SonicWall™ Global VPN Client 4.10

Getting Started Guide

SONICWALL™

Legend

⚠ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

ⓘ **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Getting Started With Global VPN Client

About SonicWall Global VPN Client

The SonicWall™ Global VPN Client creates a Virtual Private Network (VPN) connection between your computer and the corporate network to maintain the confidentiality of private data. The Global VPN Client provides an easy-to-use solution for secure, encrypted access through the Internet for remote users.

This Getting Started Guide describes the firewall and client systems supported for Global VPN Client, provides installation instructions, and tells how to initiate or disable a VPN connection.

ⓘ | **IMPORTANT:** SonicOS GroupVPN must be enabled on the SonicWall security appliance.

Before You Begin

You will need the following to run SonicWall Global VPN Client:

- A computer running supported version of Windows
- An active Internet connection
- The SonicWall Global VPN Client installer
- A Zip program if needed for unzipping the downloaded Global VPN Client installer files

ⓘ | **NOTE:** For complete instructions on installing, configuring, managing and troubleshooting the SonicWall Global VPN Client, see the *SonicWall Global VPN Client Getting Started Guide*.

ⓘ | **NOTE:** For information on supported SonicWall platforms and Windows versions see Supported Platforms on page 4.

Topics:

Pre-Installation Recommendations

SonicWall strongly recommends you follow these steps before installing the SonicWall Global VPN Client (Global VPN Client) 4.10 client:

- If you have SonicWall Global VPN Client version 4.9.22 or earlier installed, you must uninstall that version before installing version 4.10. Upgrading to Global VPN Client 4.10 from earlier versions is not supported.

- SonicWall Global VPN Client encounters run time conflicts when it co-exists with any 3rd party IPsec VPN clients. Uninstall all IPsec VPN clients prior to installing SonicWall Global VPN Client..

(i) | **NOTE:** The SonicWall Global VPN Client is launched as soon as the installation completes. The **Start SonicWall Global VPN client every time I login** option can no longer be set during installation, but this option is available on the **General** tab in the **View > Options** page of the client.

Supported Platforms

This section describes the firewalls, firmware versions and clients systems that are supported by SonicWall Global VPN Client.

Supported Firewalls and Firmware

Global VPN Client is supported on SonicWall appliances running SonicOS 6.1 and higher shown the Supported SonicWall appliances running SonicOS 6.x. table.

Supported SonicWall appliances running SonicOS 6.x.

• SuperMassive 9600	• NSA 6600	• TZ600
• SuperMassive 9400	• NSA 5600	• TZ500 and TZ500 Wireless
• SuperMassive 9200	• NSA 4600	• TZ400 and TZ400 Wireless
	• NSA 3600	• TZ300 and TZ300 Wireless
	• NSA 2600	• SOHO Wireless

Global VPN Client is supported on SonicWall appliances running SonicOS 5.8.0.0 and higher shown in the Supported SonicWall appliances SonicOS 5.x. table.

Supported SonicWall appliances SonicOS 5.x.

• NSA E8510	• NSA 2400	• TZ 215	• TZ 215 Wireless
• NSA E8500	• NSA 2400MX	• TZ 210	• TZ 215 Wireless
• NSA E7500	• NSA 250M	• TZ 205	• TZ 215 Wireless
• NSA E6500	• NSA 250M Wireless	• TZ 200	• TZ 215 Wireless
• NSA E5500	• NSA 240	• TZ 105	• TZ 215 Wireless
• NSA 5000	• NSA 220	• TZ 100	• TZ 215 Wireless
• NSA 4500	• NSA 220 Wireless	• SOHO	
• NSA 3500			

Supported Client Systems

Global VPN Client is supported on SonicWall security appliances running one of these client operating systems:

- The SonicWall Global VPN Client operates on 32-bit and 64-bit versions of:
    - Windows 10
    - Windows 8.1
    - Windows 8
    - Windows 7

Installing the Global VPN Client

Installing the Global VPN Client

The SonicWall Global VPN Client uses an easy-to-use wizard to guide you through the installation process.

ⓘ | **NOTE:** Installing the Global VPN Client requires Administrator rights.

