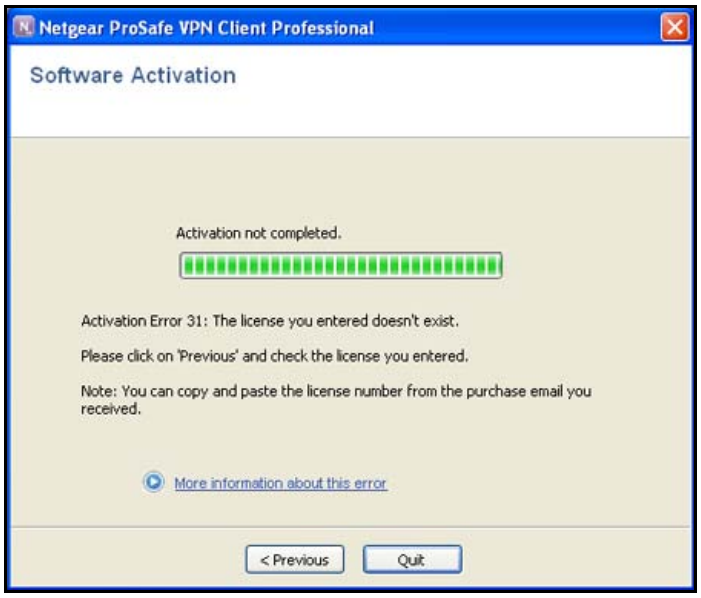


Figure 1. Activation Error 31

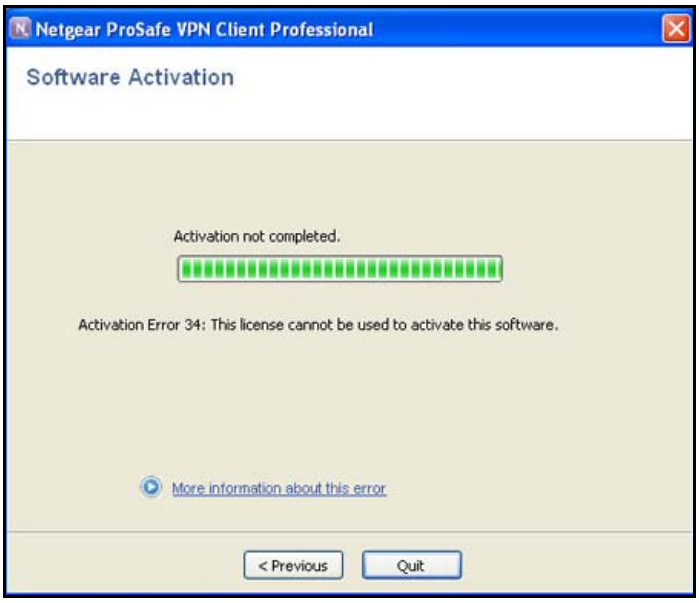


Figure 2. Activation Error 34

Software Upgrade Concepts

You need to reactivate the VPN Client after each software upgrade. Depending on your maintenance contract, a software upgrade activation might be rejected. Carefully read the recommendations in this section.

➢ **To check the status of the VPN Client's software release:**

From the main menu of the Connection Panel screen, select **? > Check for Update**.

The NETGEAR website displays. You can check if the VPN Client is running that latest software release or download a new software release.

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, 4.00, or 5.00.

If you want to subscribe or extend your maintenance period, 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 for access control (see *Configure Access Control* on page 92), you need to enter it to be able to upgrade the software.

Software Uninstallation

To transfer a license to a new computer, you need to 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.

If your computer is not connected to the Internet and you need to inactivate your license, contact NETGEAR support by email at *support@netgear.com*, or call the technical center to inactivate your license.

There are several methods to uninstall the VPN Client software. Depending on your Windows operating system, these methods might differ slightly from the following procedures.

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.

➢ **To uninstall the VPN Client through the Control Panel:**

1. Make sure that your computer is connected to the Internet.
2. Select **Start > Control Panel**.
3. Double-click **Programs and Features**. (In some Windows versions, you need to double-click **Add or Remove Programs**.)
4. Right-click the **NETGEAR VPN Client** and select **Uninstall**. (In some Windows versions, you need to select **Remove**.)

➢ **To uninstall the VPN Client through the All Programs menu:**

1. Make sure that your computer is connected to the Internet.
2. Select **Start > All Programs**.
3. Select the path to the VPN Client, for example:

   Start > All Programs > NETGEAR > NETGEAR VPN Client.
4. Select the uninstall option.

3 Overview of the User Interface

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

- *Overview of the User Interface Components*
- *Configuration Panel Screen*
- *System Tray Icon and System Tray Menu*
- *System Tray Pop-Up Screens*
- *Connection Panel Screen*
- *VPN Console Active Screen*
- *Keyboard Shortcuts*

Overview of the User Interface Components

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 pre-shared key or certificates.

The user interface consists of the following components:

- Configuration Panel
- Connection Panel
- Main menus
- System tray icon and pop-up screens
- Status bar
- Wizards
- Preferences

Configuration Panel Screen

When you launch the VPN Client, the Configuration Panel screen displays by default. (The following figure shows configured VPN tunnels, which would be absent if you launched the Configuration Panel for the first time.)

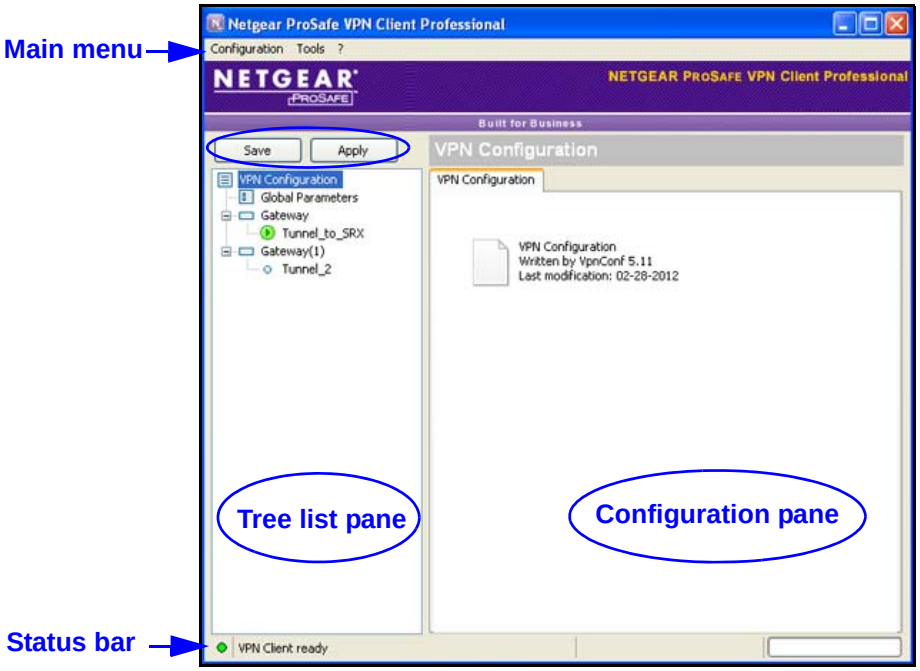


Figure 3. Configuration Panel screen

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

- Main menu (at the top of the screen), showing the Configuration, Tools, and ? menu selections.
- The Save and Apply buttons in the left column of the screen:
  - **Save**. The VPN tunnel is saved for immediate and future use. The VPN tunnel is saved to the startup configuration. The next time that you start the VPN Client, the configuration is present.
  - **Apply**. The VPN tunnel is saved for immediate use only. The VPN tunnel is not saved to the startup configuration. The next time that you start the VPN Client, the configuration is no longer present.
- A tree list pane (in the left column of the screen) that contains the Global Parameters button and all authentication phase names (that is, phase 1 names) with their associated IPSec configuration names (that is, phase 2 names or tunnel names).
- A configuration pane (in the right column of the screen) that shows the associated settings for each tree level.
- Status bar (at the bottom of the screen).

Note: For information about restricting access to the Configuration Panel screen, see *Configure Access Control* on page 92.
For information about hiding the Configuration Panel link from the system tray menu, see *Configure the User Interface* on page 94.

Main Menu

The main menu lets you make the following selections:

- **Configuration**. 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), access the Configuration Wizard, and quit the VPN Client.
- **Tools**. Lets you access the Connection Panel, access the Console screen, reset the IKE settings, and access the Option screen to configure miscellaneous preferences such as the way the VPN Client starts and the language of the VPN Client.
- **?**. Lets you access online help, check for software updates, connect to the NETGEAR website to purchase a license online, access the Activation Wizard, and access the About screen.

Note: Some selections that are available from the Configuration menu are also available by right-clicking a component of the tree list pane in the Configuration Panel screen.

Status Bar

The status bar at the bottom displays the following information:

- The radio button indicates whether the VPN Client is ready for use. (Green indicates ready; gray indicates not ready.)
- The text to the right of the radio button provides the status of the VPN Client (for example, VPN Client Ready, or Apply VPN configuration).
- The progress bar at the very right displays the progress when you apply or save the configuration.

About Screen

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

Figure 4. About screen

Options Screen

This screen is available in the VPN Client Professional but not in the VPN Client Lite.

The Options screen, which you access by selecting **Tools > Options** from the main menu, has four tabs that provide access to the following panes:

- **View pane**. From the View pane, you can configure access control to the user interface (see *Configure Access Control* on page 92) and change the appearance of the user interface (see *Configure the User Interface* on page 94).
- **General pane**. From the General pane, you can configure the startup mode and configure detection of the state of the network interface (see *Configure VPN Client Startup Mode and Network Interface Detection* on page 95).
- **PKI Options pane**. From the PKI Options pane, you can configure how certificates are checked, accessed, and read (see *Configure PKI Options* on page 84).
- **Language pane**. From the Language pane, you can select the language for the user interface and modify the default translations (see *Configure Languages* on page 97).

Wizards

There are several wizards available:

- **VPN Configuration Wizard**. Access this wizard by selecting **Configuration > Wizard** from the main menu (for more information, see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 36).
- **Software Activation Wizard**. Access this wizard by selecting **? > Activation Wizard** from the main menu (for more information, see *Software Activation Wizard* on page 18).
- **USB Mode Wizard**. Access this wizard by selecting **File > Move to USB Drive** from the main menu (for more information, see *USB Mode* on page 68).
- **Certificate Export Wizard**. Access this wizard in the following way:

  1. On the Certificate pane, select **View Certificate**.
  2. On the View Certificate screen, click the **Details** tab.
  3. Select **Copy to File**.

  For more information, see *View Certificate Details* on page 79.

System Tray Icon and System Tray Menu

After you have launched the VPN Client (see *Launch the VPN Client* on page 14), the VPN Client displays an icon in the system tray that indicates whether a tunnel is opened, using a color code.

Green icon:
at least one VPN tunnel opened.

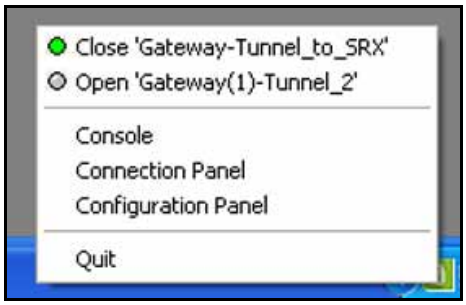
Purple icon:
no VPN tunnel opened.

Figure 5. VPN Client icon colors in the system tray

➢ **To open the system tray menu:**

Right-click the purple VPN Client icon in the system tray.

The system tray menu displays:



By default, the system tray menu shows the following links from top to bottom:

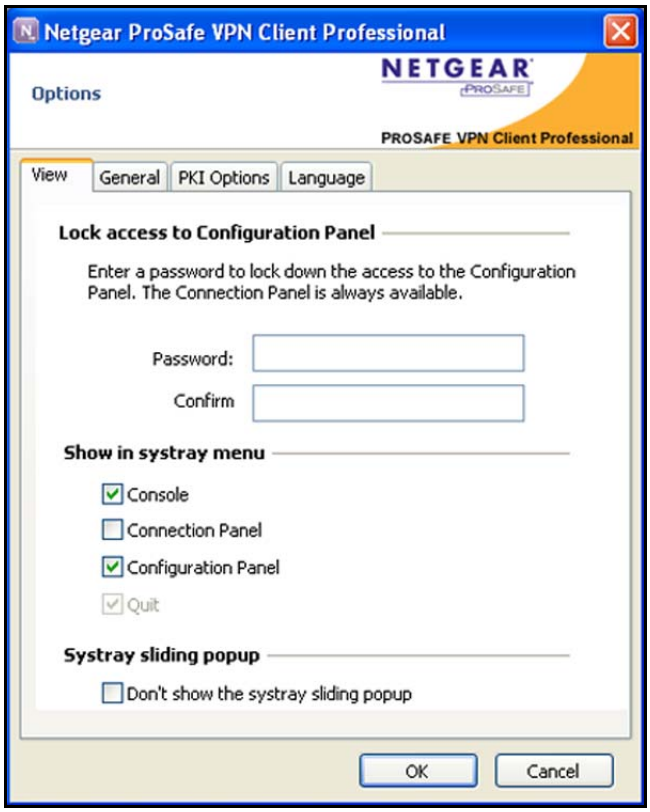
- **Configured tunnels with their status**. You can open or close tunnels by selecting **Open '<gateway name-tunnel name>'** or **Close '<gateway name-tunnel name>'**.
- **Console**. Clicking the link opens the VPN Console Active screen.
- **Connection Panel**. Clicking the link opens the Connection Panel screen, which lets you open and close VPN tunnels and displays information about VPN tunnels.
- **Configuration Panel**. Clicking the link opens the Configuration Panel screen, which lets you create and configure VPN tunnels.
- **Quit**. Clicking the link closes all established VPN tunnels, then closes the VPN Client.

Note: The Quit link for the system tray menu is disabled in the VPN Client Lite. For the VPN Client Professional, you can remove this link during the software setup through the **`menuitem`** software setup command (see *Configure Which Items of the System Tray Menu Are Visible* on page 111).

➢ **To hide one or more links from the system menu tray:**

1. From the main menu, select **Tools > Options**.

   The Options screen displays. The View pane is selected by default.



2. In the Show in systray menu section of the screen, configure which links are hidden in the system tray menu:
   - **Console**. Clear the check box to hide the Console link from the system menu tray.
   - **Connection Panel**. Clear the check box to hide the Connection Panel link from the system menu tray.
   - **Configuration Panel**. Clear the check box to hide the Configuration Panel link from the system menu tray.

   Note: *The Quit check box is disabled. You cannot disable the Quit link in the system tray menu from the View pane. For information about disabling the Quit link in the system tray menu, see* *Configure Which Items of the System Tray Menu Are Visible on page 111.*

3. Click **OK**.

System Tray Pop-Up Screens

When a VPN tunnel opens or closes, by default, a small pop-up screen comes out from the system tray icon and shows the following:

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

Figure 6. Tunnel opened pop-up screen

- VPN tunnel closing, followed by tunnel closed.

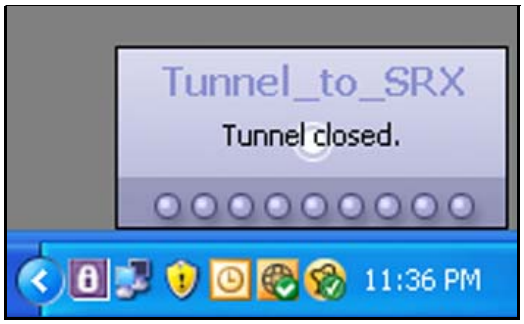


Figure 7. Tunnel closed pop-up screen

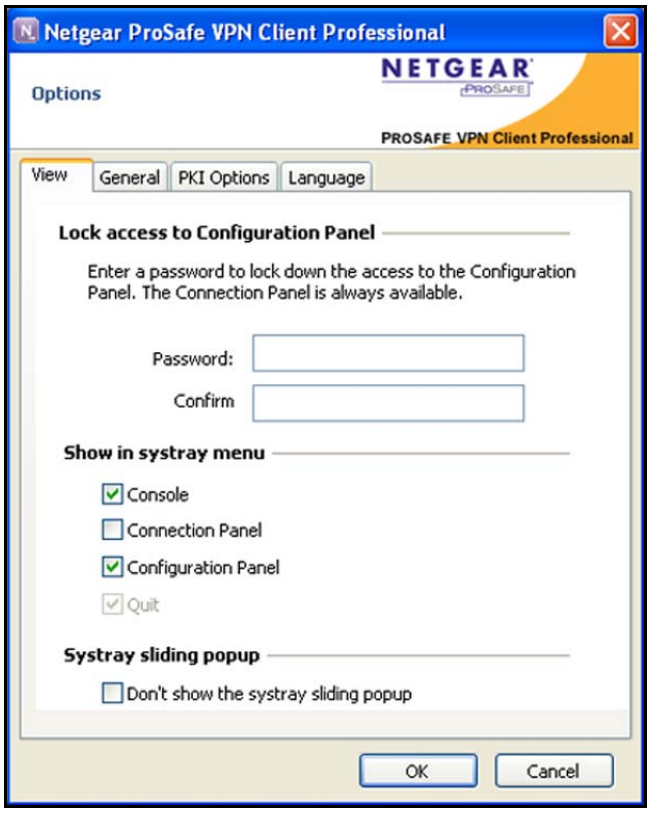
- If the VPN tunnel cannot open, the screen might display an error or warning with a link to more information.

Figure 8. Pre-shared key mismatched pop-up screen

➢ **To disable the systray pop-up screens:**

1. From the main menu of the Configuration Panel, select **Tools > Options**.

   The Options screen displays. The View pane is selected by default.



2. In the systray sliding pop-up section of the pane, select the **Don’t show the systray sliding popup** check box.
3. Click **OK**.

Connection Panel Screen

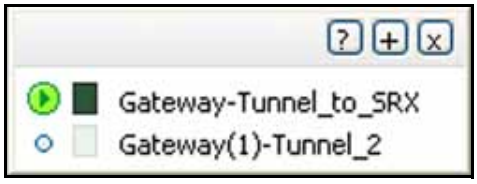
The Connection Panel screen enables you to open and close each tunnel that has been configured. If a network administrator has configured the VPN tunnels, the end user needs access only to the Connection Panel screen to open and close tunnels.

Note: For information about hiding the Connection Panel link from the system tray menu, see *Configure the User Interface* on page 94.

➢ **To open the Connection Panel screen:**

Use one of the following methods:

- Select **Tools > Connection Panel** from the main menu on the Configuration Panel screen.
- Right-click the system tray icon and select **Connection Panel**.



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

The Connection Panel screen consists of the following components:

- For each tunnel, the following components:
  - An icon that shows the status of the tunnel:
    - The tunnel is closed.
    - The tunnel is being opened.
    - The tunnel is open.
    - An incident occurred during the opening or closure of the tunnel.
  - A rectangular traffic gauge ( ) that shows the traffic volume passing through the tunnel.
  - The connection name (tunnel name) in the format authentication phase name–IPSec configuration name.
- Three icons in the upper right corner:
  - **?**. Opens the About screen.
  - **+**. Opens the Configuration Panel screen.
  - **x**. Closes the Connection Panel screen.

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

VPN Console Active Screen

The VPN Console Active screen allows you to analyze how VPN tunnels are set up or fail to be set up, which can be useful if you are a network administrator and need to configure a secure network. The messages on the VPN Console Active screen are mostly IKE messages.

You can also enable debugging mode, which is also referred to as trace mode. The trace logs become large rather quickly.

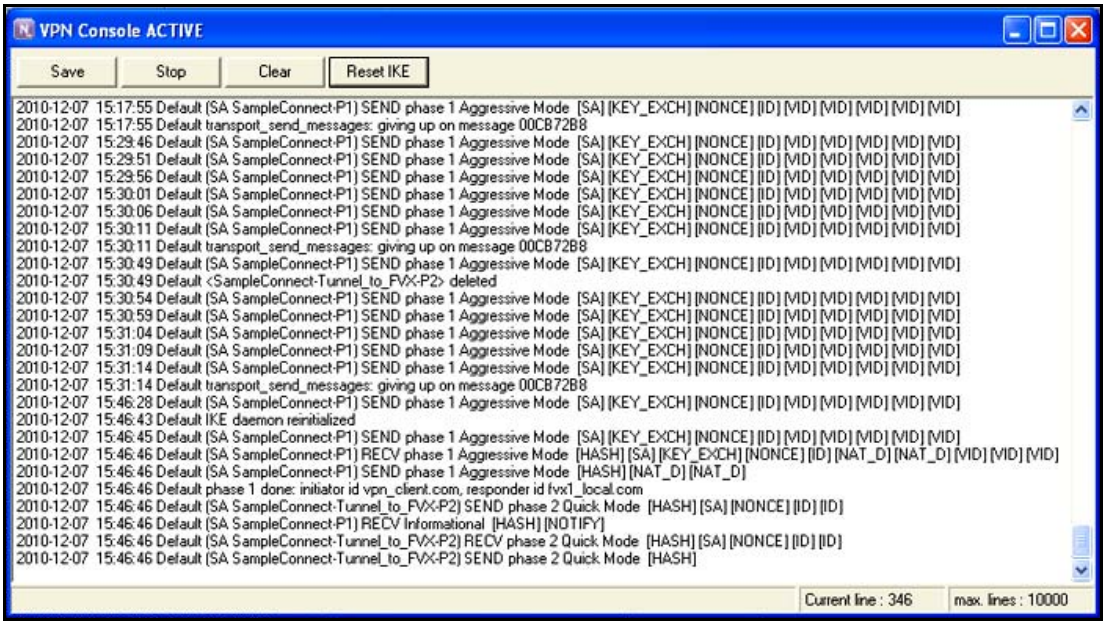
The VPN Console Active screen and trace mode can help you or NETGEAR support to diagnose tunnel problems and software's incidents.

Note: For information about hiding the Console link from the system tray menu, see *Configure the User Interface* on page 94.

➢ **To display the VPN Console Active screen:**

Use one of the following methods:

- In system tray menu, click the **Console** link.
- From the main menu of the Console Panel screen, select **Tools > Console**.



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 onscreen at a time.

- **Clear**. Removes the content from the screen.
- **Reset IKE**. Restarts the IKE process.

➢ **To enable debugging mode:**

1. Go to the Console Panel screen.
2. On your keyboard, press **Ctrl + Alt + T**.

   The status bar displays the message *Trace Mode is ON (Ctrl+Alt+T)*.

Keyboard Shortcuts

The user interface supports the following keyboard shortcuts.

Table 3. Keyboard shortcuts

Shortcut	Action
General shortcuts	
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	Opens the VPN Console for network debugging.
Ctrl + Alt + T	Activates the trace mode for the generation of logs.
Ctrl + Alt + R	Resets the IKE settings.
Shortcuts for the tree list pane of the Configuration Panel screen (see *Figure 3* on page 24)	
F2	Lets you edit the name of a selected phase.
Del	Lets you delete the selected phase or the entire VPN configuration. To delete the entire VPN configuration, first select the VPN configuration.
Ctrl + O	Opens the VPN tunnel of the selected phase 2.
Ctrl + W	Closes the VPN tunnel of the selected phase 2.
Ctrl + C	Copies the selected phase.
Ctrl + V	Pastes the selected phase.
Ctrl + N	Creates a new phase: • To create a phase 1, first select the VPN configuration. • To create a phase 2, first select the phase 1.
Ctrl + S	Saves and applies a VPN configuration.

Create VPN Tunnel Connections

4

This chapter describes how to create VPN tunnels. The 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 the following figure 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 9. VPN connection from a remote computer to a corporate LAN

➢ **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 **Configuration > Wizard**.

   The VPN Client Configuration Wizard Step 1/3 screen displays:

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 2/3 screen displays:

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**. (By default, the screen displays myrouter.dyndns.org.)
   - **Preshared key**. The pre-shared 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 3/3 screen displays:

   This screen is a summary screen of the new VPN configuration. If necessary, 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 **Tools > Connection Panel**.
2. Double-click the newly created tunnel (Gateway-Tunnel).

Open and Close VPN Tunnels with the User Interface

You can open a tunnel only after the VPN configuration has been specified. The following table provides an overview of the methods that are available to open and close VPN tunnels with the user interface.

For information about how to open tunnels automatically, see *Configure How VPN Tunnels Are Opened* on page 59.

For information about how to open tunnels using CLI commands, see *Customize the VPN Client Using CLI Commands* on page 123.

Table 4. Methods to open and close VPN tunnels from the user interface

User Interface Components	Methods to Open a Tunnel	Methods to Close an Open Tunnel
Configuration Panel screen	1. Click the IPSec configuration name (by default, Tunnel). 2. Press **Ctrl + O**.	1. Click the IPSec configuration name (by default, Tunnel). 2. Press **Ctrl + W**.
	1. Right-click the IPSec configuration name (by default, Tunnel). 2. Select **Open tunnel**.	1. Right-click the IPSec configuration name (by default, Tunnel). 2. Select **Close tunnel**.
Connection Panel screen	Double-click the tunnel (anywhere, the icon, gauge, or name)	Double-click the tunnel (anywhere, the icon, gauge, or name).
	1. Right-click the tunnel. 2. Click **Open tunnel**.	1. Right-click the tunnel. 2. Click **Close tunnel**.
	1. Click the tunnel. 2. Press **Ctrl + O**.	1. Click the tunnel. 2. Press **Ctrl + W**.
System tray icon	1. Right-click the system tray icon. 2. Click the IPSec configuration name (by default, Tunnel).	1. Right-click the system tray icon. 2. Click the IPSec configuration name (by default, Tunnel).

The Configuration Panel screen and Connection Panel screen show an icon to the left of the VPN tunnel that indicates the status of the tunnel:

The tunnel is closed.

The tunnel is configured to open automatically when traffic is detected.

The tunnel is being opened.

The tunnel is open.

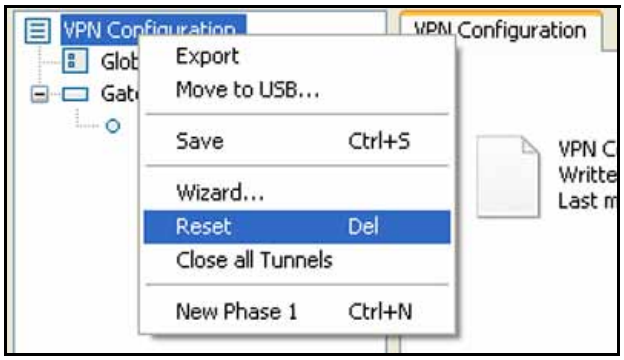
An incident occurred during the opening or closure of the tunnel.

High-Level Steps to Manually Create a VPN Tunnel Connection

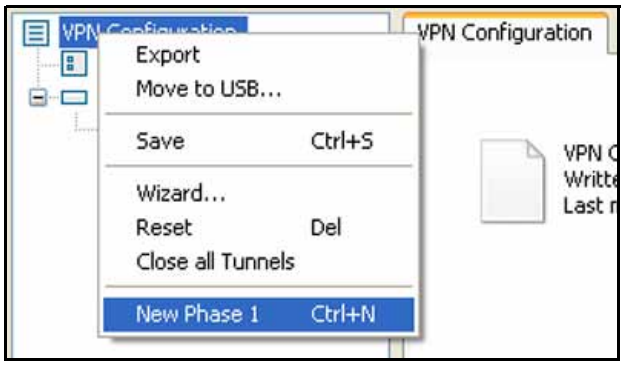
Using the Configuration Wizard is the easiest way to create a VPN tunnel, but the configuration and security options are limited. A manual configuration gives you all the options to customize a VPN tunnel to your specific needs and network.

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

1. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**.
2. Select **Reset**.



1. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**.
2. Select **New Phase 1**.



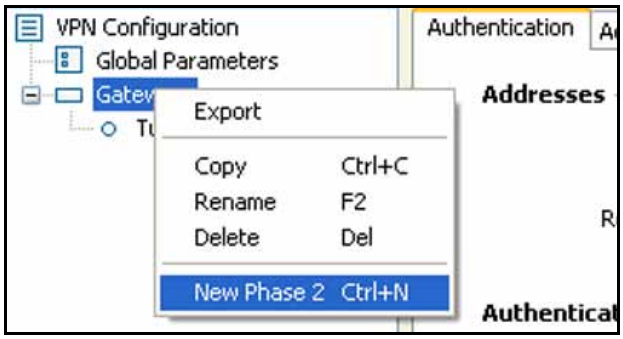
The Authentication pane displays in the right column of the Configuration Panel screen.

