NETGEAR®

NETGEAR ProSAFE VPN Client

VPNG01L and VPNG05L Version 6.0

User Manual

May 2015
202-10684-07

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

NETGEAR, Inc., NETGEAR and the NETGEAR logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory/*.

See the regulatory compliance document before connecting the power supply.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10684-07	6.0	May 2015	Documented VPN Client 6.0 software with new GUI displays. Added the new features, SHA-512, DH groups, and IPv6. The index was removed.
202-10684-06	–	May 2013	Color correction and minor nontechnical edits.
202-10684-05	–	April 2013	• Rewrote the manual to be task-based. • Described new features, command references, certificates, and 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 Settings

Chapter 6 VPN Client Software Setup and Network Deployment

Introduction

1

The VPN Client allows you to establish secure connections over the Internet, for example, between a computer and a remote corporate Intranet. IPSec is the most secure way to connect because it provides strong user authentication and strong tunnel encryption and it works with existing network and firewall settings.

Note: To set up a VPN tunnel between a computer and a VPN gateway, first configure the VPN gateway. For information about how to set up a NETGEAR router as a VPN gateway, see *Appendix A, Configure a NETGEAR VPN Gateway*.

This chapter includes the following sections:

- *VPN Client Features*
- *VPN Client Licenses for Lite and Professional*
- *Linux Appliance Support*
- *References and Useful Websites*

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 *http://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 must update your firmware.

VPN Client Features

The VPN Client includes the following features.

Table 1. List of features

Feature	Specifications
Supported operating systems	• Windows Server 2003 32-bit • Windows Server 2008 32/64-bit • Windows 2012 32/64-bit • Windows Vista 32/64-bit • Windows 7 32/64-bit • Windows 8.1 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 with the VPN Client installed). • Supports peer-to-gateway connections, for example, between a computer with 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
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)

Table 1. List of features (continued)

Feature	Specifications
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 is supported on Windows Vista, Windows 2012, Windows 7, Windows 8, Windows server 2003, and Windows server 2008 to enable Windows logon using a VPN tunnel or enable to log in on a local machine. • Credential providers are supported on Windows Vista and Windows 7 to enable Windows logon using a VPN tunnel or enabling logging 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.
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 and VPN Configuration Panel 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.

Table 1. List of features (continued)

Feature	Specifications
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 for Lite and Professional

You can download a free 30-day trial version of VPN Client Light software, or you can purchase VPN Client Lite or VPN Client Professional, which includes more features.

Note: After the evaluation period expires, the VPN Client is disabled. By purchasing and activating a permanent license, you can transfer the trial version to a permanent version.

The following table lists the features that are included in the VPN Client Lite and VPN Client Professional versions.

Table 2. VPN Client Lite and VPN Client Professional comparison

VPN Client Feature	Lite	Professional
Connection Panel	Yes	Yes
Console logs	Yes	Yes
System tray pop-up	Yes	Yes
X-Auth	Yes	Yes
Mode Config	Yes	Yes
DNS/WINS server manual configuration	Yes	Yes
Hybrid mode	No	Yes
IKE/NAT-T ports can be modified	No	Yes
Disable split tunneling	Yes	Yes
Dead Peer Detection	Yes	Yes
GUI protection (password)	No	Yes

Table 2. VPN Client Lite and VPN Client Professional comparison (continued)

VPN Client Feature	Lite	Professional
Auto Open (Windows on startup on traffic detection)	No	Yes
Start VPN tunnel before Windows logon	No	Yes
Multitunnel configurations	No	Yes
Redundant gateways	Yes	Yes
Easy deployment by command-line interface (CLI)	No	Yes
Scripts	No	Yes
USB mode	No	Yes

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/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:

- *Install the VPN Client Software*
- *Launch the VPN Client*
- *Use the VPN Client Lite Evaluation Version*
- *License Number Concepts*
- *Activate the VPN Client License*
- *Uninstall the VPN Client Software*

Install the VPN Client Software

You can download a free 30-day trial version of VPN Client Lite software, or you can purchase and download VPN Client Lite or VPN Client Professional software, which includes more features. (See *VPN Client Features* on page 7.)

Note: If you use the 30-day trial version, when the evaluation period expires, the VPN Client is disabled. By purchasing and activating a permanent license, you can transfer the trial version to a permanent version.

To download the VPN client software, visit *http://support.netgear.com/product/vpng05l*.

➢ **To install the VPN client software:**

1. To download the VPN client software, visit *http://support.netgear.com/product/vpng05l*.
2. Unzip the file that you downloaded.
3. Double-click the file.

   The Welcome page displays.
4. Follow the onscreen prompts to complete installation.
5. If you are prompted to restart your computer, than do so.

   Whether you must restart depends on your operating system. Windows 8, Windows 7, or Windows Vista computers do not need to be restarted.

   The VPN Client Activation Wizard page displays.

How you activate VPN client depends on whether you activate a trial license or a permanent license:

- For information about the free trial software version, see *Use the VPN Client Lite Evaluation Version* on page 14.
- For information about software with a permanent license, see *Activate the VPN Client License* on page 16.

Launch the VPN Client

After you install 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 Windows Start menu, select the path to the VPN Client, for example, **Start > All Programs > NETGEAR > NETGEAR VPN Client Professional**.

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.

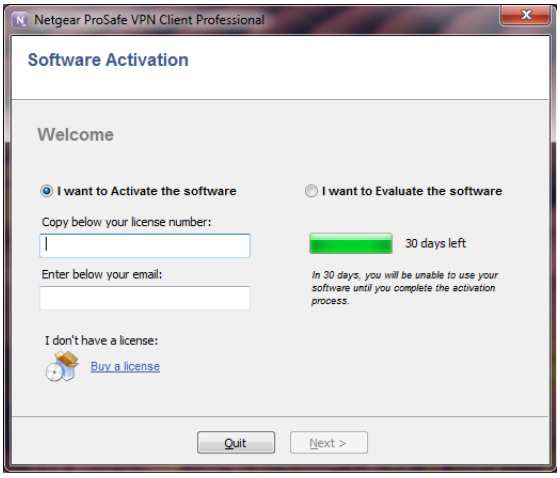
The VPN Client creates new rules in the Windows firewall (Vista and later operating systems) so that VPN traffic is enabled: UDP ports 500 and 4500 are authorized both for authentication (phase 1) traffic and for IPSec (phase 2) traffic.

If you use an earlier Windows operating system or another firewall, you might need to create firewall rules to enable the VPN Client. For information, see *VPN Console Log Errors* on page 113.

Use the VPN Client Lite Evaluation Version

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

1. On your desktop, double-click the **VPN Client** shortcut  .



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 the **Next** button.

   The VPN Configuration page displays.

During the evaluation period, the Software Activation page displays each time that you start the VPN Client. The remaining days of the evaluation period are displayed. You can also see the remaining days of the evaluation period on the About page (see *View the Remaining Days in the Evaluation Period* on page 15).

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 disabled.

- The message *Evaluation period expired* displays.
- The software is disabled.

For you to use the VPN Client, you must 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 expires.

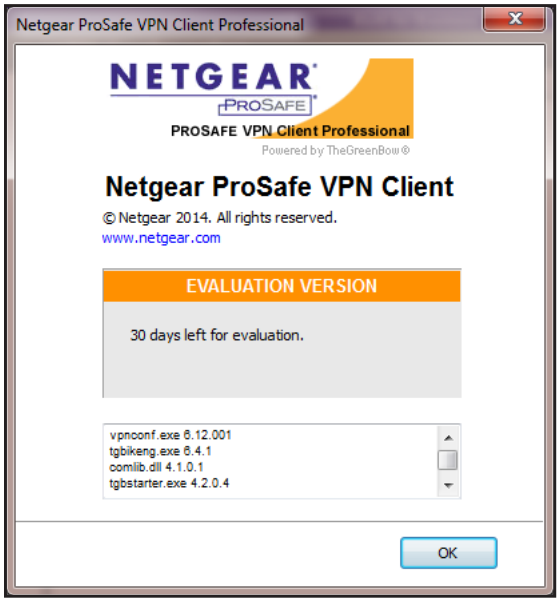
View the Remaining Days in the Evaluation Period

➢ **To view the remaining days in the evaluation period from VPN Client's user interface:**

1. On your desktop, double-click the **VPN Client** shortcut .

   The VPN Configuration page displays.

2. Select **? > About**.



   The About page displays the number of days that remain in the evaluation period.

Buy a License When the Evaluation Period Expires

When the evaluation period expires, the VPN Client is disabled. By purchasing and activating a permanent license, you can transfer the trial version to a permanent version.

➢ **To buy a permanent license:**

1. On your desktop, double-click the **VPN Client** shortcut .

   The Software Activation page displays. If the trial period expired, the page displays *Evaluation period expired*.

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

The NETGEAR website displays.

3. Follow the instructions onscreen to purchase a permanent license.
4. After you purchase a license, activate the permanent license.

   For more information about how to activate a permanent license, see *Activate the VPN Client License* on page 16.

License Number Concepts

A license number is attached to a single computer after activation. However, you can deactivate the license number (see *Uninstall the VPN Client Software* on page 18) and transfer it to another computer.

You can also change the license number at any time, but you first must 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 occurs. Also, keep the CD label for technical support.

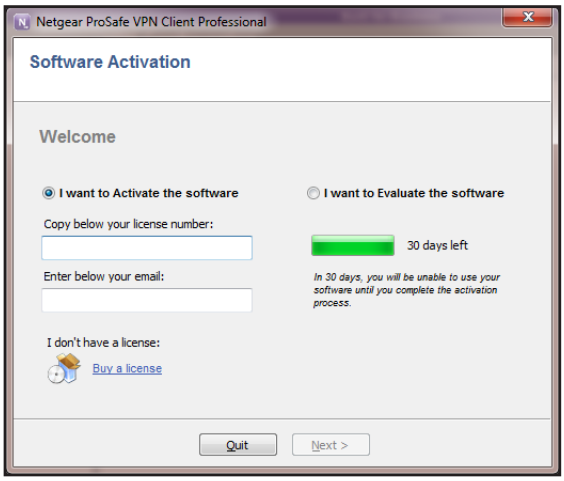
Activate the VPN Client License

When you purchase a license, you must activate it before you can use the VPN Client. You must activate the VPN Client license on your computer. You need the license number or key and an email address.

➢ **To activate your VPN Client license:**

1. Make sure that your computer is connected to the Internet.
2. On your desktop, double-click the **VPN Client** shortcut  .

   The VPN Configuration page displays.
3. Select **? > Activation Wizard**.



4. Select the **I want to Activate the software** radio button.
5. When prompted, enter your license number.
6. If a field displays to enter an email address, complete the field.

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

   Note: If the network administrator set up VPN Client to suppress the email address field, this field does not display. Some network administrators use this method to direct all software activation confirmation email to a single email address.

7. Click the **Next** button.

   The Software Activation Wizard connects to the activation server to activate the VPN Client software. The progress bar shows the activation progress. The page displays a message when activation is complete.

8. If an error occurs, click the **More information about this error** link.

   For troubleshooting information, see *Troubleshoot Software Activation* on page 17.

9. Click the **Run** button.

   The VPN Client relaunches with the new license. The VPN Configuration page displays.

Troubleshoot Software Activation

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

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.

To view a list of all activation errors, visit *http://.support.netgear.com*.

Software Upgrade Concepts

Your VPN configuration is saved during a software upgrade and automatically reenabled within the new release. If you specified a password for access control (see *Access Control Overview* on page 69), you must enter it to be able to upgrade the software.

After each software upgrade, you must reactivate the VPN Client. Depending on your maintenance contract, a software upgrade activation might be rejected. The success of 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 expired or if your license does not include a maintenance contract, only maintenance software upgrades are allowed. Maintenance software upgrades are identified by the last digit of a version.

  Example: Your maintenance period expired and your current software release is 4.12. You can upgrade to releases 4.13 through 4.19 but not to release 4.20, 5.00, or 6.00.

To subscribe or extend your maintenance period, contact NETGEAR by email at *sales@netgear.com*.

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

1. On your desktop, double-click the **VPN Client** shortcut  .

   The VPN Configuration page displays.
2. Select **? > Check for Update**.

   The NETGEAR website displays.
3. Check to see if the VPN Client is running the latest software release.
4. Download the updates that are supported by your license.

Uninstall the VPN Client Software

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

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

Several methods are available for uninstalling the VPN Client software. Depending on your Windows operating system, these methods might differ slightly from the following procedures.

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

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

1. Make sure that your computer is connected to the Internet.
2. Select **Start > Control Panel**.

3. Double-click **Programs and Features**.

   IIn some Windows versions, you must double-click **Add or Remove Programs**.

4. Right-click **NETGEAR VPN Client Professional** and select **Uninstall**.

   In some Windows versions, you must select **Remove**.

   The software is uninstalled from your computer.

➢ **To uninstall the VPN Client through the Windows 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 Professional**.
4. Select the uninstall option.

   The software is uninstalled from your computer.

Overview of the User Interface

3

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

- *User Interface Components*
- *VPN Configuration Panel*
- *System Tray Icon and System Tray Menu*
- *Connection Panel*
- *Keyboard Shortcuts*

User Interface Components

The VPN Client configuration is defined in a VPN configuration file. You can create, modify, save, export, or import the VPN configuration together with security elements such as a pre-shared key or certificates. You can also configure the VPN client to start and stop tunnels automatically, depending on traffic to certain destinations.

The user interface consists of the following components:

- VPN Configuration Panel that you use to specify VPN settings
- VPN Connection Panel that lets you open and close tunnels that you configured
- System tray icon and pop-up windows to view and manage the VPN tunnel status

For information about how to control the user interface display for end users, see *Hide User Interface Features* on page 71 and *Configure Which Items of the System Tray Menu Are Visible* on page 89.

VPN Configuration Panel

When you launch the VPN Client, the VPN Configuration page displays.

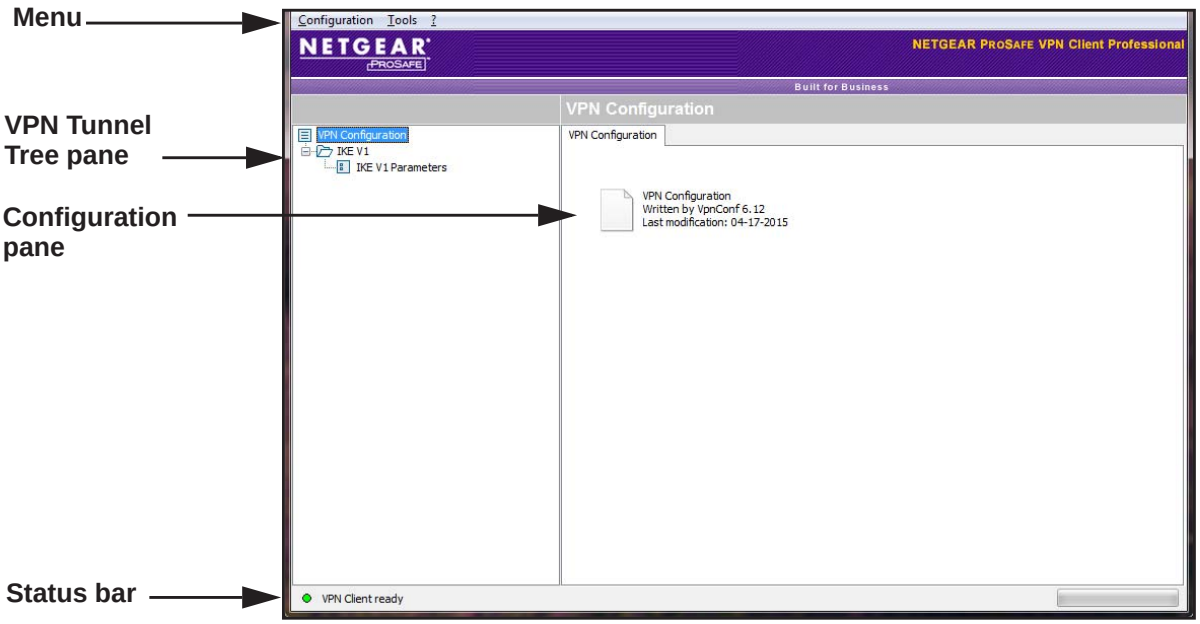


Figure 1. VPN Configuration page

You can use this page to configure VPN tunnels to connect the client computer to remote destinations that are configured to accept VPN client connections.

Note: For information about restricting access to the VPN Configuration page, see *Access Control Overview* on page 69.
For information about hiding the **VPN Configuration** link from the system tray menu, see *Hide User Interface Features* on page 71.

The menu at the top of the window includes 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 page, reset the IKE settings, and access the Option page 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 page.

Note: Some selections on the Configuration menu are also available by right-clicking a component of the VPN Tunnel Tree pane.

System Tray Icon and System Tray Menu

After you launch the VPN Client, the VPN Client displays an icon in the system tray that indicates whether a tunnel is open, using a color code.

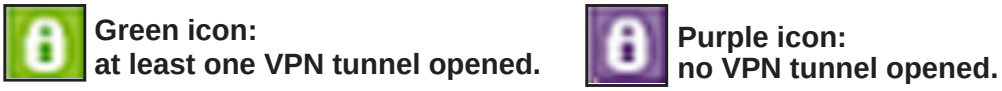
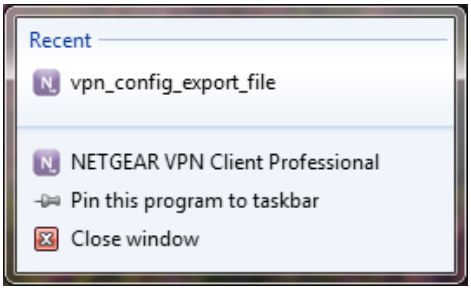


Figure 2. VPN Client icon colors in the system tray

➢ **To open the system tray menu:**

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



Some menu items do not display until you configure a working VPN tunnel. The following options are available in the system tray menu:

- **Close <gateway name-tunnel name>** Close the VPN tunnel that is currently open.
- **Open <gateway name-tunnel name>** Open an established VPN tunnel that is currently closed.
- **Console**. Open the VPN Console Active page.
- **Connection Panel**. Open the Connection Panel, which lets you open and close VPN tunnels and displays information about VPN tunnels.
- **Configuration Panel**. Open the Configuration Panel, which lets you create and configure VPN tunnels.
- **Quit**. Close all established VPN tunnels, then close the VPN Client.