Using the Setup Wizard

This section explains how to install the SonicWall Global VPN Client program using the **Setup Wizard**.

ⓘ | **IMPORTANT:** Remove any installed 3rd Party VPN client program before installing the latest SonicWall Global VPN Client.
  | If you have SonicWall Global VPN Client installed, you must uninstall it before installing version 4.10.x.

To install Global VPN Client using the Setup Wizard:

1 Download the self-extracting installer, `GVCSetupXX.exe` (where `XX` is either **32** for 32-bit Windows platforms or **64** for 64-bit Windows platforms), from MySonicWall.

2 Double-click `GVCSetupXX.exe`. The **Setup Wizard** launches.
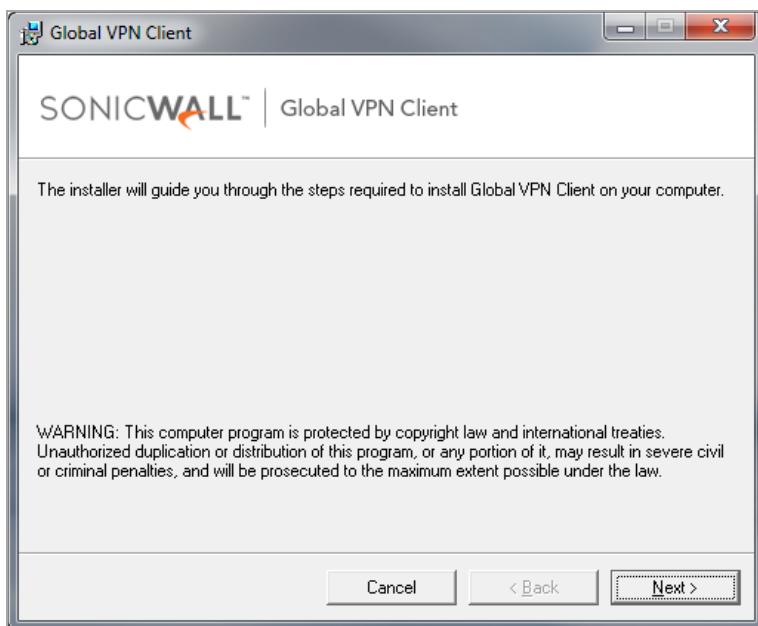
3   Click **Next** to continue installation of the VPN Client. The **License Agreement** page displays.
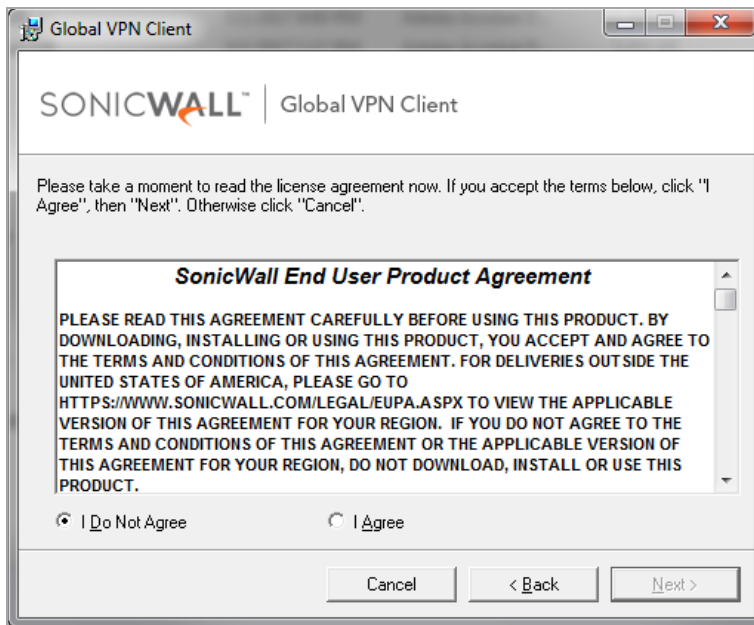
4   Select the **I Agree** radio button.