3. Configure the authentication that enables you to connect to the remote gateway or computer.

   For more information, see *Manually Configure Authentication or Phase 1* on page 41.

4. In the tree list pane of the Configuration Panel screen, right-click **Gateway** (which is the default name of the new phase 1 configuration).

5. Select **New Phase 2**.



The IPSec pane displays in the right column of the Configuration Panel screen.

6. Specify the IPSec configuration that enables the VPN Client to communicate securely with the remote gateway or computer.

For more information, see *Manually Configure IP Security or Phase 2* on page 49.

7. Click **Save**.
8. Right-click the tunnel that you just configured.
9. Click **Open Tunnel**.

The new VPN tunnel opens.

Manually Configure Authentication or Phase 1

The Authentication pane 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. The purpose of phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of phase 1, each end system must identify and authenticate itself to the other.

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

A pre-shared key is the authentication method that is the easiest to implement but is also the weakest in terms of security. The VPN Client supports the following authentication methods, which are listed in the order of increased security (from weakest to strongest security):

- Pre-shared key (see *Configure Authentication* on page 42).
- Static extended authentication (*Configure Advanced Authentication* on page 44).
- Dynamic extended authentication (see *Configure Advanced Authentication* on page 44).
- Certificate stored in the VPN security policy (see *Configure Authentication* on page 42 and *Certificate Management* on page 73).
- Certificate in the Windows Certificate Store (see *Configure Authentication* on page 42 and *Certificate Management* on page 73).
- Certificate on smart card or token (see *Configure Authentication* on page 42 and *Certificate Management* on page 73).

Configure Authentication

The Authentication pane lets you create authentication settings or edit existing authentication settings.

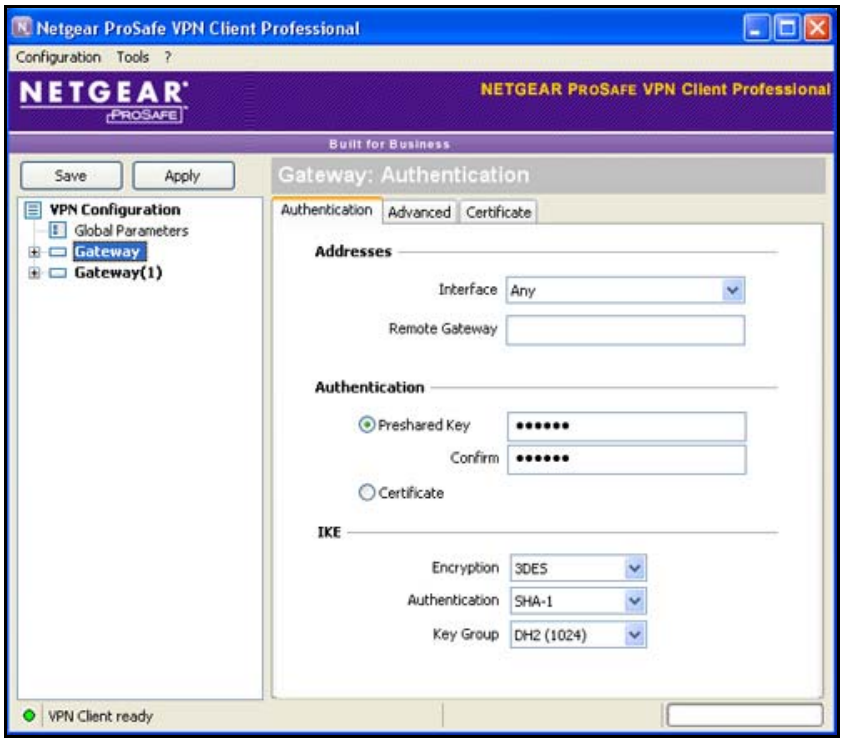
➢ **To create authentication settings:**

1. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**.
2. Select **New Phase 1**.

   The VPN Client creates an authentication phase with the name Gateway or Gateway(x), in which x is a number.

3. Click the new authentication phase name.

   The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.



4. (Optional) Change the name of the authentication settings (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Enter a new name.
   d. Click anywhere in the tree list pane.

5. Configure the settings as described in the following table.

Setting	Description	
Interface	From the Interface drop-down menu, select the IP address of the network interface of the computer through which the VPN connection is established. If the IP address changes (when it is received dynamically from an ISP or router), select **Any**. **Note:** If your selection of the Interface drop-down menu refers to an IP address that does not exist on the computer, Any is used automatically.	
Remote Gateway	Enter the IP address or DNS address of the remote gateway. This field is mandatory.	
Preshared Key	Enter the password or key that is shared with the remote gateway. You need to enter the same password or key in the Confirm field.	
Certificate	(Optional) The X509 certificate that the VPN Client uses. On the IPSec pane, click the **Certificate** tab to open the Certificate pane that lets you select the certificate source. You can use a PEM file, PKCS#21 file, smart card, or token, or a certificate from the Personal Certificate Store. Specify only one certificate per tunnel. For information about certificates, see *Certificate Management* on page 73.	
IKE	Encryption	The encryption algorithm that is used during the authentication phase. Select one of the following from the drop-down menu: • **DES**. • **3DES**. This is the default setting. • **AES128**. • **AES192**. • **AES256**.
	Authentication	The authentication algorithm that is used during the authentication phase. Select one of the following from the drop-down menu: • **MD5**. • **SHA-1**. This is the default setting. • **SHA-256**.
	Key Group	The Diffie-Hellman key length that is used during the authentication phase. Select one of the following from the drop-down menu: • **DH1 (768)**. • **DH2 (1024)**. This is the default setting. • **DH5 (1536)**. • **DH14 (2048)**.

6. Click **Save**.

➢ **To edit existing authentication settings:**

1. In the tree list pane of the Configuration Panel screen, select an existing authentication phase name (for example, Gateway in the previous figure).

   The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

2. (Optional) Change the name of the authentication settings (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Enter a new name.
   d. Click anywhere in the tree list pane.
3. Configure the settings as described in the previous table.
4. Click **Save**.

Configure Advanced Authentication

For authentication settings (phase 1 settings), the advanced configuration settings apply to *all* its associated IPSec configurations (phase 2 settings).

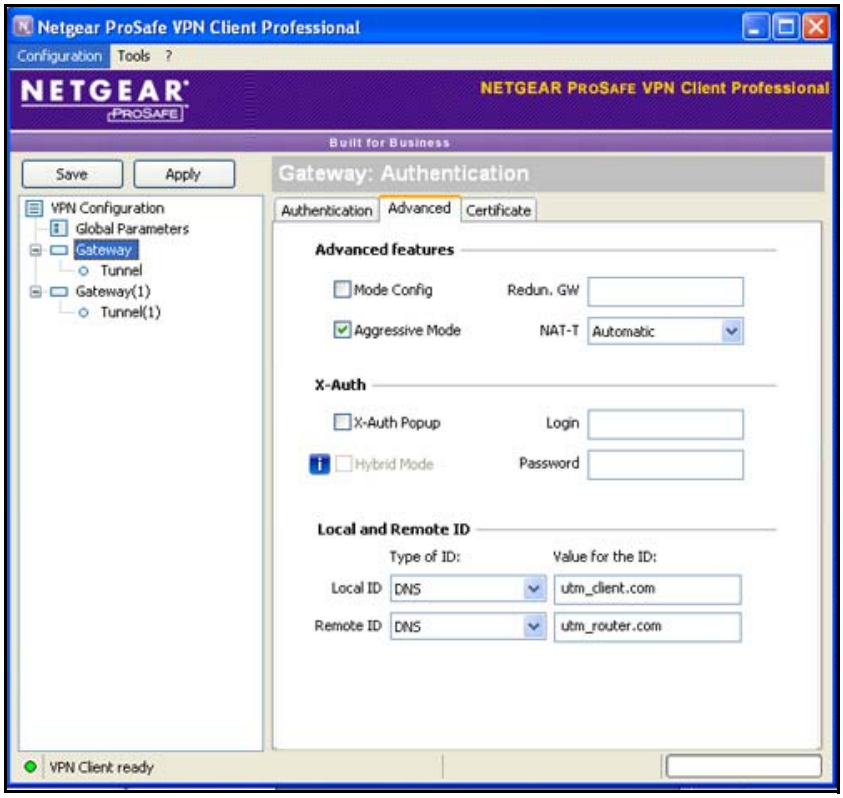
➢ **To configure advanced authentication settings:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to configure the advanced settings (for example, Gateway in the following figure).

   The Authentication pane displays.

2. In the Authentication pane, click the **Advanced** tab.

   The Advanced authentication pane displays:



3. Configure the settings as described in the following table.

Setting	Description
Advanced features	
Mode Config	Select the **Mode Config** check box to enable the Mode Config feature, which 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:** The virtual IP address that is issued by the remote VPN gateway is displayed in the VPN Client Address field on the IPSec pane with the IPSec tab selected. **Note:** If the Mode Config feature is not available or not supported on the remote VPN gateway, manually specify the DNS and WINS server addresses on the VPN Client. For more information, *Configure How VPN Tunnels Are Opened* on page 59
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.
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 pane of the Configuration Panel screen (see *Configure the Global VPN Parameters* on page 55), the VPN Client uses 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 *Configure the Global VPN Parameters* on page 55) 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** or **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.

Setting	Description
NAT-T	From the NAT-T drop-down menu, 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, 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. If extended authentication is configured on the gateway, select the **X-Auth Popup** check box to enable a pop-up screen in which the login name and password can be entered during the authentication phase. This pop-up screen 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:** If you enter a name in the Login field and a password in the Password field, the pop-up screen does not display, and the tunnel is established if the credentials match those on the gateway. (This method is referred to as static extended authentication.) However, this defeats the purpose of extended authentication. NETGEAR recommends that you do not enter a name and password on the Advanced authentication pane but let the user enter these credentials. (This method is referred to as dynamic extended authentication.) For more information, see *Extended Authentication* on page 47.
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. **Note:** Hybrid Mode requires you to configure a certificate for the authentication phase (see *Configure Authentication* on page 42) and to select Extended authentication (XAUTH), that is, the X-Auth Popup check box. Hybrid mode is an authentication method that is used within the authentication phase. 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 authentication phase, these authentication methods are used to establish an IKE SA that is unidirectionally authenticated. To ensure that the IKE is bidirectionally authenticated, the authentication phase 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.

Setting	Description
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 menu, 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). • **DER ASN1 DN**. Enter a certificate issuer (for more information, see *Certificate Management* on page 73). 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 73). **Note:** If a VPN tunnel closes because the computer has changed its IP address, the VPN tunnel does not reopen automatically when the network becomes available again.
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 menu, 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, 203.0.113.4). • **DNS**. Enter a fully qualified domain name (FQDN) (for example, gateway.mydomain.com). • **DER ASN1 DN**. Enter a certificate issuer (for more information, see *Certificate Management* on page 73). If you do not enter a certificate, the IP address of the VPN gateway is used.

4. Click **Save**.

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 on the remote VPN gateway. The VPN Client supports several authentication protocols, including CHAP and one-time password (OTP).

After you have configured XAUTH, an end user needs to enter credentials to be able to open a tunnel.

➢ **High-level steps to configure XAUTH:**

1. Configure extended authentication on the remote VPN gateway.
2. Select the **X-Auth Popup** check box on the Advanced authentication pane of the VPN Client.
3. Click **Save**.

When an end user opens a tunnel, the end user needs to enter credentials on the XAUTH pop-up screen.

Figure 10. XAUTH pop-up screen

The credentials need to match those on the remote VPN gateway.

Note: The XAUTH pop-up screen 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 displays in the pop-up screen.

The end user has some time to enter the credentials. If the time allowed to enter XAUTH credentials expires, a warning screen displays and the end user has to reopen the VPN tunnel. The expiration time depends on the settings of the X-Auth timeout field on the Parameters pane of the Connection Panel screen (see *Configure the Global VPN Parameters* on page 55).

Figure 11. X-Auth login failed warning

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 screen displays again.
- A pop-up warning similar to the following one alerts the user to try to open the VPN tunnel again.

Figure 12. Wrong login or password warning

Manually Configure IP Security or Phase 2

The purpose of the IPSec configuration, which is also referred to as phase 2, is to negotiate the IP security settings that are applied to the traffic that goes through the tunnels.

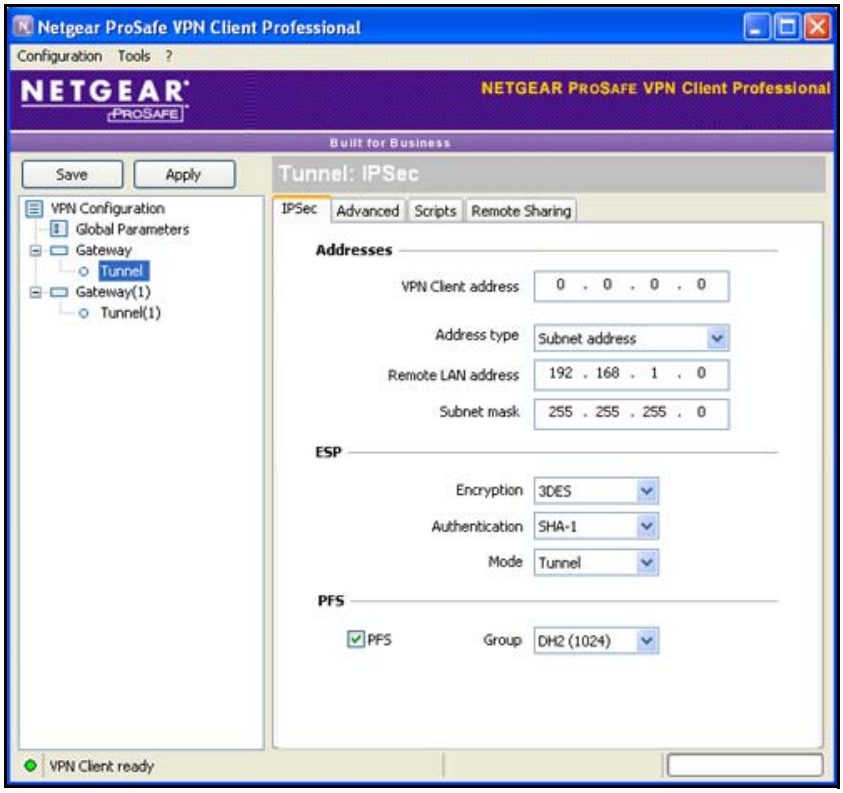
Note: You can create several IPSec configurations (phase 2 settings) for a single set of authentication settings (phase 1 settings).

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click an existing authentication phase name (for example, Gateway in the following figure).
2. Select **New Phase 2**.

   The VPN Client creates an IPSec configuration with the name Tunnel or Tunnel(x), in which x is a number.

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.



3. (Optional) Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Enter a new name.
   d. Click anywhere in the tree list pane.
4. Configure the settings as described in the following table.

Setting	Description
VPN Client address	Enter the virtual IP address that the VPN Client uses 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 can also enter **0.0.0.0** as the IP address. 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 Advanced IPSec pane (see *Configure How VPN Tunnels Are Opened* on page 59). 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. **Note:** If Mode Config is enabled and the remote VPN gateway has issued an IP address to the VPN Client, the IP address is displayed in the VPN Client address field.

<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 menu, 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 pane adjusts to display the associated address fields:
• Single address. The remote endpoint is a single computer. Fill in the Remote host address and Subnet Mask fields.
• Subnet address. The remote endpoint is a LAN. Fill in the Remote LAN address and Subnet Mask fields.
To force all traffic from the computer to pass through the VPN tunnel, select Subnet address, and enter 0.0.0.0 as the subnet mask.
• Range address. The remote endpoint is a LAN that consists of a range of addresses. Fill in the Start address and End address fields.

Note: When you select Range address from the drop-down menu and the Automatically open this tunnel on traffic detection check box on the Advanced IPSec pane (see Configure How VPN Tunnels Are Opened on page 59), 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></td><td>Single address</td><td>Remote host address</td><td rowspan="5">Enter the addresses.</td></tr>
<tr><td></td><td rowspan="2">Subnet address</td><td>Remote LAN address</td></tr>
<tr><td></td><td>Subnet Mask</td></tr>
<tr><td></td><td rowspan="2">Range address</td><td>Start address</td></tr>
<tr><td></td><td>End address</td></tr>
<tr><td rowspan="3">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 menu:
• DES.
• 3DES. This is the default setting.
• AES128.
• AES192.
• AES256.</td></tr>
<tr><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 menu:
• MD5.
• SHA-1. This is the default setting.
• SHA-256.</td></tr>
<tr><td>Mode</td><td colspan="2">IPSec encapsulation mode. Select one of the following from the drop-down menu:
• 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>

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 menu: • **DH1 (768)**. • **DH2 (1024)**. This is the default setting. • **DH5 (1536)**. • **DH14 (2048)**.

5. (Optional) Click the **Advanced** tab.

   The Advanced IPSec pane opens, allowing you to configure how VPN tunnels are opened and to configure alternate servers (for more information, see *Configure How VPN Tunnels Are Opened* on page 59).

6. (Optional) Click the **Scripts** tab.

   The IPSec Scripts pane opens, allowing you to specify scripts. (For information, see *Configure Scripts* on page 64.)

7. Click **Save**.
8. (Optional) Open the newly configured tunnel:
   a. In the tree list pane, right-click the IPSec configuration name (for example, Tunnel).
   b. Click **Open Tunnel**.

      (When the tunnel is opened, the button changes to Close Tunnel.)

➢ **To edit an existing IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, click an existing IPSec configuration name (for example, Tunnel in the previous figure).

   The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.

2. (Optional) Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Enter a new name.
   d. Click anywhere in the tree list pane.
3. Configure the settings as described in the previous table.
4. (Optional) Click the **Advanced** tab.

   The Advanced IPSec pane opens, allowing you to configure how VPN tunnels are opened and to configure alternate servers (for more information, see *Configure How VPN Tunnels Are Opened* on page 59).

5. (Optional) Click the **Scripts** tab.

   The IPSec Scripts pane opens, allowing you to specify scripts. (For information, see *Configure Scripts* on page 64.)

6. Click **Save**.
7. (Optional) Open the modified tunnel:
   a. In the tree list pane, right-click the IPSec configuration name (for example, Tunnel).
   b. Click **Open Tunnel**.

      (When the tunnel is opened, the button changes to Close Tunnel.)

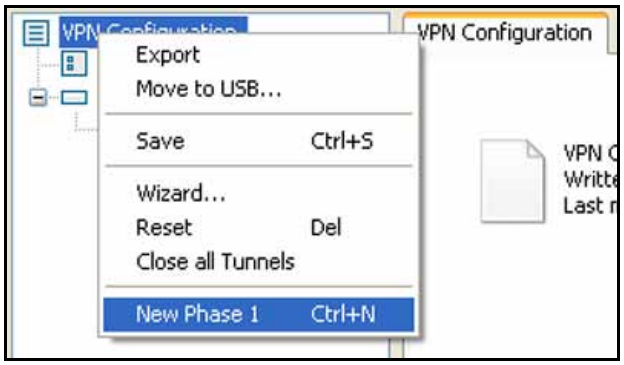
High-Level Steps to Specify a Certificate for User Authentication

Certificates provide the highest level of security in the user authentication process. For information about certificates, see *Import Certificates* on page 73. The following procedure provides high-level steps only.

➢ **To configure new authentication settings (phase 1 settings), configure an associated IPSec configuration (phase 2 settings), and specify a certificate for the tunnel:**

1. Create authentication settings (phase 1 settings).

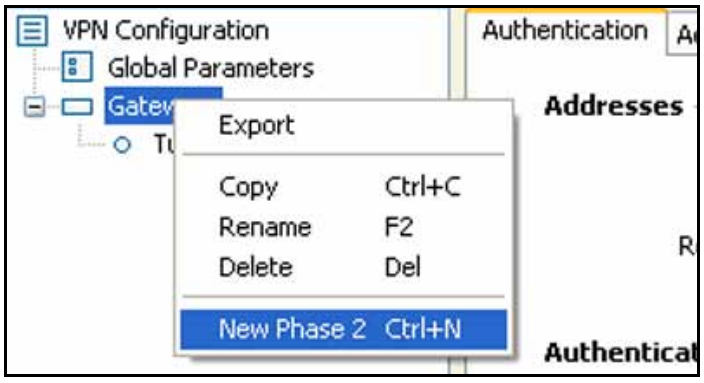
   For more information, see *Configure Authentication* on page 42.



2. Configure the advanced authentication settings.

   For more information, see *Configure Advanced Authentication* on page 44.

3. Add an IPSec configuration.



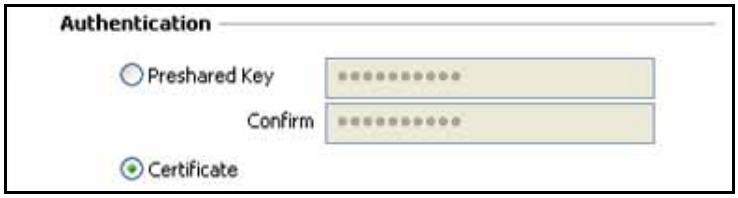
4. Configure the IPSec settings (phase 2 settings).

   For more information, see *Manually Configure IP Security or Phase 2* on page 49.

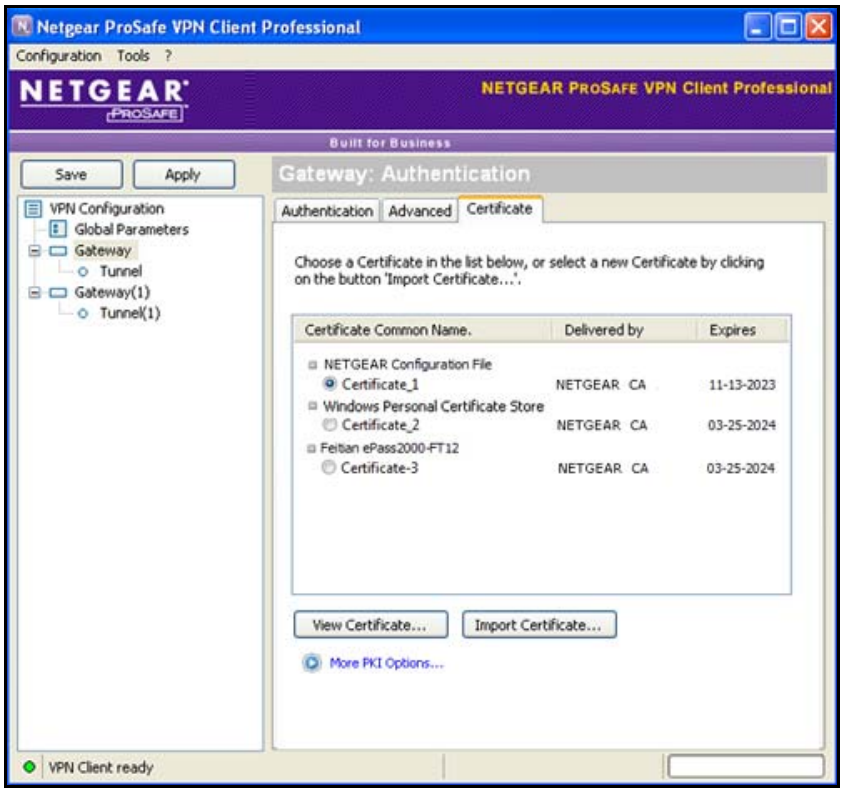
5. Go back to the Authentication pane.
6. Click the **Advanced** tab.

   The Advanced authentication pane displays.

7. Select the **Certificate** radio button.



The Certificate pane displays automatically:



8. (Optional) Import a certificate:
   a. Click **Import Certificate**.

      For more information, see *Import Certificates* on page 73).

   b. Click **OK**.
9. From the list of certificates, select the radio button for the certificate that you want to use.

   For more information, see *View and Assign Certificates* on page 77.
10. Click **Save**.

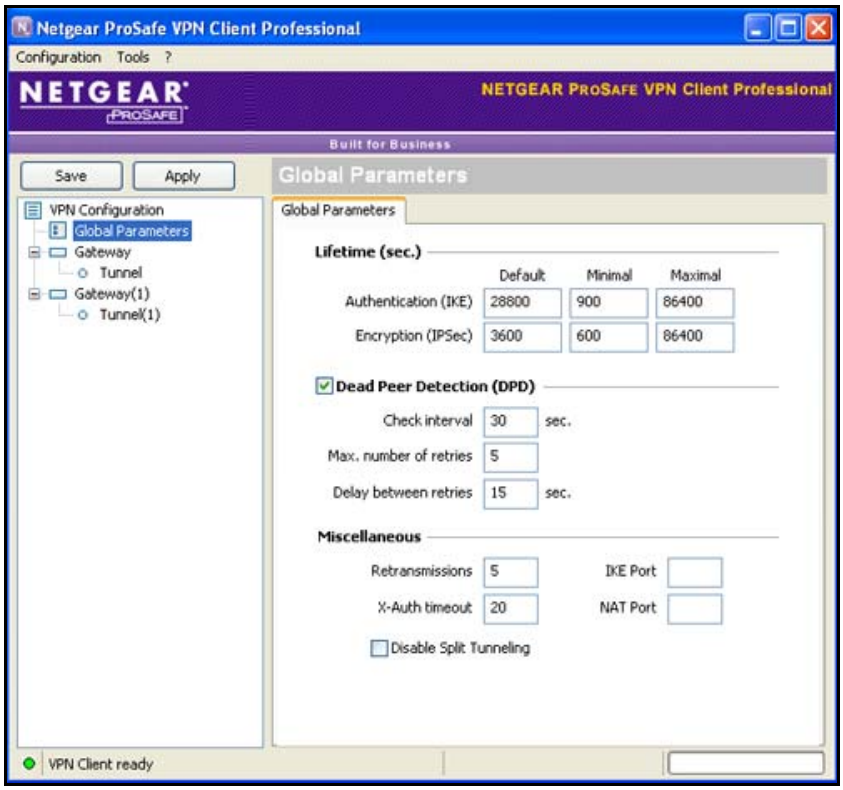
Configure the Global VPN Parameters

The global parameters are generic settings that apply to all VPN tunnels that you create. The default global parameters work well for most VPN configurations. You can modify the global parameters for your specific network. The default settings are shown in the table in the following procedure.

➢ **To configure global parameters:**

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

The Global Parameters pane displays in the Configuration Panel screen.



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

Setting		Description
Lifetime (sec.)		
Authentication (IKE)	Default	Enter the default lifetime for IKE rekeying. The default is 28800 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 3600 sec.
	Minimal	Enter the minimum lifetime for IPSec rekeying. The default is 600 sec.
	Maximal	Enter the maximum 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 Dead Peer Detection (DPD) check box is selected by default; if you want to disable DPD, clear the check box. 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 *Configure How VPN Tunnels Are Opened* on page 59).		
Check interval (sec.)		Enter the interval between DPD messages. The default is 30 sec.

Setting	Description
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 users to enter their XAUTH credentials. The default is 20 sec.
IKE Port	Enter the default UDP port that is used in the IKE negotiation during the authentication phase. 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 the 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.
Disable Split Tunneling	Select this check box to limit traffic to encrypted traffic and force all traffic to go through the VPN tunnel.

3. Click **Save**.

5. Advanced Configuration Options

This chapter describes the advanced configuration options. The chapter includes the following sections:

Configure How VPN Tunnels Are Opened

You can configure a VPN tunnel to open automatically. Automatic tunnel opening is an advanced IPSec setting that applies *only* to the associated IPSec configuration (phase 2 settings) for a VPN tunnel. That is, automatic tunnel opening is not a global setting for the VPN Client.

Configure a Tunnel to Open Automatically

The Advanced IPSec pane provides various options that let you configure a tunnel to open automatically.