System Tray Pop-Up Window

When a VPN tunnel opens or closes, a small window pops up from the system tray icon.

Figure 3. Tunnel opened pop-up window

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

Connection Panel

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

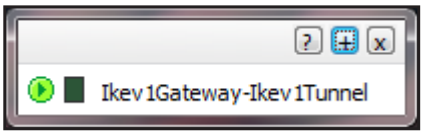
> **Note:** For information about hiding the **Connection Panel** link from the system tray menu, see *Hide User Interface Features* on page 71.

➢ **To open the Connection Panel:**

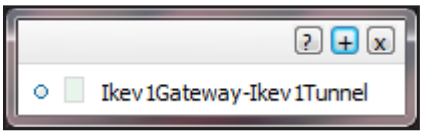
1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. Select **Tools > Connection Panel**.



Open tunnel



Closed tunnel

These examples show the Connection Panel after the VPN tunnel was already established.

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

The Connection Panel 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 page.
  - **+**. Opens the Configuration Panel.
  - **x**. Closes the Connection Panel.

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

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 VPN Tunnel Tree pane (see *Figure 1* on page 21)	
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.

Configure VPN Tunnels

4

This chapter describes how to create VPN tunnels. The chapter includes the following sections:

VPN Tunnel Overview

You can configure a computer as a VPN client. The computer can use the VPN tunnel to connect to a remote corporate LAN through a VPN gateway and for peer-to-peer connections. The remote gateway or peer must be configured to accept VPN clients.

The VPN tunnel in the following figure is set up with these characteristics:

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

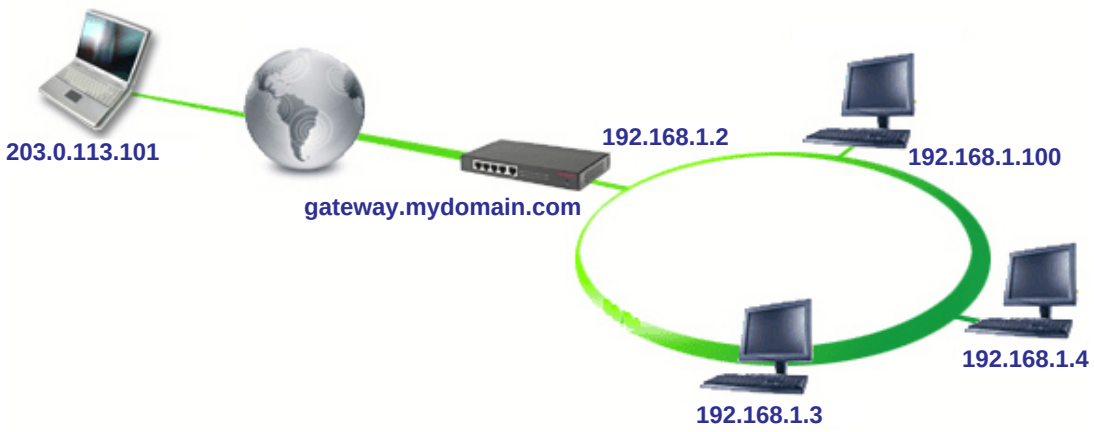


Figure 4. VPN connection between a computer and a remote corporate LAN

➢ **To configure the tunne:**

1. Set up the gateway for VPN connections.

   For information about how to set up a NETGEAR router as a VPN gateway, see *Appendix A, Configure a NETGEAR VPN Gateway*.

2. Specify the authentication (phase 1) settings.

   See *Configure IKE Authentication Settings* on page 28.

3. Specify the advanced authentication settings.

   See *Configure Advanced Authentication Settings* on page 30.

4. Specify the IPSec (phase 2) settings.

   See *Configure IPSec Settings* on page 37.

5. Specify the parameters.

   See *Configure the Parameter Settings* on page 40.

Note: You can use the VPN Wizard to enter some authentication settings (select **Configuration > Wizard**), but after you complete the wizard, you must also specify the advanced authentication, IPSec, and parameter settings.

Configure IKE Authentication Settings

You can 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.

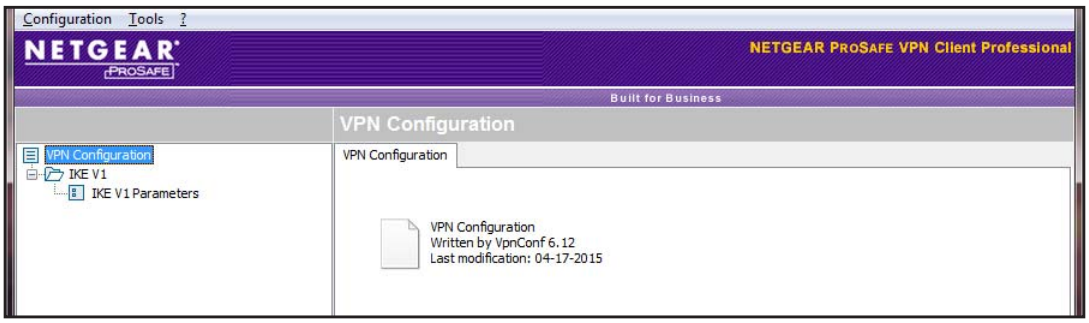
You can specify settings for several authentication phases, enabling one computer to establish IPSec VPN connections with several gateways or other computers (peer-to-peer connections).

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):

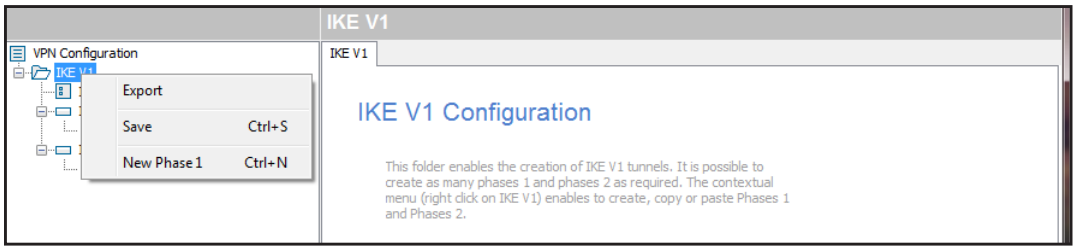
- Pre-shared key
- Static extended authentication
- Dynamic extended authentication
- Certificate stored in the VPN security policy
- Certificate in the Windows Certificate Store
- Certificate on a smart card or token

➢ **To configure authentication IKE settings:**

1. On your desktop, double-click the VPN Client shortcut  .



2. In the VPN Tunnel Tree pane, right-click the name of the IKE configuration.



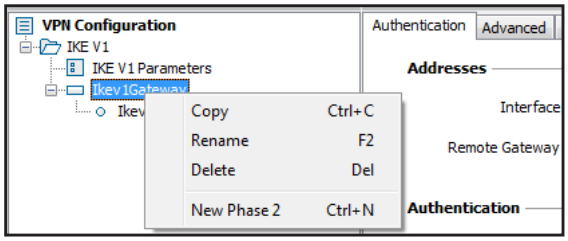
3. Select **New Phase 1** or select the configuration.

   The Ikev1Gateway: Authentication page displays in the Configuration pane on the right.

   The default name for authentication phase 1 is Ikev1Gateway. This authentication phase is used only for the VPN Client, not during IKE negotiation.This name must be unique.

4. To change the authentication phase 1 name, do the following:

   a. In the VPN Tunnel Tree pane, right-click the name.



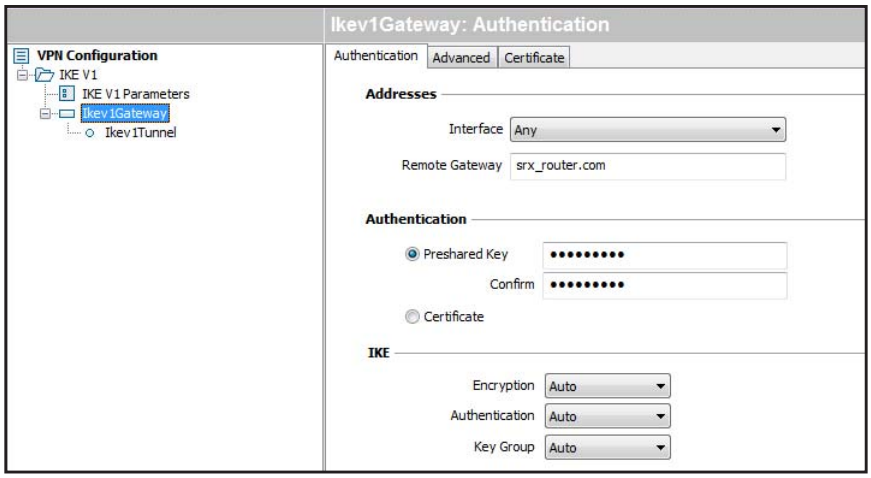
   b. Select **Rename**.

   c. Type the new name.

   d. Click anywhere in the VPN Tunnel Tree pane.

   The authentication name changes on the VPN Tunnel Tree pane and also in the Configuration pane on the right.

5. Specify the Addresses settings in the Authentication page:



a. In the **Interface** menu, leave **Any** selected if the IP address changes (when it is received dynamically from an ISP or router).

   You can enter the IP address of the network interface of the computer through which the VPN connection is established. If you select an IP address that does not exist on the computer, Any is used automatically.

b. In the **Remote Gateway** field, type the remote IP address or the DNS name of the VPN gateway.

   For example, type myrouter.dyn.com or 10.200.13.18.

6. To specify a preshared key, do the following:
   a. Select the **Preshared Key** radio button.
   b. Enter the preshared key that you already specified in the VPN gateway in the **Preshared Key** field and in the **Confirm** field.
7. To specify a X509 certificate, do the following:
   a. Click the **Certificate** tab.

      The Certificate page displays 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.

   b. Select the certificate.

      For information about certificates, see *Manage Certificates* on page 57.

   c. Click the **Authentication** tab.
8. In the **Encryption** menu, select the encryption algorithm that is used during the authentication phase.

   For a typical NETGEAR VPN gateway, select **3DES.**
9. In the **Authentication** menu, select the authentication algorithm that is used during the authentication phase.

   For a typical NETGEAR VPN gateway, select **SHA1.**
10. In the **Key Group** field, select the Diffie-Hellman key length that is used during the authentication phase.

    For a typical NETGEAR VPN gateway, select **DH2 (1024)**. On NETGEAR routers, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).
11. Select **Configuration > Save** or press Ctrl + S.

    Your settings are saved.

Configure Advanced Authentication Settings

For IKE authentication settings, the advanced configuration settings apply to *all* its associated IPSec policy settings.

Note: IKE authentication settings are sometimes referred to as phase 1 settings. IPsec policy settings are sometimes referred to as phase 2 settings.

➢ **To configure advanced authentication settings:**

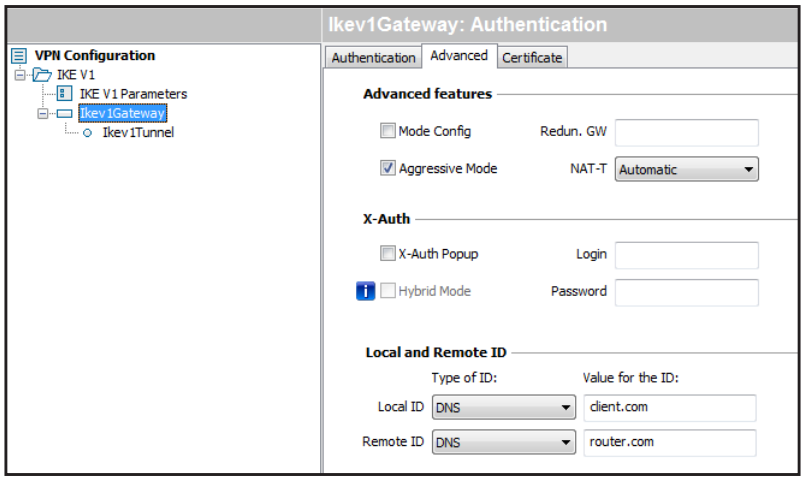
1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, right-click the name of the IKE configuration.

   The Authentication page displays.

3. Click the **Advanced** tab.



4. In the Advanced Features section, complete the fields:
   a. To allow the VPN Client to receive VPN configuration information from the remote VPN gateway, select the **Mode Config** check box.
   b. To allow the VPN Client to use aggressive mode as the negotiation mode, leave the **Aggressive Mode** check box selected.
   c. To enable the VPN Client to open an IPSec tunnel with an alternate gateway when the primary VPN gateway is down or stops responding, enter the IP address or URL of an alternate VPN gateway in the **Redund. GW** field.
   d. In the **NAT-T** menu, select one of the following NAT Traversal (NAT-T) modes:
      - **Automatic**. The VPN Client and VPN gateway negotiate NAT-T. This is the default setting.
      - **Forced**. The VPN Client forces 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.
5. To enable XAUTH, select the **X-Auth Popup** check box.

Note: For XAUTH, NETGEAR recommends that you do not complete the **Login** and **Password** fields on this page. Leave these fields blank so that the VPN Client user enters these credentials. This method is referred to as dynamic extended authentication.

For more information about XAUTH, see *Configure XAUTH* on page 32.

6. To enable this mode, select the **Hybrid Mode** check box and enter a name in the **Login** field and a password in the **Password** field.
7. Select the type of local ID and enter the associated value for the ID in the field to the right.

   The following selections are available:

   - **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 *Manage Certificates* on page 57). 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 a PEM Certificate* on page 58 and *Import a P12 Certificate* on page 59).

   Note: If a VPN tunnel closes because the computer changed its IP address, the VPN tunnel does not reopen automatically when the network becomes available again.

8. Select the type of remote ID and enter the associated value for the ID in the field to the right.

   The remote ID is the identity that the VPN Client receives from the VPN gateway during the authentication phase. The following selections are available:

   - **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 *Manage Certificates* on page 57). If you do not enter a certificate, the IP address of the VPN gateway is used.
9. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Configure XAUTH

Extended authentication (XAUTH) is an extension of the IKE protocol. 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).

When an end user opens a tunnel, a pop-up window opens and the end user must enter the XAUTH user name (login) and password. In a multiple VPN tunnel configuration, the name of the VPN tunnel displays in the pop-up window. The credentials must match those on the remote VPN gateway. If XAUTH authentication fails, the tunnel establishment fails too.

The end user is allowed some time to enter the credentials. If the time expires, a warning displays and the end user must 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 (see *Configure the Parameter Settings* on page 40).

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 page displays again.
- A pop-up warning alerts the user to try to open the VPN tunnel again.

➢ **To configure XAUTH:**

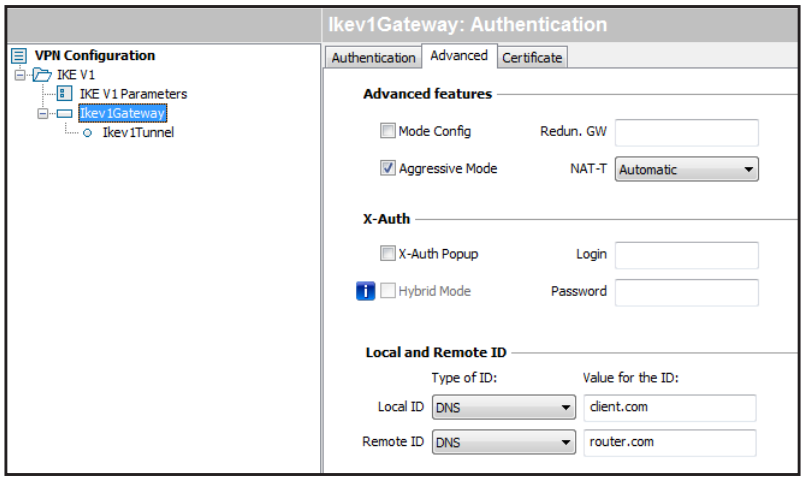
1. On the client computer desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, right-click the name of the IKE configuration.

   The Authentication page displays.

3. Click the **Advanced** tab.



4. Select the **X-Auth Popup** check box.

   Note: NETGEAR recommends that you do not complete the **Login** and **Password** fields on this page. Leave these fields blank so that the VPN Client user enters these credentials. This method is referred to as dynamic extended authentication.

   If you enter a name in the **Login** field and a password in the **Password** field, the pop-up window does not open, 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.

5. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Configure a Redundant Gateway

You can configure a redundant gateway. An alternate gateway is used under the following circumstances:

- 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 page (see *Configure the Parameter Settings* on page 40), the VPN Client uses the alternate gateway as the new tunnel endpoint. The interval between two attempts is about 10 seconds.
- A tunnel is established with the primary gateway with the Dead Pear Detection (DPD) feature 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 save the configuration or close and exit the VPN Client.

If the primary gateway can be reached but tunnel establishment fails (that is, VPN configuration errors occur), the VPN Client does not attempt to establish a tunnel with the alternate gateway. In this case, you must first resolve the configuration errors.

➢ **To configure a redundant gateway:**

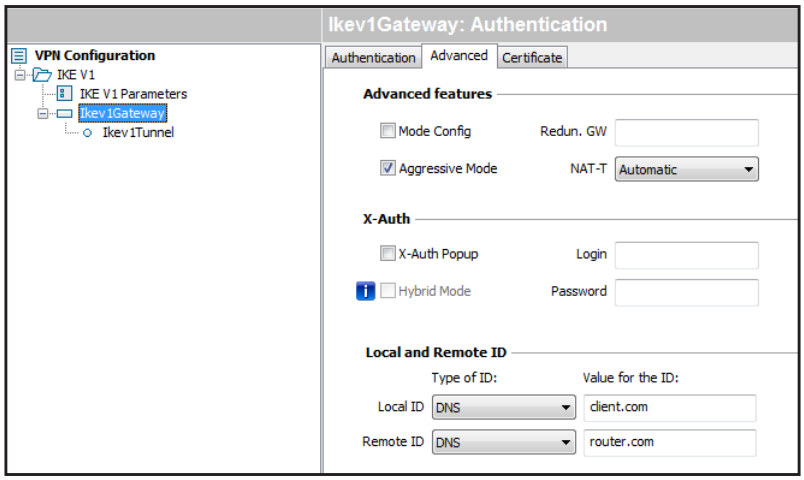
1. On the client computer desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, right-click the name of the IKE configuration.

