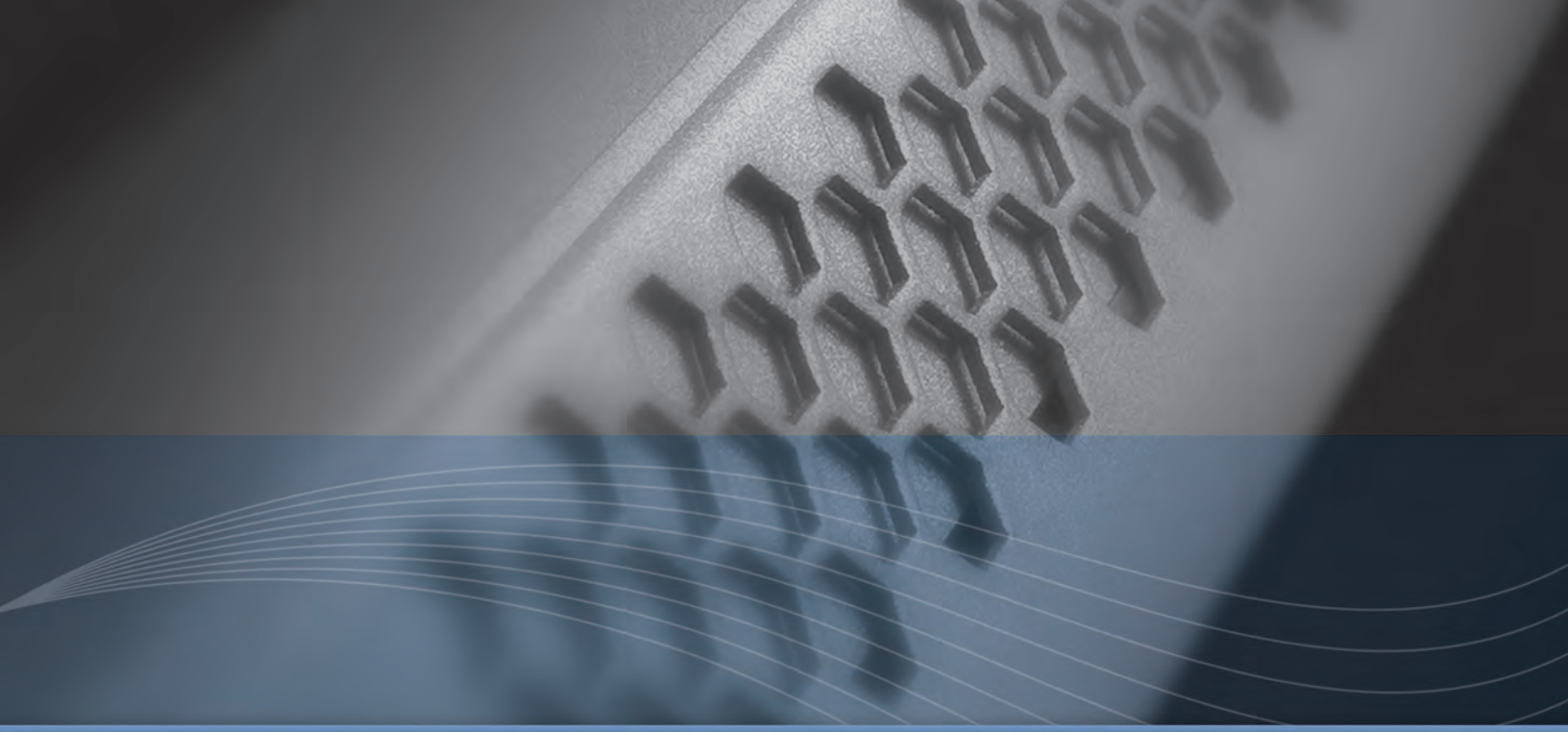


Global VPN Client 4.6 Administrator's Guide

SonicWALL® E-CLASS

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Table of Contents

SonicWALL Global VPN Client Overview

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 or corporate dial-up facilities for remote users as well as secure wireless networking for SonicWALL Secure Wireless appliance clients using SonicWALL's WiFiSec technology.