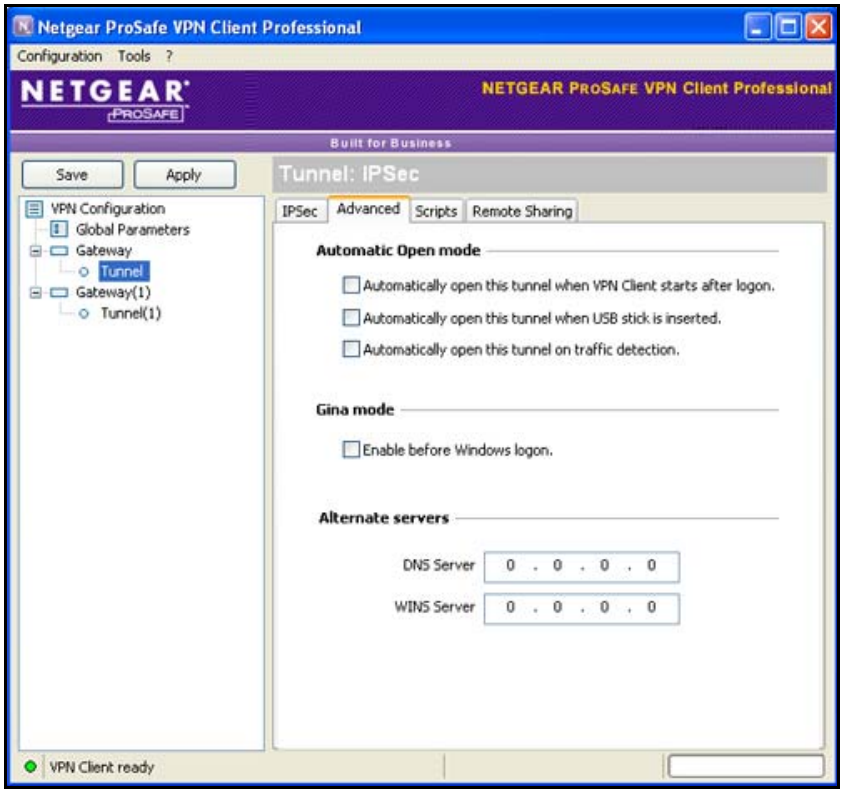
➢ **To configure tunnels to open automatically:**

1. In the tree list pane of the Configuration Panel screen, click the IPSec configuration name (that is, the tunnel) for which you want to configure the advanced settings (for example, Tunnel in the following figure).

   The IPSec pane displays.

2. In the IPSec pane, click the **Advanced** tab.

   The Advanced IPSec pane displays:



3. Configure the settings as described in the following table.

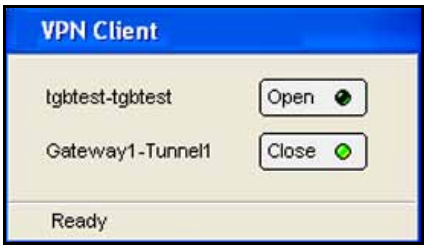
Setting	Description
Automatic Open mode **Note:** When you select any of these check boxes, the VPN Client automatically opens the tunnel to which these advanced settings apply.	
Automatically open this tunnel when the VPN Client starts after login.	Select this check box to automatically open the tunnel when the VPN Client starts after you have logged in. (For more information, see *Open a Tunnel with a Double-Click on a Desktop Icon* on page 62.)
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 68). **Note:** This check box is disabled before Windows logon.
Automatically open this tunnel on traffic detection.	Select this check box to automatically open the tunnel when the VPN Client detects traffic.
Gina Mode	
Enable before Windows logon.	Select this check box to enable Windows Gina mode for Windows 2000 or Windows XP or to enable Windows credential providers for Windows Vista or Windows 7. Gina mode and credential providers allow a tunnel to be used for the Windows logon process. This can be useful when a corporate employee database is used for logon and the remote computer needs to connect to the corporate network before processing the Windows logon. For more information, see the section following this table, *Configure a VPN Tunnel to Open before Windows Logon*. **Note:** When Gina mode or credential providers is enabled, the Scripts pane is disabled.

4. Click **Save**.

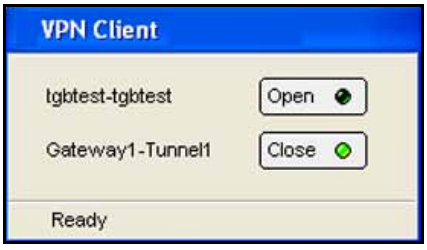
Configure a VPN Tunnel to Open before Windows Logon

You can manually or automatically open one or more VPN tunnels before Windows logon by using a Windows logon technology that is referred to as credential providers in Windows 7 and Windows Vista and as Gina mode in Windows XP and Windows 2000.

➢ To manually open a VPN tunnel before Windows logon:

Procedure	VPN Client Behavior
1. Go to the Configuration Panel screen. 2. Open the Advanced IPSec pane. 3. Select the **Enable before Windows logon** check box. 4. Clear the **Automatically open this tunnel on traffic detection** check box. For more information, see *Configure How VPN Tunnels Are Opened* on page 59.	Before Windows logon, the following pop-up screen displays to allow you to open the required VPN tunnel.  The pop-up screen lists all VPN tunnels for which you have selected the Enable before Windows logon check box on the Advanced IPSec pane.

➢ To configure a VPN tunnel to open automatically before Windows logon:

Procedure	VPN Client Behavior
1. Go to the Configuration Panel screen. 2. Open the Advanced IPSec pane. 3. Select the **Enable before Windows logon** check box. 4. Select the **Automatically open this tunnel on traffic detection** check box. For more information, see *Configure How VPN Tunnels Are Opened* on page 59.	Before Windows logon, the following pop-up screen displays to show the VPN tunnels that are opened automatically.  The pop-up screen lists all VPN tunnels for which you have selected the Enable before Windows logon check box on the Advanced IPSec pane.

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 Advanced IPSec pane:

- You cannot hide the pop-up 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 are running.

- Scripts that you might have configured are disabled.
- The VPN Client cannot function in USB mode (see *USB Mode* on page 68).
- The Mode Config feature is disabled, so you might have to specify DNS or WINS server addresses (see *Configure How VPN Tunnels Are Opened* on page 59).
- When extended authentication (XAUTH) is enabled (see *Extended Authentication* on page 47), a pop-up screen displays when tunnels open to enable you to enter the login name and password.
- When you use a USB token or smart card, a pop-up screen displays when tunnels open to enable you to enter the PIN code.

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

The following procedure lets you create a desktop icon for easy opening of a VPN tunnel.

➢ **To configure a tunnel to open with a double-click on a desktop icon:**

1. In the Advanced authentication pane of the Configuration Panel screen, select the **Automatically open this tunnel when the VPN Client starts after login** check box.
2. From the main menu on the Configuration Panel screen, select **Configuration > Export**.

   The Export Protection screen displays:

3. Select one of the following radio buttons:
   - **Don’t protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. The VPN configuration file requires a password before it can be opened.
     a. (Optional) Clear the **Hide password** check box.
     b. Enter a password in the Password field.
     c. Enter the same password in the Confirm field.

4. Click **OK**.
5. Navigate to the location where you want to save the VPN configuration file.
6. Type a name for the VPN configuration file.

   An exported VPN configuration file has a .tgb extension. Do not change this extension.

   The VPN configuration is exported.
7. Place a shortcut of the VPN configuration file on the desktop.

Figure 13. VPN configuration shortcut icon

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

Configure Alternate DNS and WINS Servers

Alternate DNS and WINS servers are part of an advanced IPSec setting that applies *only* to the associated IPSec configuration (phase 2 settings) for a VPN tunnel. That is, these alternate servers do not apply to the global setting of the VPN Client.

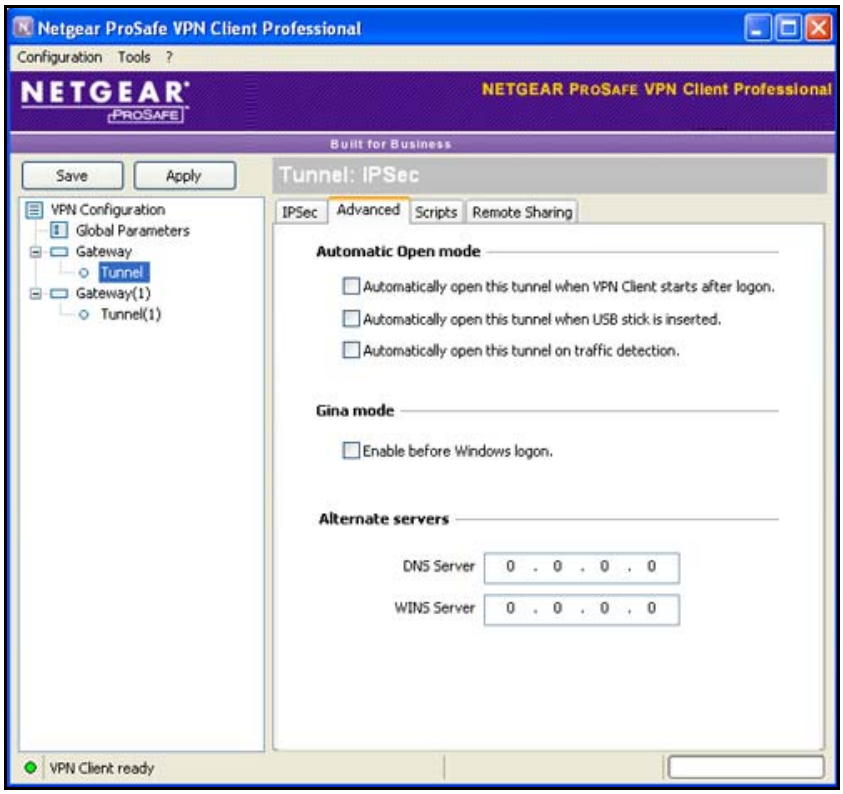
You can configure the alternate servers only when the Mode Config feature is disabled. When the Mode Config feature is enabled (see *Configure Advanced Authentication* on page 44), the Alternate server fields are disabled.

➢ **To configure alternate DNS and WINS servers:**

1. In the tree list pane of the Configuration Panel screen, click the IPSec configuration name (that is, the tunnel) for which you want to configure the advanced settings (for example, Tunnel in the following figure).

   The IPSec pane displays.
2. In the IPSec pane, click the **Advanced** tab.

The Advanced IPSec pane displays:



3. (Optional) In the Alternate Server section, configure the following settings:
   - **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.

     If Mode Config is enabled, the DNS server address that is issued by the remote VPN gateway is displayed in this field.
   - **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.

     If Mode Config is enabled, the WINS server address that is issued by the remote VPN gateway is displayed in this field.
4. Click **Save**.

Configure Scripts

This feature enables you to specify and execute scripts (including batches and applications) at each step of a tunnel connection for various purposes. For example, you can use a script to detect the current software release, to detect the database availability before launching a backup application, to configure the network, or to detect whether a software application is running or a logon procedure is specified.

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

- Before the tunnel is opened
- After the tunnel is opened
- Before the tunnel closes
- After the tunnel is closed

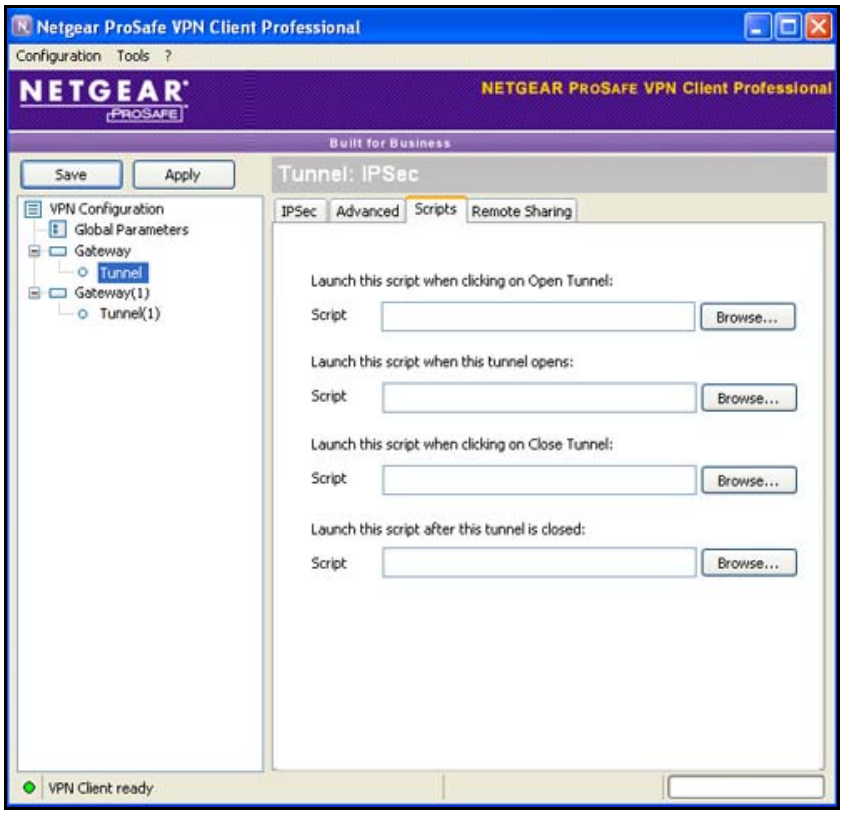
➢ **To configure scripts:**

1. In the tree list pane of the Configuration Panel screen, click the IPSec configuration name (that is, the tunnel) for which you want to configure the advanced settings (for example, Tunnel in the following figure).

   The IPSec pane displays.

2. In the IPSec pane, click the **Scripts** tab.

   The Scripts pane displays:



3. Click **Browse** to navigate to a script file and open it.

   You can open up to four script files in the Scripts pane:

   - 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.

4. Click **Save**.

➢ **To configure a web page to open automatically when a VPN tunnel opens:**

1. In the IPSec pane of the Configuration Panel screen, click the **Scripts** tab.

   The Scripts pane displays.

2. In the Launch this script when this tunnel opens field, enter the URL of the web page that you want to open.

   For example, enter http://support.netgear.com/product/VPNG05L.

3. Click **Save**.

When the tunnel for which the script is defined opens, the web page opens automatically.

Configure Remote Sharing

This feature enables you to specify remote computers that you can connect to for desktop sharing after the VPN tunnel has been established.

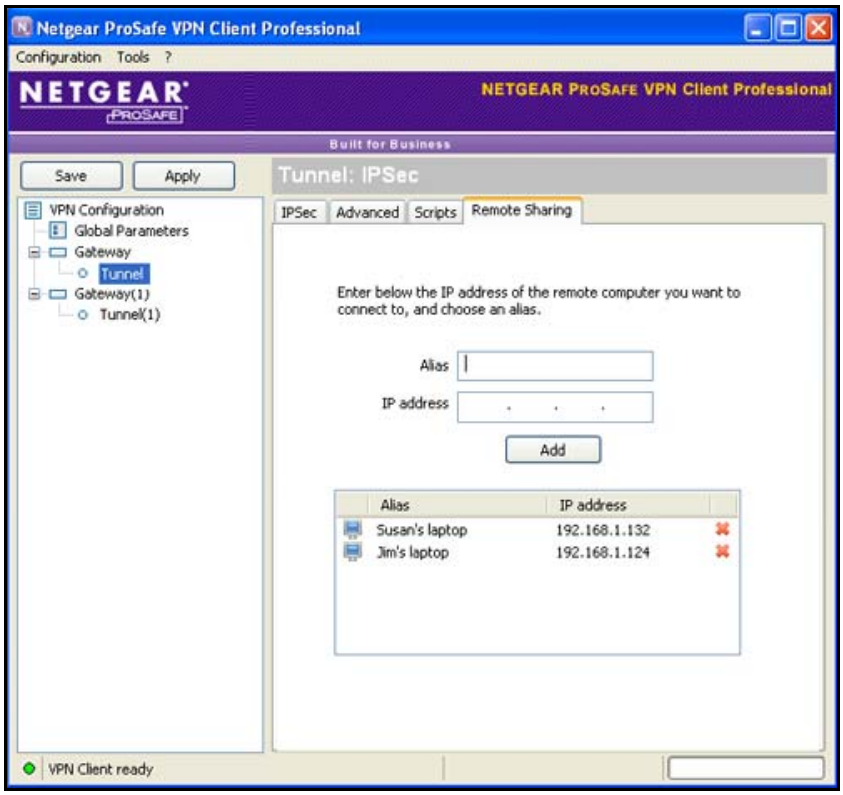
➢ **To add a computer for remote sharing:**

1. In the tree list pane of the Configuration Panel screen, click the IPSec configuration name (that is, the tunnel) for which you want to configure the advanced settings (for example, Tunnel in the following figure).

   The IPSec pane displays.

2. In the IPSec pane, click the **Remote Sharing** tab.

The Remote Sharing pane displays:



3. In the Alias field, enter a name for the remote computer.
4. In the IP address field, enter the IP address for the remote computer.

   This IP address needs to be an address in the subnet or IP range of the remote LAN.
5. Click **Add**.

   The computer is added to the computer to the table.

After you have defined a remote computer, you can connect to it from the system tray menu. The VPN tunnel with which the remote computer is associated opens automatically.

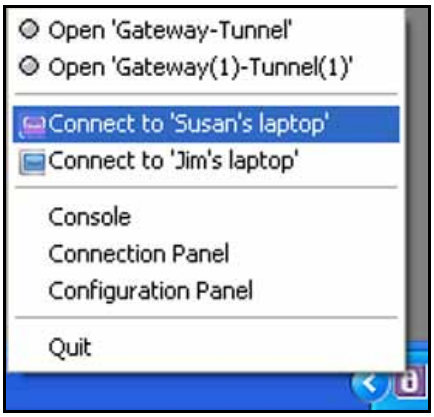


Figure 14. Remote computer option in the system tray menu

USB Mode

The VPN Client lets you save VPN configurations and VPN security elements such as pre-shared 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.

This section includes the following subsections:

Enable a New USB Drive with a VPN Configuration

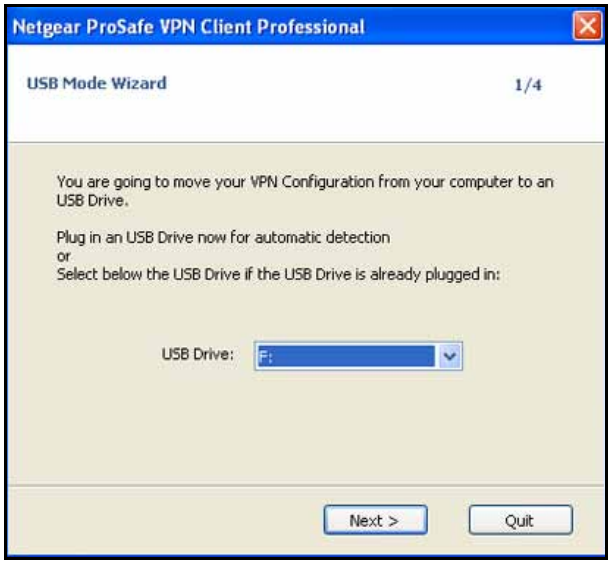
You can enable a new USB drive by copying a VPN configuration and its security elements onto it in one of the following ways:

- From the main menu of the Configuration Panel screen, select **Configuration > Export**, and 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. From the main menu of the Configuration Panel screen, select **Configuration > Move to USB Drive**.

   The USB Mode Wizard 1/4 screen displays:



   If one or more USB drives are already inserted, the VPN Client detects and displays them. In the previous figure, drive F: is selected.

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**.

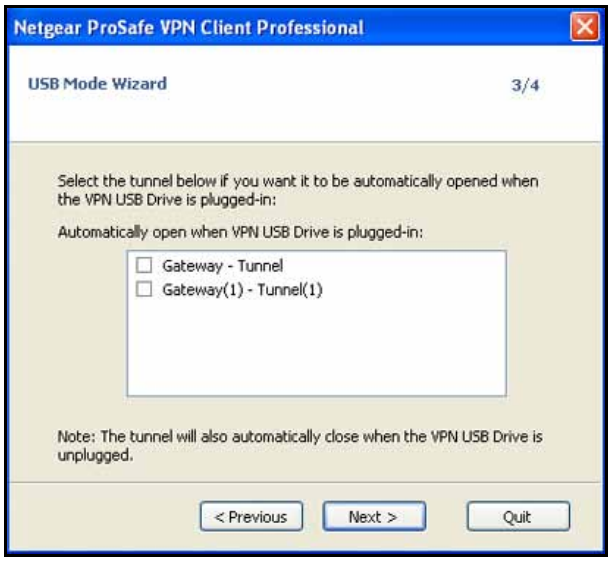
The USB Mode Wizard 2/4 screen displays:

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. (Optional) Protect the VPN configuration with a password by entering one in the Password field.
5. (Optional) 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.

6. Click **Next**.

The USB Mode Wizard 3/4 screen displays:

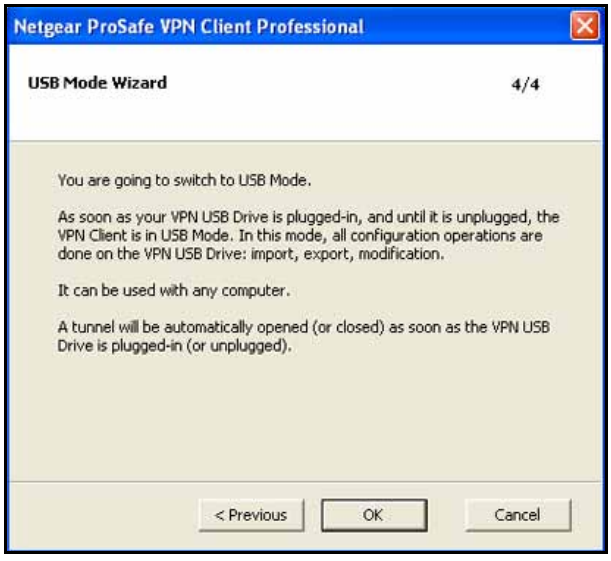


7. Specify the tunnel or tunnels that you want to open automatically by selecting the associated check boxes.

   Tip: If there is only one tunnel configured, select the **Automatically open this tunnel when USB stick is inserted** check box on the Advanced IPSec screen (see *Configure How VPN Tunnels Are Opened* on page 59).

8. Click **Next**.

   USB Mode Wizard 4/4 screen displays. This screen is a summary screen.



9. Click **OK**.

The USB settings are saved. The VPN configuration and its associated security information are 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 a VPN Configuration* on page 87.

To Configure Tunnels to Open Automatically with a USB Drive

After you have enabled a USB drive with a VPN tunnel configuration, you can configure the VPN Client to open the tunnel automatically when you insert the USB drive.

➢ **To enable a tunnel to open automatically when you insert a USB drive:**

1. In the tree list pane of the Configuration Panel screen, click the tunnel for which you want to configure the advanced settings.

   The IPSec pane displays.

2. In the IPSec pane, click the **Advanced** tab.

   The Advanced IPSec pane displays.

3. On the Advanced IPSec pane, select the **Automatically open this tunnel when USB stick is inserted** check box.

   Note: *If there is more than one tunnel configured, make sure that, on the USB Mode Wizard 3/4 screen, you have selected which tunnel or tunnels should be opened. For more information, see Enable a New USB Drive with a VPN Configuration on page 68.*

4. (Optional) Insert a USB drive that contains a VPN configuration.

   The tunnel opens automatically.

Note: *If you insert a USB drive without a VPN configuration, or if you do not insert a USB drive, the VPN Client starts in local mode and uses a VPN configuration that is available on the local disk.*

Certificate Management

This section includes the following subsections:

Certificate Concepts

The VPN Client can use X509 certificates from various sources:

- PEM format file (also referred to as PEM certificate)
- PKCS#12 format file (also referred to as P12 certificate)
- Personal Certificate Store
- USB token or smart card

The Certificate pane 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 smart card 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 or purchase certificates from the Microsoft Certificate Store. You can store certificates on USB tokens and smart cards.

For information about how to specify if and how a certificate is validated, which certificate is used, and which USB token or smart card reader is used, see *Configure PKI Options* on page 84.

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).

For each tunnel, you can import and assign one PEM certificate and one P12 certificate.

Note: After you have imported a PEM or P12 certificate, the Local ID fields on the associated Advanced authentication pane 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 *Configure Advanced Authentication* on page 44.

PEM Certificates

➢ **To import a PEM certificate in a tunnel configuration:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to import a certificate.

   The Authentication pane displays.

2. In the Authentication pane, click the **Certificate** tab.

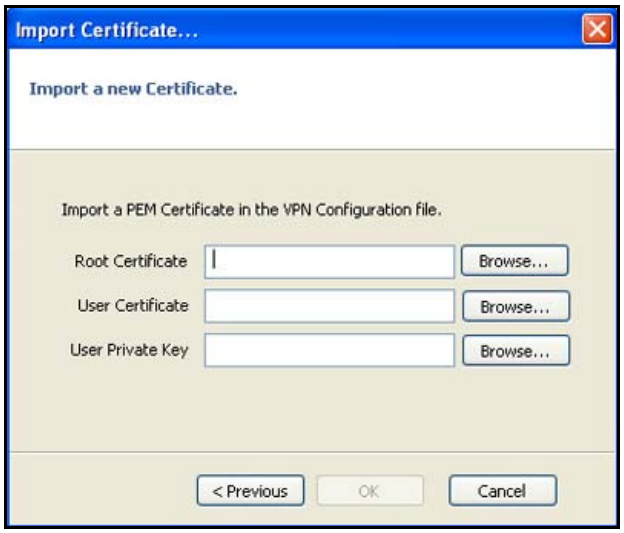
   The Certificate pane displays.

3. Click **Import Certificate**.

   The Import Certificate screen displays:

4. Select the **PEM Format** radio button.
5. Click **Next**.

6. The (PEM) Import Certificate screen displays:



7. Import the three PEM certificate files:
   - **Root Certificate**. Click **Browse**, and locate the root certificate file that you want to import. This file has either a .pem or a .crt extension.
   - **User Certificate**. Click **Browse**, and locate the user certificate file that you want to import. This file has either a .pem or a .crt extension.
   - **User Private Key**. Click **Browse**, and 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 cannot be encrypted or protected with a password.*

8. Click **OK**.

   The certificate is imported, and the Certificate pane displays the certificate.

9. Click **Save**.

P12 Certificates

➢ **To import a P12 certificate in a tunnel configuration:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to import a certificate.

   The Authentication pane displays.

2. In the Authentication pane, click the **Certificate** tab.

   The Certificate pane displays.

3. Click **Import Certificate**.

The Import Certificate screen displays:

4. Select the **P12 Format** radio button.
5. Click **Next**.

   The (P12) Import Certificate screen displays:

6. Click **Browse**, and 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**.

The PKCS12 password file screen displays:

8. Enter the password.
9. Click **OK**.

   The certificate is imported, and the Certificate pane displays the certificate.
10. Click **Save**.

View and Assign Certificates

The Certificate pane lets you can view and assign certificates that you have imported in the VPN Client.

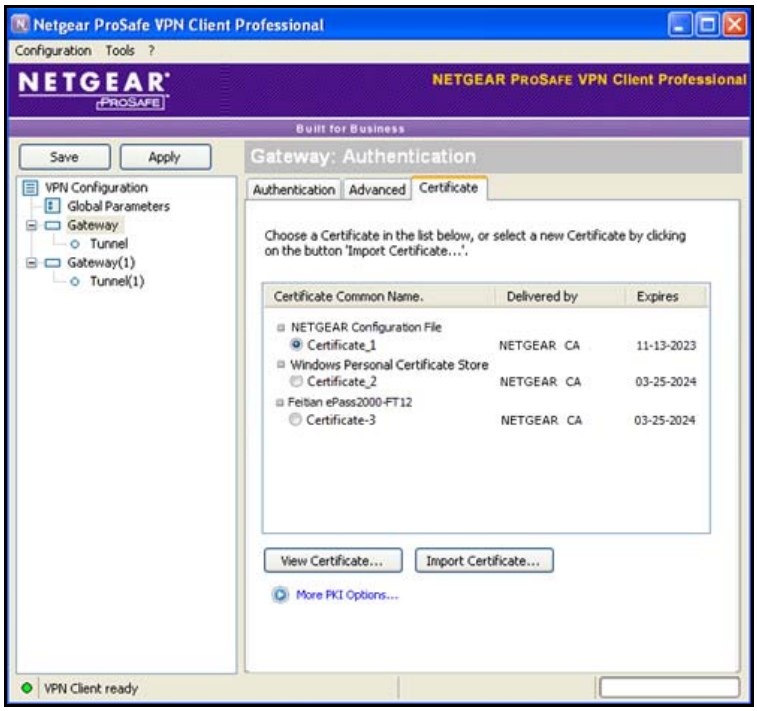
➢ **To view certificates and assign a certificate to a tunnel:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to configure a certificate (for example, Gateway in the following figure).