   The Authentication page displays.

3. Click the **Advanced** tab.



4. Complete the **Redun. GW** field.
5. Enter the IP address of the gateway.
6. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Configure Mode Config Settings

Mode Config 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 Mode Config 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)

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.

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, *Control How VPN Tunnels Are Opened* on page 45.

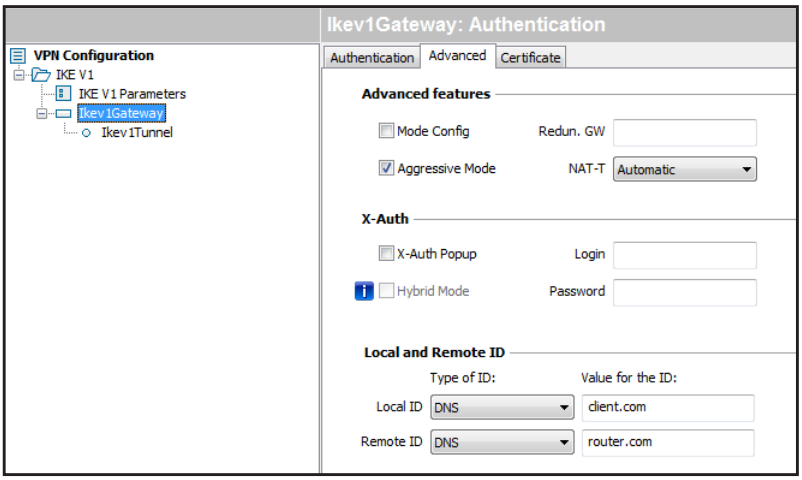
➢ **To set up Mode Config:**

1. On the client computer desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.
2. In the VPN Tunnel Tree pane, right-click the name of the IKE configuration.

   The Authentication page displays.

3. Click the **Advanced** tab.



4. Select the **Mode Config** check box.
5. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Configure Hybrid Mode

Note: Hybrid mode is supported in VPN Client Professional, but not in VPN Client Lite.

Hybrid mode requires you to configure a certificate for the authentication phase 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 security association (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.

The VPN Client implements the RFC draft-ietf-ipsec-isakmp-hybrid-auth-05.txt.

➢ **To configure hybrid mode:**

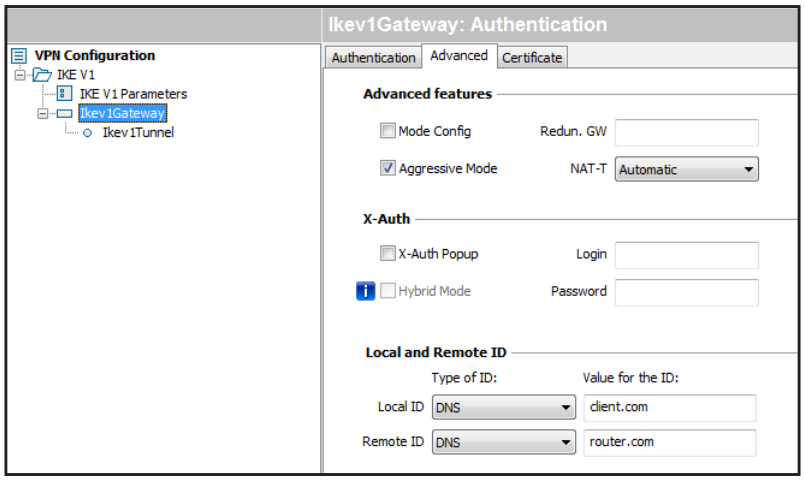
1. On the client computer desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, right-click the name of the IKE configuration.

   The Authentication page displays.

3. Click the **Advanced** tab.



4. Select the **X-Auth Popup** check box.

   For you to configure hybrid mode, you must select this check box.

5. Select the **Hybrid Mode** check box.
6. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Configure IPSec Settings

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

You can create several phase 2 configurations for a single set of phase 1 settings. For information about how to specify scripts, see *Configure Scripts* on page 51.

This example assumes that the client is connecting to a VPN gateway.

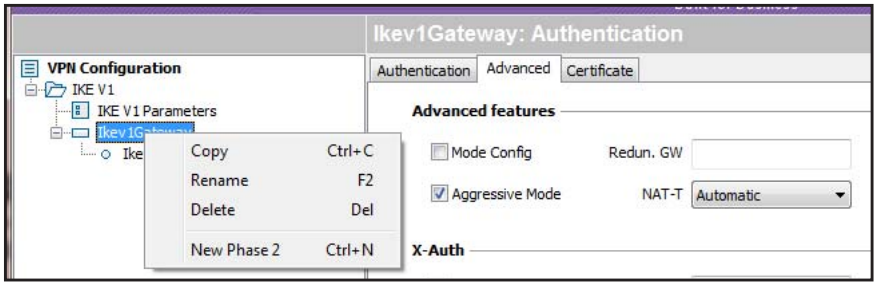
➢ **To create an IPSec configuration:**

1. On the client computer desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, right-click the authentication phase name.

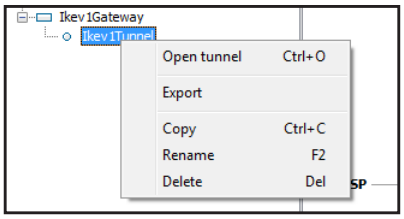
3. Select **New Phase 2**.



The Ikev1Tunnel: IPSec page displays in the Configuration pane on the right.

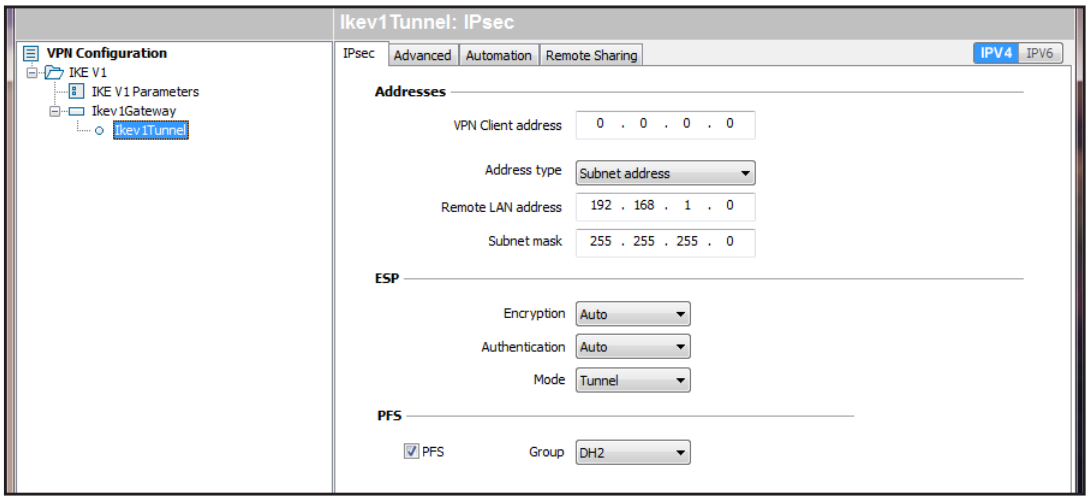
The default name for the tunnel is Ikev1Tunnel. This name is used only for the VPN Client, not during IKE negotiation.This name must be unique.

4. To change the tunnel name, do the following:
   a. In the VPN Tunnel Tree pane, right-click the name.



   b. Select **Rename**.
   c. Type the new name.
   d. Click anywhere in the VPN Tunnel Tree pane.

The tunnel name changes in the VPN Tunnel Tree pane and also in the Configuration pane on the right.



5. In the **VPN Client Address** field, enter the virtual IP address that the VPN Client uses in the VPN router's LAN.

This computer (the client) 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.

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 *Control How VPN Tunnels Are Opened* on page 45). 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 issued an IP address to the VPN Client, the IP address is displayed in the **VPN Client address** field.

6. In the **Address Type** menu, select the remote endpoint's type of address:
   - **Single address**. The remote endpoint is a single computer. Specify the remote host address and the subnet mask.
   - **Subnet address**. The remote endpoint is a LAN. Specify the remote LAN address and the subnet mask.
   - 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. Specify the start and end addresses.

   Depending on your selection, the pane adjusts to display the associated address fields:

   Note: When you select **Range address** and the **Automatically open this tunnel on traffic detection** check box on the Advanced IPSec pane (see *Control How VPN Tunnels Are Opened* on page 45), 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.

7. In the **Remote LAN address** field, enter the remote IP address, or LAN network address, of the VPN gateway.
8. In the **Subnet Mask** field, enter the subnet mask of the gateway.
9. In the **Encryption** menu, select the encryption algorithm.

   For a NETGEAR router, select **3DES**.

10. In the **Authentication** menu, select an authentication method.

    For a NETGEAR router, select **SHA1**.

11. Select the IPSec encapsulation mode:
    - **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.

12. To use Perfect Forward Secrecy (PFS), do the following:
    a. Leave the **PFS** check box selected.
    b. Specify the key length to be used during the IPSec configuration phase.
    c. Select a group.

       The default group is **DH2 (1024)**. NETGEAR routers use Diffie-Hellman Group 2 (1024 bit).

13. Select **Configuration > Save** or press Ctrl + S.

    Your settings are saved.

Configure the Parameter Settings

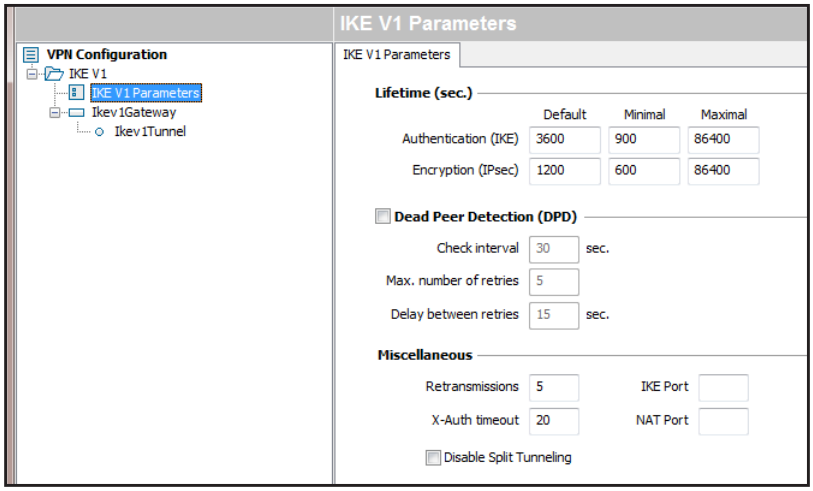
The parameters are generic settings that apply to all VPN tunnels that you create. The default parameters work well for most VPN configurations. You can modify the parameters for your specific network. The following table describes the parameter settings.

➢ **To specify the parameters:**

1. On the client computer desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree, click the parameters name.



3. Specify the lifetime in seconds for authentication and encryption.

   For a typical NETGEAR VPN gateway, 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.

4. Select or clear the **Dead Peer Detection** check box.

   Dead Peer Detection (DPD) is an Internet Key Exchange (IKE) extension (RFC3706) for detecting a dead IKE peer. This check box is selected by default. 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 configured one (see *Control How VPN Tunnels Are Opened* on page 45).

5. To specify the number of retransmissions, enter a value in the **Retransmissions** field.
6. To specify the XAUTH time-out, enter a value in the **X-Auth Timeout** field.
7. To specify the default UDP port that is used in the IKE negotiation during the authentication phase, enter the port in the **IKE Port** field.

   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.

8. To specify the default NAT port that is used during the IPSec negotiation, enter a value in the **NAT Port** field.

   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.

9. Select or clear the **Disable Split Tunnelling** check box.

   Selecting this check box limits traffic to encrypted traffic and forces all traffic to go through the VPN tunnel.

10. Select **Configuration > Save** or press Ctrl + S.

    Your settings are saved.

Open and Close VPN Tunnels

You can open a tunnel only after you specify its VPN configuration.

For information about how to open tunnels automatically, see *Control How VPN Tunnels Are Opened* on page 45.

For information about how to open tunnels using CLI commands, see *Customize the VPN Client Using CLI Commands* on page 101.

➢ **To open the tunnel from the VPN Configuration panel:**

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. Select **Tools > Connection Panel**.

   The Connection Panel lists the tunnel.

3. Double-click the tunnel.

   The tunnel opens.

The following table provides an overview of the methods that you can use to open and close VPN tunnels.

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
VPN Configuration page	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	Double-click the Connection Panel.	Double-click the Connection Panel.
	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. Select the IPSec configuration name (by default, Tunnel).	1. Right-click the system tray icon. 2. Select the IPSec configuration name (by default, Tunnel).

The VPN Configuration page and Connection Panel 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 closing of the tunnel.

Advanced Settings

5

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

- *Control How VPN Tunnels Are Opened*
- *Configure Alternate DNS and WINS Servers*
- *Configure Scripts*
- *Configure Remote Sharing*
- *USB Mode*
- *Manage Certificates*
- *Manage VPN Configuration Files*
- *Access Control Overview*
- *Hide User Interface Features*
- *Configure VPN Client Startup Mode and Network Interface Detection*
- *Change the Language*
- *Edit a Software Language*

Control 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.

Open a Tunnel Automatically

You can configure a tunnel to open automatically.

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

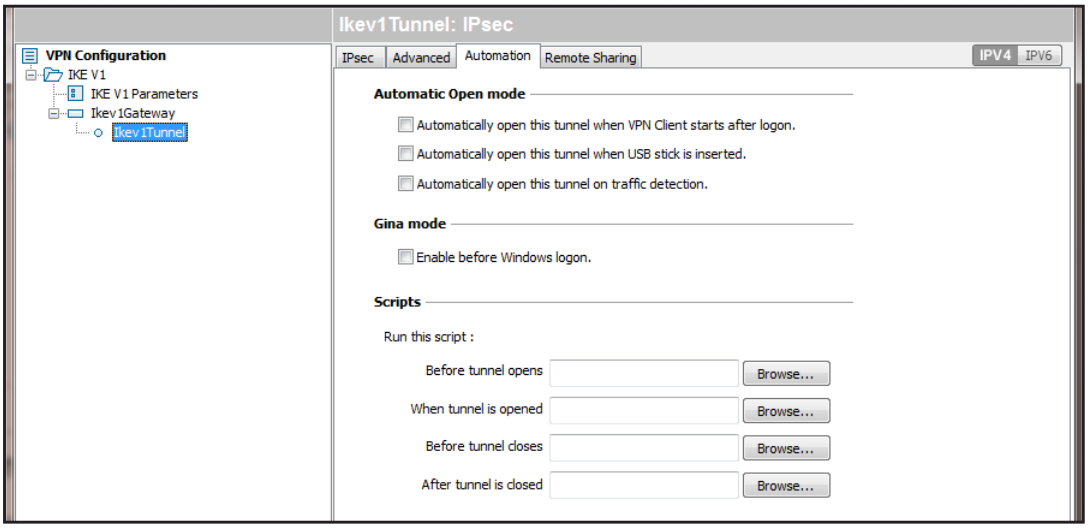
1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.

3. In the IPSec pane, click the **Automation** tab.



Note: When you select an Automatic Open mode check box, the VPN Client automatically opens the tunnel to which these advanced settings apply.

4. Select one of the following check boxes:
   - **Automatically open this tunnel when the VPN Client starts after login**. For more information, see *Open a Tunnel by Double-Clicking on a Desktop Icon* on page 47.
   - **Automatically open this tunnel when USB stick is inserted**. For more information, see *USB Mode* on page 53).

- **Automatically open this tunnel on traffic detection**. Open the tunnel when the VPN Client detects traffic.

5. Select or clear the **Enable before Windows logon** check box.

   Selecting this check box enables Windows credential providers for Windows Vista or Windows 7.

   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 must connect to the corporate network before processing the Windows logon.

   For more information, see *Open a Tunnel Before Windows Logon* on page 46.

   Note: When the credential providers feature is enabled, the Scripts pane is disabled.

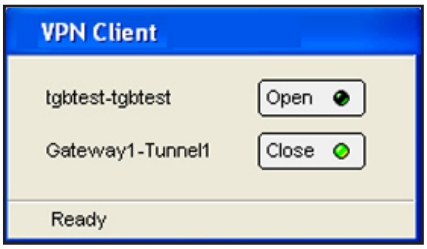
6. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Open a Tunnel 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.

Before Windows logon, the following pop-up window opens to allow you to open the required VPN tunnel.



The pop-up window lists all VPN tunnels for which you selected the **Enable before Windows logon** check box on the Advanced IPSec pane.

The following information applies to these tunnels:

- You cannot hide the pop-up window that opens before Windows logon.
- If two tunnels are 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.
- If you configured scripts, they are disabled.
- The VPN Client cannot function in USB mode (see *USB Mode* on page 53).
- The Mode Config feature is disabled, so you might need to specify DNS or WINS server addresses (see *Control How VPN Tunnels Are Opened* on page 45).

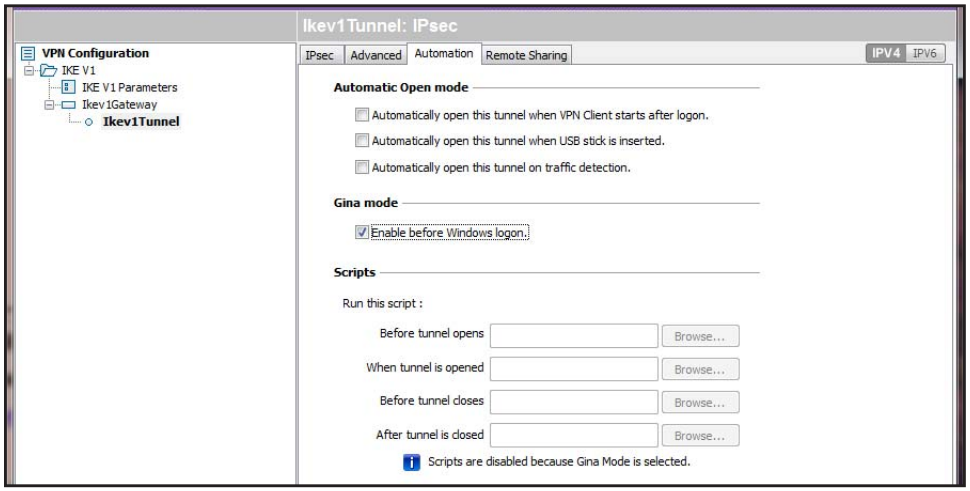
- When extended authentication (XAUTH) is enabled, a pop-up window opens when tunnels open and you are prompted to enter the login name and password.
- When you use a USB token or smart card, a pop-up window opens when tunnels open to enable you to enter the PIN code.