Custom developed by SonicWALL, the Global VPN Client combines with GroupVPN on SonicWALL Internet Security Appliances to dramatically streamline VPN deployment and management. Using SonicWALL's Client Policy Provisioning technology, the SonicWALL administrator establishes the VPN connections policies for the Global VPN Clients. The VPN configuration data is transparently downloaded from the SonicWALL VPN Gateway (SonicWALL Internet Security Appliance) to Global VPN Clients, removing the burden of provisioning VPN connections from the user.

SonicWALL Global VPN Client Features

The SonicWALL Global VPN Client delivers a robust IPSec VPN solution with these features:

- **Easy to Use** - Provides an easy-to-follow Installation Wizard to quickly install the product, an easy-to-follow Configuration Wizard with common VPN deployment scenarios, point-and-click activation of VPN connections, and streamlined management tools to minimize support requirements.
- **Client Policy Provisioning** - Using only the IP address or Fully Qualified Domain Name (FQDN) of the SonicWALL VPN gateway, the VPN configuration data is automatically downloaded from the SonicWALL VPN gateway via a secure IPSec tunnel, removing the burden from the remote user of provisioning VPN connections.
- **XAUTH Authentication with RADIUS** - Provides added security with user authentication after the client has been authenticated via a RADIUS server.
- **VPN Session Reliability** - Allows automatic redirect in case of a SonicWALL VPN gateway failure. If a SonicWALL VPN gateway is down then the Global VPN Client can go through another SonicWALL VPN gateway.
- **Multiple Subnet Support** - Allows Global VPN Client connections to more than one subnet in the configuration to increase networking flexibility.
- **Third-Party Certificate Support** - Supports VeriSign, Entrust, Microsoft, and Netscape Certificate Authorities (CAs) for enhanced user authentication.
- **Tunnel All Support** - Provides enhanced security by blocking all traffic not directed to the VPN tunnel to prevent Internet attacks from entering the corporate network through a VPN connection.
- **DHCP over VPN Support** - Allows IP address provisioning across a VPN tunnel for the corporate network while allowing WAN DHCP for Internet Access from the ISP.
- **Secure VPN Configuration** - Critical Global VPN Client configuration information is locked from the user to prevent tampering.
- **AES and 3DES Encryption** - Supports 168-bit key 3DES (Data Encryption Standard) and the new U.S. Government encryption standard AES (Advanced Encryption Standard) for dramatically increased security. AES requires SonicOS 2.0.
- **GMS Management** - Allows Global VPN Client connections to be managed by SonicWALL's award-winning Global Management System (GMS).
- **Multi-Platform Client Support** - Supports Windows 2000 Professional (service pack 3 or later) and 32-bit and 64-bit versions of Windows XP, Windows Vista, Windows Server 2003/2008, and Windows 7.
- **NAT Traversal -** Enables Global VPN Client connections to be initiated from behind any device performing NAT (Network Address Translation). The SonicWALL Global VPN Client encapsulates IPSec VPN traffic to pass through NAT devices, which are widely deployed to allow local networks to use one external IP address for an entire network.