   The Authentication pane displays.
2. Select the **Certificate** radio button.

   The Certificate pane displays.

3. (Optional) If the Certificate pane does not display, click the **Certificate** tab.



The previous figure shows several sources from which you can select certificates. These sources are described in the following table.

Source	Description
NETGEAR configuration file	Certificates are located in the VPN configuration file that the VPN Client uses. These certificates have been imported previously from another source such as a certificate file or the Microsoft Certificate Store.
Windows Personal Certificate Store	Certificates are located in the Personal Certificate Store. To be visible and usable, certificates need to be certified and in the correct location: • Certificates need to be certified by a certificate authority (CA), and the certificate status needs to be OK (see also *Troubleshoot Certificates* on page 82). • Certificates need to 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 smart card (such as Feitian ePass2000-FT21)	Certificates are located on one or more USB tokens and smart cards and are configured on the VPN Client. For you to use a certificate from a USB token or smart card, the USB token or smart card needs to be plugged into the computer. **Note:** When you remove the USB token or smart card from the computer, the certificate remains displayed on the Certificates pane but cannot be used until you plug the USB token or smart card back into the computer.

4. Select one certificate from the list by selecting its associated radio button.

   You can select and assign only one certificate to a tunnel.

5. (Optional) Click the **More PKI Options** link.

   The PKI Options pane of the Options screen displays. For information about how to configure these options, see *Configure PKI Options* on page 84.

6. Click **Save**.

View Certificate Details

You can view many details about a certificate, such as the certificate issuer, the period during which the certificate is valid, the signature algorithm, and type of public key.

➢ **To view the details of a certificate:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to view a certificate.

   The Authentication pane displays.

2. In the Authentication pane, click the **Certificate** tab.

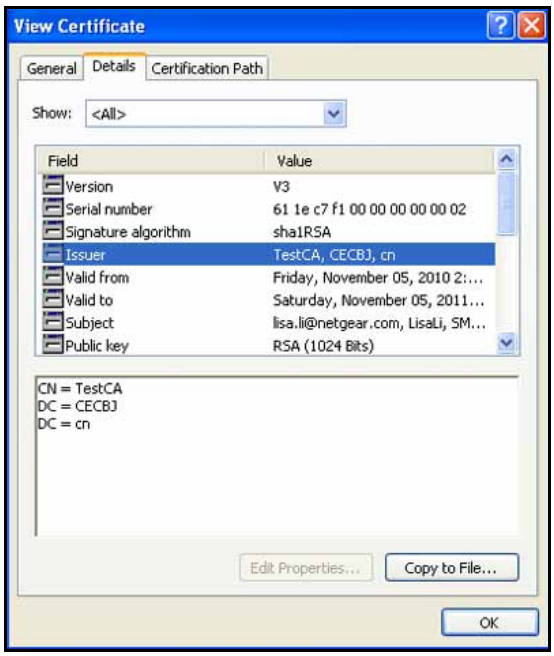
   The Certificate pane displays.

3. Select the certificate for which you want to view the details from the certificate list.
4. Click **View Certificate**.

   The View Certificate screen displays (this can take up to 30 seconds), with the General tab selected by default.

5. Click the **Details** tab.

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



6. (Optional) Click the **Certification Path** tab.

   The certification path (a chain of related certificates) displays.

7. (Optional) Click **Copy to File**.

   The Certificate Export Wizard opens. This wizard enables you to export the certificate to a file.

8. Click **OK**.

   The View Certificate screen closes.

Use Certificates from USB Tokens and Smart Cards

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 smart card:**

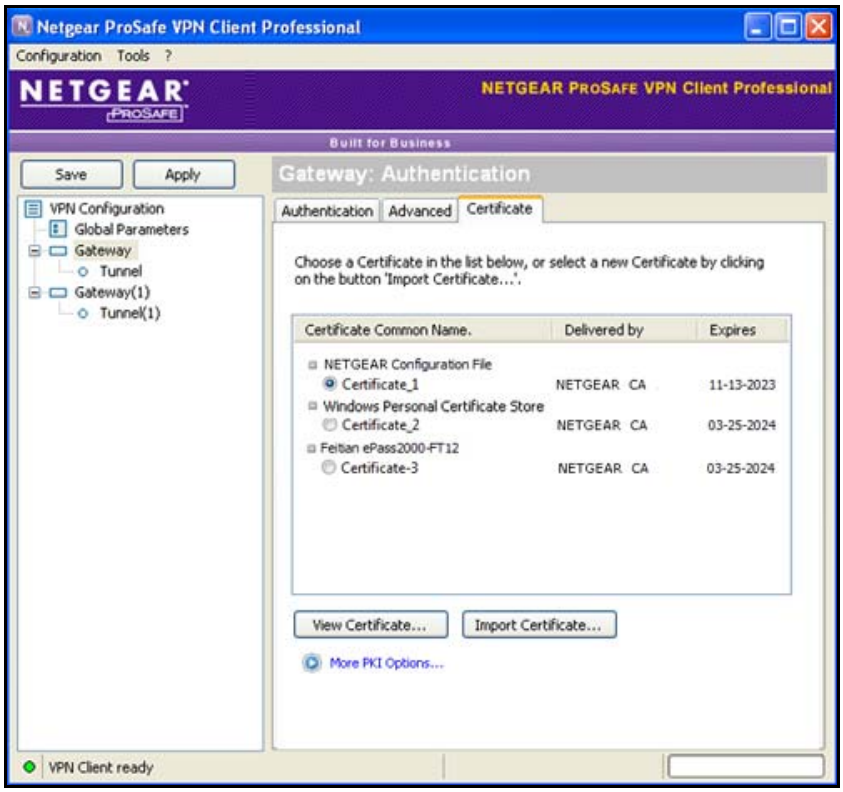
1. Insert a USB token or smart card into the computer.
2. If requested as part of USB token or smart card reader identification process, enter the PIN code.

   Note: *If the PIN code is incorrect, the VPN Client displays a message that the USB token or smart card will be locked out after three consecutive attempts to access the USB token or smart card with an incorrect PIN code.*

3. Click **OK**.
4. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to use the certificate from the USB token or smart card.

   The Authentication pane displays.
5. In the Authentication pane, click the **Certificate** tab.

   The Certificate pane displays:



   The certificates from the USB token or smart card have been automatically imported and display in the certificates list.
6. Select a certificate by selecting its radio button.
7. (Optional) Click the **More PKI Options** link.

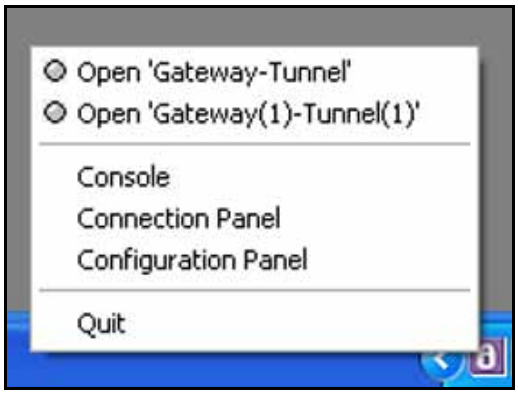
   The PKI Options pane of the Options screen displays. For information about how to configure these options, see *Configure PKI Options* on page 84.
8. Click **Save**.

Open a Tunnel with Certificates from a USB Token or Smart Card

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

➢ **To open a tunnel with a certificate from a USB token or smart card:**

1. Ensure that either the smart card reader is inserted in the computer and contains a smart card or the USB token is inserted in the computer.
2. Right-click the system tray icon, and select **Open '*<gateway name-tunnel name>*'**.



3. Enter the PIN code that is associated with the USB token or smart card.

   The tunnel opens.

Troubleshoot Certificates

This section provides information about troubleshooting USB tokens, smart cards, and the Personal Certificate Store.

Troubleshoot USB Tokens and Smart Cards

When an error occurs while you use a USB token or smart card, a small warning icon displays next to the token name. Click this warning icon to open a pop-up screen 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 smart card.

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

  Resolution. Install the software (middleware) that enables your computer to read the smart card, 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.

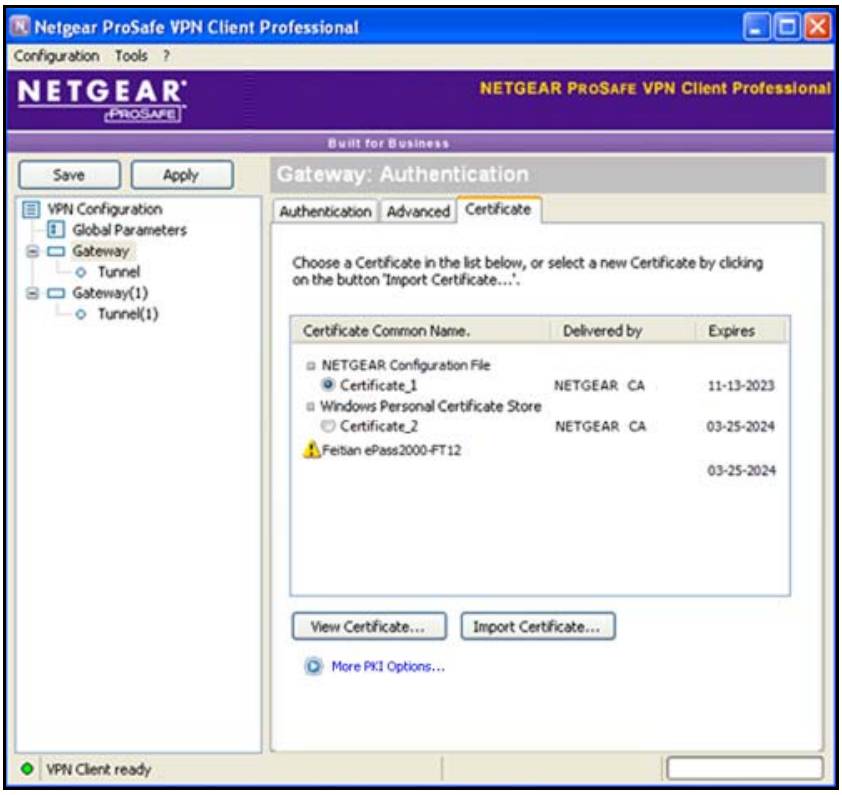


Figure 15. Example of a certificate error

Troubleshoot the Personal Certificate Store

To prevent errors in the Personal Certificate Store, ensure the following:

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

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

Configure PKI Options

The PKI Options pane lets you specify if and how a certificate is validated, which certificate is used, and which USB token or smart card reader is used.

Note: The PKI Options pane is not available in the VPN Client Lite.

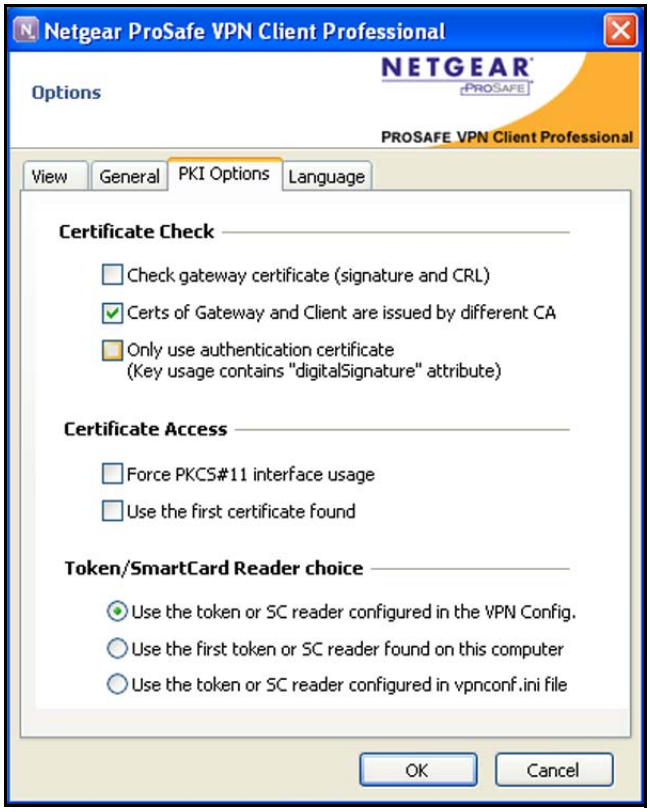
➢ **To configure the public key infrastructure (PKI) options:**

1. From the main menu, select **Tools > Options**.

   The Options screen displays. The View pane is selected by default.

2. Click the **PKI Options** tab.

   The PKI Options pane displays:



3. Configure the settings as described in the following table:

Setting	Description
Certificate Check	
Check gateway certificate (signature and CRL)	Select this check box to force the VPN Client to validate the certificate of the VPN gateway during the opening of the tunnel. The certificate expiration date is validated, and the signatures of the certificates in the certification chain and the associated Certificate Revocation Lists (CRLs) are validated. For this option to function, make sure that: • The root certificate, intermediate certificates, and the server certificate are imported into the Windows Certificate Store. • The CRLs for the certificate of the VPN gateway are imported into the Windows Certificate Store or are downloadable. By default, this check box is cleared and the VPN Client does not validate the certificate of the VPN gateway during the opening of the tunnel.
Certs of Gateway and Client are issued by different CA	Select this check box to allow the VPN Client and the VPN gateway to use certificates from different certificate authorities. By default, this check box is cleared and the VPN Client and VPN gateway need to use certificates from the same certificate authority.
Only use authentication certificate (Key usage contains “digitalSignature” attribute)	Select this check box to force the VPN Client to use only an authentication certificate for which the digitalSignature key extension is configured. This option lets you specify a particular certificate among multiple ones. For example, this is useful when several certificates with the same subject are stored on a smart card or token. By default, this check box is cleared and the VPN Client can use any certificate.
Certificate Access	
Force PKCS#11 interface usage	Select this check box to force the VPN Client to use only PKCS #11 middleware to access tokens or smart cards. By default, this check box is cleared and the VPN Client uses cryptographic service provider (CSP) middleware to access smart cards or tokens.
Use the first certificate found	Select this check box to force the VPN Client to use the first certificate that it detects on a specified smart card or token, regardless of the subject of the certificate that might be configured in the Local ID field on the Advanced authentication pane (see *Configure Advanced Authentication* on page 44). By default, this check box is cleared and the VPN Client can use any certificate.

Setting	Description
Token/SmartCard Reader choice	
Use the token or SC reader configured in the VPN config	Select this check box to force the VPN Client to first look for smart card readers and token readers that are stored in the VPN configuration. By default, this check box is cleared and the VPN Client can use any smart card readers and token readers.
Use the first token or SC reader found on this computer	The VPN Client uses the first smart card reader or token reader that it detects on the computer. By default, this check box is cleared and the VPN Client can use any smart card readers and token readers.
Use the token or SC reader configured in vpnconfig.ini file	Select this check box to force the VPN Client to first look for smart card readers and token readers that are stored in the vpnconf.ini configuration file. For information about how to modify the vpnconfig.ini file, see *Customize How the VPN Client Handles Readers and Certificates* on page 126. By default, this check box is cleared and the VPN Client can use any smart card readers and token readers.

4. Click **OK**.

VPN Configuration Management

A VPN configuration is a file that contains the configuration and tunnel information of the VPN Client. You import an existing VPN configuration, export your current VPN configuration, merge your current VPN configuration with an existing VPN configuration, split your current VPN configuration, and perform other tasks in relation to a VPN configuration.

> **Note:** For information about how to use the command-line interface (CLI) to perform tasks with a VPN configuration file, see *Import, Export, Add, or Replace the VPN Configuration* on page 124.

This section includes the following subsections:

- *Import a VPN Configuration*
- *Export a VPN Configuration*
- *Merge VPN Configurations*
- *Split a VPN Configuration*
- *Easily Import a VPN Configuration and Open a Tunnel*

Import a VPN Configuration

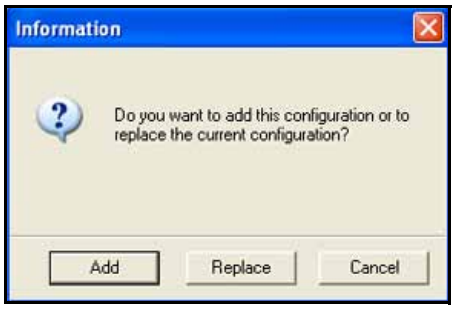
The VPN Client can import or export a VPN configuration. A network administrator typically uses this capability to prepare a configuration and deliver it to end users.

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.

➢ **To import a VPN configuration:**

1. From the main menu on the Configuration Panel screen, select **Configuration > Import**.
2. Navigate to the location of the VPN configuration file that you want to import.
3. Click **Open**.

   An Information screens displays:



4. Click 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 pane of the Configuration Panel screen.

Export a VPN Configuration

When you export authentication settings (phase 1 settings), the associated IPSec configurations (phase 2 settings) are also exported, including certificates that might have been defined in the IPSec configuration, and global parameters.

➢ **To export a VPN configuration:**

1. From the main menu on the Configuration Panel screen, select **Configuration > Export**.

   The Export Protection screen displays:

   As a security measure, you can 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**. The VPN configuration file requires a password before it can be opened.
     a. (Optional) Clear the **Hide password** check box.
     b. Enter a password in the Password field.
     c. Enter the same password in the Confirm field.
3. Click **OK**.
4. Navigate to the location where you want to save the VPN configuration file.
5. Type a name for the VPN configuration file.

   An exported VPN configuration file has a .tgb extension. Do not change this extension.

6. Click **Save**.

You can now forward the VPN configuration or navigate to the location of the VPN configuration and double-click the VPN configuration shortcut icon to start the VPN Client.

Figure 16. VPN configuration shortcut icon

Merge VPN Configurations

You can import one or several tunnels into an existing VPN configuration. A network administrator typically uses this capability to merge a new VPN configuration with new gateways into an existing VPN configuration and deliver it to end users. There are several methods that you can use to merge VPN configurations.

Regardless of how you import a VPN configuration, the following rules apply:

- If at least one tunnel is already configured before you import and add the VPN configuration, global parameters are *not* imported.
- If you import and replace the VPN configuration, or if no tunnel is configured when you import and add the VPN configuration, global parameters *are* imported.
- If there is a tunnel name conflict between an existing and an imported VPN configuration, the VPN Client automatically resolves this conflict by adding an increment between parentheses—for example, tunnel_office(1)—to the imported tunnel name.

➢ **To merge a VPN configuration with your current VPN configuration:**

1. Do one of the following:
   - From the main menu on the Configuration Panel screen, select **Configuration > Import**.
   - Drag and drop a new VPN configuration onto the tree list pane of the Configuration Panel screen.
2. Navigate to the location of the VPN configuration file that you want to import.
3. Click **Open**.

   An Information screens displays.
4. Click **Add**.

   The imported VPN configuration is merged with your current VPN configuration.

Split a VPN Configuration

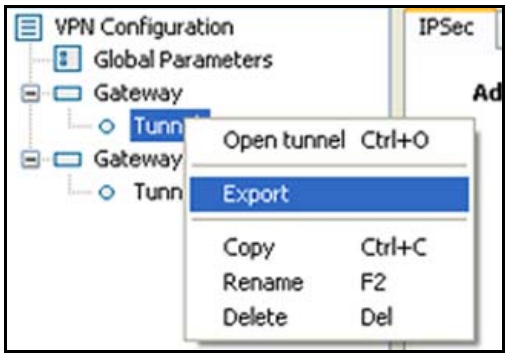
You can split and export a single tunnel configuration from an existing VPN configuration. A network administrator typically uses this capability to split an existing large VPN configuration into a smaller VPN configuration and deliver it to end users.

When you split and export an IPSec configuration (phase 2 settings), the associated authentication settings (phase 1 settings) are also exported, including certificates that might have been defined in the authentication settings, and global parameters.

➢ **To export a single tunnel configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the IPSec configuration name (that is, the tunnel) for which you want to export the tunnel configuration (for example, Tunnel in the following figure).

2. Select **Export**.



The Export Protection screen displays:

As a security measure, you can specify a password for the exported file.

3. Select one of the following radio buttons:
   - **Don't protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. The VPN configuration file requires a password before it can be opened.
     a. (Optional) Clear the **Hide password** check box.
     b. Enter a password in the Password field.
     c. Enter the same password in the Confirm field.
4. Click **OK**.
5. Navigate to the location where you want to save the VPN configuration file.
6. Type a name for the VPN configuration file.

   An exported VPN configuration file has a .tgb extension. Do not change this extension.
7. Click **Save**.

You can now forward the VPN configuration or navigate to the location of the VPN configuration and double-click the VPN configuration shortcut icon to start the VPN Client.

Figure 17. VPN configuration shortcut icon

Easily Import a VPN Configuration and Open a Tunnel

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) or use a drag-and-drop procedure to add the VPN configuration to the existing configuration or replace the existing VPN configuration.

> **Note:** You can include a preconfigured VPN configuration in the VPN Client software setup. A network administrator typically uses this capability to deploy a preconfigured VPN Client in a single package to end users. For information about this capability, see *Embed a VPN Configuration in a VPN Client Software Setup Deployment* on page 118.

The following procedure provides high-level steps only.

➢ **To create a VPN configuration shortcut icon on the desktop and easily open a tunnel:**

1. Configure a tunnel on the Configuration Panel screen.

   For information about how to configure a VPN tunnel, see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 36 or *High-Level Steps to Manually Create a VPN Tunnel Connection* on page 40.

2. Configure the tunnel to automatically open when the VPN Client starts after login.

   For more information, see *Configure How VPN Tunnels Are Opened* on page 59.

3. Export the VPN configuration onto your computer desktop.

   For more information, see *Export a VPN Configuration* on page 87.

4. To open the VPN tunnel, do one of the following:
   - Double-click the VPN configuration icon.
   - Use a drag-and-drop procedure to add the VPN configuration to the existing configuration or replace the existing VPN configuration:
     a. Drag and drop the VPN configuration icon onto the Configuration Panel.
     b. Click **Add** or click **Replace**.
     c. Click **Apply** or click **Save**.

   The VPN tunnel is opened.

Configure Access Control

Note: This option is not available in the VPN Client Lite.

Access control is a feature that is intended for use by a network administrator. 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 protected with a password; 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) 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.

In all of these circumstances, the Access Control screen displays.

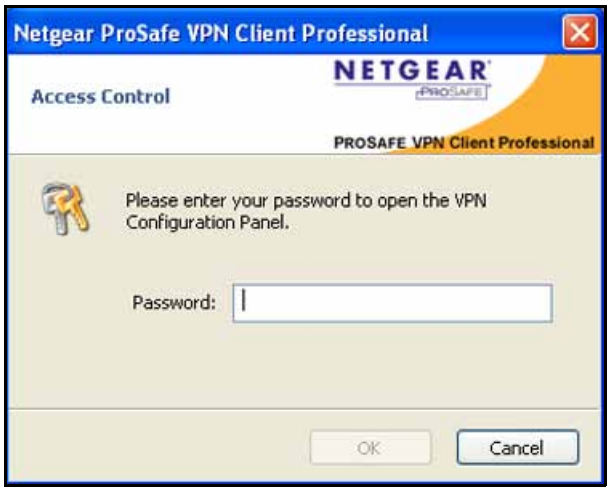


Figure 18. Access Control screen

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

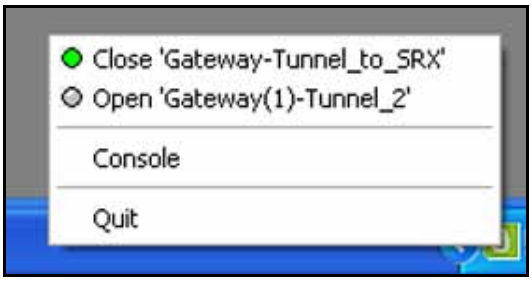
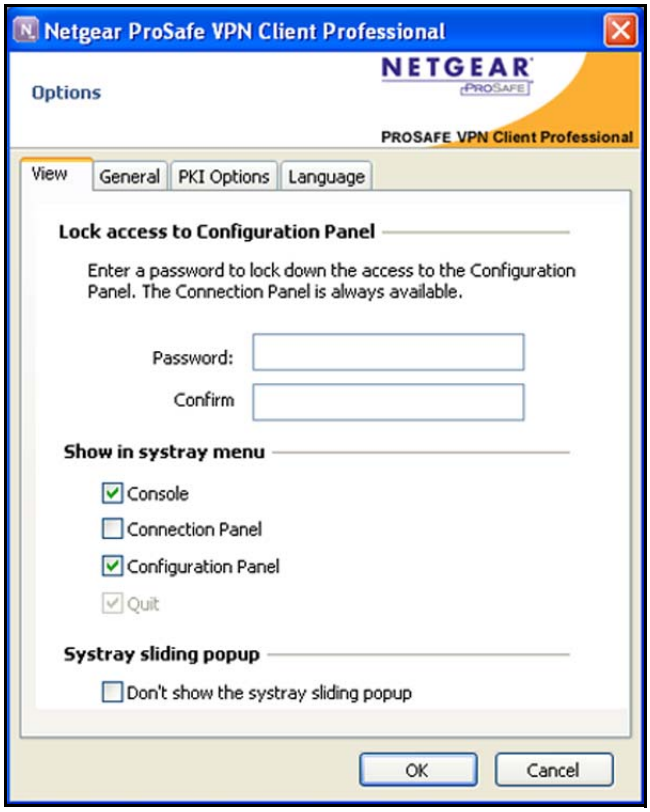


Figure 19. System tray menu with access control enabled

➢ **To configure access control:**

1. From the main menu, select **Tools > Options**.

   The Options screen displays. The View pane is selected by default.



2. Enter a password in the Password and Confirm fields.
3. Click **OK**.

Note: You can also configure this password as an option of the software setup (see *Require a Password to Access the Configuration Panel Screen* on page 110).

➢ **To remove access control:**

1. From the main menu, select **Tools > Options**.

   The Options screen displays. The View pane is selected by default.

2. Clear the Password and Confirm fields.
3. Click **OK**.

Configure the User Interface

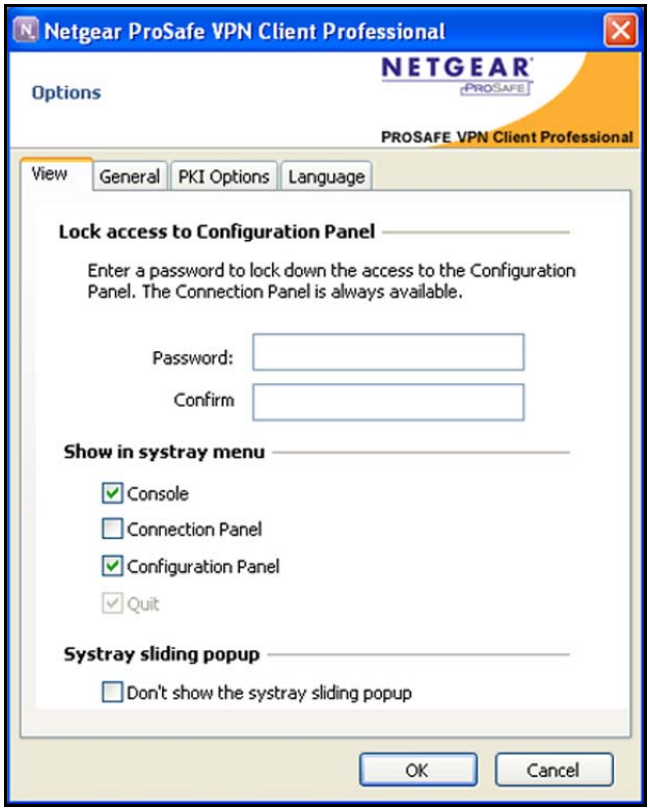
Note: The View pane is not available in the VPN Client Lite.