➢ **To configure the VPN tunnel to open before Windows logon:**

1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.
2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.
3. In the IPSec pane, click the **Automation** tab.



4. Select the **Enable before Windows logon** check box.

   You are notified that scripts are disabled.
5. Select or clear the **Automatically open this tunnel on traffic detection** check box.

   If you clear this check box, you must manually open the tunnel.

Open a Tunnel by Double-Clicking on a Desktop Icon

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

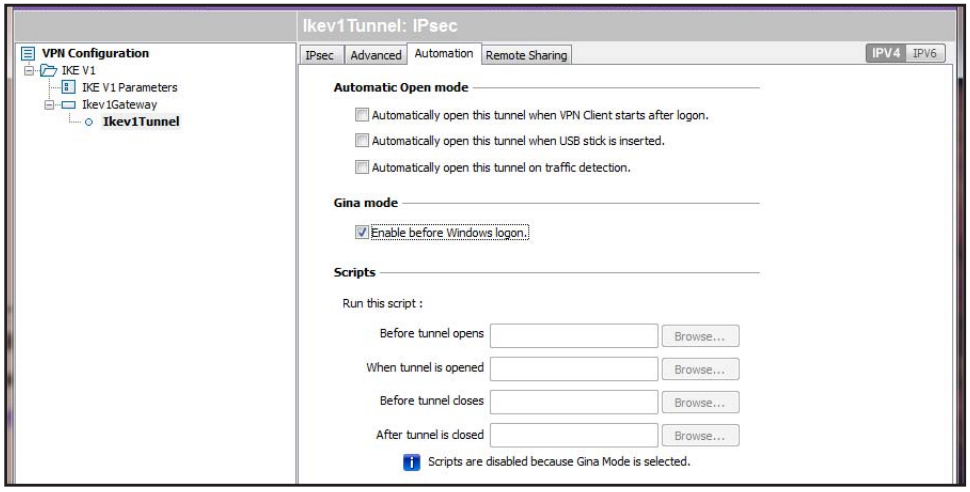
➢ **To configure a tunnel to open when a desktop icon is double-clicked:**

1. On your desktop, double-click the VPN Client shortcut .

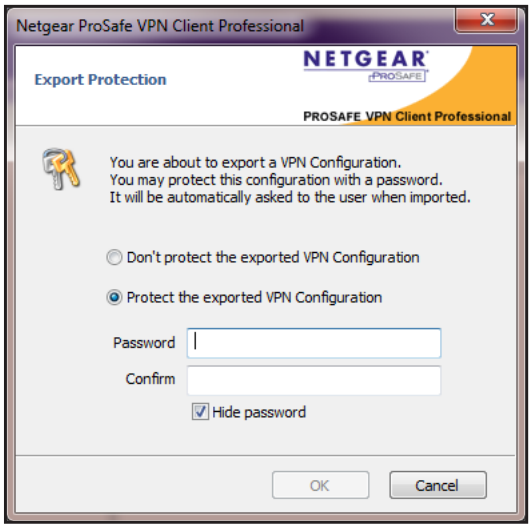
   The VPN Configuration page displays.
2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.

3. In the IPSec pane, click the **Automation** tab.



4. Select the **Automatically open this tunnel when the VPN Client starts after login** check box.
5. Select **Configuration > Export**.



6. Select a radio button:
   - **Don’t protect the exported VPN Configuration**. No password is required.
   - **Protect the exported VPN Configuration**. The VPN configuration file requires a password before it can be opened, do the following:
     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.
7. Click the **OK** button.
8. Navigate to the location to save the VPN configuration file.
9. Type a name for the VPN configuration file.

An exported VPN configuration file name ends with a `.tgb` extension. Do not change this extension.

The VPN configuration is exported.

10. Place a shortcut of the VPN configuration file on the desktop.

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

Automatically Open a Web Page When a VPN Tunnel Opens

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

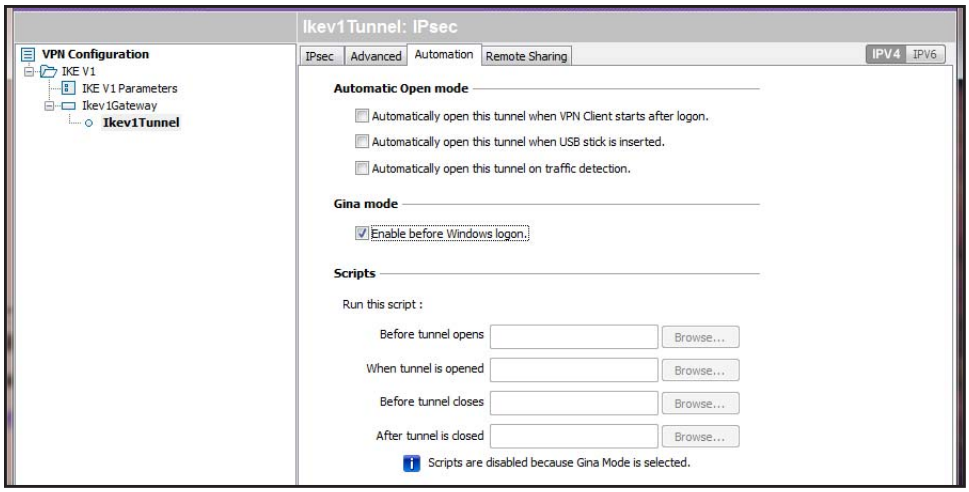
1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.

3. In the IPSec pane, click the **Automation** tab.



4. In the **When tunnel is opened** field, enter the URL of the web page that you want to open.

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

5. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

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

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 settings 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 Settings* on page 30), the Alternate server fields are disabled.

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

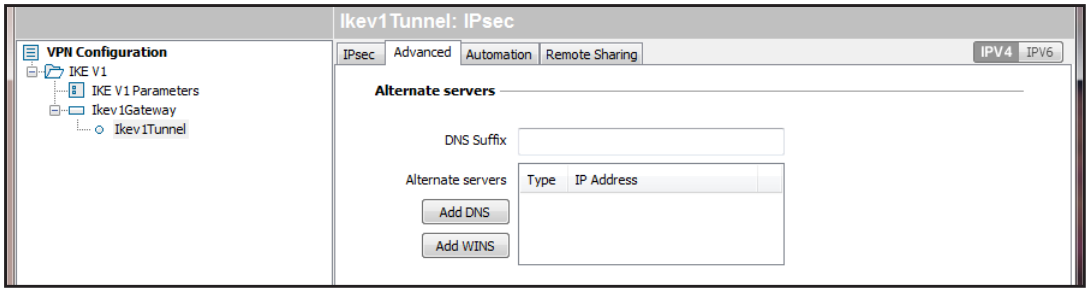
1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.

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



4. Click the **IPv4** or **IPv6** button, based on the VPN gateway's Internet connection.
5. To add a server, do the following:
   a. Click the **Add DNS** button.
   b. When prompted, enter the IP address for the server of the remote LAN.

      The DNS server is used to resolve intranet addressing while the tunnel is open.
6. To add a WINS server, do the following:
   a. Click the **Add WINS** button.
   b. When prompted, enter the IP address for the WINS server of the remote LAN.

      The WINS server is used to resolve intranet addressing while the tunnel is open.
7. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Configure Scripts

Note: Scripts are supported in VPN Client Professional, but not in VPN Client Lite.

You can 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:**

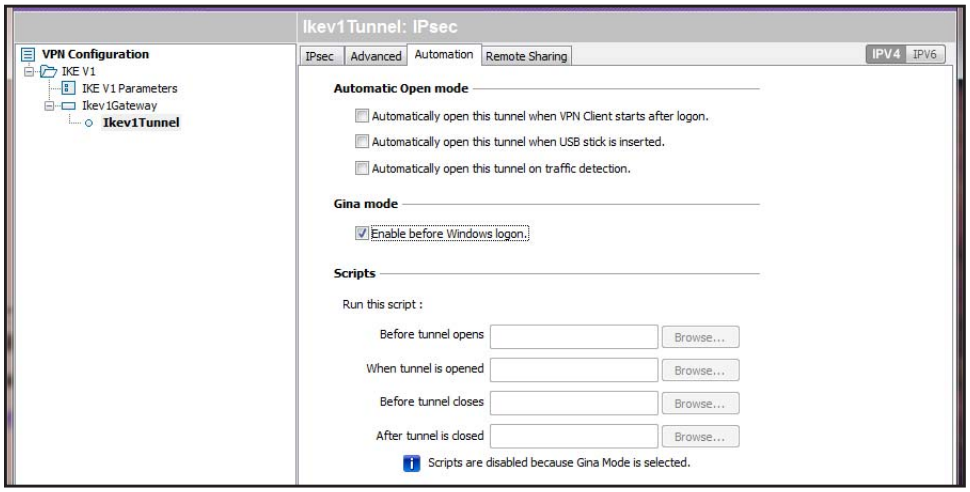
1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.

3. In the IPSec pane, click the **Automation** tab.



4. In the Scripts section, click the **Browse** button to navigate to a script file and open it.

You can implement scripts to run in up to four circumstances. Select scripts from each of the following lists:

- Before tunnel opens.
- When tunnel is opened.
- Before tunnel closes.
- After tunnel is closed.

5. Select **Configuration > Save** or press Ctrl + S.

   Your settings are saved.

Configure Remote Sharing

You can specify remote computers that you can connect to for desktop sharing after the VPN tunnel is established.

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

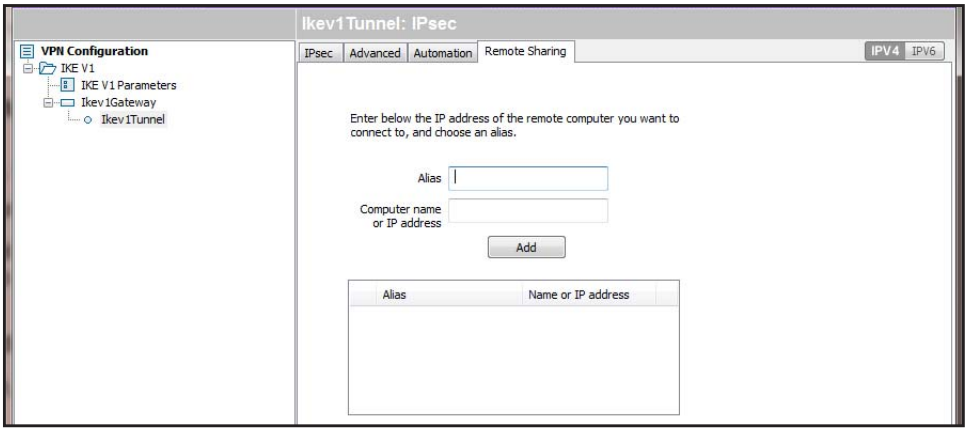
1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.

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



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

   This IP address must be an address in the subnet or IP range of the remote LAN.

6. Click the **Add** button.

   The computer is added.

After you define 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.

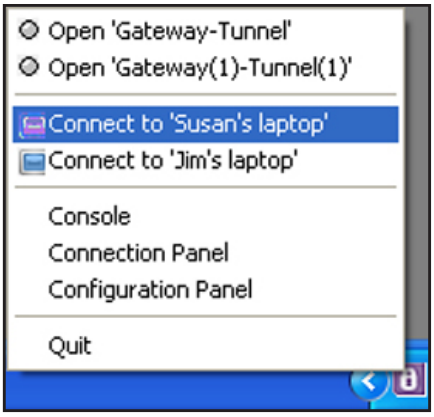


Figure 5. Remote computer option in the system tray menu

USB Mode

Note: USB mode is supported in VPN Client Professional, but not in VPN Client Lite.

You can 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 move a VPN configuration and its security elements onto a USB drive and remove the USB drive, insert the USB drive into a computer to automatically open the tunnels. When you remove the USB drive from the computer, all open tunnels are automatically closed.

Enable a New USB Drive with a VPN Configuration

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

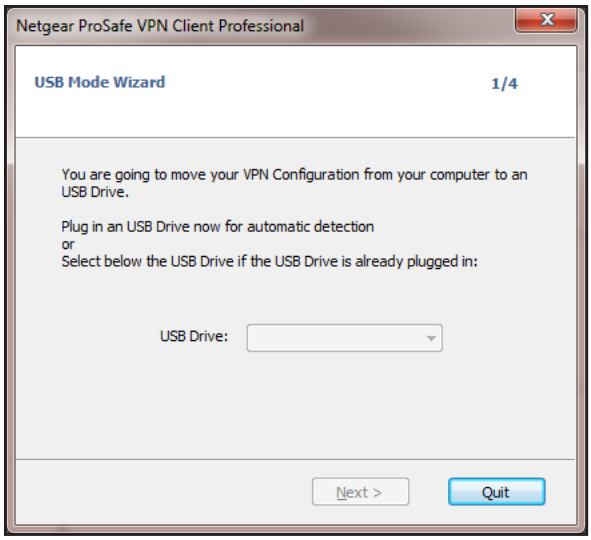
- Export the configuration and copy the VPN configuration file onto the USB drive. (See *Export a VPN Configuration* on page 67.)
- Use the USB Mode Wizard.

➢ **To use the USB Mode Wizard and copy VPN configuration onto a USB drive:**

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. Select **Configuration > Move to USB Drive**.



If one or more USB drives are already inserted, the VPN Client detects and displays them.

Note: If you insert a USB drive with a VPN configuration while the USB Mode Wizard 1/4 page 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 page, USB Mode Wizard 2/4.

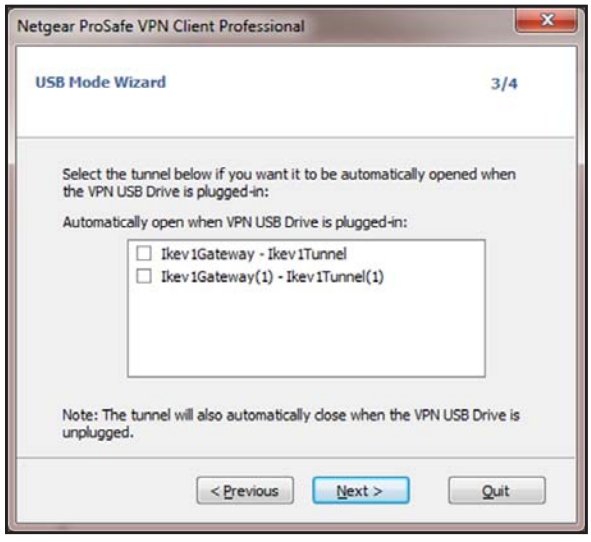
Note: If you insert a USB drive with a VPN configuration while another USB drive with another VPN configuration is already inserted, a warning message asks you to remove one of the USB drives.

3. Click the **Next** button.

4. Select a security option:
   - **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.
5. (Optional) Protect the VPN configuration with a password by entering one in the **Password** field.
6. (Optional) Select the **Hide password** check box to make the password characters invisible.

   Note: If you remove the USB drive, the wizard automatically returns to the USB Mode Wizard 1/4 page.

7. Click the **Next** button.



8. Select the tunnel or tunnels to open automatically.

   Tip: If only one tunnel is configured, select the **Automatically open this tunnel when USB stick is inserted** check box on the Advanced IPSec page (see *Control How VPN Tunnels Are Opened* on page 45).

9. Click the **Next** button.

   The USB Mode Wizard 4/4 page displays. This page is a summary.

10. Click the **OK** button.

    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.

When you remove the USB drive from the computer, the VPN configuration is reset, that is, an empty configuration displays in the Configuration Panel. The next time that the VPN Client starts when the USB drive that contains the VPN configuration is not inserted, the VPN configuration is not present in the VPN Client.

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 66.

Configure Tunnels to Open Automatically with a USB Drive

After you 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:**

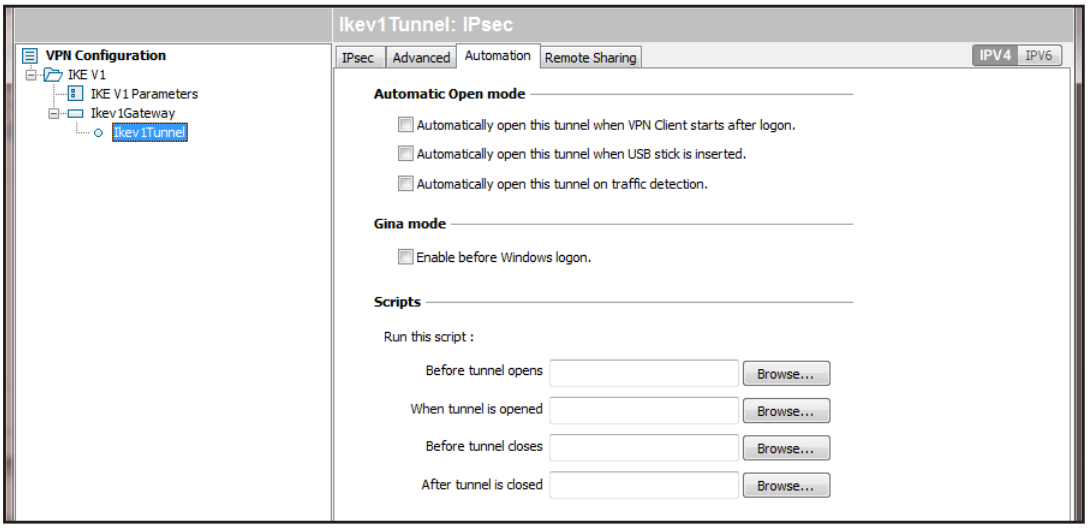
1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The IPSec pane displays.

3. In the IPSec pane, click the **Automation** tab.



4. Select the **Automatically open this tunnel when USB stick is inserted** check box.

   Note: If more than one tunnel is configured, make sure that, on the USB Mode Wizard 3/4 page, you selected which tunnel or tunnels to open. For more information, see *Enable a New USB Drive with a VPN Configuration* on page 53.