- **Automatic Reconnect When Error Occurs** - Allows the Global VPN Client to keep retrying a connection if it encounters a problem connecting to a peer. This feature allows the Global VPN Client to automatically make a connection to a SonicWALL VPN gateway that is temporarily disabled, without manual intervention.
- **Ghost Installation for Large Scale Installations** - Enables the Global VPN Client's virtual adapter to get its default address after installation and then create a ghost image.
- **NT Domain Logon Script Support** - Allows Global VPN Clients to perform Windows NT/2000 domain authentication after establishing a secure IPSec tunnel. The SonicWALL VPN gateway passes the logon script as part of the Global VPN Client configuration. This feature allows the VPN user to have access to mapped network drives and other network services.
- **Dual Processor Support** - Enables the Global VPN Client to operate on dual-processor computers.
- **Group Policy Management** - Global VPN Clients access can be customized and restricted to specific subnet access (Requires SonicOS Enhanced).
- **Hub and Spoke VPN Access** - Allows IP addressing from SonicWALL VPN Gateway's DHCP Server to Global VPN Client for configuring a different subnet for all remote Global VPN Clients than the subnet of the LAN. Makes hub-and-spoke VPN access simpler. When a Global VPN Client successfully authenticates with the central site, it receives a virtual IP address that also grants it access to other trusted VPN sites.
- **Default VPN Connections File** - Enables the SonicWALL administrator to configure and distribute the corporate VPN connections with the Global VPN Client software to streamline VPN client deployment.
- **Integration with Dial-Up Adapter** - Allows Global VPN Client connections using Microsoft Dial-Up Networking or third-party dial-up applications either as an automatic backup to a broadband connection or as the primary connection.
- **Single VPN Connection to any SonicWALL Secure Wireless Appliance for Roaming** - Allows users to use a single VPN connection to access the networks of multiple SonicWALL Secure Wireless appliances.
- **Automatic Configuration of Redundant Gateways from DNS** - When an IPSec gateway domain name resolves to multiple IP addresses, the Global VPN Client (version 2.1.0.0 or higher) uses the IP addresses in the list as failover gateways.
- **Tunnel State Display Enhancement** - The Global VPN Client now provides additional information about the state of VPN tunnels. In addition to the states of enabled, disabled, and connected, the Global VPN Client now indicates when tunnels are authenticating, provisioning, and connecting.
- **Tunnel Status Pop-Up Window** - The Global VPN Client now alerts users when tunnels are connected or disconnected by displaying a small pop-up window.
- **Smart Card and USB Token Authentication -** The Global VPN Client is now integrated with the Microsoft Cryptographic Application Program (MS CryptoAPI or MSCAPI), which enables the Global VPN Client to support user authentication using digital certificates on Smart cards and USB tokens.
- **NAT-T RFC 3947 Support** - Allows for automatic detection of NAT along the path between two IKE peers during IKE Phase 1 negotiation. On detection of NAT in middle, packets are UDP encapsulated using port 4500.
- **DNS Redirect** - DNS queries to DNS suffix associated with Virtual Adapter are not sent on the physical adapter.
- **Tunnel All Support Enhancement** - Provides the ability to route clear traffic to directly connected network interfaces that are configured with the Route All policy, which is generally used in the WLAN zone.
- **Program Auto-Start on VPN Connection** - Automatically launches a program, with optional arguments, when successful VPN connections are established, as specified in the **Connection Properties** dialog box.

Global VPN Client Enterprise

Global VPN Client Enterprise provides the same functionality as the Global VPN Client with the added feature of license sharing.

About this Guide

The *SonicWALL Global VPN Client Administrator's Guide* provides complete documentation on installing, configuring, and managing the SonicWALL Global VPN Client 4.6. This guide also provides instructions for SonicWALL Global VPN Client 4.6 Enterprise.

The SonicWALL Global VPN Client operates on Windows 2000 Professional (service pack 3 or later) and 32-bit and 64-bit versions of Windows XP, Windows Vista, Windows Server 2003/2008, and Windows 7 client operating systems. The Global VPN Client is supported on all SonicWALL security appliances running Gen3 (6.6 and higher), Gen4 (1.0 and higher), and Gen5 (5.0 and higher) SonicOS firmware versions.

For configuring your SonicWALL security appliance to support Global VPN Clients using SonicWALL's GroupVPN, see the *Administrator's Guide* for the firmware or SonicOS version running on your SonicWALL security appliance.

Tip! *Always check http://www.sonicwall.com/support/VPN_documentation.html for the latest version of this manual and other upgrade manuals as well.*

Conventions Used in this Guide

Conventions used in this guide are as follows:

Convention	Use
Bold	Highlights items you can select on the Global VPN Client interface or the SonicWALL Management Interface.
Italic	Highlights a value to enter into a field. For example, "type *192.168.168.168* in the **IP Address** field."
>	Indicates a multiple step menu choice. For example, "select **File>Open**" means "select the **File** menu, then select the **Open** item from the **File** menu.