The View pane lets you configure the system tray menu items such as the Console, Connection Panel, and Configuration Panel, and the pop-up screens in the system tray (which are referred to as the systray sliding pop-ups). In this way, a network administrator can limit the access that the user interface provides or even completely hide the user interface.

➢ **To configure the user interface and systray pop-up screens:**

1. From the main menu of the Configuration Panel, select **Tools > Options**.

   The Options screen displays. The View pane is selected by default.



2. (Optional) In the Show in systray menu section of the pane, select any or all of the following items to be hidden in the user interface by clearing the associated check boxes:
   - **Console**.
   - **Connection Panel**.
   - **Configuration Panel**.

   Note: *The Quit check box is disabled. You cannot disable the Quit link in the system tray menu from the View pane. For information about disabling the Quit link in the system tray menu, see* *Configure Which Items of the System Tray Menu Are Visible on page 111.*

3. (Optional) In the systray sliding pop-up section of the pane, select the **Don't show the systray sliding popup** check box to hide the system tray pop-up screen in the user interface.
4. Click **OK**.

Configure VPN Client Startup Mode and Network Interface Detection

Note: These options are not available in the VPN Client Lite.

The General pane lets you specify if the VPN Client starts automatically after you have logged in to Windows and whether the VPN Client detects disconnection of the network interface.

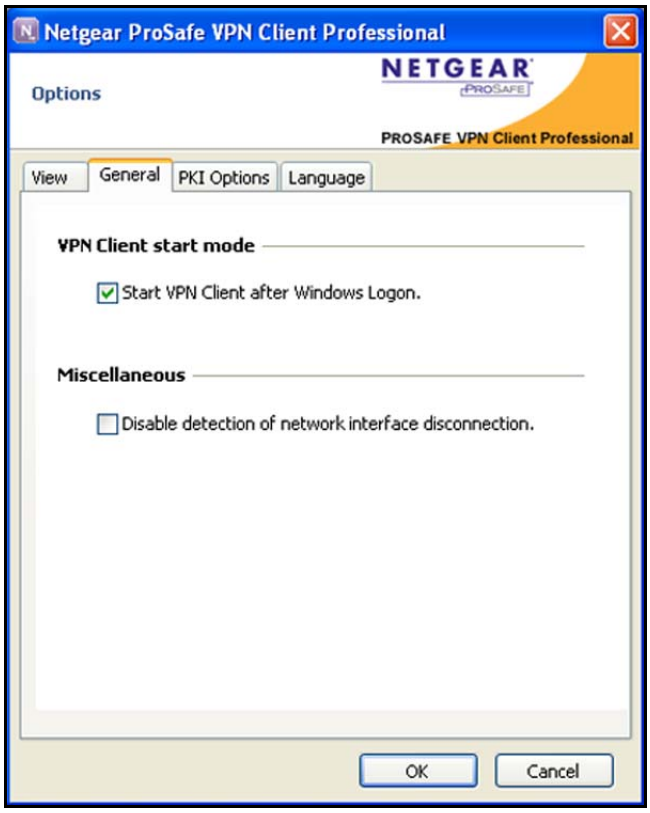
➢ **To configure the VPN Client startup mode and network interface failure detection:**

1. From the main menu, select **Tools > Options**.

   The Options screen displays. The View pane is selected by default.

2. Click the **General** tab.

The General pane displays:



3. (Optional) Clear the **Start VPN Client after Windows Logon** check box to prevent the VPN Client from starting after you have logged in to Windows.

   In this case, you need to manually start the VPN Client or use a script to start it.

   By default, the check box is selected to start the VPN Client after you have logged in to Windows.

   Note: *You can also configure how the VPN Client starts in the software setup (see Customize VPN Client Display and Access for End Users on page 108).*

4. (Optional) Select the **Disable detection of network interface disconnection** check box to enable network interface failure detection.

   By default, the check box is cleared to disable the detection of interface disconnection so that 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, such as a WiFi, GPRS, or 3G interface, is unstable.

5. Click **OK**.

Configure Languages

Note: This option is not available in the VPN Client Lite.

The Language pane includes a drop-down menu that lets you change the VPN Client language without having to restart the VPN Client. You can also manually edit the translation in a very easy way, or even translate an existing language into another language that is not yet supported on the VPN Client to create a new localization.

For a list of the supported languages, see *Table 1* on page 8.

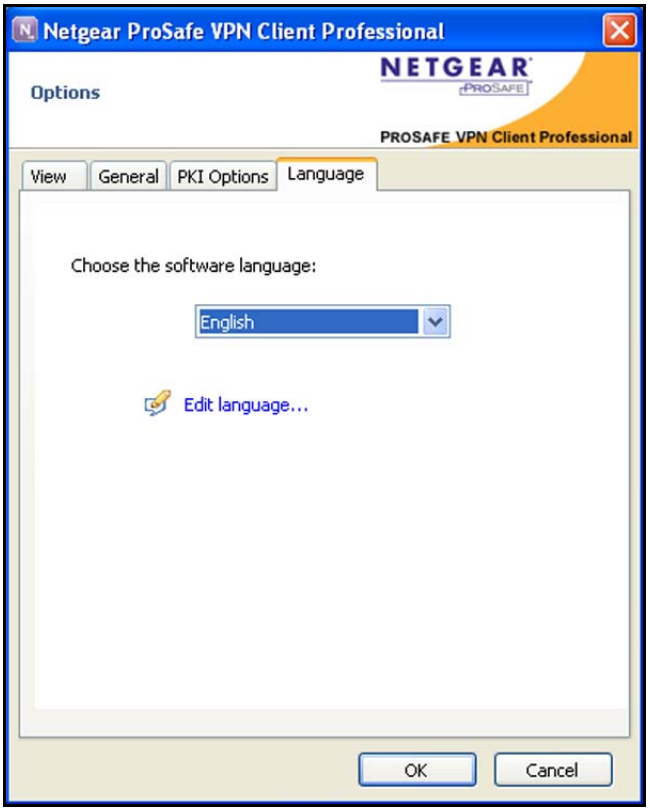


Figure 20. Language pane

If you modify the existing translation, do not change the following characters, which are generic expressions:

- %s is replaced by a string.
- %d is replaced by a number.
- \n stands for carriage return.
- & underlines the characters that follow it.

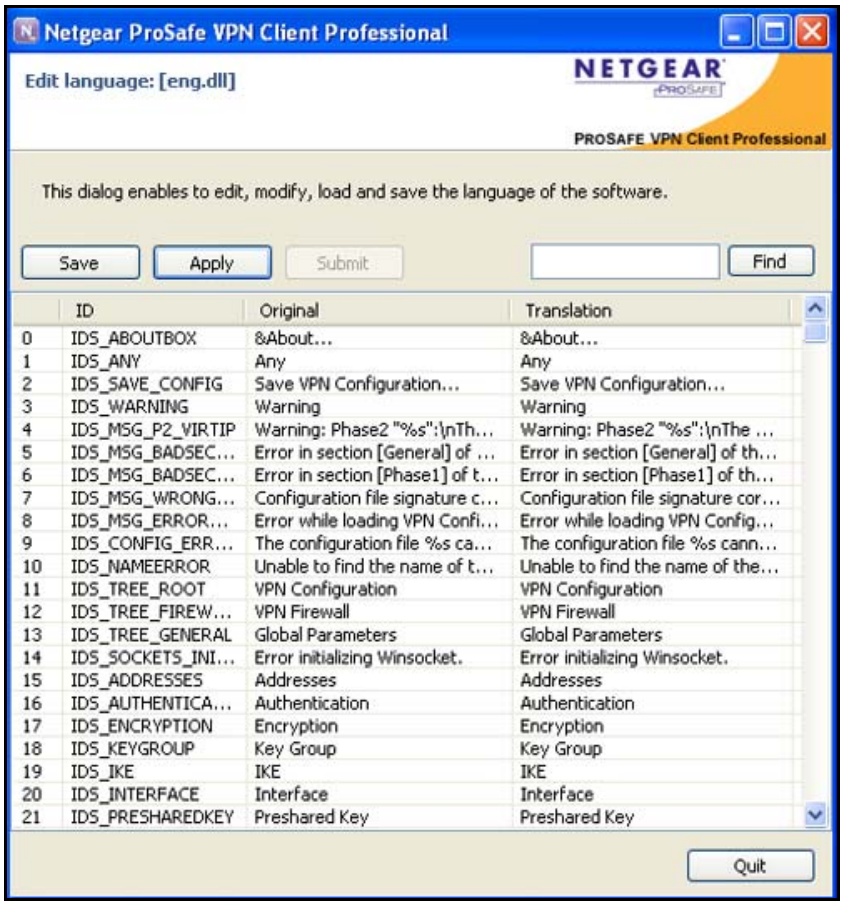
Also note the following restrictions:

- The IDS_DATE_FORMAT is %m-%d-%Y. Modify the date only if you know the appropriate syntax.
- Do not translate IDS_SC_P11_3.

➢ **To modify the translation:**

1. Click **Edit language**.

   The Edit language screen displays:



	ID	Original	Translation
0	IDS_ABOUTBOX	&About...	&About...
1	IDS_ANY	Any	Any
2	IDS_SAVE_CONFIG	Save VPN Configuration...	Save VPN Configuration...
3	IDS_WARNING	Warning	Warning
4	IDS_MSG_P2_VIRTIP	Warning: Phase2 "%s":\nTh...	Warning: Phase2 "%s":\nThe ...
5	IDS_MSG_BADSEC...	Error in section [General] of ...	Error in section [General] of th...
6	IDS_MSG_BADSEC...	Error in section [Phase1] of t...	Error in section [Phase1] of th...
7	IDS_MSG_WRONG...	Configuration file signature c...	Configuration file signature cor...
8	IDS_MSG_ERROR...	Error while loading VPN Confi...	Error while loading VPN Config...
9	IDS_CONFIG_ERR...	The configuration file %s ca...	The configuration file %s cann...
10	IDS_NAMEERROR	Unable to find the name of t...	Unable to find the name of the...
11	IDS_TREE_ROOT	VPN Configuration	VPN Configuration
12	IDS_TREE_FIREW...	VPN Firewall	VPN Firewall
13	IDS_TREE_GENERAL	Global Parameters	Global Parameters
14	IDS_SOCKETS_INI...	Error initializing Winsocket.	Error initializing Winsocket.
15	IDS_ADDRESSES	Addresses	Addresses
16	IDS_AUTHENTICA...	Authentication	Authentication
17	IDS_ENCRYPTION	Encryption	Encryption
18	IDS_KEYGROUP	Key Group	Key Group
19	IDS_IKE	IKE	IKE
20	IDS_INTERFACE	Interface	Interface
21	IDS_PRESHAREDKEY	Preshared Key	Preshared Key

2. Select the row that you want to change. A pop-up screen displays and shows the following four columns:
   - **line number**.
   - **ID**. The name of the string.
   - **Original**. The string in English.
   - **Translation**. The translated string.
3. Enter your alternate translation in the pop-up screen.
4. Click **OK**.

5. Do one of the following:
   - Click **Save** to save the .lng file in the Language folder of the VPN Client software directory.
   - Click **Apply** to immediately show the new translation in the user interface.

   Note: *The saved file is added as a new selection in the language drop-down menu of the Language pane. The name of the new selection is the name of the original language followed by an exclamation mark. For example, if you change the English language file, the new language option that is shown in the drop-down menu is English!*

6. Click **Quit**.

   The Language pane closes.

VPN Client Software Setup and Network Deployment

6

The VPN Client is designed to be easily deployed and managed. It implements several features that enable a network administrator to preconfigure the VPN Client software setup before deployment to end users, 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.

Software Setup and Deployment Concepts

You can create a VPN Client software setup installation file by using software setup commands and optional CLI commands. You can deploy through several media:

- **Network drive**. Enables users to download and install the VPN Client by simply double-clicking an icon on a drive in your network.
- **CD-ROM disk**. Enables users to insert the VPN Client installation CD to let the installation 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 run automatically.

For more information, see *VPN Client Silent Software Setup Deployment to End Users* on page 112.

Software Setup File Example

The following procedure describes how you can create a software setup file.

➢ **To create a VPN Client software setup file:**

1. Download the NETGEARVPNClientPro_setup.exe file or copy it from the installation CD.
2. Open a command screen.
3. Enter the software setup commands:

   `[software path][name]_setup.exe /S [software setup commands] /D=[install path] [optional CLI commands]`

   in which

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

   `[software setup commands]` are the software setup commands that customize the VPN Client.

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

   `[optional CLI commands]` are the optional CLI commands that you can add.
4. Press **Enter**.
5. Close the command screen.

The following is an example of the syntax for a software setup:

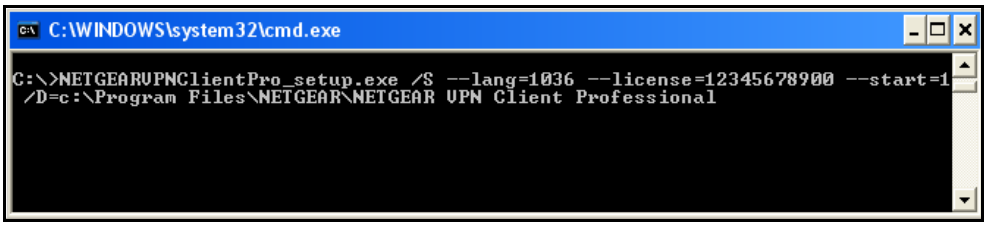


Figure 21. Example of the syntax for a software setup

Software Setup Command Requirements

These are requirements for the composition of a software setup file:

- Precede all software setup commands by two hyphens (--).
- Place a space character following each software setup command. The same applies to optional CLI commands.
- Include the **/S** switch to enable a silent uninstallation of an already installed version followed by a silent installation of a specified version (no dialog boxes are displayed during the uninstallation and installation). If there is no version installed, the uninstallation is ignored. The **/S** switch needs to be preceded by only one slash and is case-sensitive.
- Include the **/D=[install path]** switch to specify installation location for the VPN Client, in which **[install path]** is the entire path where the VPN Client is installed. This switch does not recognize a relative directory. Quotation marks are not allowed, even if there is a space in the path. The **/D** switch needs to be used with the **/S** option, needs to be preceded by only one slash, is case-sensitive, and needs to be the last switch in the command line.
- Specify software setup commands that require a parameter without a space between the command and the parameter. Quotation marks are required if the parameter contains spaces, for example, “C:\Temporary Downloads\Program Files”. However, if there are spaces in the installation path **[install path]**, quotation marks are not required.
- Do not include the brackets that are shown in the examples in this chapter in the software setup commands. For example, if the example states *[software path] is the path to the setup software file*, do not include the brackets in the actual software path.

Examples of Options that You Can Include in a Software Setup File

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 the user interface is hidden, and if so, to what degree
- Whether the user needs to enter a password to access the user interface

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

Software Setup Command Reference

The following table describes all software setup switches and commands.

All software setup commands need to be used with the **/S** switch. Some software setup commands are self-explanatory; other commands are described in more detail in the sections that follow in this chapter.

Table 5. Software setup switches and commands in alphabetical order

Switch or Command	Description
/D=[install path]	**[install path]** is the path where the VPN Client is installed. **Note:** **/D** needs to 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** needs to be placed at the end of the command line, as the last option, and you need to use it with the **/S** option (silent mode). **Example**: NETGEARVPNClientPro_Setup.exe /S --guidefs=user /D= C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
/S	Enables a silent uninstallation of an already installed version followed by a silent installation of a specified version (no dialog boxes are displayed during the uninstallation and installation). **Note:** **S** needs to be preceded by only one slash and is case-sensitive. **Note:** If there is no version installed, the uninstallation is ignored. **Example**: NETGEARVPNClientPro_Setup.exe /S
--activmail=[activation_email]	Automatically enters the email address that is used for activation confirmation. During the activation process, the field that is used to enter the email address is disabled. **[activation_email]** is the email address that is required for activation. **Note:** **activmail** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --activmail= salesgroup@company.com

Table 5. Software setup switches and commands in alphabetical order (continued)

<table>
<tr><th>Switch or Command</th><th>Description</th></tr>
<tr><td>--autoactiv=1</td><td>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 address have already been entered in a previous installation.
--autoactiv=1 needs to be the last command in the command line.

Note: autoactiv=1 needs to be preceded by two hyphens (--).

Example:
NETGEARVPNClientPro_Setup.exe /S --autoactiv=1</td></tr>
<tr><td>--guidefs=[full|user|hidden]</td><td>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 is displayed. Only the system tray menu can be opened. Tunnels can be opened from the system tray menu.

Note: guidefs needs to be preceded by two hyphens (--).

Example:
NETGEARVPNClientPro_Setup.exe /S --guidefs=hidden</td></tr>
<tr><td>--lang=[language code]</td><td>Specifies the language for the software setup and for the VPN Client.
[language code] is the code for the language. The codes are shown in the following rows in this table.

Note: lang needs to be preceded by two hyphens (--).

Example:
NETGEARVPNClientPro_Setup.exe /S --lang=1040
<table>
<tr><th>ISO 639-2 Code</th><th>Language Code</th><th>English Name</th></tr>
<tr><td>AR</td><td>1025</td><td>Arabic</td></tr>
<tr><td>CZ</td><td>1029</td><td>Czech</td></tr>
<tr><td>DK</td><td>1030</td><td>Danish</td></tr>
<tr><td>DE</td><td>1031</td><td>German</td></tr>
<tr><td>EL</td><td>1032</td><td>Greek</td></tr>
<tr><td>EN</td><td>1033 (Default)</td><td>English</td></tr>
<tr><td>ES</td><td>1034</td><td>Spanish</td></tr>
</table>
</td></tr>
</table>

Table 5. Software setup switches and commands in alphabetical order (continued)

Switch or Command	Description		
`--lang=[language code]` (continued)	FI	1035	Finnish
	FR	1036	French
	HU	1038	Hungarian
	IT	1040	Italian
	JA	1041	Japanese
	KO	1042	Korean
	NL	1043	Dutch
	NO	1044	Norwegian
	PL	1045	Polish
	RU	1049	Russian
	TH	1054	Thai
	TR	1055	Turkish
	SL	1060	Slovenian
	FA	1065	Farsi
	HI	1081	Hindi
	ZH	2052	Chinese simplified
	PT	2070	Portuguese
	SR	2074	Serbian
`--license=[number]`	Automatically enters the license number that is used for activation. **`[number]`** is the license number that consists of 20 or 24 hexadecimal characters. **Note:** **`license`** needs to be preceded by two hyphens (**`--`**). **Example**: NETGEARVPNClientPro_Setup.exe /S --license= 1234567890ABCDEF12345678		

Table 5. Software setup switches and commands in alphabetical order (continued)

Switch or Command	Description
--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. • **16**. Configuration Panel menu item displays. • **31**. All menu items 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 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** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --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 network 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** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --noactiv=1
--password=[password]	Protects the user interface or a protected screen of the user interface. **[password]** is the password that the end user needs to enter to gain access under the following circumstances. • When the user clicks or double-clicks the VPN system tray icon. • When the user wants to switch from the Connection Panel screen to the Configuration Panel screen. **Note:** **password** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --password=adm253q

Table 5. Software setup switches and commands in alphabetical order (continued)

Switch or Command	Description	
--pkicheck=1	Forces the VPN Client to check the certificate root authority when it receives a certificate from the VPN gateway. The certificate expiration date is validated, and the signatures of the certificates in the certification chain and the associated Certificate Revocation List (CRL) are validated. **Note: pkicheck** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --pkicheck=1	
--reboot=1	Automatically reboots the computer after a silent installation of the VPN Client. **Note: reboot** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --reboot=1	
--smartcardroaming	Sets rules for the VPN Client to select a certificate from a token or smart card when there are several tokens and smart cards. **Note: smartcardroaming** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --smartcardroaming=1 The value is a bit field:	
	The card reader is configured in the VPN configuration.	• Not configured. The VPN Client uses the certificate with the subject that is specified in the VPN Configuration. • **1**. The VPN Client can use any certificate.
	The card reader is configured in the roaming section of the vpnconf.ini file.	• **2**. The VPN Client uses the certificate with the subject that is specified in the VPN Configuration. • **3**. The VPN Client can use any certificate.
	The first card reader that is inserted and that contains a token or smart card.	• **4**. The VPN Client uses the certificate with the subject that is specified in the VPN Configuration. • **5**. The VPN Client can use any certificate.

Table 5. Software setup switches and commands in alphabetical order (continued)

Switch or Command	Description
`--start=[1|2]`	Configures the start mode for the VPN Client. These are the options: • **1**. The VPN Client starts after Windows logon. This is the default setting. • **2**. The VPN Client needs to be started manually. **Note:** `start` needs to be preceded by two hyphens (`--`). **Example**: NETGEARVPNClientPro_Setup.exe /S --start=2

Customize VPN Client Display and Access 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. You can hide this screen.
- By right-clicking the system tray icon and opening the system tray menu. Except for the tunnels (these are always shown), you can hide most menu items of the system tray menu.

A network administrator can 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.

The following is an example of the syntax for a software setup:

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

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

Note: Before you configure software setup commands, NETGEAR recommends that you read the information in *Software Setup Command Requirements* on page 102.

This section provides the configuration examples that are described in the following subsections:

- *Display the Configuration Panel Screen after Startup*
- *Display the Connection Panel Screen after Startup*
- *Display the System Tray Menu Only after Startup*
- *Require a Password to Access the Configuration Panel Screen*
- *Limit Usage to the System Tray Menu and Require a Password to Access Other Screens*
- *Configure Which Items of the System Tray Menu Are Visible*

Display the Configuration Panel Screen after Startup

To configure theVPN Client to display the Configuration Panel screen after startup, use the **`--guidefs=full`** software setup command.

By default, the VPN Client is configured to display the Configuration Panel screen after startup. The following is an example of the syntax for this software setup command:

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

Display the Connection Panel Screen after Startup

To configure theVPN Client to display the Connection Panel screen after startup, use the **`--guidefs=user`** software setup command.

The following is an example of the syntax for this software setup command:

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

Display the System Tray Menu Only after Startup

To configure theVPN Client to display the system tray menu after startup and hide the Configuration Panel screen and the Connection Panel screen, use the **`--guidefs=hidden`** software setup command.

Only the system tray menu can be opened. Tunnels can be opened from the system tray menu. The following is an example of the syntax for this software setup command:

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

The following figure shows and example of the system tray menu after you have deployed a configuration that includes the **`--guidefs=hidden`** software setup command.

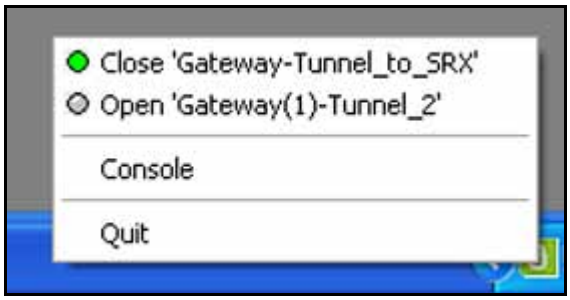


Figure 22. System tray menu with hidden items

Require a Password to Access the Configuration Panel Screen

To require the end user to enter a password to access the Configuration Panel screen, use the **`--guidefs=user --password=[password]`** software setup command, in which **`[password]`** is the specified password.

The following is an example of the syntax for this software setup command, in which *admin01* is the password:

```
NETGEARVPNClientPro_Setup.exe /S --guidefs=user --password=admin01
/D=C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
```

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

When access control is enabled, the end user is asked for the password under the following circumstances:

- When the user clicks (or double-clicks) the VPN Client icon in the system tray.
- When the user switches from the Connection Panel screen to the Configuration Panel screen.
- When the user starts a software upgrade.

In all of these circumstances, the Access Control screen displays.

Figure 23. Access Control screen

Limit Usage to the System Tray Menu and Require a Password to Access Other Screens

To limit usage of the VPN Client to the system tray menu and protect access to both the Connection Panel screen and Configuration Panel screen with a password, use the **`--guidefs=hidden --password=[password]`** software setup command.

The following is an example of the syntax for this software setup command, in which *28!Grp2YO* is the password:

```
NETGEARVPNClientPro_Setup.exe /S --guidefs=hidden --password=28!Grp2YO
/D=C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
```

Configure Which Items of the System Tray Menu Are Visible

To configure the items that are visible to the end user in the system tray menu, use the **`--menuitem=[0`**...**`31]`** software setup command.

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.
- **16**. Configuration Panel menu item displays.
- **31**. All menu items display. This is the default setting.

The following is an example of the syntax for this software setup command, in which the Quit and Console menu items are visible in the system tray menu:

```
NETGEARVPNClientPro_Setup.exe /S --menuitem=5 /D=C:\Program
Files\NETGEAR\NETGEAR VPN Client Professional
```

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 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.

VPN Client Silent Software Setup Deployment to End Users

The VPN Client software deployment lets the software setup run silently. A silent VPN Client software setup is an installation that is automatically processed without end user input through software setup commands. The VPN Client software setup is specifically designed to run silently.

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

> **Note:** Before you configure software setup commands, NETGEAR recommends that you read the information in *Software Setup Command Requirements* on page 102.

This section provides the configuration examples that are described in the following subsections:

- *Create a Silent VPN Client Software Setup*
- *Deploy a VPN Client Software Setup from a CD-ROM*
- *Deploy a VPN Client Software Setup from a Shortcut*
- *Deploy a VPN Client Software Setup Using a Batch Script*
- *Deploy a VPN Client Software Setup from a Network Drive*

Create a Silent VPN Client Software Setup

➢ **To create a silent VPN Client software setup:**

1. Download the NETGEARVPNClientPro_setup.exe file or copy it from the installation CD.
2. Open a command screen.
3. Enter the following software setup commands:

   ```
   [software path][name]_setup.exe /S --lang=[code] --license=[number]
   --start=1 /D=[install path] [optional CLI commands]
   ```

   in which

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

   `[name]` is the name of the setup software file.

   `[code]` is the language code.

   `[number]` is the license number.

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

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

4. Press **Enter**.
5. Close the command screen.

The following is an example of the syntax for a silent software setup for a VPN Client that starts automatically after Windows logon (defined by **--start=1**) and without any optional CLI commands:

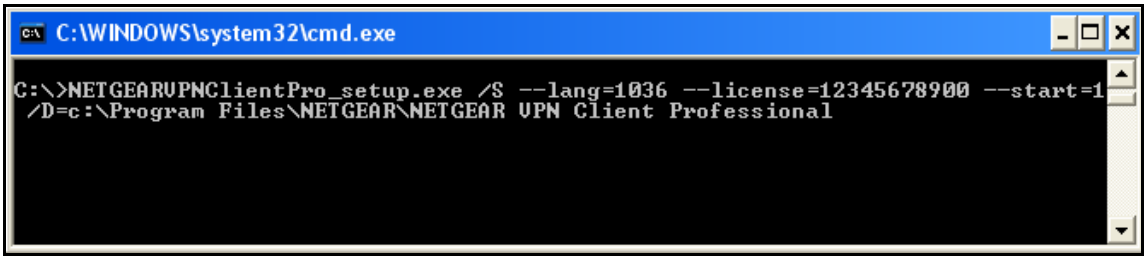


Figure 24. Example of the syntax for a software setup

Deploy a VPN Client Software Setup from a CD-ROM

➢ **To deploy a VPN Client software setup from a CD-ROM:**

1. Create a silent VPN Client software setup.

   For information, see *Create a Silent VPN Client Software Setup* on page 112.