5. (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.

Manage Certificates

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.

Import a PEM Certificate

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 import 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 Settings* on page 30.

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

1. On your desktop, double-click the VPN Client shortcut  .

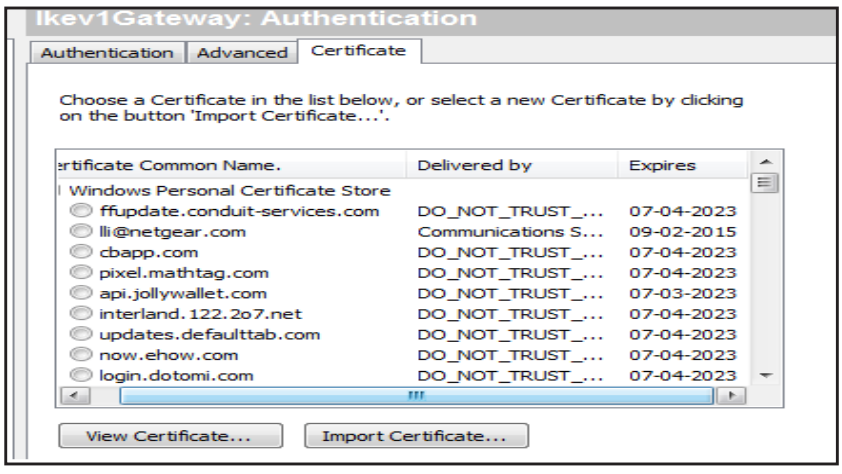
   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

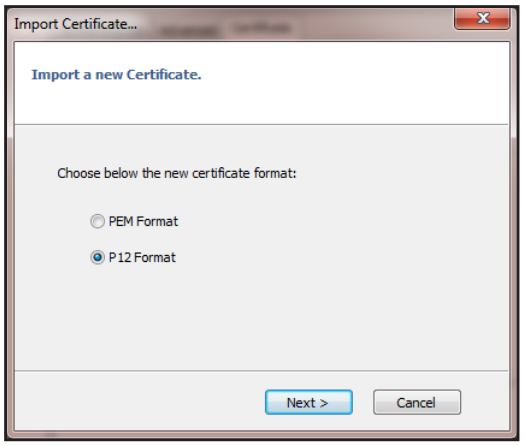
   The Authentication page displays.

3. Select the **Certificates** radio button.

   For you to import certificates, you must select this radio button on the Authentication page.



4. Click the **Import Certificate** button



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

   You are prompted to locate the root certificate, user certificate, and user private key files.

7. To complete the **Root Certificate** field, click the **Browse** button, and locate the root certificate file to import.

   This file name ends with either a `.pem` or a `.crt` extension.

8. To complete the **User Certificate** field, click the **Browse** button, and locate the user certificate file to import.

   This file name ends with either a `.pem` or a `.crt` extension.

9. To complete the **User Private Key** field, click the **Browse** button, and locate the user private key file to import.

   This file name ends with a `.key` extension.

   Note: A PEM certificate file that includes a user private key cannot be encrypted or protected with a password.

10. Click the **OK** button.

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

11. Select **Configuration > Save** or press Ctrl + S.

    Your settings are saved.

Import a P12 Certificate

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 import 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 Settings* on page 30.

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

1. On your desktop, double-click the VPN Client shortcut  .

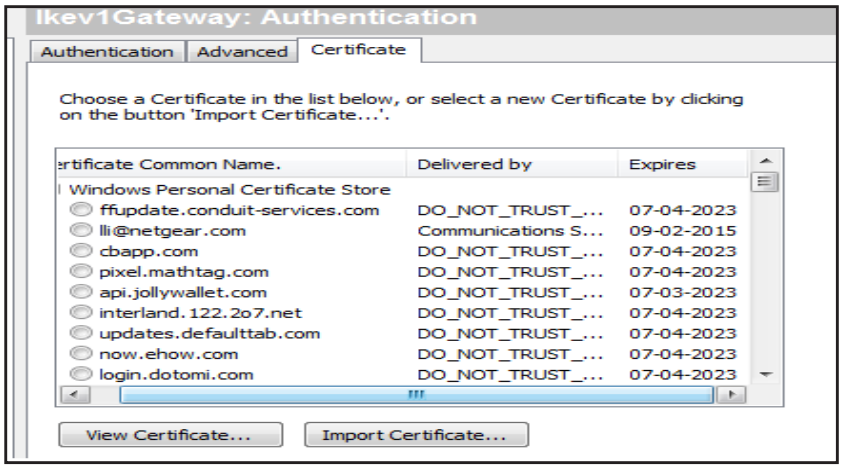
   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

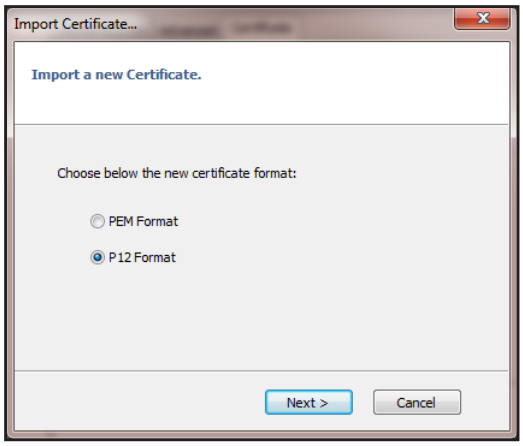
   The Authentication page displays.

3. Select the **Certificates** radio button.

   For you to import certificates, you must select this radio button on the Authentication page.



4. Click the **Import Certificate** button



5. Leave the **P12 Format** radio button selected.
6. Click the **Next** button.
7. When prompted, click the **Browse** button, locate, and open the certificate file to import.

   This file NAME can end with either a `.p12` or a `.pfx` extension.
8. Click the **OK** button.
9. When prompted, enter the PKS12 file password and click the **OK** button.

   The certificate is imported, and the Certificate pane displays the certificate.
10. Select **Configuration > Save** or press Ctrl + S.

    Your settings are saved.

View and Assign Certificates

You can view and assign certificates that you imported in the VPN Client. Certificate sources are described in the following table.

Table 5. Certificate sources

Source	Description
NETGEAR configuration file	Certificates are located in the VPN configuration file that the VPN Client uses. These certificates were imported previously from another source such as a certificate file or the Microsoft Certificate Store.

Table 5. Certificate sources

Source	Description
Windows Personal Certificate Store	Certificates are located in the Personal Certificate Store. To be visible and usable, certificates must be certified and in the correct location: • Certificates must be certified by a certificate authority (CA), and the certificate status must be OK (see also *Troubleshoot Certificates* on page 65). • Certificates must be located in the Personal Certificate Store to represent the personal identity of the user attempting to connect to a corporate network.
USB token or 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 must 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.

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

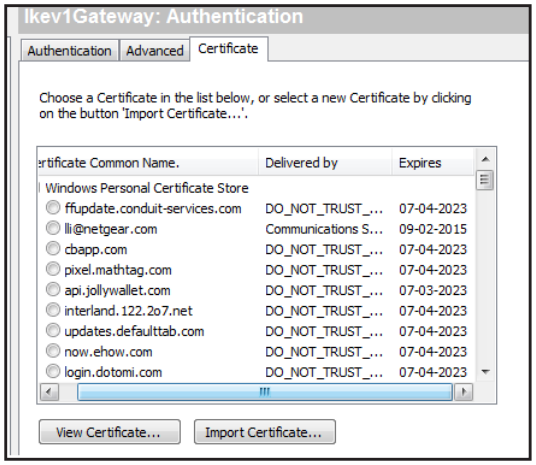
1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The Authentication page displays.

3. Click the **Certificates** tab.



The previous figure shows several sources from which you can select certificates. To select a certificate from the list, select its associated radio button. You can select and assign only one certificate to a tunnel.

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. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

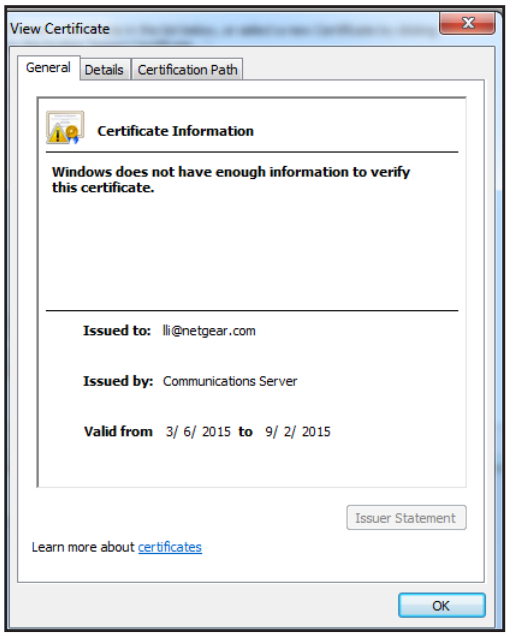
   The Authentication page displays.

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

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

6. 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.



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

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

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

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

9. Click the **OK** button.

   The View Certificate page 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:**

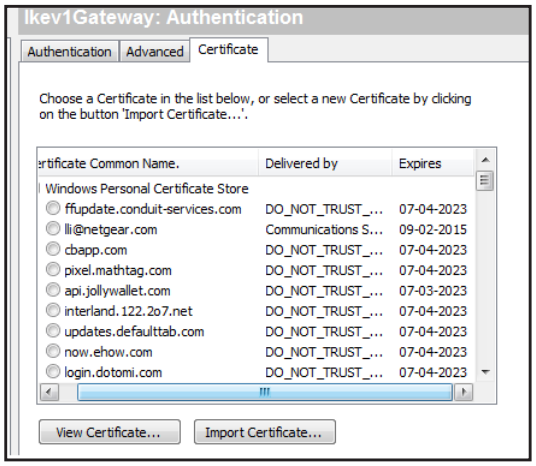
1. Insert a USB token or smart card into the computer.
2. If requested as part of USB token or smart card reader identification process, enter the PIN code.

   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 with an incorrect PIN code.

3. Click the **OK** button.
4. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.
5. In the VPN Tunnel Tree pane, click the IPSec configuration name of the tunnel.

   The Authentication page displays.
6. Click the **Certificates** tab.



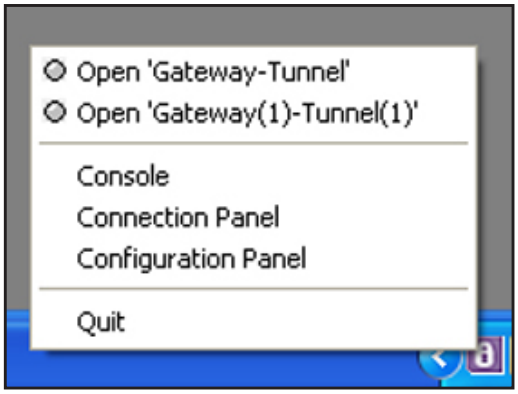
   The certificates from the USB token or smart card are automatically imported and display in the certificates list.
7. Select a certificate by selecting its radio button.

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

When you configure a tunnel to use a certificate from a USB token or smart card, you must enter the PIN code that is associated with the USB token or smart card each time 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

The following sections provide information about troubleshooting USB tokens, smart cards, and the Personal Certificate Store.

Troubleshoot USB Tokens and Smart Cards

When an error occurs while you are using 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 window that provides more information about the error. One of the following errors might occur:

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

  Resolution. Reinsert the USB token or 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.

Troubleshoot the Personal Certificate Store

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

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

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

Manage VPN Configuration Files

A VPN configuration is a file that contains the configuration and tunnel information of the VPN Client. You can 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.

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 102.

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.

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. On your desktop, double-click the VPN Client shortcut  .

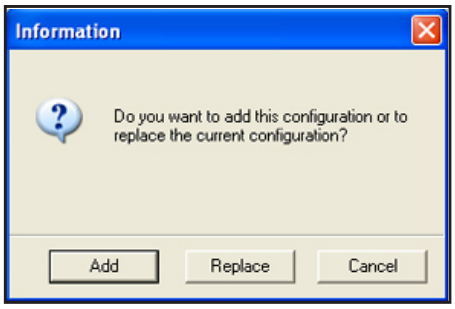
   The VPN Configuration page displays.

2. Select **Configuration > Import**.

   A file selection window opens.

3. Navigate to the location of the VPN configuration file to import.
4. Click the **Open** button.

5. If you are prompted to enter a password, type the password and click the **OK** button.



6. To add the imported VPN configuration to the existing VPN configuration, click the **Add** button.
7. To replace the existing VPN configuration with the imported VPN configuration, click the **Replace** button.

   The imported VPN configuration displays in the VPN Tunnel Tree.

Export a VPN Configuration

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

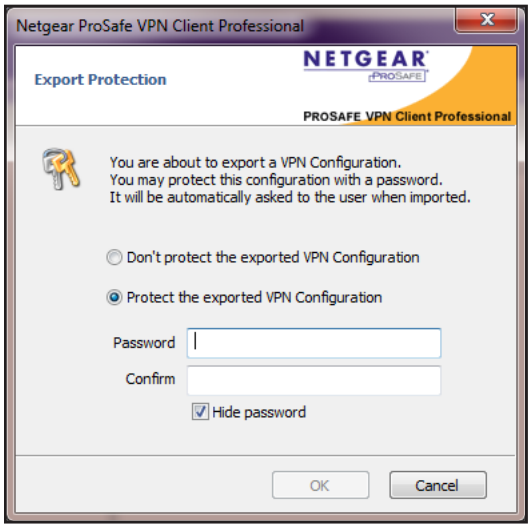
You can split and export a single tunnel configuration from an existing VPN configuration. A network administrator typically uses this capability to split a large VPN configuration into a smaller VPN configuration and deliver it to end users.

➢ **To export a VPN configuration:**

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. Select **Configuration > Export**.



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

3. Select a radio button:
   - **Don’t protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. The VPN configuration file requires a password before it can be opened, do the following:
     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 the **OK** button.
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 name ends with a `.tgb` extension. Do not change this extension.
7. Click the **Save** button.

   The VPN configuration file is saved. A shortcut displays on the desktop.

You can 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.

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. You can use several methods 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, VPN 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, VPN 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. On your desktop, double-click the VPN Client shortcut  .

The VPN Configuration page displays.

2. Do one of the following:
   - Select **Configuration > Import**.
   - Drag and drop a new VPN configuration onto the VPN Tunnel Tree pane.
3. Navigate to the location of the VPN configuration file to import.
4. Click the **Open** button.

   An Information screens displays.
5. Click the **Add** button.

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

Access Control Overview

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

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

When access control is enabled, the password prompt displays 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 to the Configuration Panel.
- When you import a configuration file.
- When you start a software upgrade.

When access control is enabled, you cannot open the Configuration Panel 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.

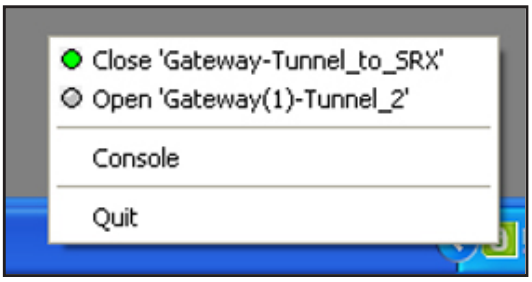


Figure 6. System tray menu with access control enabled

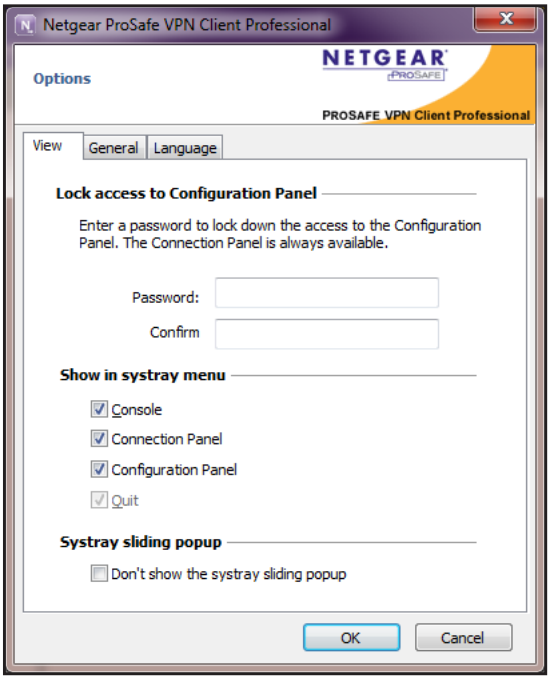
Configure Access Control

➢ **To configure access control:**

1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. Select **Tools > Options**.



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

Note: You can also configure this password as an option of the software setup (see *Require a Password to Access the Configuration Panel* on page 88).

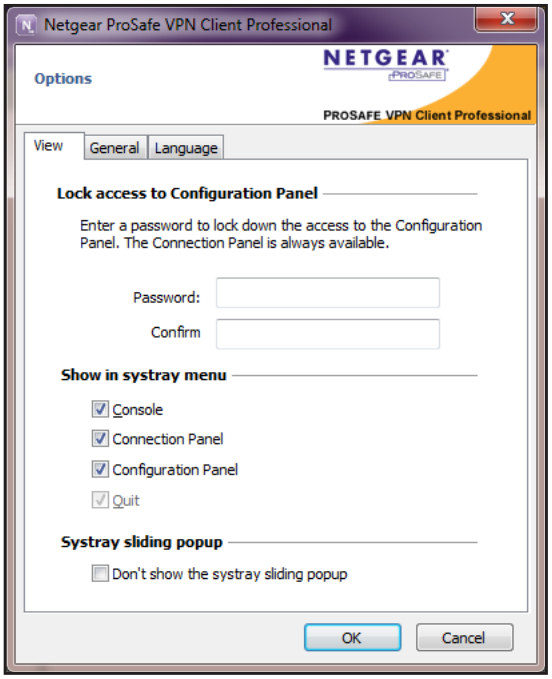
Remove Access Control

➢ **To remove access control:**

1. On your desktop, double-click the VPN Client shortcut .

   The VPN Configuration page displays.