Icons Used in this Guide

Alert! *Important information about features that can affect performance, security features, or cause potential problems with your SonicWALL.*

Tip! *Useful information about security features and configurations on your SonicWALL.*

Note! *Related information to the topic.*

Copyright Notice

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Getting Started with the SonicWALL Global VPN Client

This section provides information about installing and launching the SonicWALL Global VPN Client.

Installing the SonicWALL Global VPN Client

The SonicWALL Global VPN Client uses an easy-to-use wizard to guide you through the installation process. The Global VPN Client supports Windows 2000 Professional (service pack 3 or later) and 32-bit and 64-bit versions of Windows XP, Windows Vista, Windows Server 2003/2008, and Windows 7.

Alert! *If you are upgrading SonicWALL Global VPN Client from an earlier version to version 4.6.x, you must uninstall the earlier version before installing Global VPN Client 4.6.x.*

Alert! *Installing the Global VPN Client on Windows XP or later requires Administrator rights.*

The SonicWALL Global VPN Client requires a SonicWALL Internet Security Appliance running firmware version 6.6 (or higher), SonicOS 1.0.0.0 (or higher), SonicOS Standard 2.0.0.0 (or higher), or SonicOS Enhanced 2.0.0.0 (or higher).

Tip! *For information on the number of SonicWALL Global VPN Client connections supported by your SonicWALL and Global VPN Client licensing for your SonicWALL, see "SonicWALL Global VPN Client Licenses" on page 37.*

Using the Setup Wizard

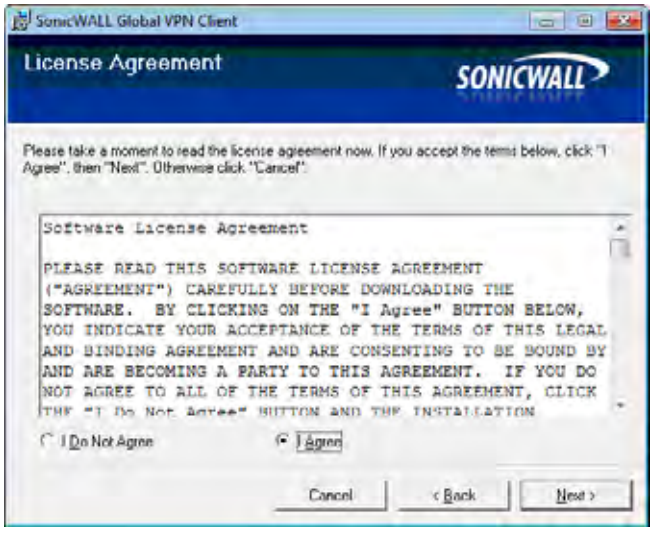
The following steps explain how to install the SonicWALL Global VPN Client program using the **Setup Wizard**. You use the **Setup Wizard** for a new Global VPN Client installation. If you're upgrading your Global VPN Client software, the **Setup Wizard** doesn't display all the same pages as a new installation.

Alert! *Remove any installed 3rd Party VPN client program before installing the SonicWALL Global VPN Client.*

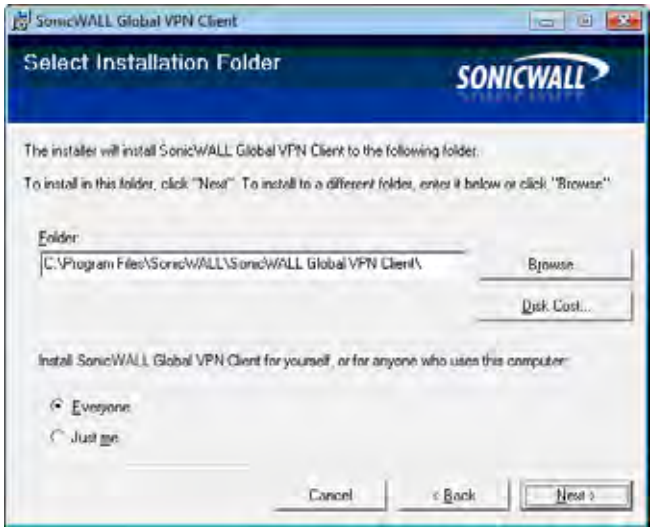
To use the Setup Wizard, perform the following steps:

1. After downloading 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, double-click **GVCSetupXX.exe**. The **Setup Wizard** launches.