5   Click **Next**. The **Installation Folder Selection** page displays.
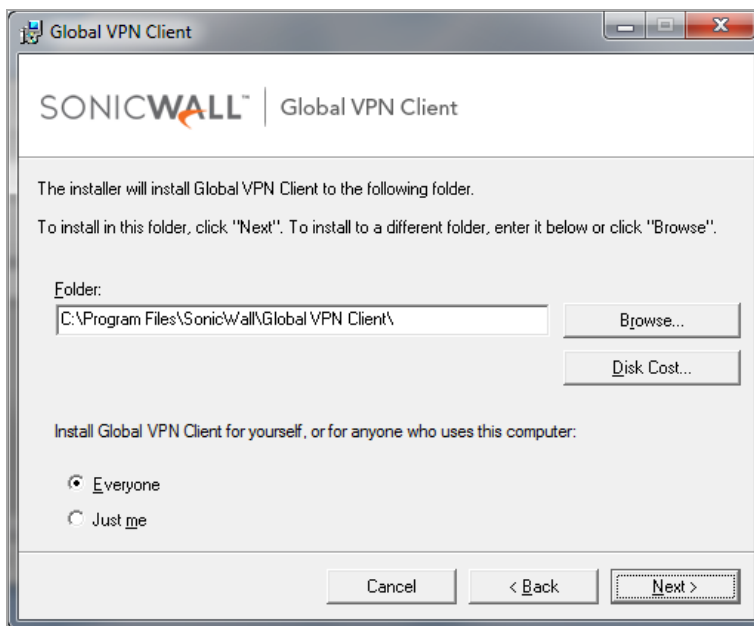
6   Optionally, to specify a custom installation location, click **Browse**.

    a   Select the location.

    b   Click **OK**.

7   Optionally, click the **Disk Cost** button to see the disk space requirements.
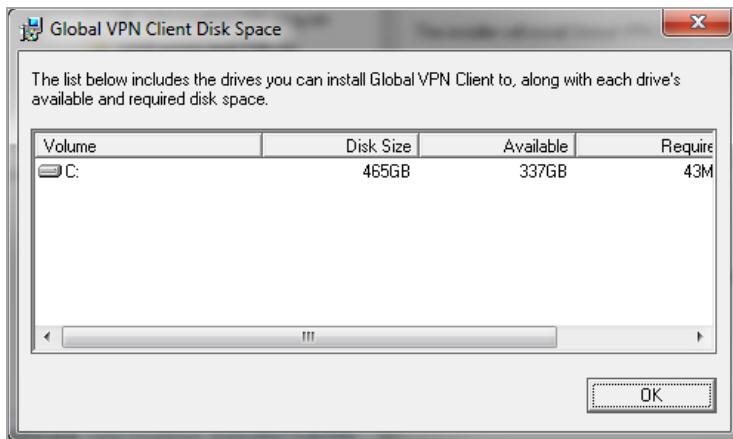
8   Under **Install SonicWall Global VPN Client for yourself, or for anyone who uses this computer**, select either **Everyone** or **Just me**.