2. Create an autorun file:
   a. Create a text file.
   b. Save the file 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\][name]_setup.exe /S /D=[install path] [optional CLI commands]
   ICON=[cdpath\][name]_setup.exe
   ```

   in which

   [name] is the name of the setup file, for example NETGEARVPNClientPro, so that the entire name for the setup file is NETGEARVPNClientPro_setup.exe.

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

   [optional 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 an example of the syntax for this software setup command:

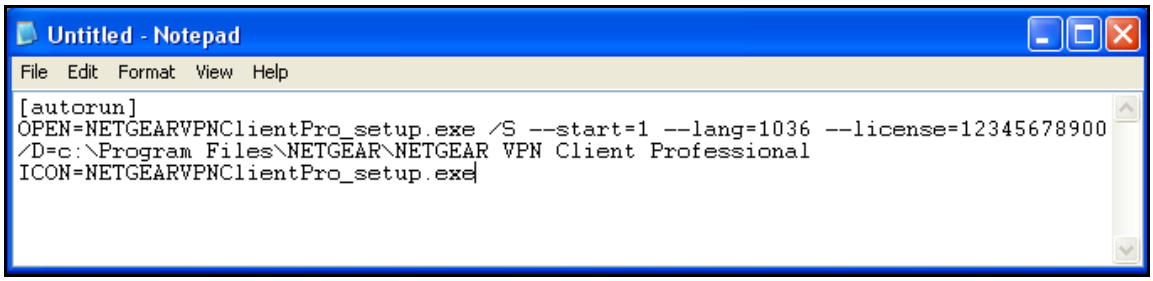


Figure 25. Example of the syntax for a software setup for CD-ROM deployment

Deploy a VPN Client Software Setup from a Shortcut

➢ **To deploy a VPN Client software setup from a shortcut, that is, by letting the end user double-click an icon:**

1. Create a silent VPN Client software setup.

   For information, see *Create a Silent VPN Client Software Setup* on page 112.

2. In the setup directory, right-click the **[name]_setup.exe** file.

   [name] is the name of the setup file, for example NETGEARVPNClientPro, so that the entire name for the setup file is NETGEARVPNClientPro_setup.exe.

3. From the pop-up menu, select **Create Shortcut**.

   A shortcut to the setup file in the setup directory is created.

4. Right-click the new shortcut.
5. From the pop-up menu, select **Properties**.
6. In the Target field, *add* the following software setup commands to the command line:

   `/S --start=1 --lang=[code] --license=[number] /D=[install path]`

   in which

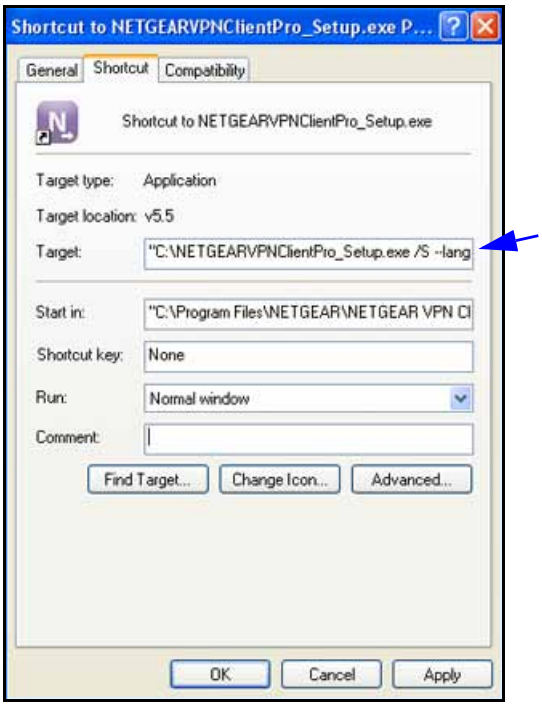
   `[code]` is the language code.

   `[number]` is the license number.

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

7. Move the shortcut to a location where the user can easily click the shortcut (for example, on the desktop).

The following is an example of the syntax for this software setup command:




```
"C:\NETGEARVPNClientPro_Setup.exe /S
--lang=1036 --license=12345678900
--start=1 /D=C:\Program
Files\NETGEAR\NETGEAR VPN Client
Professional"
```

Figure 26. Example of the syntax for a software setup from a shortcut

Deploy a VPN Client Software Setup Using a Batch Script

➢ **To deploy a VPN Client software setup using a batch script:**

1. Create a silent VPN Client software setup.

   For information, see *Create a Silent VPN Client Software Setup* on page 112.

2. Create a text file with a .bat extension, for example, VPN Client Setup.bat.
3. Edit the .bat file.
   a. Right-click the .bat file.
   b. Select **Edit**.
   c. Enter the commands that you want to be processed.

      For example, enter:

```
cd .\setup
NETGEARVPNClientPro_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.

(For information about the `importance` command, see *Command-Line Interface Command Reference* on page 120.)

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

Deploy a VPN Client Software Setup from a Network Drive

➢ **To deploy a VPN Client software setup from a network drive:**

1. Create a silent VPN Client software setup on a network drive.

   For information, see *Create a Silent VPN Client Software Setup* on page 112.

2. In the setup directory, right-click the **[name]_setup.exe** file.

   [name] is the name of the setup file, for example NETGEARVPNClientPro, so that the entire name for the setup file is NETGEARVPNClientPro_setup.exe.

3. From the pop-up menu, select **Create Shortcut**.

   A shortcut to the setup file in the setup directory is created.

4. Right-click the new shortcut.
5. From the pop-up menu, select **Properties**.
6. In the Target field, add the following software setup commands to the command line:

   ```
   /S --start=1 --lang=[code] --license=[number] /D=[install path]
   ```

   in which

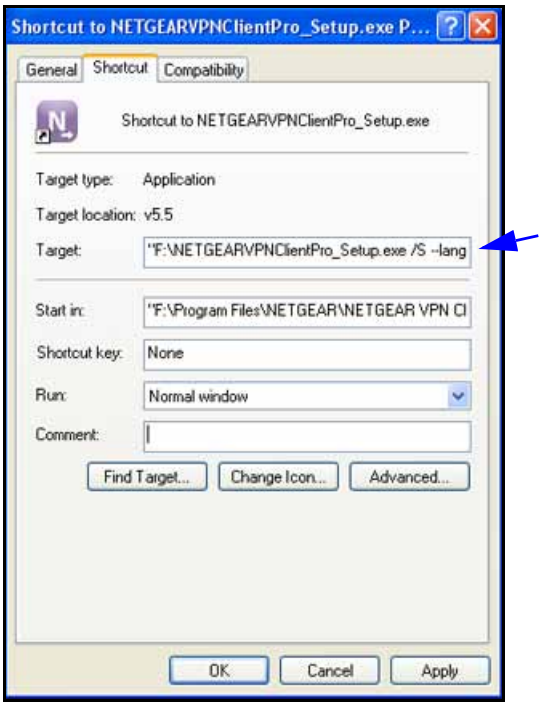
   `[code]` is the language code.

   `[number]` is the license number.

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

7. Move the shortcut to a location where the user can easily click the shortcut (for example, on the desktop).

The following is an example of the syntax for this software setup command:




```
“F:\NETGEARVPNClientPro_Setup.exe /S
--lang=1036 --license=12345678900
--start=1 /D=C:\Program
Files\NETGEAR\NETGEAR VPN Client
Professional”
```

Figure 27. Example of the syntax for a software setup from a shortcut on a network drive

Deliver a VPN Configuration to an End User

You can deliver a VPN configuration, that is, a configuration with one or more preconfigured VPN tunnels, to an end user.

One method is to embed the VPN configuration in a VPN Client software setup deployment. When the VPN Client is installed, the VPN configuration is automatically imported by the VPN Client. When you embed a VPN configuration, you cannot protect the VPN configuration with a password.

If you prefer to protect the VPN configuration with a password, do not embed the VPN configuration file with a VPN Client software setup file. Instead, export the VPN configuration file and make it available to end users, either by email or through file sharing.

This section provides the configuration examples that are described in the following subsections:

- *Embed a VPN Configuration in a VPN Client Software Setup Deployment*
- *Export and Deploy a VPN Configuration*

Embed a VPN Configuration in a VPN Client Software Setup Deployment

➤ **To embed a VPN configuration in a VPN Client software setup:**

1. Do one of the following:
   - Create a silent software setup.

     For information about how to create a silent software setup, see *Create a Silent VPN Client Software Setup* on page 112.

   - Unzip the NETGEAR VPN Client Professional software setup file (NETGEARVPNClientPro_Setup.exe).
2. Create a VPN configuration.

   You can do this on any computer on which the VPN Client is installed. For information about how to create a VPN configuration, see *Chapter 4, Create VPN Tunnel Connections*.
3. Export the VPN configuration:
   a. From the main menu on the Configuration Panel screen, select **Configuration > Export**.

      The Export Protection screen displays:

   b. Select the **Don't protect the exported VPN Configuration** radio button.
   c. Click **OK**.
4. Navigate to the location where you want to save the VPN configuration file.
5. Type a name for the VPN configuration file.

   An exported VPN configuration file has a .tgb extension. Do not change this extension.
6. Click **Save**.

7. Add the VPN configuration (that is, the conf.tgb file) to the directory in which you have placed the software setup file or on the target computer or server.
8. (Optional) If you intend to use the software setup file on a USB drive, copy the VPN configuration onto the USB drive together with the software setup file.
9. Deploy the package to the end user.

   The VPN configuration (that is, the conf.tgb file) is automatically imported during the software setup process.

Export and Deploy a VPN Configuration

➢ **To export and deploy a VPN configuration:**

1. Create a VPN configuration.

   You can do this on any computer on which the VPN Client is installed. For information about how to create a VPN configuration, see *Chapter 4, Create VPN Tunnel Connections*.

2. Export the VPN configuration:
   a. From the main menu on the Configuration Panel screen, select **Configuration > Export**.

      The Export Protection screen displays:

3. Select one of the following radio buttons:
   - **Don't protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. The VPN configuration file requires a password before it can be opened.
     a. (Optional) Clear the **Hide password** check box.
     b. Enter a password in the Password field.
     c. Enter the same password in the Confirm field.
     d. Click **OK**.

4. Navigate to the location where you want to save the VPN configuration file.
5. Type a name for the VPN configuration file.

   An exported VPN configuration file has a .tgb extension. Do not change this extension.
6. Click **Save**.
7. 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 the end user needs to entered it before the VPN configuration is processed.

Command-Line Interface Command Reference

You can use the command-line interface (CLI) commands to customize the VPN Client software setup to adapt the VPN Client to a specific environment and integrate the VPN Client with other applications. Use CLI commands in batch files, in scripts, or in software setup autorun.inf files.

CLI commands always include the vpnconf.exe file because all CLI commands control a VPN tunnel configuration, for example by opening, closing, or importing a VPN tunnel configuration.

The following is the standard syntax for CLI commands:

```
[install directory]\vpnconf.exe [/option[:value]]
```

in which

`[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.

These are requirements for the use of CLI commands in a software setup file:

- When you include CLI commands in a software setup file, the CLI commands need to be the last commands in the command line, that is, they are placed after the **`/D`** switch and its associated install path.
- Place a space character following each CLI command.
- Place an argument that contains space characters between double quotes.
- Do not include the brackets that are shown in the examples in this chapter. For example, if the example states *[install directory] is the installation directory of the VPN Client software files*, do not include the brackets in the actual install directory.

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

Table 6. CLI commands in alphabetical order

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 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 while the VPN Client remains running. **[ConfigFileName]** is the name of the 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 while the VPN Client remains running. **[ConfigFileName]** is the name of the 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 6. CLI commands in alphabetical order (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 starts automatically. If the VPN Client is running, the VPN configuration is imported while the VPN Client remains 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:** 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 while the VPN Client remains running. 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. 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
/pwd:[Password]	Enables you to set a password for import and export operations. **[Password]** is the password that you need to 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 need to 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

Table 6. CLI commands in alphabetical order (continued)

Command	Description
/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

Customize the VPN Client Using CLI Commands

This section provides the configuration examples that are described in the following subsections:

- *Open or Close a VPN Tunnel*
- *Close All Active Tunnels and Close the VPN Client*
- *Import, Export, Add, or Replace the VPN Configuration*

Open or Close a VPN Tunnel

You can open or close a VPN tunnel through a CLI command. You can do this whether or not 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.

[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.

[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.

Note: 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.

Close All Active Tunnels and Close the VPN Client

➢ **To close all active tunnels and 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.

[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 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 second 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 second 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. You need to place the **/pwd:[password]** CLI command *after* the other command that you are combining it with. For example:

```
[path]\vpnconf.exe /import:[ConfigFileName] /pwd:[password]
```

The **/export:** and **/exportonce:** commands always require a password.

Customize How the VPN Client Handles Readers and Certificates

The PKI options let you configure how the VPN Client selects and uses certificates, smart card readers, and token readers. This section describes how to configure the PKI options in the vpnsetup.ini file and how to specify new smart card readers and token readers in the vpnconfig.ini file.

Note: The PKI options that you can configure in the vpnsetup.ini file are the same options that you can configure through the user interface (see *Configure PKI Options* on page 84).

Customize the vpnsetup.ini File

The vpnsetup.ini file is an editable initialization file that is used to configure the VPN Client during the software setup installation process. You can use any text editor to configure the vpnsetup.ini file.

The vpnsetup.ini file needs to be located in the same folder as the VPN Client setup.exe file. The vpnsetup.ini file consists of several sections, tags, and values. One of the sections is the PKI Options section, in which you can define how the VPN Client selects and uses certificates from smart card readers and token readers.

The following is an example of the PKI Options section in the vpnsetup.ini file:

```
[PKIOptions]
PkiCheck=01
SmartCardRoaming=01
NoCACertReq=01
KeyUsage=01
PKCS11Only=01
```

In this example, the VPN Client is configured to do the following:

- Validate the certificate root authority when it receives a certificate from the VPN gateway (PkiCheck=01)
- Use any certificate from the card reader that is configured in the VPN configuration (SmartCardRoaming=01)
- Use a certificate from a different certificate authority than the VPN gateway (NoCACertReq=01)
- Use only an authentication certificate for which the digitalSignature key extension is configured (KeyUsage=0)
- Use only PKCS #11 middleware to access tokens or smart cards (PKCS11Only=01)

The following table describes the PKI options parameters that let you define rules for certificate handling in the vpnsetup.ini file.

Table 7. PKI options parameters for the vpnsetup.ini file in alphabetical order

Option	Description	Settings
`KeyUsage`	This option lets you specify a particular certificate among multiple ones. For example, this is useful when several certificates with the same subject are stored on a smart card or token.	• Not configured. The VPN Client can select any certificate. • **01**. The VPN Client uses only an authentication certificate for which the digitalSignature key extension is configured.
`NoCACertReq`	This option lets you specify that the VPN Client and VPN gateway can use certificates from different certificate authorities.	• Not configured. The VPN Client and VPN gateway need to use certificates from the same certificate authority. • **01**. The VPN Client and the VPN gateway can use certificates from different certificate authorities.
`PKC11Only`	This option lets you force the VPN Client to use only a PKCS #11 reader. **Note:** When the VPN Client accesses the Windows Certificate Store, the VPN Client uses CSP middleware to access tokens or smart cards irrespective of the setting of the `PKC11Only` option.	• Not configured. The VPN Client uses cryptographic service provider (CSP) middleware to access smart cards or tokens. • **01**. The VPN Client uses only PKCS #11 middleware to access smart cards or tokens. With this option, the VPN Client uses the smart card reader or token reader that is defined in the ROAMING section of the vpnconf.ini file (for more information, see *Customize the vpnconf.ini File* on page 129).
`PKICheck`	The option lets you force the VPN Client to validate the certificate root authority when it receives a certificate from the VPN gateway. For more information, see *PKICheck Option Concepts* on page 128. **Note:** This PKI option is also available as a software setup command (see *Software Setup Command Reference* on page 103). The setting in the vpnsetup.ini file overrides the setting in the software setup command.	• Not configured. The VPN Client does not validate the certificate root authority. • **01**. The VPN Client validates the certificate root authority when it receives a certificate from the VPN gateway. The certificate expiration date is validated, and the signatures of the certificates in the certification chain and the associated Certificate Revocation List (CRL) are validated.

Table 7. PKI options parameters for the vpnsetup.ini file in alphabetical order (continued)

Option	Description	Settings
SmartCardRoaming	This option lets you set rules for the VPN Client to select a certificate from a token or smart card when there are several tokens and smart cards. **Note:** This PKI option is also available as a software setup command (see *Software Setup Command Reference* on page 103). The setting in the vpnsetup.ini file overrides the setting in the software setup command. **Note:** The value is a bit field:	
	Not configured or 01 specifies that the smart card reader or token reader is configured in the VPN configuration.	• Not configured. The VPN Client uses the certificate with the subject that is specified in the VPN configuration. • **01**. The VPN Client can use any certificate.
	02 or 03 specifies the smart card reader or token reader that is defined in the ROAMING section of the vpnconf.ini file (for more information, see *Customize the vpnconf.ini File* on page 129).	• **02**. The VPN Client uses the certificate with the subject that is specified in the VPN configuration. • **03**. The VPN Client can use any certificate.
	04 or 05 specifies the first smart card reader or token reader that is inserted and that contains a smart card or token.	• **04**. The VPN Client uses the certificate with the subject that is specified in the VPN configuration. • **05**. The VPN Client can use any certificate.

PKICheck Option Concepts

For the PKICheck option to function correctly, make sure that the root certificate, intermediate certificates, and the server certificate are imported into the Windows Certificate Store. Similarly, the Certificate Revocation List (CRL) for the certificate of the VPN gateway needs to be in the Windows Certificate Store or downloadable. If the CRL is absent from the Windows Certificate Store or not downloadable while a VPN tunnel is being opened, the VPN Client cannot validate the certificate of the VPN gateway.

Certificate validation includes validation of the following items:

- The expiration date of the certificate
- Signatures of all certificates in the certificate chain, including the root certificate, intermediate certificates, and the server certificate
- The absence of certificate revocation in the CRLs

In addition, the CRLs of all certificate issuers in the certificate chain are downloaded and validated:

- All CRL distribution points (CDPs) are validated.
- The CRLs are downloaded from the CDPs.

- The expiration dates of the CRLs are validated.
- The signatures of the CRLs are validated and compared with the public keys of the certificate issuers.
- The CRLs are imported into the Windows Certificate Store.

Customize the vpnconf.ini File

The VPN Client automatically recognizes smart cards and tokens of the leading manufacturers. The cards are recognized based on their Answer to Reset (ATR) code, which enables the VPN Client to use the associated cryptographic service provider (CSP) or PKCS#11 middleware.

By adding a vpnconf.ini file, you can specify a specific smart card reader or token reader and the path to its associated middleware, and you can add custom smart cards and tokens that are not automatically recognized by the VPN Client.

The vpnconf.ini file is an editable initialization file that is used to configure the VPN Client during the startup process. You can use any text editor to configure the vpnconf.ini file. The vpnconf.ini file needs to be located in the same folder as the VPN Client, for example, C:\Program Files\NETGEAR\NETGEAR VPN Client Professional.

The vpnconf.ini file consists of several sections, tags, and values. The following sections are used to specify custom smart cards and tokens and the paths to custom middleware:

- **ROAMING**. Specifies a specific smart card reader or token reader and the path to its associated middleware.
- **ATR**. Specifies one or more custom smart cards or tokens that are not automatically recognized by the VPN Client.

The following is an example of a vpnconf.ini file with a ROAMING and ATR section:

```
[ROAMING]
SmartCardReader="Reader Name"
SmartCardMiddleware="middleware.dll"
SmartCardMiddlewareType="PKCS#11"
SmartCardMiddelwarePath="c:\path\to\middleware\mdlw.dll"
SmartCardMiddlewareRegistry=
"KEY_LOCAL_MACHINE:SOFTWARE\\CompanyName\\ProductName\\CK:PKCS#11DLL"

// New Token description#1
[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:00:01]
mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"
scname="Card Name"
manufacturer="Company Name"
pkcs11DllName="mdlw.dll"
registry=
"KEY_LOCAL_MACHINE:SOFTWARE\\CompanyName\\ProductName\\CK:PKCS#11DLL"
```

The ROAMING and ATR options are described in the following sections.

Configure the ROAMING Section of the vpnconf.ini File

The VPN Client accesses the information in the ROAMING section of the vpnconf.ini file only when the SmartCardRoaming option in the vpnsetup.ini file is configured to be 02 or 03 and when the PKCS11Only option in the vpnsetup.ini file is configured to be 01.

The following table describes the ROAMING parameters that let you specify a specific smart card reader or token reader and the path to its associated middleware. You enter this information in the ROAMING section of the vpnconf.ini file.

Table 8. ROAMING parameters for the vpnconf.ini file in the order of entry

Parameter	Description	
`SmartCardReader`	The name of smart card reader or token reader that is used to access the smart card or token.	
`SmartCardMiddleware`	The middleware (DLL file) that is used to communicate with the smart card or token.	
`SmartCardMiddlewareType`	The type of middleware, which is always PKCS#11.	
`SmartCardMiddelwarePath`	The path to the middleware, including the name of the middleware (that is, the name of the DLL file).	**Note:** You need to specify either `SmartCardMiddelwarePath`. or `SmartCardMiddlewareRegistry`
`SmartCardMiddlewareRegistry`	The name of the key in the registry that contains the path to the middleware (that is, the DLL file). The format is: `PRIMARY_KEY:..\\..\\..: middleware`	

The following is an example of a ROAMING section in a vpnconf.ini file with the SmartCardMiddelwarePath parameter:

```
SmartCardReader="Axalto reader"
SmartCardMiddleware="middleware.dll"
SmartCardMiddlewareType="PKCS#11"
SmartCardMiddelwarePath="c:\path\to\middleware\mdlw.dll"
```

The following is an example of a ROAMING section in a vpnconf.ini file with the SmartCardMiddlewareRegistry parameter:

```
SmartCardReader="Axalto reader"
SmartCardMiddleware="middleware.dll"
SmartCardMiddlewareType="PKCS#11"
SmartCardMiddlewareRegistry=
"HKEY_LOCAL_MACHINE:SOFTWARE\\Axalto\\Access\\CK:PKCS#11DLL"
```

Note: The information in the ROAMING section of the vpnconf.ini file overrides the information in the VPN configuration.

Configure the ATR Section of the vpnconf.ini File

Each new software release of the VPN Client includes the latest list of Answer to Reset (ATR) codes that are available from smart card and token vendors. Because new ATR codes are released frequently, you can manually add one or more new ATR codes to the ATR section in the vpnconf.ini file.

The following table describes the ATR parameters that let you specify one or more custom smart cards and tokens that are not automatically recognized by the VPN Client. You enter this information in the ATR section of the vpnconf.ini file.

Table 9. ATR parameters for the vpnconf.ini file in the order of entry

Parameter	Description	
`[ATR#]`	Token ID. This is also the delimiter to separate ATR codes if there is more than one ATR code in the vpnconf.ini file.	
`mask`	The mask code for the smart card or token.	
`scname`	The name of the smart card or token.	
`manufacturer`	The name of the manufacture of the smart card or token.	
`pkcs11DllName`	The name of the PKCS#11 middleware file for the smart card or token.	
`registry`	The name of the key in the registry that contains the path to the middleware (that is, the DLL file). The format is: `PRIMARY_KEY:..\\..\\..:middleware`	**Note:** You need to specify either `registry` or `DLLPath`.
`DLLPath`	The path to the PKCS11 DLL file.	

The following is an example of an ATR section in a vpnconf.ini file:

```
[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:00:01]
mask="FF:FF:FF:FF:FF:FF:FF:00:FF:00:00:FF:FF:00:00:00:FF"
scname="Access"
manufacturer="Axalto"
pkcs11DLLName="mdlw.dll"
registry="KEY_LOCAL_MACHINE:SOFTWARE\\Axalto\\Access\\CK:PKCS#11DLL"
```

Troubleshoot the VPN Client

7

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

Overview

You can find information about the VPN connection state, VPN traces, and VPN logs on the VPN Console Active screen (see *VPN Console Active Screen* on page 33).

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, Wireshark is a good and free network analysis software tool (see *http://www.wireshark.org/*) 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 software activation, see *Troubleshoot Software Activation* on page 20.

Note: For difficulties with certificates, see *Troubleshoot Certificates* on page 82.

Resolve Firewall Interference

If you cannot establish a VPN tunnel, your firewall might be interfering. Create firewall rules that allow all traffic to and from the following ports:

- TCP port 500
- UDP port 500
- TCP port 4500
- UDP port 4500

Typical Errors

The following typical errors might occur on the VPN Client:

Note: Dates, times, and numbers that can precede the actual messages have been removed from these examples.

PAYLOAD_MALFORMED Error (Wrong Phase 1 [SA])

VPN Console Log:

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

```
Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
Default dropped message from 195.100.205.114 port 500 due to notification type
INVALID_COOKIE
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:

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

Explanation. The pre-shared key or local ID might be incorrect. The logs of the remote endpoint might provide more information.

Resolution. Ensure that you use the same pre-shared key on each side of the VPN tunnel and that the local IDs are correctly defined. For information about configuring the pre-shared key, see *Configure Advanced Authentication* on page 44.

received remote ID other than expected Error

VPN Console Log:

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
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 *Configure Advanced Authentication* on page 44).

NO_PROPOSAL_CHOSEN Error (Phase 1)

VPN Console Log:

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
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 information about authentication, see *Configure Authentication* on page 42.

NO_PROPOSAL_CHOSEN Error (Phase 2)

VPN Console Log:

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
```

```
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
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
Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
Default RECV Informational [HASH][DEL]
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 information about configuring encryption algorithms, see *Manually Configure IP Security or Phase 2* on page 49.

INVALID_ID_INFORMATION Error

VPN Console Log:

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.3.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
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
Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
Default RECV Informational [HASH][DEL]
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 *Manually Configure IP Security or Phase 2* on page 49) match the remote endpoint's address configuration. Ensure that no old SA is still alive on the VPN router.

Other Common Problems

Note: Dates, times, and numbers that can precede the actual messages have been removed from these examples.

There Is No Response to a Phase 1 Request

VPN Console Log:

```
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
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 information about configuring algorithms, see *Configure Authentication* on page 42.

Also ensure that the local and remote IDs are correctly specified on each side of the VPN tunnel. For information about configuring local and remote IDs, see *Configure Advanced Authentication* on page 44.

The Console Shows Only SEND and RECV

VPN Console Log:

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

Explanation. The pre-shared key might mismatch on the tunnel endpoints.

Resolution. Ensure that you use the same pre-shared key on each side of the VPN tunnel and that there is no second VPN tunnel to the VPN Client on the VPN router.