2. Click **Next** to continue installation of the VPN Client.
3. In the **License Agreement** screen, select **I Agree** and then click **Next**.

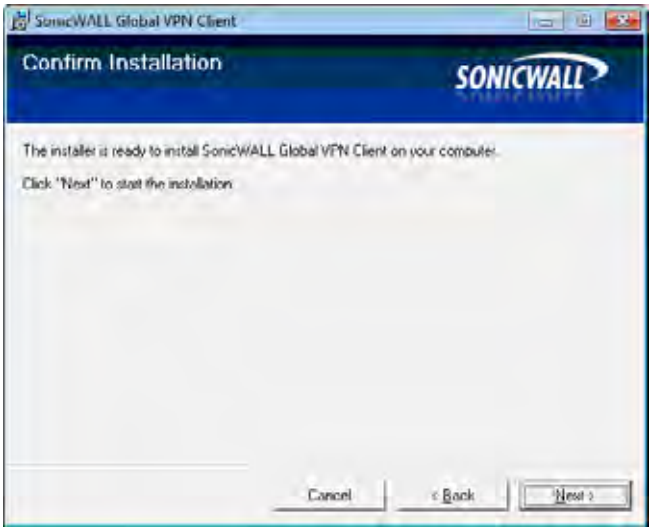


4. In the **Select Installation Folder** screen, optionally click **Browse** to specify a custom installation location.

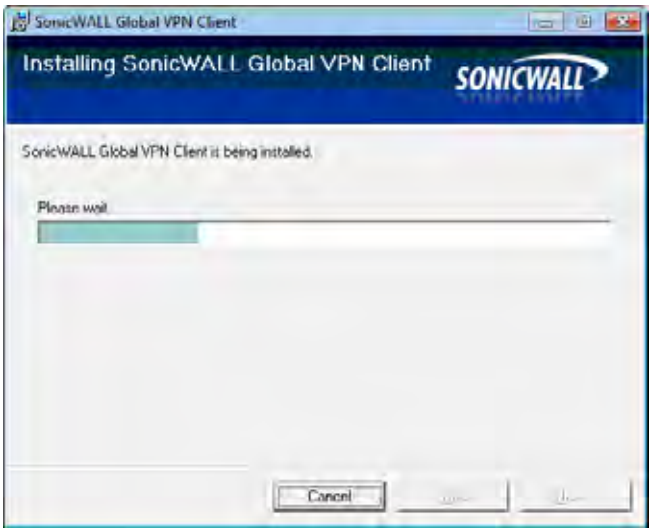


5. Under **Install SonicWALL Global VPN Client for yourself, or for anyone who uses this computer**, select either **Everyone** or **Just me**, and then click **Next**.

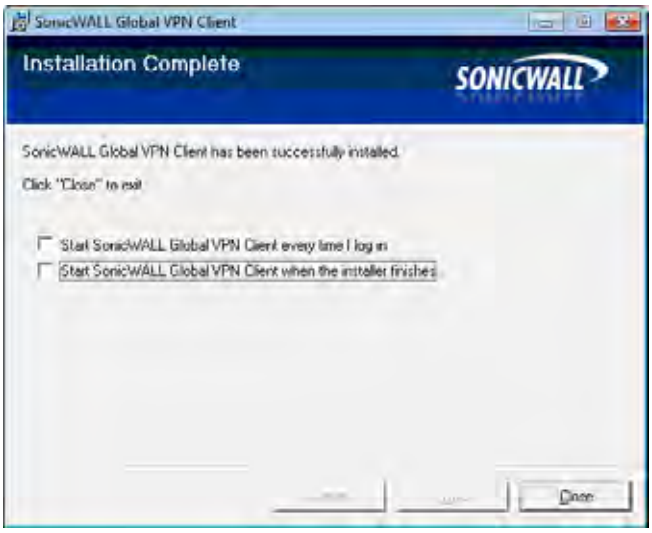
6. In the **Confirm Installation** screen, click **Next** to begin the installation.