9   Click **Next**. The next page indicates that the installer is ready to begin installation.

10 Click **Next**. The **Global VPN Client is being installed** page displays, which indicates the status of the installation.
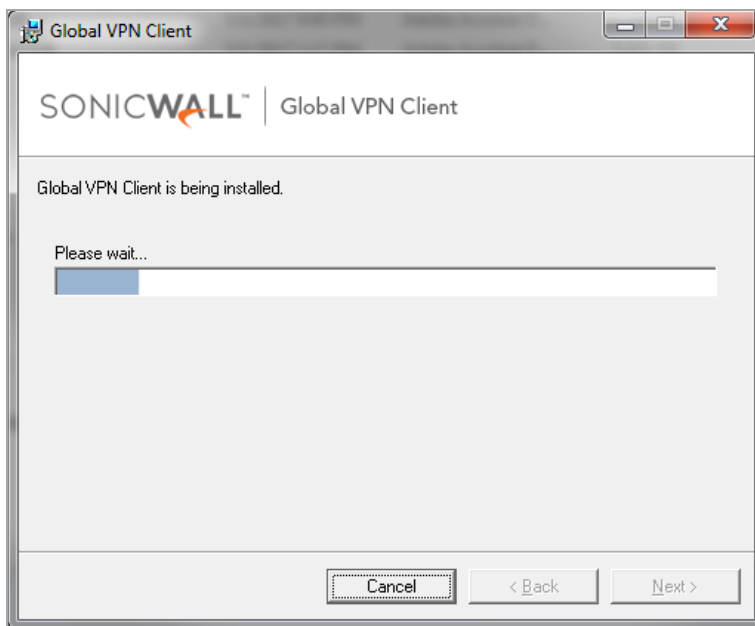
11 Wait while the SonicWall Global VPN Client files are installed on your computer. When the installation is complete, the **Global VPN Client has been successfully installed** page displays.
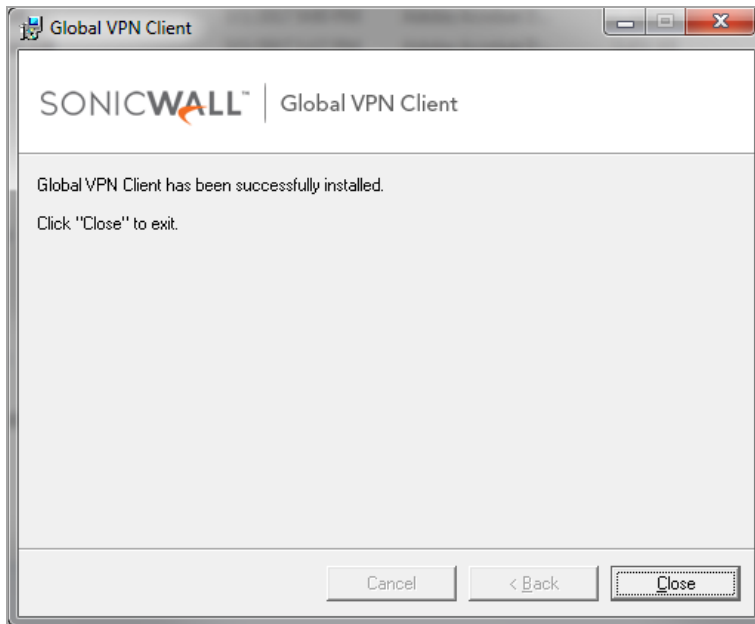
12 Click **Close** to exit the wizard. After a successful installation, what happens next depends on whether you had saved connections:

- If you saved the connection configurations from a previous version of the SonicWall Global VPN Client when uninstalling it, the Global VPN Client launches, and your default connection prompts you for login credentials.

- If no previous connections exist, the New Connection Wizard launches automatically. This only occurs the first time the Global VPN Client starts up. You can configure the Global VPN Client to launch automatically every time you log onto your computer, on the **General** tab in the **View > Options** page. For more information, see the *SonicWall Global VPN Client Getting Started Guide*.

ⓘ | **NOTE:** You can configure the Global VPN Client to launch automatically every time you log onto your computer, on the **General** tab in the **View > Options** page.

Upgrading Global VPN Client from a previous version

Upgrades from previous versions are not supported. If you have SonicWall Global VPN Client version 4.9.22 or earlier installed, you must uninstall that version and reboot your PC before installing version 4.10.x. The 4.10.x installer does not allow upgrading from earlier versions.

Using VPN Connections

Adding a VPN Connection

Adding a new VPN connection is easy because SonicWall's Client Policy Provisioning automatically provides all the necessary configuration information to make a secure connection to the local or remote network. The burden of configuring the VPN connection parameters is removed.

This section describes how to use the **New Connection** wizard to create and save a VPN connection. The wizard downloads a VPN connection policy for the Global VPN Client automatically from a local or remote SonicWall VPN gateway over a secure IPsec VPN tunnel.

ⓘ **NOTE:** If a `default.rcf` file is included with the downloaded Global VPN Client software, the VPN policy configured by you is used to create a connection automatically when the client software is installed.