2. Select **Tools > Options**.



3. Clear the **Password** and **Confirm** fields.
4. Click the **OK** button.

Hide User Interface Features

You can control which VPN Client features are available for users who use VPN clients on their computers to connect to remote gateways or peers. For example, you can hide some VPN Client features to prevent nontechnical users from accidentally changing settings that might interfere with the performance of VPN tunnels.

Hide Links on the System Tray Menu

After you launch the VPN Client, the VPN Client displays an **i** icon in the system tray that indicates whether a tunnel is open or closed.

Green icon:
at least one VPN tunnel opened.

Purple icon:
no VPN tunnel opened.

Figure 7. VPN Client icon colors in the system tray

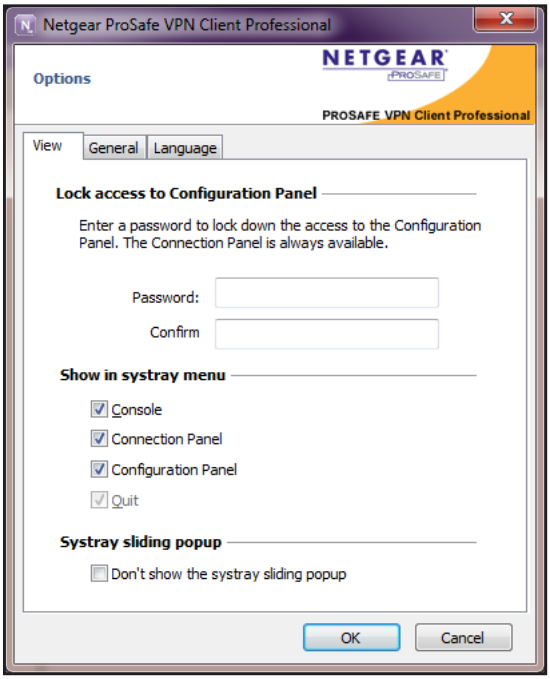
When you click the icon, the system tray menu opens.

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

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. Select **Tools > Options**.



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

Note: The **Quit** check box is disabled. You cannot disable the **Quit** menu item 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 89.

4. Click the **OK** button.

   Your settings are saved.

Disable the Systray Pop-Up Screens

When a VPN tunnel opens or closes, by default, a small window pops up from the system tray icon.

Figure 8. Tunnel opened pop-up window

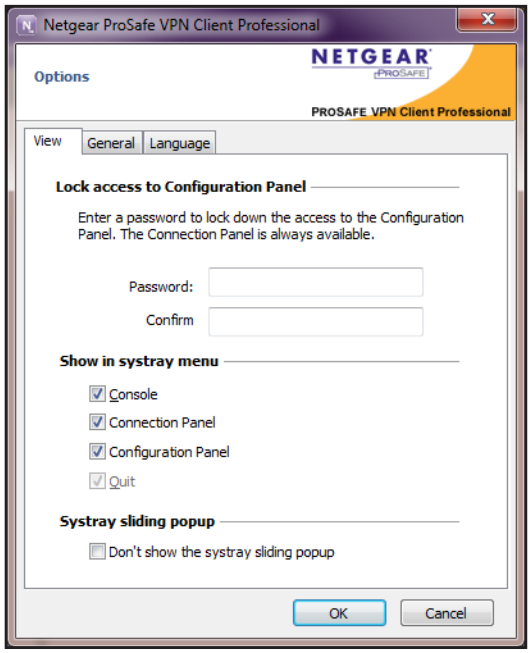
If the VPN tunnel cannot open, the window might display an error or warning with a link to more information.

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

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. Select **Tools > Options**.



3. In the systray sliding pop-up section, select the **Don't show the systray sliding popup** check box.
4. Click the **OK** button.

   Your settings are saved.

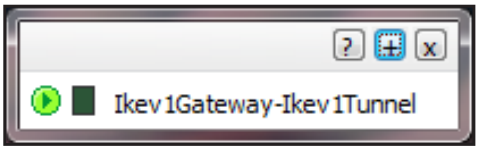
Hide the Connection Panel

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

➢ **To open the Connection Panel:**

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.
2. Select **Tools > Connection Panel**.



Configure VPN Client Startup Mode and Network Interface Detection

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

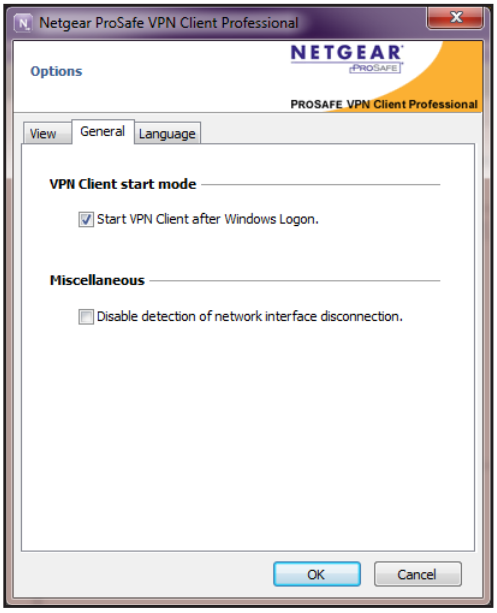
You can specify if the VPN Client starts automatically after you log in to Windows and whether the VPN Client detects disconnection of the network interface.

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

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.

2. Select **Tools > Options > General**.



3. Select or clear the **Start VPN Client after Windows Logon** check box.

   If you clear this check box, to use VPN Client, you must 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 log 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 87).

4. Select or clear the **Disable detection of network interface disconnection** check box.

   By default, the check box is cleared to allow 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 the **OK** button.

   Your settings are saved.

Change the Language

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

You can change the VPN Client language without restarting the VPN Client.

➢ **To change the language:**

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.
2. Select **Tools > Options > Language**.

   The Language page displays.
3. Select a language.
4. Click the **OK** button.

   The VPN Client display changes to the selected language.

Edit a Software Language

If you edit a language, 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.

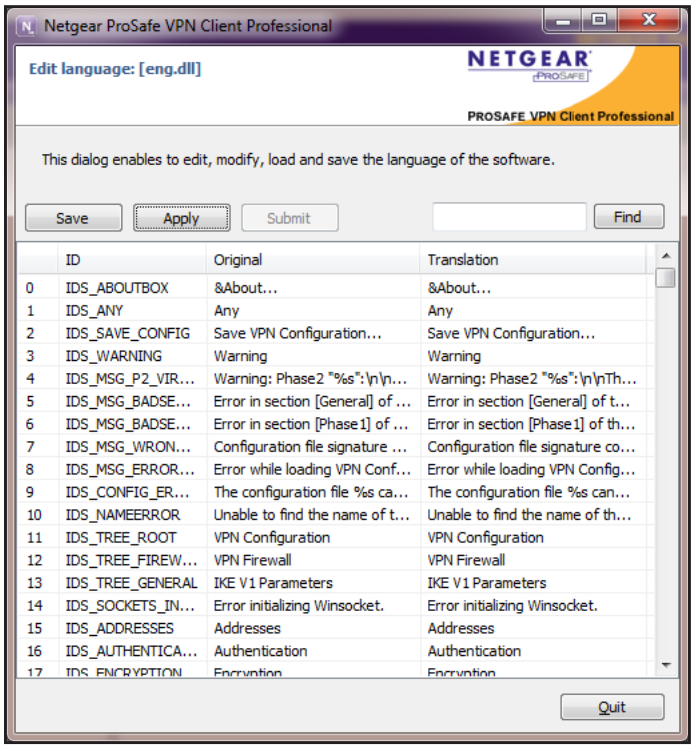
➢ **To edit the software language translation:**

1. On your desktop, double-click the VPN Client shortcut  .

   The VPN Configuration page displays.
2. Select **Tools > Options > Language**.

   The Language page displays.

3. Click the **Edit language** link.



4. Select the row to change.

   The pop-up window that displays depends on your selection.

5. Enter your alternate translation in the pop-up window.
6. Click the **OK** button.
7. Click the **Save** button.

   Your settings are saved.

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:

- *Software Setup and Deployment Concepts*
- *Software Setup Command Reference*
- *Customize VPN Client Display and Access for End Users*
- *VPN Client Silent Software Setup Deployment to End Users*
- *Deliver a VPN Configuration to an End User*
- *Command-Line Interface Command Reference*
- *Customize the VPN Client Using CLI Commands*
- *Customize How the VPN Client Handles Readers and Certificates*

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 the file 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**. Enables users to insert the VPN Client installation CD to let the installation run automatically (AutoPlay).
- **USB storage device**. Enables you to carry the installation package with you, insert the USB device 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 90.

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 window.
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 the Enter key.
5. Close the command window.

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

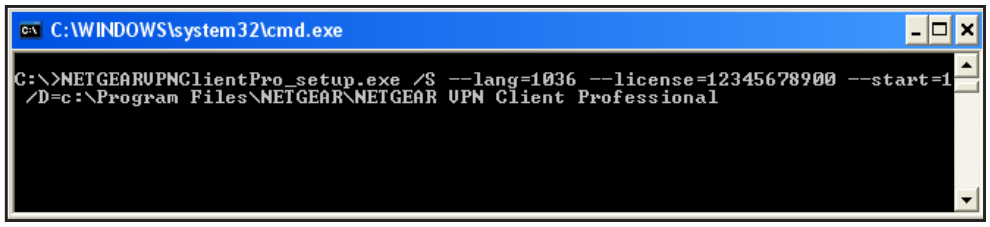


Figure 9. Example of the syntax for a software setup

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 no version is installed, the uninstallation is ignored. The **/S** switch must be preceded by only one slash and is case-sensitive.
- Include the **/D=[install path]** switch to specify the 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 the path includes a space. The **/D** switch must be used with the **/S** option, must be preceded by only one slash, is case-sensitive, and must 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 the installation path **[install path]** includes spaces, 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 must enter a password to access the user interface

The following are some options that you can specify to be automatically configured after the VPN Client is 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 must 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 6. 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` must be preceded by only one slash and is case-sensitive. Quotation marks are not allowed, even if the path includes a space. **Note:** `/D` must be placed at the end of the command line, as the last option, and you must 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** must 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`** must be preceded by two hyphens (**`--`**). **Example**: NETGEARVPNClientPro_Setup.exe /S --activmail= salesgroup@company.com

Table 6. 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 were entered in a previous installation.
--autoactiv=1 must be the last command in the command line.
Note: autoactiv=1 must 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 displays. This is the default setting.
• user. The Connection Panel displays.
• hidden. Neither the Configuration Panel nor the Connection Panel display. Only the system tray menu can be opened. Tunnels can be opened from the system tray menu.
Note: guidefs must 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 must 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 6. 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`** must be preceded by two hyphens (**`--`**). **Example**: `NETGEARVPNClientPro_Setup.exe /S --license= 1234567890ABCDEF12345678`		

Table 6. 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** must be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --menuitem=3
--noactiv=1	Prevents the Trial page 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 page but the **Evaluate** button is disabled. **Note:** **noactiv=1** must be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --noactiv=1
--password=[password]	Protects the user interface or a protected page of the user interface. **[password]** is the password that the end user must 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 to the Configuration Panel. **Note:** **password** must be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --password=adm253q

Table 6. Software setup switches and commands in alphabetical order (continued)

Switch or Command	Description
`--pkicheck=1`	Forces the VPN Client to check the root certificate 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` must 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` must 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 several tokens and smart cards are present. **Note:** `smartcardroaming` must 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.
`--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 must be started manually. **Note:** `start` must 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. This page is typically used by network administrators and can be hidden or protected by a password.
- By opening the Connection Panel. This page lets the end user open and close tunnels. You can hide this page.
- 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 81.

The following sections provide configuration examples:

Display the Configuration Panel After Startup

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

By default, the VPN Client is configured to display the Configuration Panel 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 After Startup

To configure theVPN Client to display the Connection Panel 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 and the Connection Panel, 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 an example of the system tray menu after deployment of a configuration that includes the **`--guidefs=hidden`** software setup command.

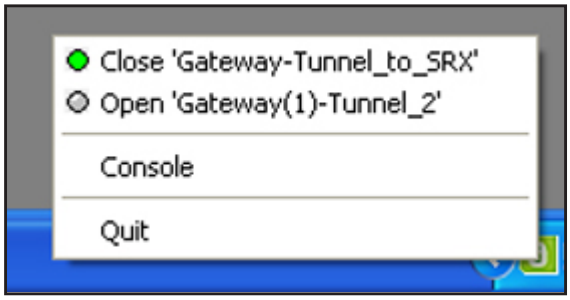


Figure 10. System tray menu with hidden items

Require a Password to Access the Configuration Panel

To require the end user to enter a password to access the Configuration Panel, 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, while access to the Configuration Panel 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 to the Configuration Panel.
- When the user starts a software upgrade.

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

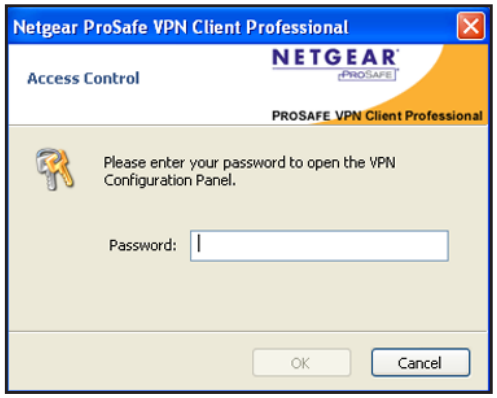


Figure 11. Access Control page

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 and Configuration Panel 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 81.

The following sections provide configuration examples:

- *Create a Silent VPN Client Software Setup* on page 91
- *Deploy a VPN Client Software Setup from a CD* on page 91
- *Deploy a VPN Client Software Setup from a Shortcut* on page 92
- *Deploy a VPN Client Software Setup Using a Batch Script* on page 93

- *Deploy a VPN Client Software Setup from a Network Drive* on page 94

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 window.
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 window.

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:

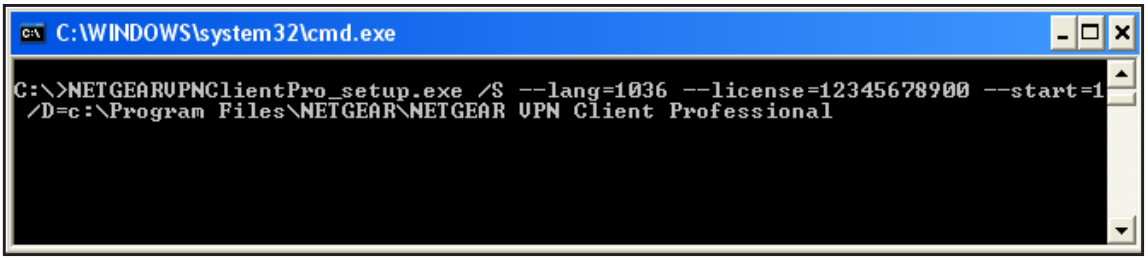


Figure 12. Example of the syntax for a software setup

Deploy a VPN Client Software Setup from a CD

➢ **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 91.

2. Create an autorun file:
   a. Create a text file.
   b. Save the file as `autorun.inf`.

   When the CD is inserted, 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.

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

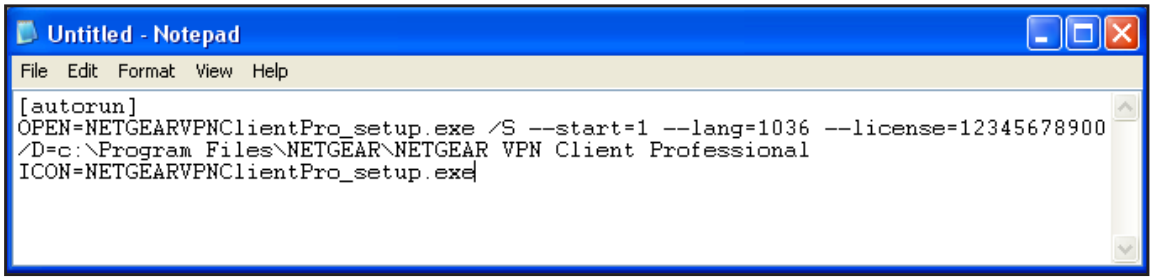


Figure 13. Example of the syntax for a software setup for CD-ROM deployment

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 91.
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:

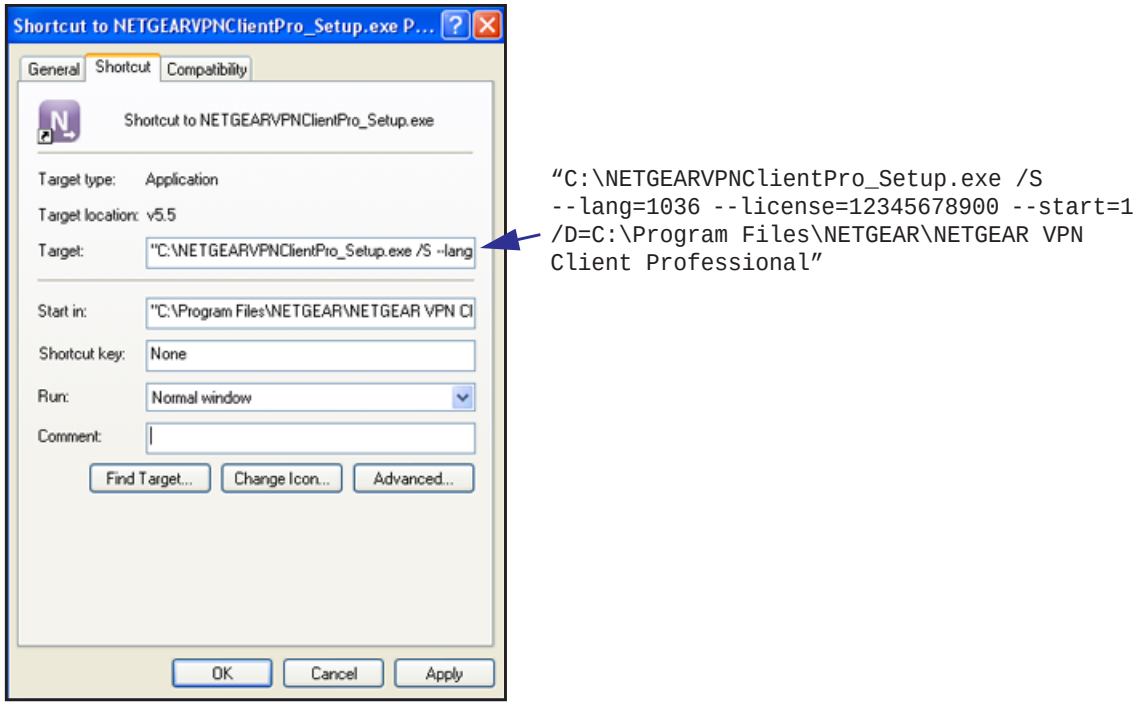


Figure 14. Example of the syntax for a software setup from a shortcut

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 91.