There Is No Response to a Phase 2 Requests

VPN Console Log:

```
Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID]
[ID]
Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID]
[ID]
Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID]
[ID]
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 information about encryption algorithms, see *Manually Configure IP Security or Phase 2* on page 49.

Ensure that both the phase 2 address types and phase 2 address values (see *Manually Configure IP Security or Phase 2* on page 49) match the remote endpoint's address configuration.

A Tunnel No Longer Opens

Resolution. Read the logs for each VPN tunnel endpoint. A firewall might have dropped the IKE requests. The VPN Client needs to 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:

- 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.
- 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.
- Look at the VPN router logs. The firewall of the VPN router might have dropped the packets.
- Verify that your ISP supports ESP.
- Use a network analysis software tool (such as the free Wireshark tool; visit *http://www.wireshark.org/*) 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.

- 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 no default gateway specified.
- Verify that the computers in the LAN are specified by their IP address and not by their FQDN.
- Use a network analysis software tool (such as the free Wireshark tool; visit *http://www.wireshark.org/*) on one of the target computers to verify that the ping arrives inside the LAN.

View the Logs

For information about how to view the VPN logs on the VPN Client, see *VPN Console Active Screen* on page 33. The following figure shows an example of VPN logs on a NETGEAR ProSAFE VPN Firewall SRX5308 router.

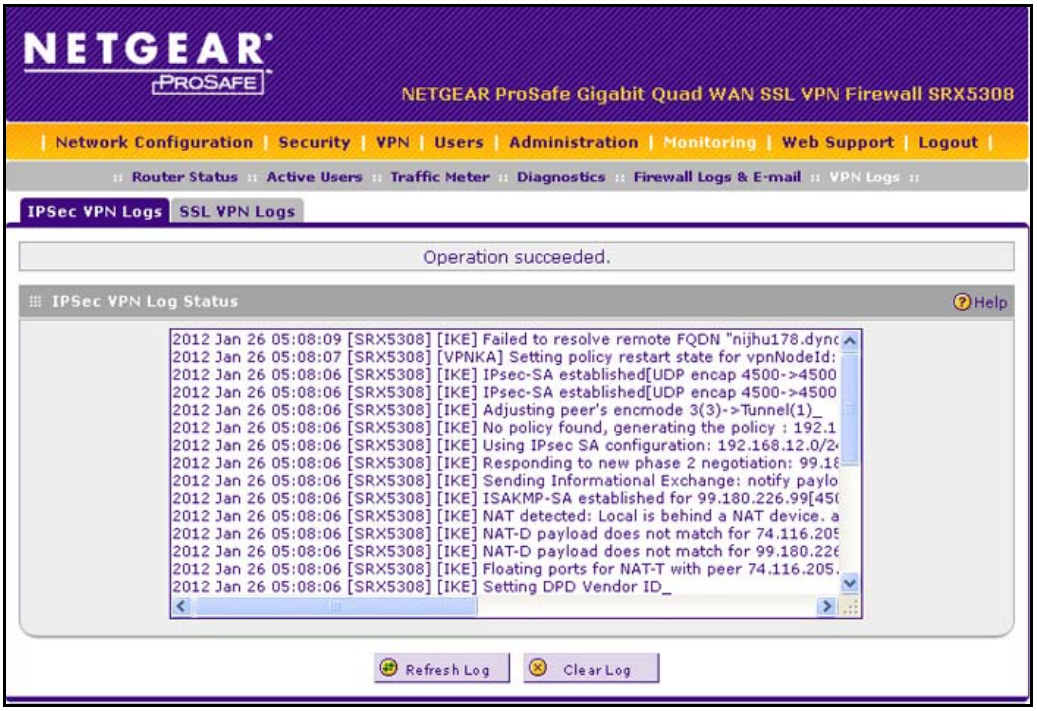


Figure 28. IPSec VPN Logs screen of a ProSAFE VPN Firewall SRX5308 router

Following is an example of a VPN log on the VPN router after a VPN Client has successfully established a VPN connection with the VPN router. (This example does not relate to the information that is shown in the previous screen; in addition, the date and times that precede the actual messages have been removed from this example.)

```
[SRX5308] [IKE] Remote configuration for identifier "srx_client.com" found_
[SRX5308] [IKE] Received request for new phase 1 negotiation:
10.200.13.18[500]<=>116.66.200.178[885]_
[SRX5308] [IKE] Beginning Aggressive mode._
```