To add a VPN connection using the New Connection Wizard:

1 Choose **Start > Programs > Global VPN Client**. The first time you open the SonicWall Global VPN Client, the **New Connection Wizard** launches automatically.
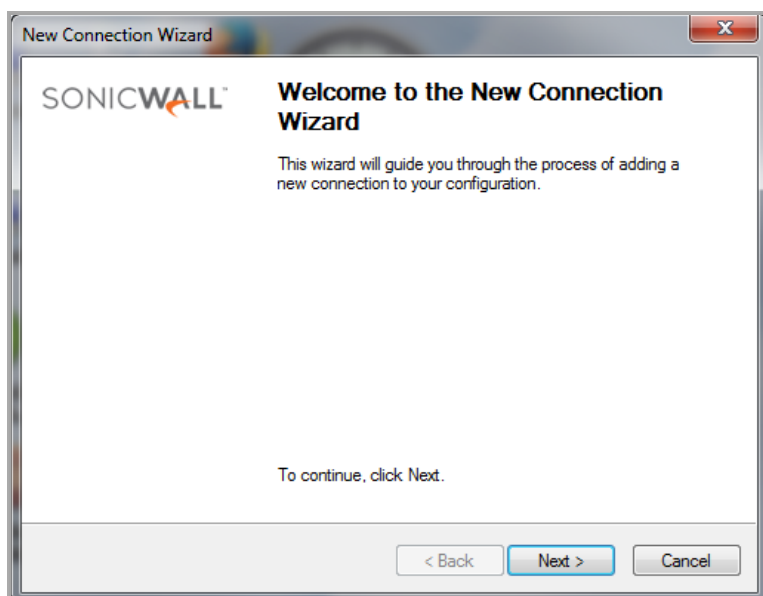
2 If the **New Connection Wizard** does not display, to launch it, click the **New Connection** ➕ button.

3   Click **Next**. The **New Connection** page displays.

4   Enter the IP address or FQDN of the gateway in the **IP Address or Domain Name** field. The information you type in the **IP Address or Domain Name** field appears in the **Connection Name** field.

5   Optionally, if you want a different name for your connection, type the new name for your VPN connection in the **Connection Name** field.
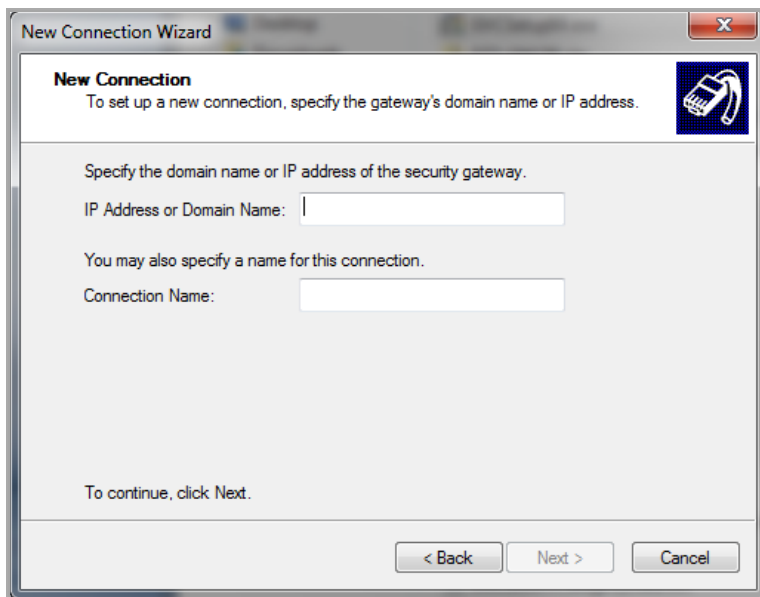
6   Click **Next**. The **Completing the New Connection Wizard** page displays.

7   Optionally, select either or both:

   • **Create a desktop shortcut for this connection** if you want to create a shortcut icon on your desktop for this VPN connection.

   • **Enable this connection when the program is launched** if you want to automatically establish this VPN connection when you launch the SonicWall Global VPN Client.