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 /importonce: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 **importonce** command, see *Command-Line Interface Command Reference* on page 98.)
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 91.
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:

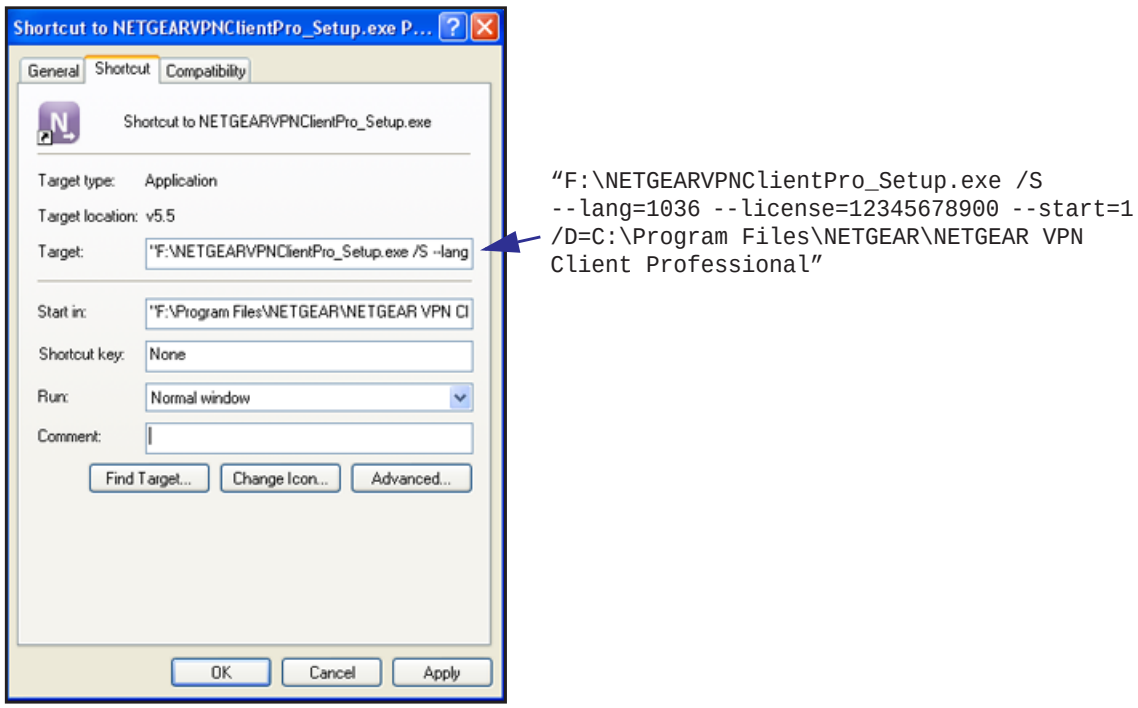


Figure 15. Example of the syntax for a software setup from a shortcut on a network drive

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.

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.

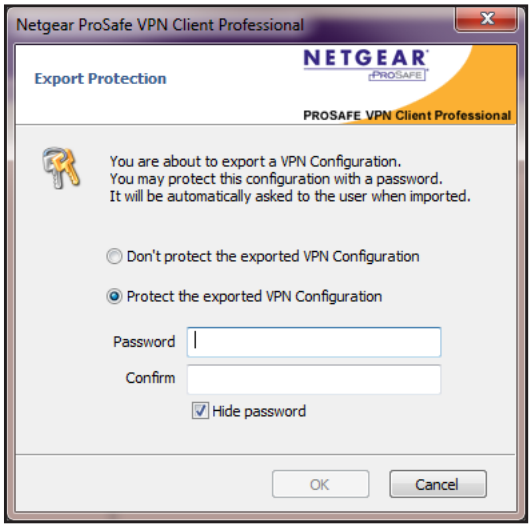
     For information about how to create a silent software setup, see *Create a Silent VPN Client Software Setup* on page 91.
   - Unzip the NETGEAR VPN Client Professional software setup file (`NETGEARVPNClientPro_Setup.exe`).
2. Create a VPN configuration.

   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, Configure VPN Tunnels*.
3. Export the VPN configuration:

   a. On your desktop, double-click the **VPN Client** shortcut  .

   The VPN Configuration page displays.

   b. Select **Configuration > Export**.



   c. Select the **Don’t protect the exported VPN Configuration** radio button.

   d. Click the **OK** button.
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 name ends with a .tgb extension. Do not change this extension.
6. Click the **Save** button.

Your settings are saved.

7. Add the VPN configuration (that is, the `conf.tgb` file) to the directory in which you 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.

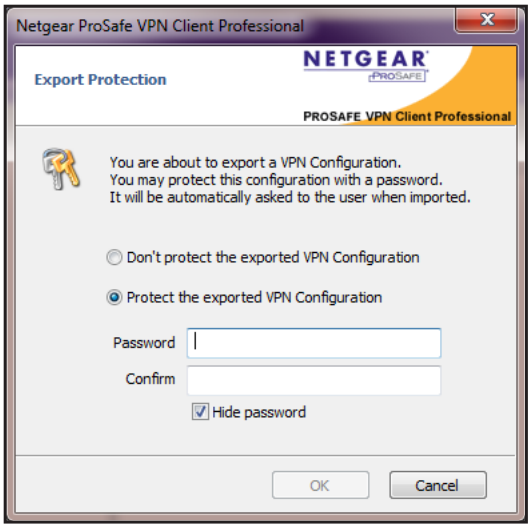
   You can do this on any computer on which the VPN Client is installed. For information about how to create a VPN configuration, see *Chapter 4, Configure VPN Tunnels*.

2. Export the VPN configuration:

   a. On your desktop, double-click the **VPN Client** shortcut  .

      The VPN Configuration page displays.

   b. Select **Configuration > Export**.



3. Select a radio button:
   - **Don’t protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. The VPN configuration file requires a password before it can be opened, do the following:

     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 the **OK** button.

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 name ends with a `.tgb` extension. Do not change this extension.

6. Click the **Save** button.

   Your settings are saved.

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 specified a password, it is automatically requested and the end user must enter 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 must 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 7. 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 the name includes a space character.
/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 7. 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 to specify whether to add or replace the 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 to specify whether to add or replace the 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 must enter to enable the command with which the **/pwd:** command is combined. The **/exportonce:** and **/exportonce:** commands require you to set a password. A password is optional for the **/import:**, **/importonce:**, **/add:**, and **/replace:** commands. **Note:** You must place the **/pwd:** command *after* the other command that you combine the **/pwd:** command with. **Example**: `vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd=mypwd`

Table 7. 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

The following sections provide configuration examples:

- *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 does not affect the tunnel status.

- **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 does not affect the tunnel status.

Note: The **`open`** and **`close`** commands are mutually exclusive.

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 manage 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 name ends with 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 must 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.

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 must 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 root certificate 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 certificate authority that is different from 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 8. 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 must use certificates from the same certificate authority. • **01**. The VPN Client and the VPN gateway can use certificates from different certificate authorities.

Table 8. PKI options parameters for the vpnsetup.ini file in alphabetical order (continued)

Option	Description	Settings
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 106).
PKICheck	The option lets you force the VPN Client to validate the root certificate authority when it receives a certificate from the VPN gateway. For more information, see *PKICheck Option Concepts* on page 106. This PKI option is also available as a software setup command (see *Software Setup Command Reference* on page 82). The setting in the vpnsetup.ini file overrides the setting in the software setup command.	• **Not configured**. The VPN Client does not validate the root certificate authority. • **01**. The VPN Client validates the root certificate 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.
SmartCardRoaming	This option lets you set rules for the VPN Client to select a certificate from a token or smart card when several tokens and smart cards are present. **Note:** This PKI option is also available as a software setup command (see *Software Setup Command Reference* on page 82). 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 106).	• **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.

Table 8. PKI options parameters for the vpnsetup.ini file in alphabetical order (continued)

Option	Description	Settings
`SmartCardRoaming` (continued)	`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 must 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 must 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#11
DLL"


// New Token description#1

[3B:0F:52:4E:42:4F:24:00:23:00:00:00:00:00:00:01]

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:

- *PKICheck Option Concepts* on page 106
- *Configure the ROAMING Section of the vpnconf.ini File* on page 107
- *Configure the ATR Section of the vpnconf.ini File* on page 109

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 9. 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 must 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 10. 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 the `vpnconf.ini` file includes more than one ATR code.	
`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 must 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:24:00:23:00:00:00:00:00:00:01]
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"
```

7. Troubleshoot the VPN Client

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

VPN Client Troubleshooting Overview

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 (visit *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.

For difficulties with software activation, see *Troubleshoot Software Activation* on page 17.

For difficulties with certificates, see *Troubleshoot Certificates* on page 65.

Resolve Firewall Interference

If you cannot establish a VPN tunnel, your firewall might be interfering. If a tunnel no longer opens, read the logs for each VPN tunnel endpoint. It is possible that a firewall dropped the IKE requests. The VPN Client must be able to use UDP port 500 and ESP port 50.

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

View and Control VPN Client Log Messages

You can analyze how VPN tunnels are set up or fail to be set up, which can be useful if you are a network administrator and are configuring a secure network. The log messages display on the VPN Console Active page. They are mostly IKE messages.

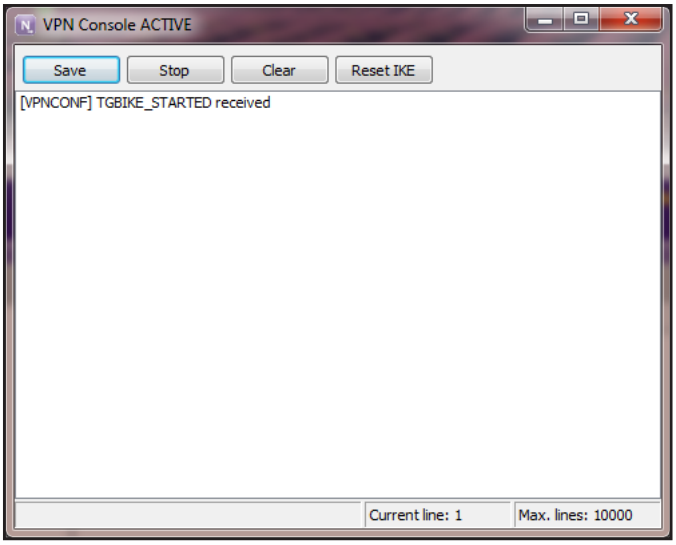
Note: For information about hiding the **Console** menu item on the system tray menu, see *Hide User Interface Features* on page 71.

➢ **To view log messages on the VPN Console Active page:**

1. On your desktop, double-click the **VPN Client** shortcut  .

   The VPN Configuration page displays.

2. Select **Tools > Console**.



The buttons on the VPN Console Active page perform 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 page.
- **Reset IKE**. Restarts the IKE process.

You can also enable debugging mode, which is also referred to as trace mode. See *Enable the VPN Console Debugging Mode* on page 112.

Enable the VPN Console Debugging Mode

You can enable debugging mode, which is also referred to as trace mode. The trace logs become large rather quickly. The VPN Console Active page and trace mode can help you or NETGEAR support to diagnose tunnel problems and software's incidents.

➢ **To enable debugging mode:**

1. On your desktop, double-click the **VPN Client** shortcut  .

   The VPN Configuration page displays.

2. Select **Tools > Console**.

   The VPN Console Active page displays.

3. Press Ctrl + Alt + T.

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

VPN Console Log Errors

The following errors might occur on the VPN Client:. The dates, times, and numbers that can precede the messages were removed from these examples.

PAYLOAD_MALFORMED error

This message indicates a problem with the phase 1 security association (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 security association (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 a security association (SA) that is no longer alive.

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

no keystate

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 IKE Authentication Settings* on page 28.

received remote ID other than expected

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 in 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 Settings* on page 30).

NO_PROPOSAL_CHOSEN error

This is a phase 1 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 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 IKE Authentication Settings* on page 28.

NO_PROPOSAL_CHOSEN error

This is a phase 2 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 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 *Configure IPSec Settings* on page 37.

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. The addresses might mismatch on the tunnel endpoints, or a security association (SA) might no longer be alive.

Resolution. Ensure that both the phase 2 address types and phase 2 address values (see *Configure IPSec Settings* on page 37) match the remote endpoint's address configuration. Ensure that no old SA is still alive on the VPN gateway.

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 IKE Authentication Settings* on page 28.

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 Settings* on page 30.

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 keys 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 no second VPN tunnel connects to the VPN Client on the VPN router.

No Response to 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 *Configure IPSec Settings* on page 37.

Ensure that both the phase 2 address types and phase 2 address values (see *Configure IPSec Settings* on page 37) match the remote endpoint's address configuration.

View VPN Gateway Logs

In addition to viewing VPN Client log messages, you might find it helpful to view log messages for the destination VPN gateway. The following figure shows an example of VPN logs on a NETGEAR ProSAFE VPN Firewall SRX5308 router.

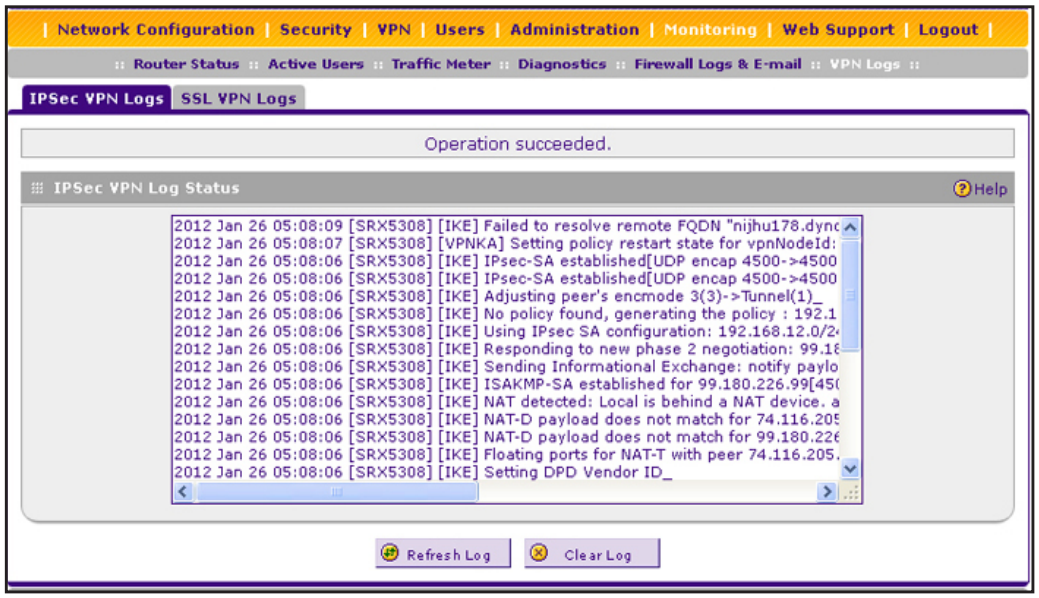


Figure 16. IPSec VPN Logs page of a ProSAFE VPN Firewall SRX5308 router

Following is an example of a VPN log on the VPN router after a VPN Client established a VPN connection with the VPN router. (This example does not relate to the information that is shown in the previous page. In addition, the date and times that precede the messages were 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)_
```

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 does 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 gateway logs. It is possible that the firewall of the VPN gateway dropped the packets.
- Verify that your ISP supports ESP.
- Use a network analysis software tool (such as the free Wireshark tool (visit *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 no default gateway is specified.
- Verify that the computers in the LAN are specified by their IP addresses and not by their FQDNs.
- Use a network analysis software tool (such as the free Wireshark tool (visit *www.wireshark.org/*) on one of the target computers to verify that the ping arrives inside the LAN.

Configure a NETGEAR VPN Gateway

A

This appendix describes how to configure a NETGEAR router as a VPN gateway. The appendix includes the following sections:

VPN Gateway Overview

The example in this appendix is the NETGEAR ProSAFE SRX5308 VPN Firewall. The information in this appendix applies to the following NETGEAR routers and UTM appliances.

Table 11. Compatible firmware versions

Router Model	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

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

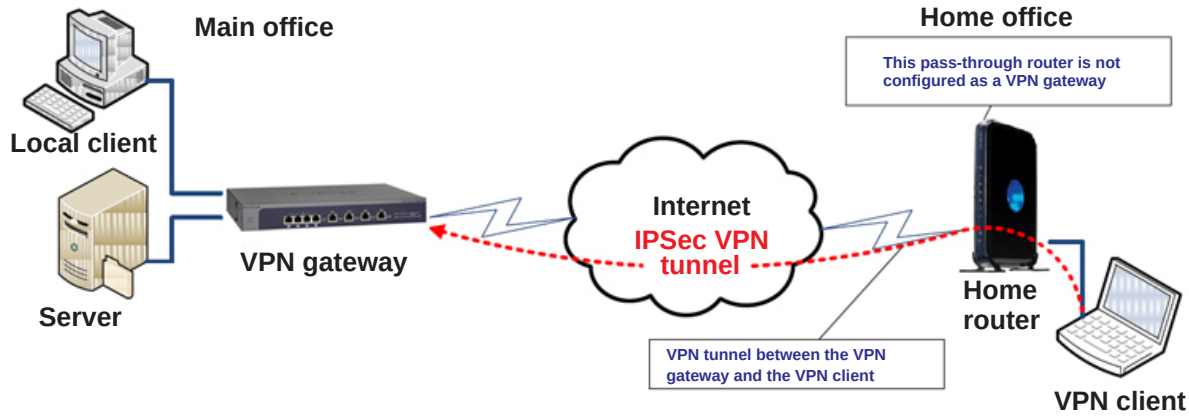


Figure 17. VPN network topology example

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 12. IP address and VPN setting for the VPN network topology example

Main Office Settings	Remote Home Office Settings
• **VPN gateway WAN IP address**. 10.200.13.18 (or myrouter.dyndns.org) • **VPN gateway LAN IP address**. 192.168.30.1 **Subnet mask**. 255.255.255.0	• **Home router IP LAN address**. 192.168.0.1 • **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	• **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

The IP addresses in this appendix are only examples. You can adjust the settings and configuration to suit your network.