7. Wait while the SonicWALL Global VPN Client files are installed on your computer.



8. In the **Installation Complete** screen, optionally select **Start SonicWALL Global VPN Client every time I log in** to automatically launch the VPN Global Client when you log onto the computer.



9. Optionally, select **Start SonicWALL Global VPN Client when the installer finishes** to automatically launch the Global VPN Client after finishing the installation.
10. Click **Close**.
    You may see a dialog box regarding the restart of your system at the end of the installation. If you see this message, then you need to reboot your system in order for the installation to complete.

Installing the Global VPN Client with a Ghost Application

The installation process is the same when using a ghost application as it is for normal installation. **DO NOT OPEN** the Global VPN Client application after installing it and BEFORE you ghost it. The FIRST time that the Global VPN Client is started after a ghost install, it randomly creates a unique MAC address for the SonicWALL VPN Adapter.

Alert! *If you open the Global VPN Client BEFORE using ghost, you receive the same MAC address on each ghosted installation for the SonicWALL VPN Adapter, resulting in network conflicts.*

Command Line Options for Installation

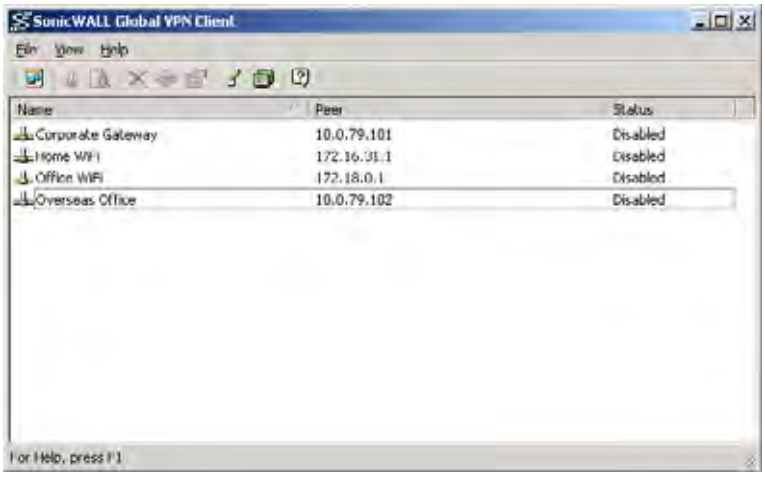
There are several command line options available for SonicWALL Global VPN Client installation.

All options are case-insensitive and must be preceded by a forward slash (*/*). The following options are available:

- **Q** – Quiet mode. A normal (non-silent) installation of the SonicWALL Global VPN Client receives the necessary input from the user in the form of responses to dialog boxes. However, a silent installation does not prompt the user for any input, but instead, uses the defaults for every option. Simply type in the following where **XX** is either **32** for 32-bit Windows platforms or **64** for 64-bit Windows platforms:
  GVCSetupXX.exe /q
- **T** – Specify a temporary working folder in which to place any temporary files generated during the installation process. The T option must be followed by a colon (**:**) and the full path to the folder that you want to use. For example, type in the following:
  GVCSetupXX.exe /t:C:\TemporaryFiles
- **C** – Place all files extracted (MSI Installer file) from the install package into the folder specified in the **T** option. The **C** option is only valid when used together with the **T** option. For example, type one of the following:
  GVCSetupXX.exe /c /t:C:\TemporaryFiles
  GVCSetupXX.exe /T:C:\TemporaryFiles /C
- **C:<Cmd>** – This command is unused at present.

Launching the SonicWALL Global VPN Client

To launch the SonicWALL Global VPN Client, choose **Start>Programs>SonicWALL Global VPN Client**.



If you click **Close,** press **Alt+F4** or choose **File>Close**, the SonicWALL Global VPN Client window closes but your established VPN connections remain active. A message dialog box appears notifying you that the Global VPN Client program and any enabled connections will remain active after the window is closed. If you don't want this notification message to display every time you close the Global VPN Client window, check **Don't show me this message again** and then click **OK**.