8   Click **Finish.** The new VPN connection appears in the **Global VPN Client** window.

Making VPN Connections

Making a VPN connection from the Global VPN Client is easy because the configuration information is managed by the SonicWall VPN gateway. The SonicOS (VPN gateway) administrator sets the parameters for what is allowed and not allowed with the VPN connection. For example, for security reasons, the administrator may not allow multiple VPN connections or the ability to access the Internet or local network while the VPN connection is enabled.

The Global VPN Client supports two IPsec authentication modes:

- IKE using Preshared Secret
- IKE using 3rd Party Certificates.

Preshared Secret is the most common form of the IPsec authentication modes. If your VPN connection policy uses 3rd party certificates, you use the Certificate Manager to configure the Global VPN Client to use digital certificates.

A Pre-Shared Key (also called a Shared Secret) is a predefined password that the two endpoints of a VPN tunnel use to set up an IKE (Internet Key Exchange) Security Association. This field can be any combination of alphanumeric characters with a minimum length of 4 characters and a maximum of 128 characters. Your Pre-Shared Key is typically configured as part of your Global VPN Client provisioning. If it is not, you are prompted to enter it before you log on to the remote network.

Topics:

Enabling a VPN Connection

This section describes how to establish a VPN connection created in the SonicWall Global VPN Client.

To establish a VPN connection using a VPN connection policy you created in the Global VPN Client:

(i) | **NOTE:** If you selected **Enable this connection when the program is launched** in the New Connection Wizard, the VPN connection is automatically enabled when you launch the SonicWall Global VPN Client.

1 Launch the SonicWall Global VPN Client from the Windows Start button or from your shortcut. The Global VPN Client window displays.
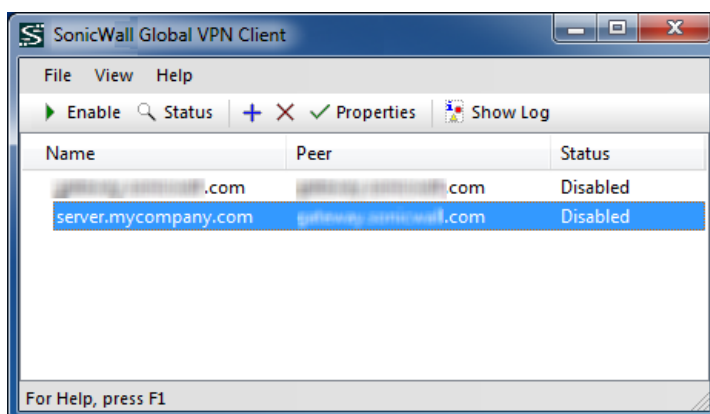
2   If your VPN connection is not automatically established when you launch the Global VPN Client, choose one of the following methods to enable a VPN connection:

- Double-click the VPN connection.

- Right-click the VPN connection icon and select **Enable** from the menu.

- Select the VPN connection and press **Ctrl+B**.

- Select the VPN connection, and click the **Enable** button on the toolbar.

- Select the VPN connection, and then choose **File > Enable.**

- If the **Global VPN Client** icon is displayed in the system tray, right-click the icon and then select **Enable >** *connection name*. The Global VPN Client enables the VPN connection without opening the **Global VPN Client** window.

3   In the **Enter Username / Password** dialog box, type your username and password. Click **OK** to continue with establishing your VPN connection.
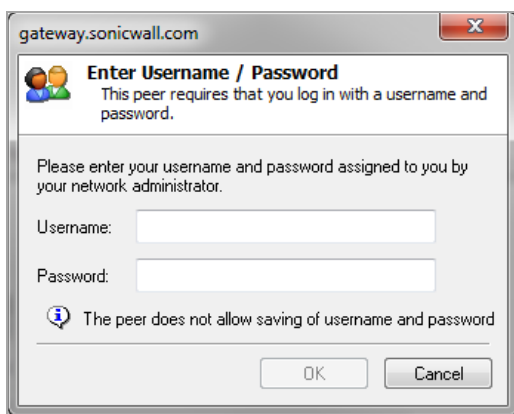
4   Depending on the attributes for the GroupVPN policy on the SonicWall security appliance, the **Enter Pre-Shared Key** or **Select Certificate** dialog may be displayed. See Entering a Pre-Shared Key on page 12 or Selecting a Certificate on page 13 for more information.