While you configure the VPN router, some settings that you specify are also used to configure the VPN client computer. You can print the following table to keep track of this information.

Pre-shared key	
Remote identifier information	
Local identifier information	
Router's LAN network IP address	
Router's LAN network mask	
Router's WAN IP address	

Use the Router's VPN Wizard to Configure a VPN Gateway

The router's web management interface includes a VPN Wizard that lets you easily set up the router as a VPN gateway that can connect to VPN clients.

You can use the router's VPN Wizard or set up the VPN connection manually. NETGEAR recommends using the VPN Wizard, which is easier. The VPN Wizard configures the default settings and provides basic interoperability so that the VPN gateway can communicate with NETGEAR or third-party VPN devices.

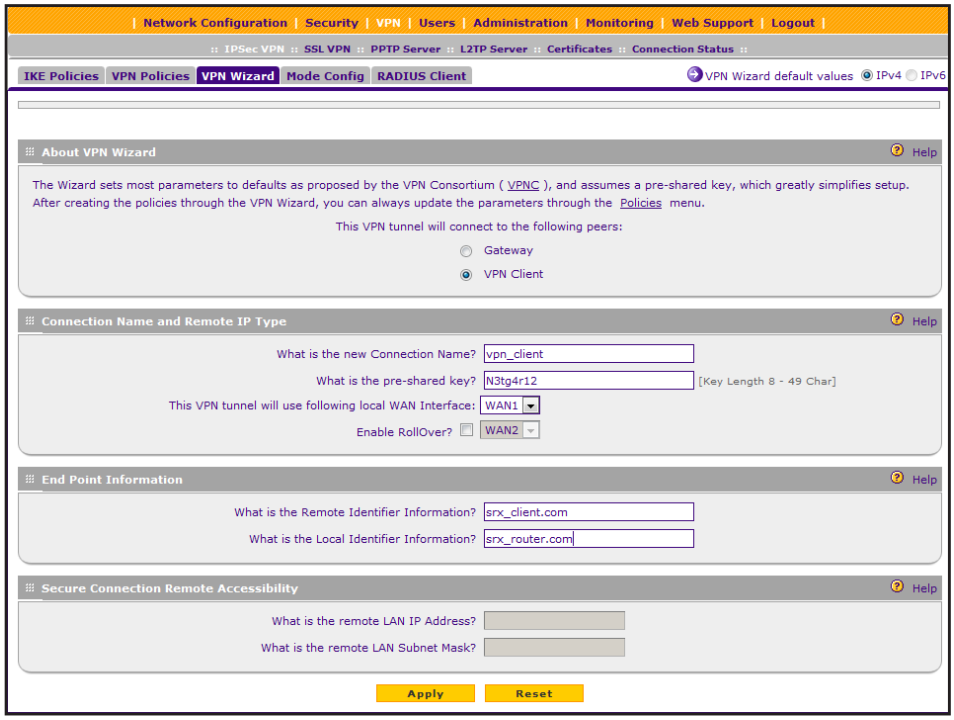
➢ **To use the router's VPN Wizard to set up a VPN gateway:**

1. Access the router's web management interface.

   For information about how to do this, see the documentation that came with your router.

In this example, the Router Status page displays.

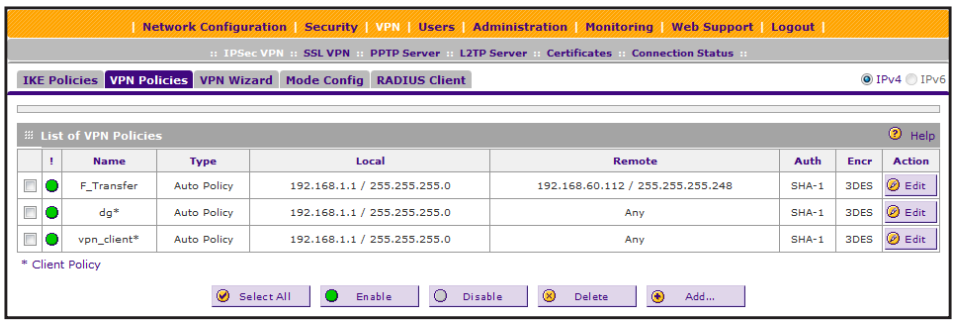
2. Select **VPN > IPSec VPN > VPN Wizard**.



3. Select the **IPv4** or **IPv6** radio button, depending on the router's Internet connection.
4. Select the **VPN Client** radio button.
5. In the **What is the Remote Identifier Information?** field, type **vpn_client**.
6. In the **What is the pre-shared key?** field, type **N3tg4ar12**.
7. In the **This VPN tunnel will use the following local WAN Interface** menu, select **WAN1**.

   This option is not available for platforms with a single WAN port.
8. In the **What is the Remote Identifier Information?** field, type **srx_client.com**.
9. In the **What is the Local Identifier Information?** field, type **srx_router.com**.
10. Click the **Apply** button.

    The VPN policy is created.
11. To review the VPN policy, select **VPN > IPSec VPN > VPN Polices**.



The Local column displays the local LAN IP address and subnet mask, both of which you must use later to configure the VPN Client.

Edit a VPN Policy

To be able to edit a VPN policy, you must disable it.

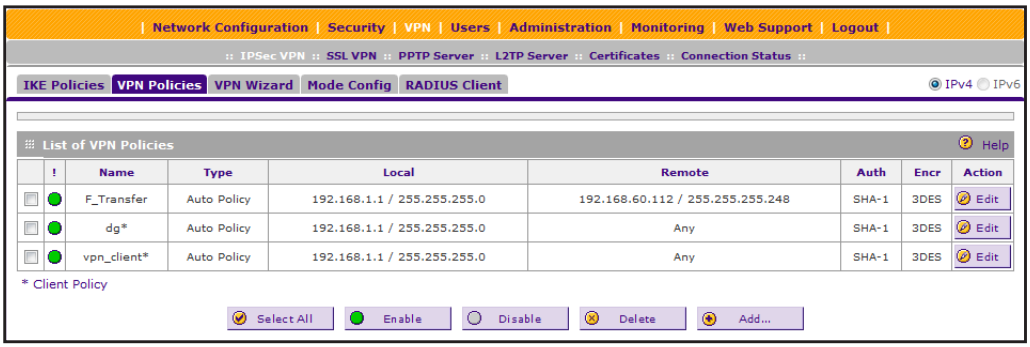
➢ **To edit a VPN policy:**

1. Access the router's web management interface.

   For information about how to do this, see the documentation that came with your router.

   In this example, the Router Status page displays.

2. Select **VPN > IPSec VPN > VPN Policies**.



3. Select the check box for the policy.
4. Click the **Disable** button.

   The VPN policy is disabled.

5. In the Action column for the selected policy, click the **Edit** button.

   The Edit VPN Policy page displays. The appearance of this page depends on the router model.

   Note: From this page, you can change the local IP address and the subnet mask settings.

6. Modify the VPN policy.
7. Click the **Apply** button.

   The VPN Policies page displays.

8. Select the check box for the policy.
9. Click the **Enable** button.

   The VPN policy is reenabled.

Edit an IKE Policy

To be able to edit an IKE policy, you must disable its associated VPN policy.

➢ **To edit an IKE policy:**

1. Access the router's web management interface.

   For information about how to do this, see the documentation that came with your router.

   In this example, the Router Status page displays.

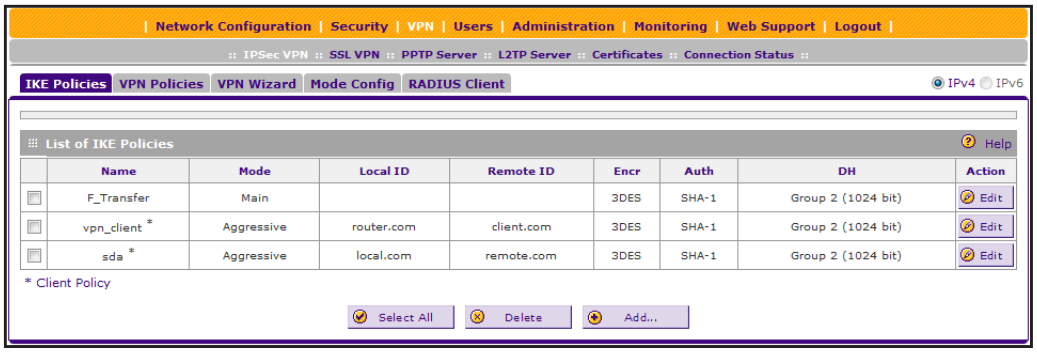
2. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies page displays.

3. Select the check box for the policy.
4. Click the **Disable** button.

   The VPN policy is disabled.

5. Click the **IKE Policies** tab.



6. In the Action column of the selected policy, click the **Edit** button.

   The Edit IKE Policy page displays. The appearance of this page depends on the router model.

   Note: From this page, you can change the local and remote identifiers and the pre-shared key.

7. Modify the IKE policy.
8. Click the **Apply** button.

   The IKE Policies page displays.

9. Click the **VPN Policies** tab.

   The VPN Policies page displays.

10. Select the check box for the policy.
11. Click the **Enable** button.

    The VPN policy is reenabled.

Manually Configure a NETGEAR Router as a VPN Gateway

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.

Set Up an IKE Policy in the Router

➢ **To set up an IKE policy:**

1. Access the router's web management interface.

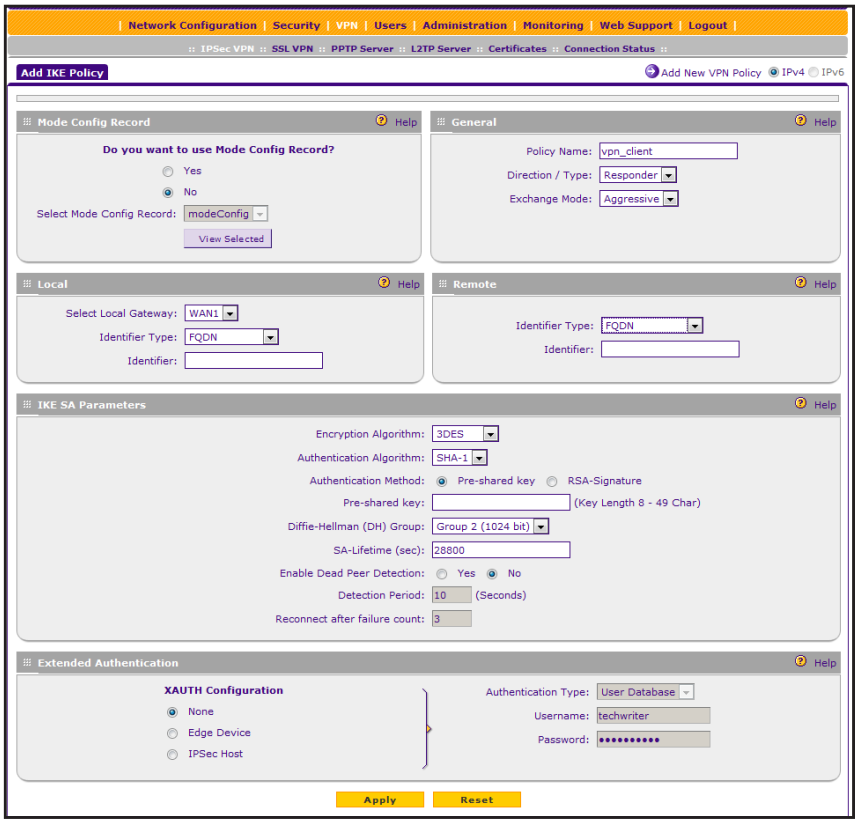
   For information about how to do this, see the documentation that came with your router.

   In this example, the Router Status page displays.

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

   The IKE Policies page displays.

3. Click the **Add** button.



4. Specify the settings that are described in the following table.
5. Click the **Apply** button.

   The IKE policy is created and displays in the IKE Policies page.

The following table describes the settings in the IKE Policies page.

Table 13. IKE Policies page settings

Setting	Selection
General	
Policy Name	**vpn_client**.
Direction / Type	**Responder** (the router responds to the client).
Exchange Mode	**Aggressive**.
Local	
Select Local Gateway	**WAN1**. **Note:** This option is not available for router with a single WAN port.
Identifier Type	**FQDN**.
Identifier	**srx_router.com**.
Remote	
Identifier Type	**FQDN**.
Identifier	**srx_client.com**.
IKE SA Parameters	
Encryption Algorithm	**3DES**.
Authentication Algorithm	**SHA-1**.
Authentication Method	**Pre-Shared Key**.
Pre-shared key	**N3tg4ar12**. **Note:** This key must be at least 8 characters long. NETGEAR recommends that you create a key that is not easy to guess.
Diffie-Hellman (DH) Group	**Group 2 (1024bit)**.
SA-Life Time (sec)	**28800**.
Enable Dead Peer Detection	**No**. (This is the default setting.)
Extended Authentication	
Extended Authentication	**No**. (This is the default setting.)

Set Up a VPN Policy in the Router

➢ **To set up a VPN policy:**

1. Access the router's web management interface.

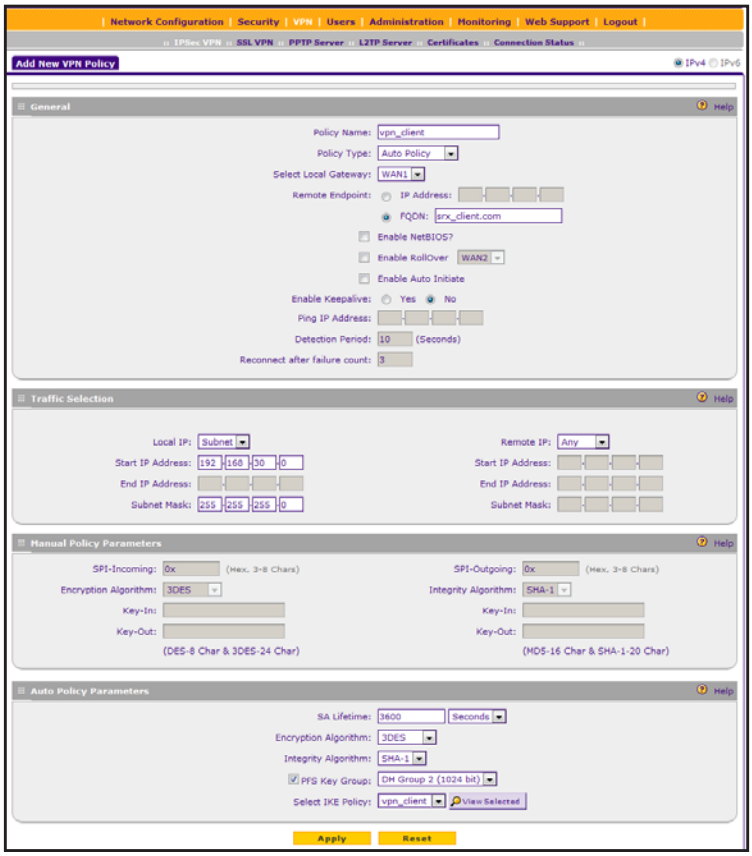
   For information about how to do this, see the documentation that came with your router.

In this example, the Router Status page displays.

2. Select **VPN > IPSec VPN > VPN Polices**.

   The VPN Policies page displays.

3. Click the **Add** button.



4. Specify the settings that are described in the following table.
5. Click the **Apply** button.

   The VPN Policies page displays.

The following table describes the VPN Policy settings.

Table 14. VPN Policy settings

Setting	Description
General	
Remote Endpoint	Enter **vpn_client**. (Keep the policy name the same as the IKE policy name.)
Policy Type	Select **Auto Policy**.

Table 14. VPN Policy settings (continued)

Setting	Description
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.
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**.
Start IP Address	Enter **192.168.30.0**.
Subnet Mask	Enter **255.255.255.0**.
Remote IP	Select **Any**.
Auto Policy Parameters **Note:** If you select **Manual Policy** from the **Policy Type** menu (see the General section), 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**.
Encryption Algorithm	Select **3DES**.
Integrity Algorithm	Select **SHA-1**.
PFS Key Group	Select the **PFS Key Group** check box, and then select **DH Group 2 (1024 bit)**.
Select IKE Policy	Select **vpn_client**. This is the IKE policy that you created in the previous section.

Configure a VPN Client to Match the VPN Gateway Settings

After you configure the VPN gateway, you must configure the following settings in the VPN Client:

1. Specify the IKE Authentication settings. (See *Configure IKE Authentication Settings* on page 28.)
2. Specify the Advanced settings. (See *Configure Advanced Authentication Settings* on page 30.)
3. Specify the IPSec Settings. (See *Configure IPSec Settings* on page 37.)
4. Specify the Parameter settings. (See *Configure the Parameter Settings* on page 40.)

The following table shows the client settings that correspond with the VPN gateway example in this appendix.

Table 15. Sample VPN Client settings based on the sample NETGEAR VPN gateway

VPN Client Page	Feature	Setting
IKE Authentication	Interface	**Any**
	Remote gateway	<your router's DNS URL or external IP address>
	Preshared key	**N3tg4ar12**
	Encryption	**3DES**
	Authentication	**SHA1**
	Key group	**DH2 (1024)**
Advanced (Authentication)	Aggressive mode	Select this check box.
	NAT-T	**Automatic**
	Local ID	**srx_client.com**
	Remote ID	**srx_router.com**
IPSec Config	VPN Client address	192.168.31.201
	Address type	**Subnet address**
	Remote LAN address	The address of the gateway
	Subnet mask	**255.255.255.0**
	Encryption	**3DES**
	Authentication	**SHA-1**
	Mode	**Tunnel**

Table 15. Sample VPN Client settings based on the sample NETGEAR VPN gateway (continued)

VPN Client Page	Feature	Setting
IPSec Config (continued)	PFS	Select this check box.
	Group	**DH2 (1024)**
Parameters	Authentication (IKE) default	**28800**
	Encryption (IPSec) default	**3600**