```
[SRX5308] [IKE] Received unknown Vendor ID_
[SRX5308] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02__
[SRX5308] [IKE] Received unknown Vendor ID_
[SRX5308] [IKE] For 116.66.200.178[885], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
[SRX5308] [IKE] Floating ports for NAT-T with peer 116.66.200.178[28950]_
[SRX5308] [IKE] NAT-D payload does not match for 10.200.13.18[4500]_
[SRX5308] [IKE] NAT-D payload does not match for 116.66.200.178[28950]_
[SRX5308] [IKE] NAT detected: Local is behind a NAT device. and also Peer is
behind a NAT device_
[SRX5308] [IKE] ISAKMP-SA established for
10.200.13.18[4500]-116.66.200.178[28950] with
spi:14e465c525b13972:87ea734ec64e1c97_
[SRX5308] [IKE] Sending Informational Exchange: notify
payload[INITIAL-CONTACT]_
[SRX5308] [IKE] Responding to new phase 2 negotiation: 10.200.13.18[0]<=
>116.66.200.178[0]_
[SRX5308] [IKE] Using IPsec SA configuration: 192.168.30.0/24<->0.0.0.0/0 from
srx_client.com_
[SRX5308] [IKE] No policy found, generating the policy : 192.168.31.201/32[0]
192.168.30.0/24[0] proto=any dir=in_
[SRX5308] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1)_
[SRX5308] [IKE] IPsec-SA established [UDP encap 28950->4500]: ESP/Tunnel
116.66.200.178->10.200.13.18 with spi=8414587(0x80657b)_
```

Configure the VPN Client with a NETGEAR Router

A

This appendix describes how to configure the VPN Client with a NETGEAR ProSAFE SRX5308 VPN Firewall (in this appendix referred to as the SRX5308 VPN router). The appendix includes the following sections:

Introduction

In addition to the NETGEAR ProSAFE SRX5308 VPN router, you can also apply the information in this appendix to the following NETGEAR ProSAFE routers and ProSecure UTM appliances. The information in this appendix has been tested with the VPN Client firmware version 5.11 and the firmware releases that are listed in the following table.

Table 10. Tested firmware versions

Router	Firmware Version
FVS318N	4.0.1-67 or later
FVG318v2	2.1.3-29 or later
FVS336Gv2	3.0.7-79 or later
SRX5308	3.0.7-65 or later
UTM5	1.3.15.9 or later
UTM10	1.3.15.9 or later
UTM9S	2.1.0-3 or later
UTM25	1.3.15.9 or later
UTM25S	3.0.1-124 or later
UTM50	1.3.15.14 or later
UMT150	1.3.15.14 or later

Sample VPN Network Topology

In the VPN network example that is shown in the following figure, the SRX5308 VPN router functions as a gateway for a main office. The VPN Client is installed on a remote laptop that runs Windows 7 and that connects to the Internet through a DSL modem. The VPN Client connects to the SRX5308 VPN router and establishes a secure IPSec VPN connection with the router so the laptop user can gain access to a file server or any other resources at the main office.

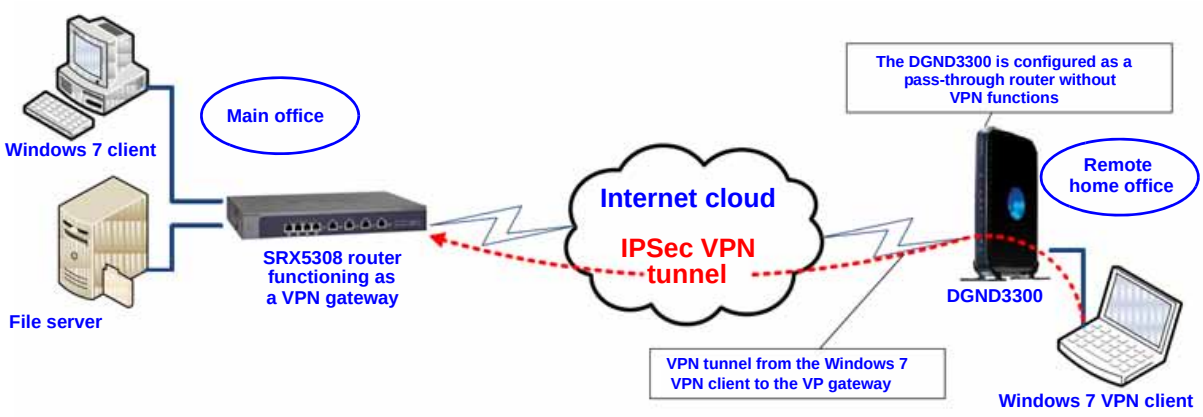


Figure 29. VPN network topology example

The following table shows the IP addresses and VPN settings that are used in the VPN network example that is shown in the previous figure.

Table 11. IP address and VPN setting for the VPN network topology example

Main Office Settings	Remote Home Office Settings
SRX5308 WAN IP address. 10.200.13.18 (or myrouter.dyndns.org) **SRX5308 LAN IP address**. 192.168.30.1 **Subnet mask**. 255.255.255.0 **File server LAN IP address**. 192.168.30.2 **Subnet mask**: 255.255.255.0 **Default gateway IP address**. 192.168.30.1 **Windows 7 client LAN IP address**. 192.168.30.3 **Subnet mask**. 255.255.255.0 **Default gateway IP address**. 192.168.30.1	**DGND3300 IP LAN address**. 192.168.0.1 **Subnet mask**. 255.255.255.0 **Windows 7 VPN Client LAN IP address**. 192.168.0.2 **Subnet mask**. 255.255.255.0 **Default gateway IP address**. 192.168.0.1 **Pre-shared key**. N3tg4ar12 **VPN Client identifier**. srx_client.com **VPN gateway identifier**. srx_router.com

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

While you configure the SRX5308 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 white font in a red circle in the figures and in the text (for example, ❸).

You can print the following table to keep track of this information.

❶	**Pre-shared key**	
❷	**Remote identifier information**	
❸	**Local identifier information**	
❹	**Router's LAN network IP address**	
❺	**Router's LAN network mask**	
❻	**Router's WAN IP address**	

Configure the SRX5308 VPN Router

The router lets you 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.

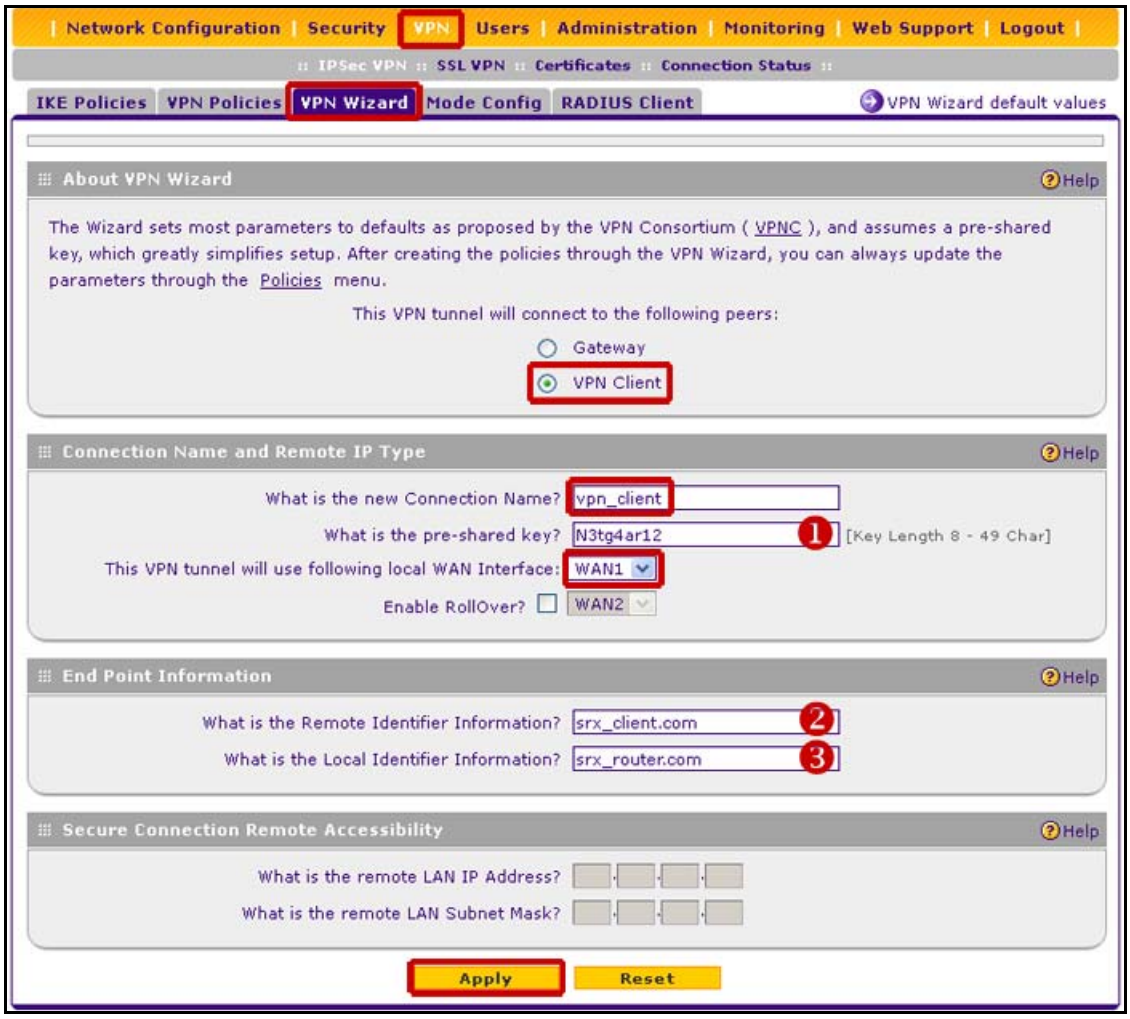
Use the VPN Wizard to Configure a Client-to-Router VPN Connection

The SRX5308 VPN router includes a VPN Wizard that lets you easily set up a 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.
2. Select **VPN > IPSec VPN > VPN Wizard**.

The VPN Wizard screen displays:



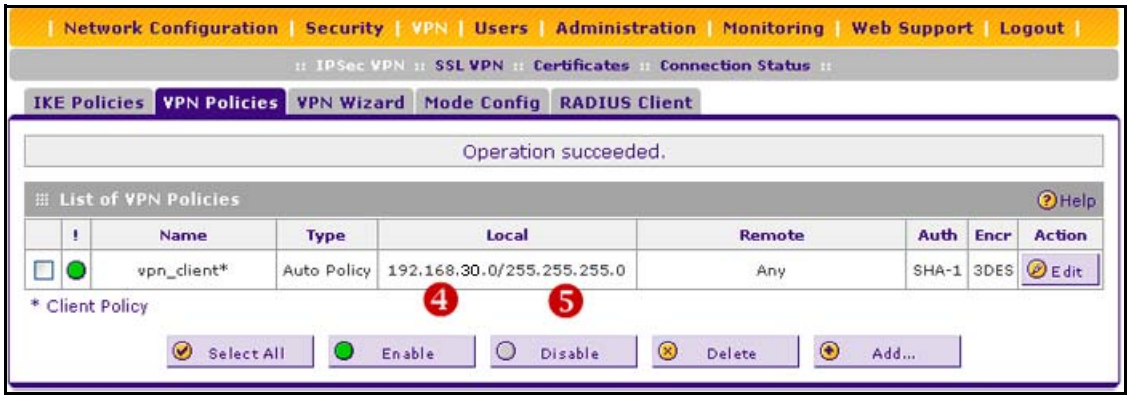
3. Specify the settings that are described in the following table.

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 **N3tg4ar12**. 1 **Note:** This key must be at least 8 characters long and should not be easy to guess.

Setting	Description
This VPN Tunnel will use the following local WAN Interface	Select **WAN1** from the drop-down menu. **Note:** This option is not available for platforms with a single WAN port.
End Point Information	
What is the Remote Identifier Information?	Enter **srx_client.com**. ❷ The default setting is srx_remote1.com.
What is the Local Identifier Information?	Enter **srx_router.com**. ❸ The default setting is srx_local1.com.

4. Click **Apply**.
5. Review the policies by selecting **VPN > IPSec VPN > VPN Polices**.

   The VPN Policies screen displays. Take note of the local LAN IP address ❹ and subnet mask **y**, both of which you will use later in the configuration of the VPN Client.

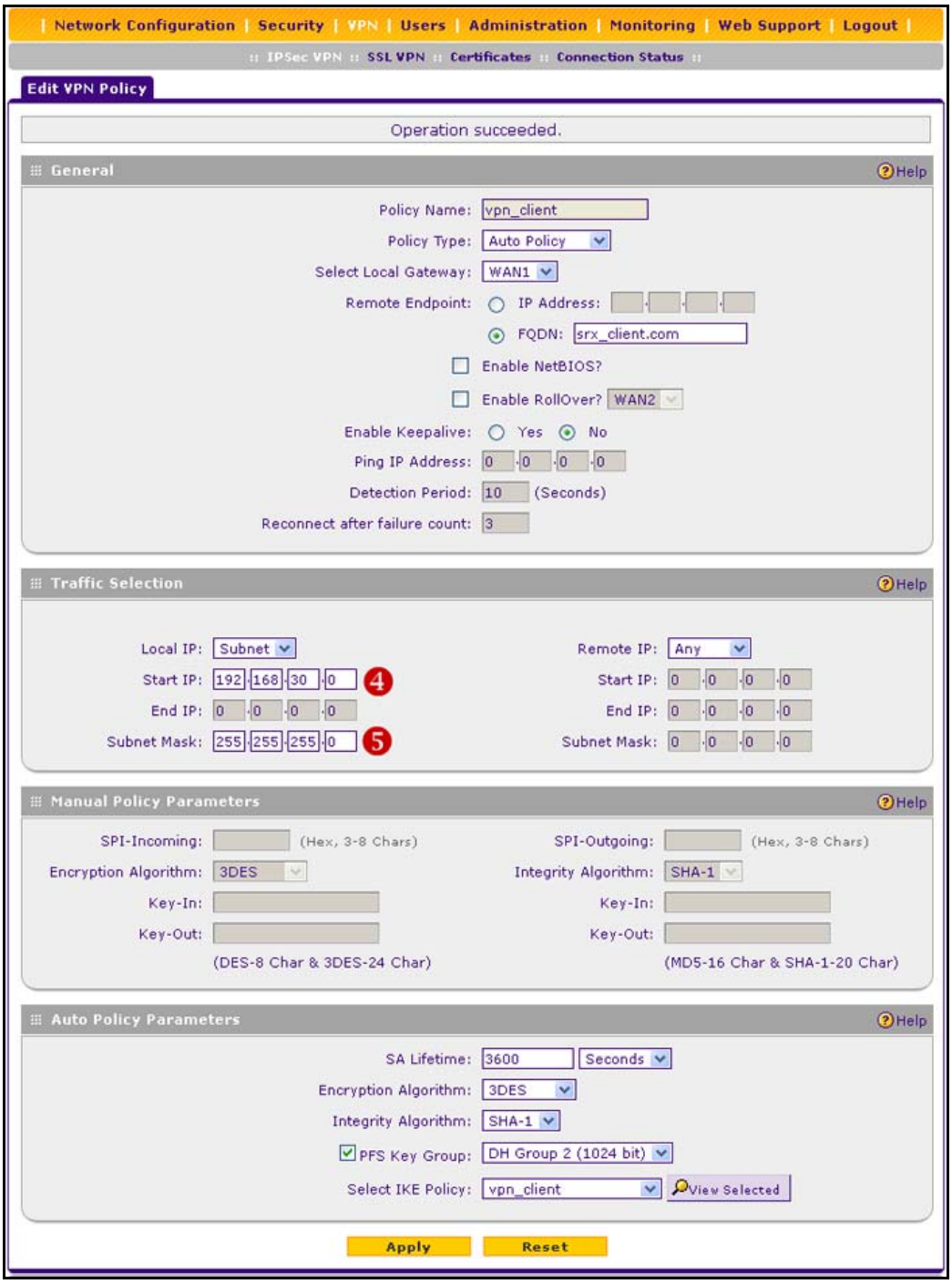


6. (Optional) Review or edit the VPN policy:
   a. Select the check box that is associated with the policy.
   b. Click **Disable**.

      The VPN policy is disabled.

   c. In the Action column of the VPN Policies screen, click **Edit**.

The Edit VPN Policy screen displays:



d. Modify the VPN policy.

e. Click **Apply**.

The VPN Policies screen displays again.

f. Select the check box that is associated with the policy.

g. Click **Enable**.

The VPN policy is reenabled.

7. (Optional) Review or edit the IKE policy.

You cannot edit the IKE policy without disabling the associated VPN policy. To edit the IKE policy:

a. On the VPN Policies screen, select the check box that is associated with the policy.

b. Click **Disable**.

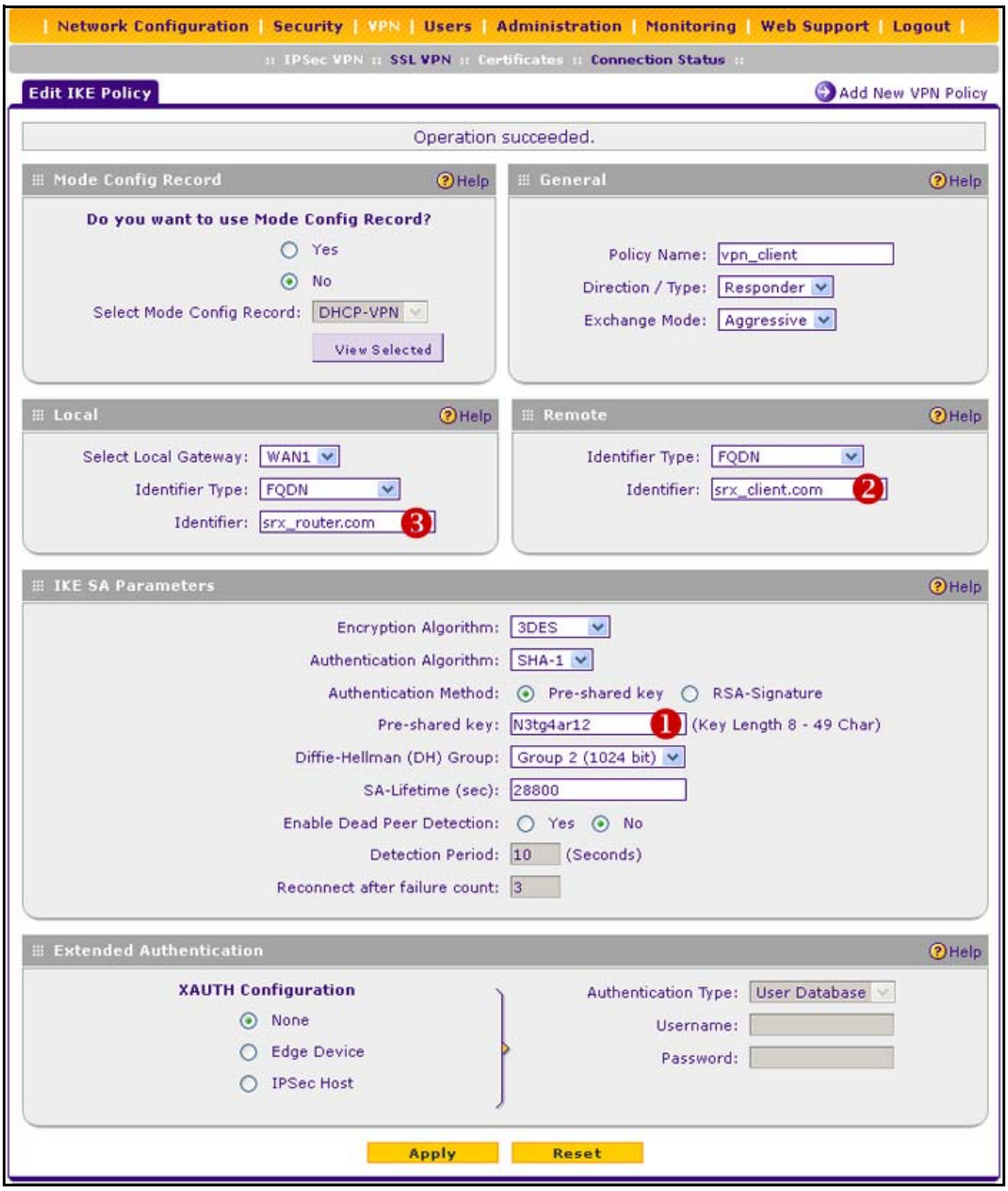
The associated VPN policy is disabled.

c. Click the **IKE Policies** tab.

The IKE Policies screen displays. Take note of the remote ID ❷ and local ID ❸, both of which you will use later in the configuration of the VPN Client.

d. In the Action column of the IKE Policies screen, click **Edit**.

The Edit IKE Policy screen displays. Take note of the pre-shared key ❶, which you will use later in the configuration of the VPN Client.



e. Modify the IKE policy.

f. Click **Apply**.

The IKE Policies screen displays again.

g. Click the **VPN Policies** tab.

The VPN Policies screen displays.

h. Select the check box that is associated with the policy.

i. Click **Enable**.

The VPN policy is reenabled.

For information about how to configure the VPN Client, see *Configure the VPN Client* on page 155.

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 create a VPN policy.

IKE Policy

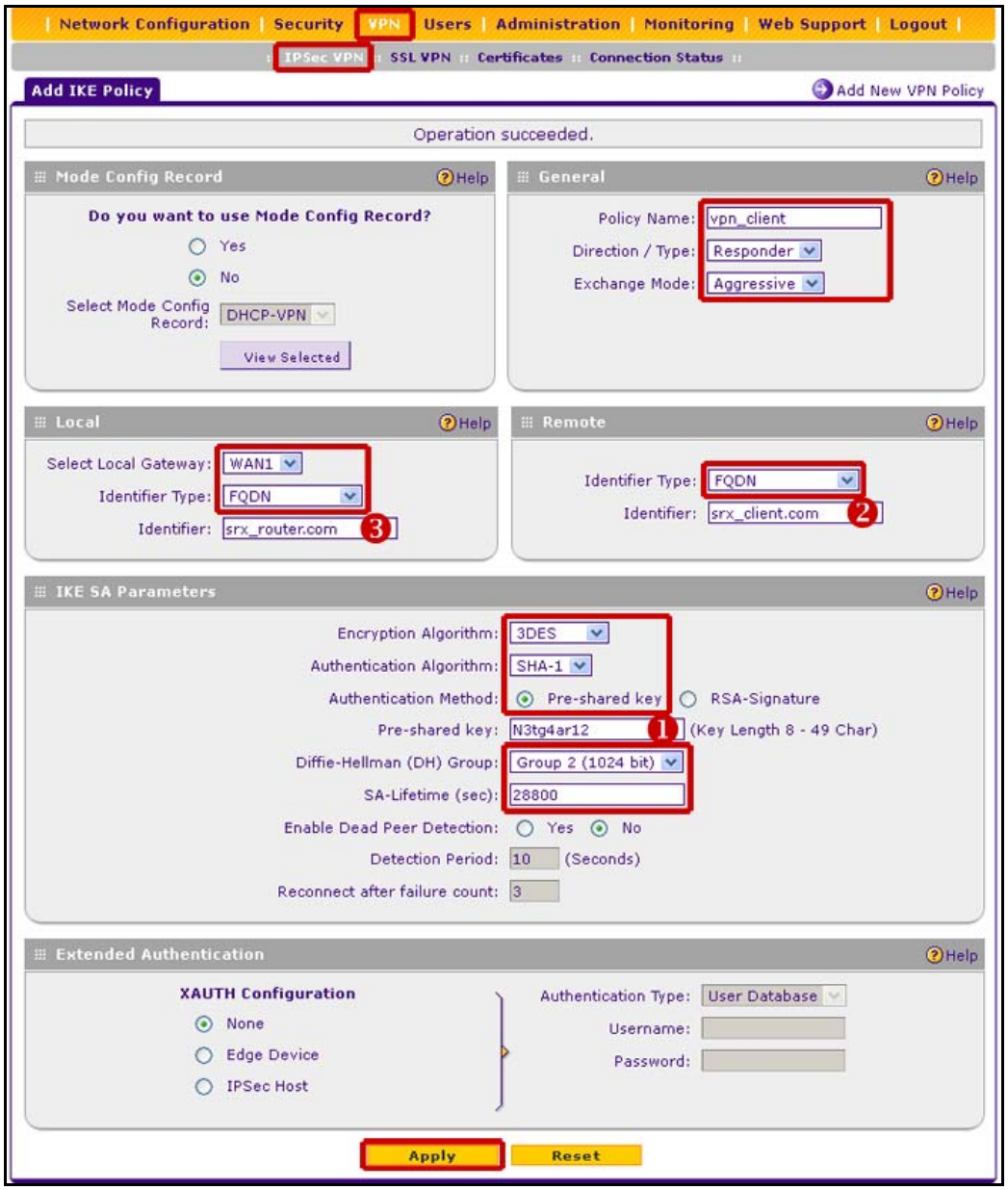
➢ **To set up an IKE policy:**

1. Select **VPN > IPSec VPN > IKE Polices**.

   The IKE Policies screen displays.

2. Click **Add**.

The Add IKE Policy screen displays:



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

Setting	Description
General	
Policy Name	Enter **vpn_client**.
Direction / Type	Select **Responder** from the drop-down menu (the router will be responding to the client).
Exchange Mode	Select **Aggressive** (mode) from the drop-down menu.

Setting	Description
Local	
Select Local Gateway	Select **WAN1** from the drop-down menu. **Note:** This option is not available for platforms with a single WAN port.
Identifier Type	Select **FQDN** from the drop-down menu.
Identifier	Enter **srx_router.com**. ❸
Remote	
Identifier Type	Select **FQDN** from the drop-down menu.
Identifier	Enter **srx_client.com**. ❷
IKE SA Parameters	
Encryption Algorithm	Select **3DES** from the drop-down menu.
Authentication Algorithm	Select **SHA-1** from the drop-down menu.
Authentication Method	Select the **Pre-Shared Key** radio button.
Pre-shared key	Enter the pre-shared key **N3tg4ar12**. ❶ **Note:** This key needs to 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 menu.
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

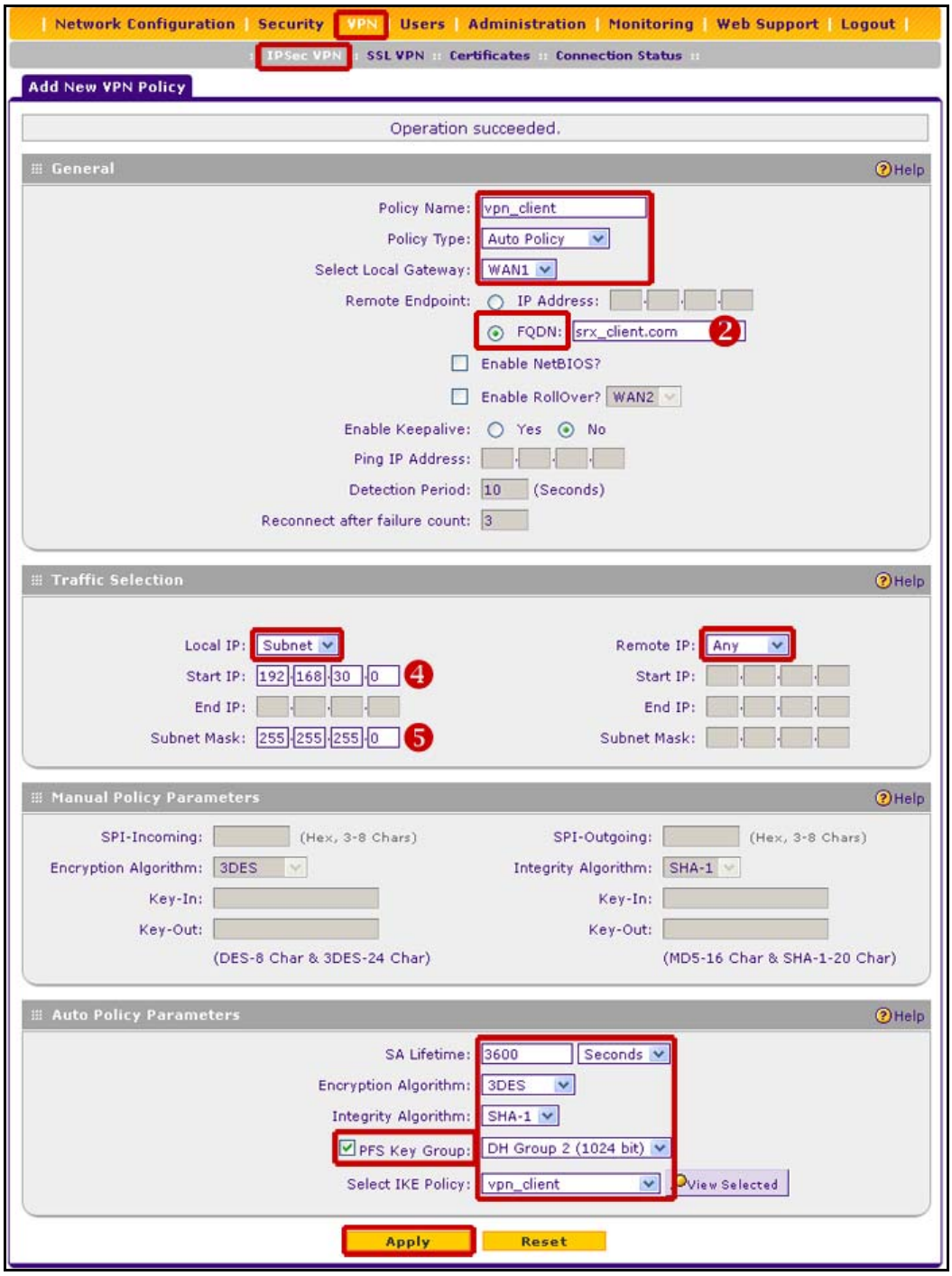
➢ **To set up a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Polices**.

   The VPN Policies screen displays.

2. Click **Add**.

The Add VPN Policy screen displays:



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

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 menu.
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 **srx_client.com** in the field to the right. ❷
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 keep-alives; select the **No** radio button. (This is the default setting.)
Traffic Selection	
Local IP	Select **Subnet** from the drop-down menu.
Start IP Address	Enter **192.168.30.0**. ❹
Subnet Mask	Enter **255.255.255.0**. ❺
Remote IP	Select **Any** from the drop-down menu.
Auto Policy Parameters **Note:** If you select **Manual Policy** from the Policy Type drop-down menu (see the General section on the screen), the Manual Policy Parameters section is enabled onscreen. Because you selected **Auto Policy**, the Auto Policy Parameters section is enabled.	
SA Lifetime	Enter **3600** and select **Seconds** from the drop-down menu.
Encryption Algorithm	Select **3DES** from the drop-down menu.
Integrity Algorithm	Select **SHA-1** from the drop-down menu.

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

4. Click **Apply**.

   The VPN Policies screen displays.

For information about how to configure the VPN Client, see the following section.

Configure the VPN Client

The VPN Client lets you 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.

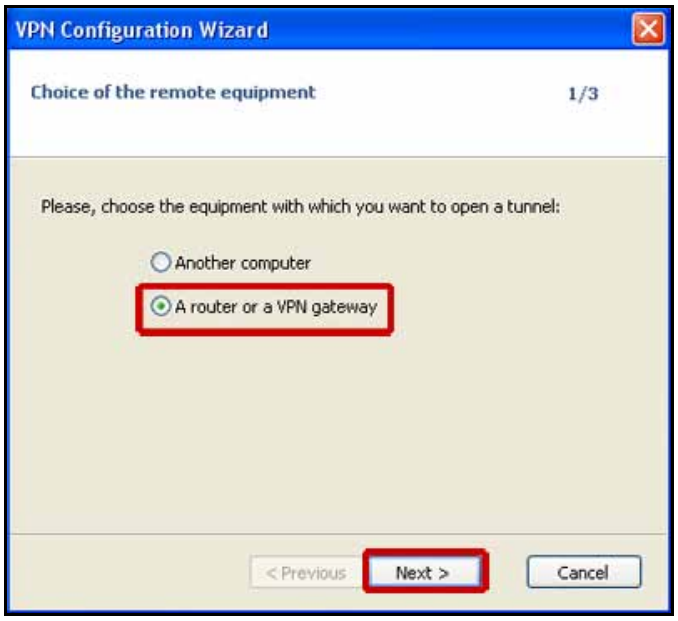
Use the Configuration Wizard to Configure the VPN Client

Note: For another example of how to use the Configuration Wizard, see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 36.

➢ **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.
2. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**.

The Choice of the remote equipment wizard screen (screen 1/3) displays:



3. Select the **A router or a VPN gateway** radio button.
4. Click **Next**.
5. The VPN tunnel parameters wizard screen (screen 2/3) displays:

6. 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.

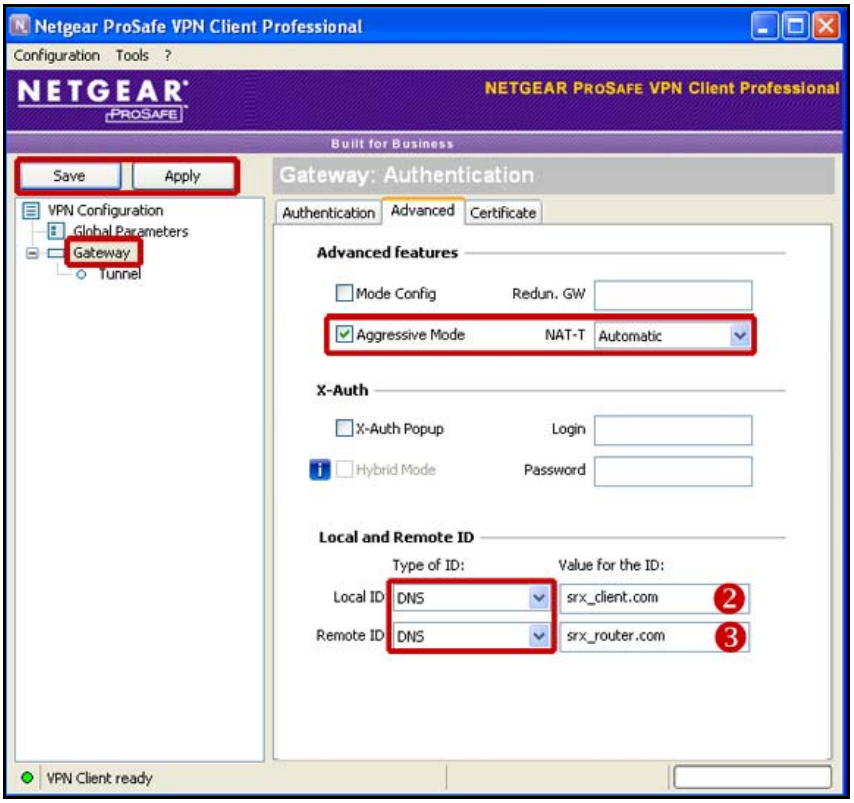
     For example, enter **myrouter.dyndns.org** or **10.200.13.18**. ❻
   - **Preshared key**. Enter **N3tg4ar12**, which is the pre-shared key that you already specified on the VPN router. ❶
   - **IP private (internal) address of the remote network**. Enter **192.168.30.0**, which is the remote private IP address of the remote VPN router.

     This IP address enables communication with the entire 192.168.30.x subnet. ❹
7. Click **Next**.

   The Configuration Summary wizard screen (screen 3/3) displays:

   This screen is a summary screen of the new VPN configuration.
8. Click **Finish**.
9. Specify the local and remote IDs:
   a. In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase).

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default:



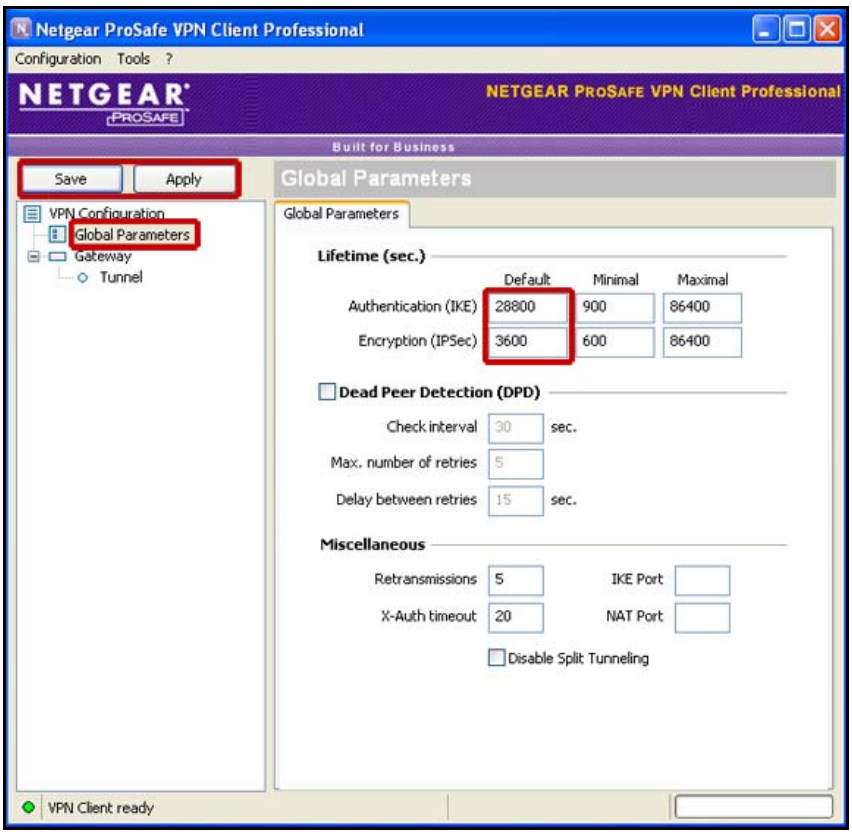
b. Specify the settings that are described in the following table.

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 menu to enable 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 menu because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_client.com** as the local ID for the VPN Client. ❷
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down menu because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_router.com** as the remote ID for the VPN router. ❸

10. Specify the global parameters:

    a. In the left column of the Configuration Panel screen, click **Global Parameters**.

    The Global Parameters pane displays in the Configuration Panel screen.



    b. Specify the following default lifetimes in seconds:

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

11. Click **Save**.

The VPN Client configuration is now complete.

For information about how to connect the VPN Client to the VPN router, see *Establish a VPN Connection* on page 166.

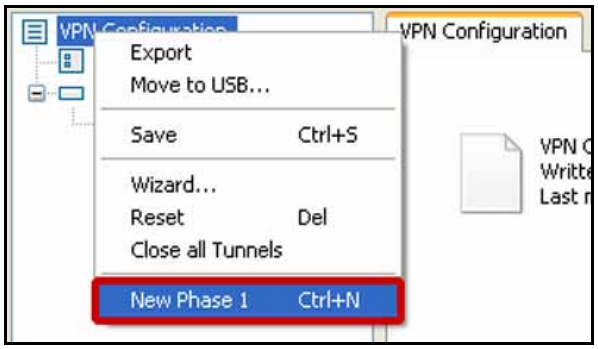
Manually Configure the VPN Client

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

Configure the Authentication Settings (Phase 1 Settings)

➢ **To create authentication settings:**

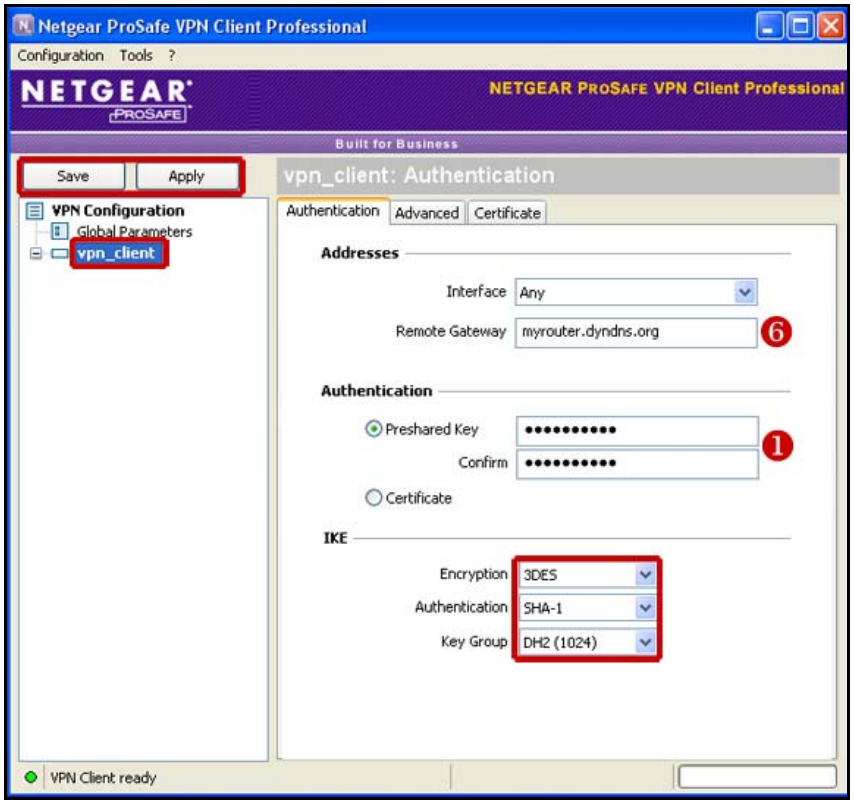
1. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**.
2. Select **New Phase 1**.



3. Change the name of the authentication phase name (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Type **vpn_client**.
   d. Click anywhere in the tree list pane.

Note: *This is the name 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 list pane. This name needs to be a unique name.*

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default:

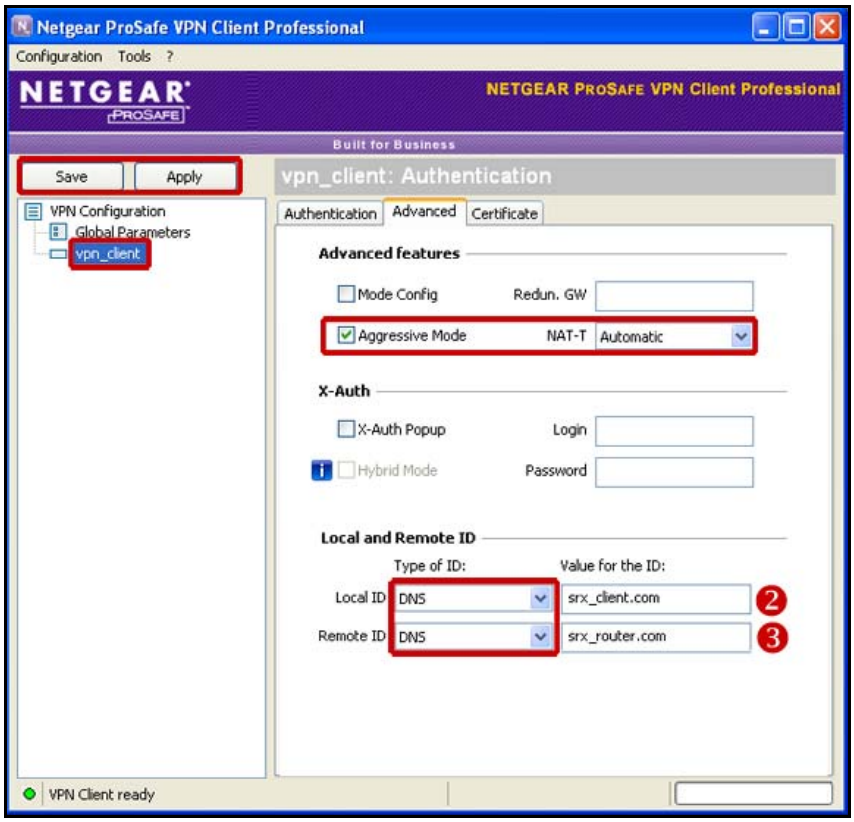


4. Specify the settings that are described in the following table.

Setting	Description	
Interface	Select **Any** from the drop-down menu.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN router. for example, **myrouter.dyndns.org** or **10.200.13.18**. 6	
Preshared Key	Select the **Preshared Key** radio button. Enter **N3tg4ar12**, which is the pre-shared 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 menu.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down menu.
	Key Group	Select the **DH2 (1024)** key group from the drop-down menu. **Note:** On NETGEAR routers, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Save**.
6. In the Authentication pane, click the **Advanced** tab.

The Advanced authentication pane displays:



7. Specify the settings that are described in the following table.

Setting	Description
Advanced Features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiating with the VPN router.
NAT-T	Select **Automatic** from the drop-down menu to enable 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 menu because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_client.com** as the local ID for the VPN Client. ❷
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down menu because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_router.com** as the remote ID for the VPN router. ❸

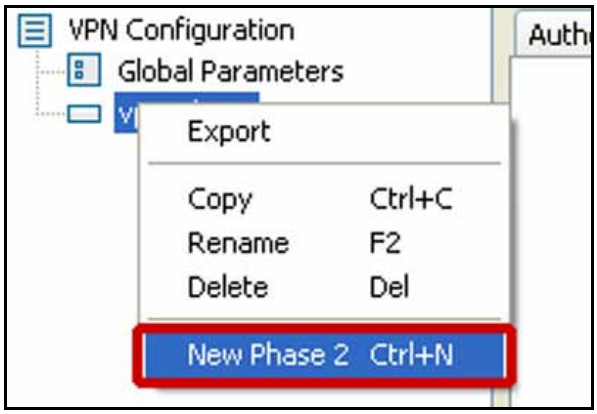
8. Click **Save**.

Create the IPSec Configuration (Phase 2 Settings)

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

➢ **To create an IPSec configuration:**

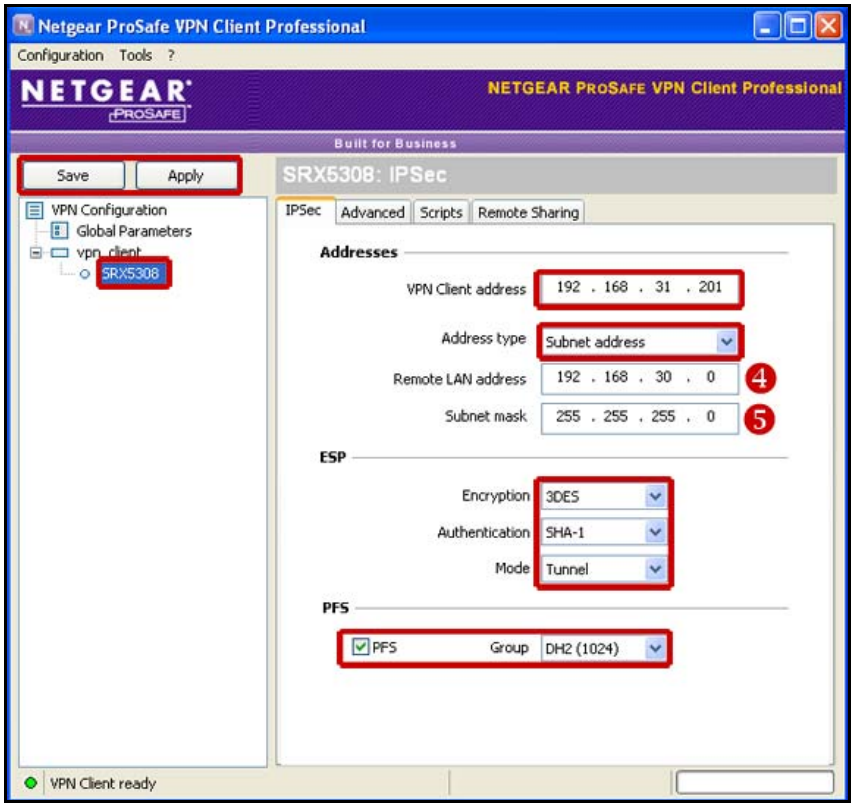
1. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name.
2. Select **New Phase 2**.



3. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **SRX5308**.
   d. Click anywhere in the tree list pane.

Note: *This is the name 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 list pane. This name needs to be a unique name.*

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default:



4. Specify the settings that are described in the following table.

Setting	Description	
VPN Client address	Enter **192.168.31.201**. This is the virtual IP address that the VPN Client uses 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 can also enter another LAN IP address or even **0.0.0.0** as the IP address.	
Address Type	Select **Subnet address** from the drop-down menu. 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 menu.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down menu.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down menu.

Setting	Description
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down menu. **Note:** On NETGEAR routers, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

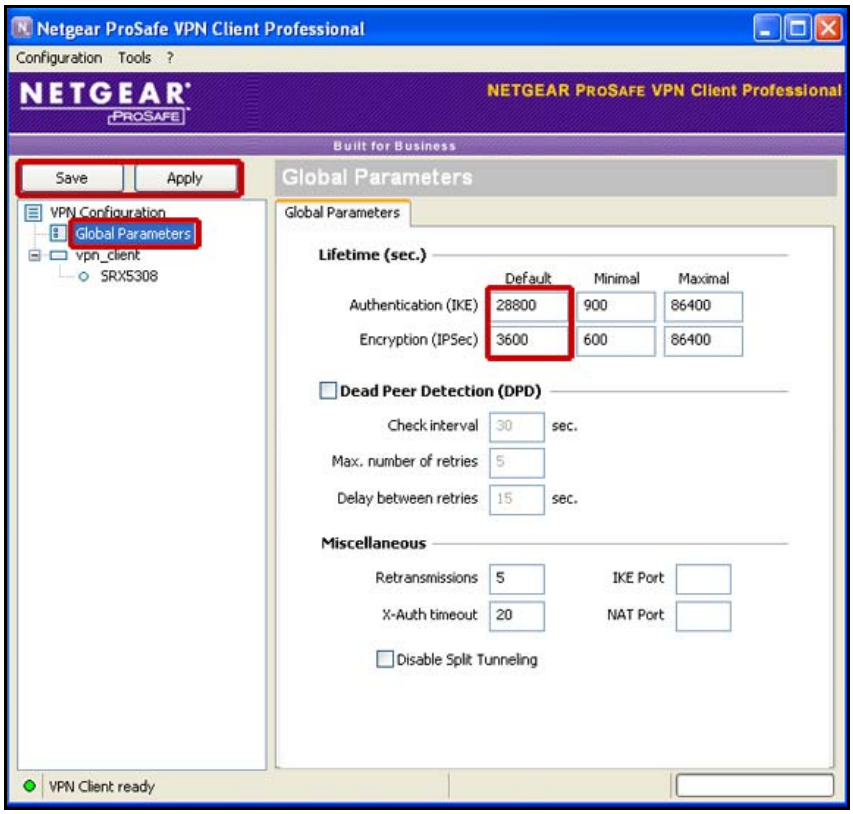
5. Click **Save**.

Global Parameters

➤ **To specify the global parameters:**

1. In the left column of the Configuration Panel screen, click **Global Parameters**.

   The Global Parameters pane displays in the Configuration Panel screen:



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

The VPN Client configuration is now complete.

For information about how to connect the VPN Client to the VPN router, see the next section.

Establish a VPN Connection

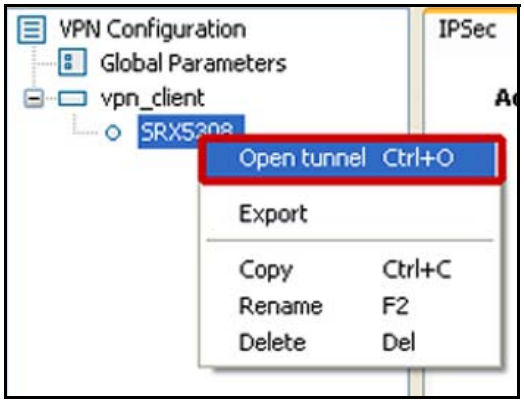
There are many ways to establish a connection. However, a network administrator can configure the VPN Client in such a way that an end user has only one way to establish a connection.

(The following procedures assume that you changed the authentication phase name to vpn_client and the IPSec configuration to SRX5308. If you did not, the default names are Gateway for the authentication phase name and Tunnel for the IPSec configuration.)

➢ **To establish a connection:**

Use one of the following methods:

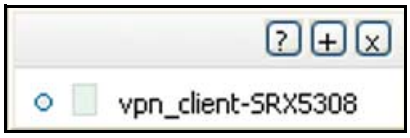
- **Use the Configuration Panel screen**. In the tree list pane of the Configuration Panel screen, perform *one* of the following tasks:
  - Click the **SRX5308** IPSec configuration name and press **Ctrl + O**.
  - Right-click the **SRX5308** IPSec configuration name and select **Open tunnel**.



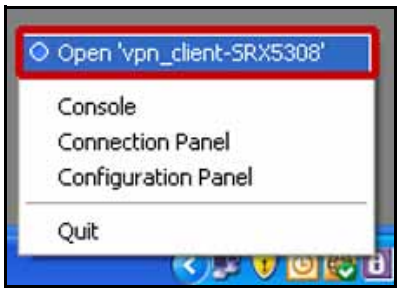
- **Use the Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen.

  Perform *one* of the following tasks:

  - Double-click **vpn_client-SRX5308**.
  - Right-click **vpn_client-SRX5308** and click **Open tunnel**.
  - Click **vpn_client-SRX5308** and press **Ctrl + O**.



- **Use the system-tray icon**. Right-click the system tray icon and click **Open 'vpn_client-SRX5308'**.



Note: After the tunnel has been established, the system tray icon changes from purple  to green  .

Index

E

F

G

H

I

K

R

S

T

U

V

W

X