5   Click **OK**.

> **TIP:** If the VPN connection policy allows only traffic to the gateway, the **Connection Warning** message appears, warning you that only network traffic destined for the remote network at the other end of the VPN tunnel is allowed. See Connection Warning on page 14 for more information.

Entering a Pre-Shared Key

Depending on the attributes for the VPN connection, if no default Pre-Shared Key is used, you must have a Pre-Shared Key provided by the gateway administrator to make your VPN connection. If the default Pre-Shared Key

is not included as part of the connection policy download or file, the Pre-Shared Key dialog appears, prompting you for the Pre-Shared key before establishing the VPN connection.

To enter a Pre-Shared Key:

1   Type your Pre-Shared Key in the **Pre-shared Key** field. The Pre-Shared Key is masked for security.

2   Optionally, to make sure you are entering the correct Pre-Shared Key, select **Don't hide the pre-shared key**. The Pre-Shared Key you enter appears unmasked in the Pre-shared Key field.

(i)   **NOTE:** If you select this option, be sure to clear it when you have verified the Pre-Shared Key.

3   Click **OK**.

Selecting a Certificate

If the SonicWall VPN Gateway requires a Digital Certificate to establish your identity for the VPN connection, the **Select Certificate** dialog appears. This dialog lists all the available certificates installed on your Global VPN Client.

To select a certificate:

1   Select the certificate from the drop-down menu.
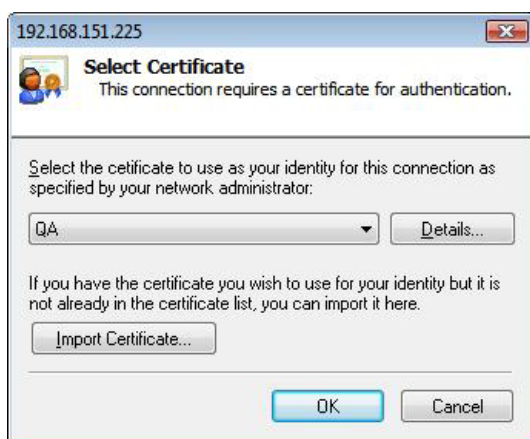
2   If you have a certificate that has not been imported into the Global VPN Client using **Certificate Manager**, click **Import Certificate** and import the certificate you need.

3   Click **OK**.

(i)   **NOTE:** See the *SonicWall Global VPN Client Getting Started Guide* for more information on using the Certificate Manager.

Connection Warning

If the VPN connection policy allows only traffic to the gateway, the Connection Warning message appears, warning you that only network traffic destined for the remote network at the other end of the VPN tunnel is allowed. Any network traffic destined for local network interfaces and the Internet is blocked.
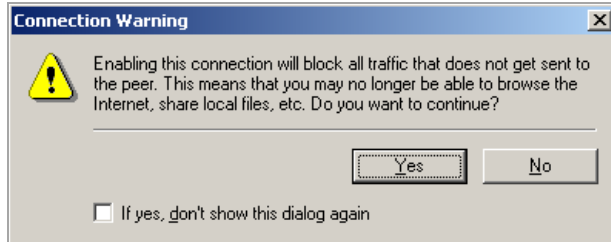
You can disable the Connection Warning message from displaying every time you enable the VPN connection by selecting **If yes, don't show this dialog box again**.

Click **Yes** to continue with establishing your VPN connection.

Disabling a VPN Connection

Disabling a VPN connection terminates the VPN tunnel. You can disable a VPN connection using these methods:

- Right-click the VPN connection in the **Global VPN Client** window, and select **Disable**.
- Right-click the **Global VPN Client** icon on the system tray, and choose **Disable > *connection***.
- Select the connection, then press **Ctrl+B**.
- Select the connection, and click the **Disable** button on the toolbar in the **Global VPN Client** window.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, refer to https://support.sonicwall.com/contact-support.

To view the SonicWall End User Product Agreement (EUPA), see https://www.sonicwall.com/legal/eupa.aspx. Select the language based on your geographic location to see the EUPA that applies to your region.