You can open the SonicWALL Global VPN Client window by double-clicking the SonicWALL Global VPN Client icon in the system tray or right-clicking the icon, and selecting **Open SonicWALL Global VPN Client**.

Alert! *Exiting the SonicWALL Global VPN Client from the system tray icon menu disables any active VPN connections.*

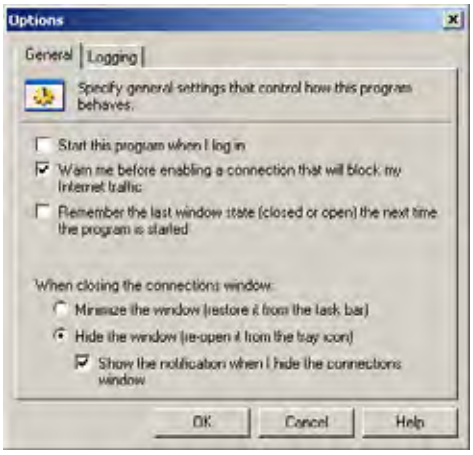
Tip! *You can change the default launch setting for SonicWALL Global VPN Client, see "Specifying Global VPN Client Launch Options" on page 10 for more information.*

Tip! *You can create a shortcut to automatically launch the* ***SonicWALL Global VPN Client*** *window and make the VPN connection from the desktop, taskbar, or Start menu. See "Creating a Connection Shortcut" on page 22 for more information.*

Tip! *You can launch the SonicWALL Global VPN Client from the command line, See "Appendix B - Running the Global VPN Client from the CLI" on page 49 for more information.*

Specifying Global VPN Client Launch Options

You can specify how the SonicWALL Global VPN Client launches and what notification windows appear using the controls in the **General** tab of the **Options** dialog box. Choose **View>Options** to display the **Options** dialog box.



The **General** page includes the following settings to control the launch of the Global VPN Client:

- **Start this program when I log in** - Launches the SonicWALL Global VPN Client when you log into your computer.
- **Warn me before enabling a connection that will block my Internet traffic**. Activates **Connection Warning** message notifying you that the VPN connection will block local Internet and network traffic.
- **Remember the last window state (closed or open) the next time the program is started** - Allows the Global VPN Client to remember the last window state (open or closed) the next time the program is started. For example, a user can launch the Global VPN Client from the system tray without opening a window on the desktop.
- **When closing the connections window** - Specifies how the Global VPN Client behaves when the window is closed. The three options include

  Minimize the window (restore it from the task bar) - Minimizes the window to taskbar and restores it from the taskbar.

  Hide the window (re-open it from the tray icon) - The default setting that hides the SonicWALL Global VPN Client window when you close it. You can open the Global VPN Client from the program icon in the system tray. Enabling this setting also displays the **Show the notification when I hide the connections window** checkbox.

  Show the notification when I hide the connections window - Checking this box activates the **SonicWALL Global VPN Client Hide Notification** window whenever you close the Global VPN Client window while the program is still running. The message tells you that the Global VPN Client program continues to run after you close (hide) the window.

Managing the Global VPN Client System Tray Icon

When you launch the SonicWALL Global VPN Client window, the program icon appears in the system tray on the taskbar.

This icon provides program and VPN connection status indicators as well as a menu for common SonicWALL Global VPN Client commands. Right clicking on the SonicWALL Global VPN Client icon in the system tray displays a menu of options for managing the program.

- **Open SonicWALL Global VPN Client** - Opens the program window.
- **Enable** - Displays a menu of VPN connections that can be enabled.
- **Disable** - Displays a menu of VPN connections that can be disabled.
- **Open Log Viewer** - Opens the Log Viewer to view informational and error messages. See “Understanding the Global VPN Client Log” on page 32 for more information on the Log Viewer.
- **Open Certificate Manager** - Opens the Certificate Manager. See “Managing Certificates” on page 31 for more information on the Certificate Manager.
- **Exit** - Exits the SonicWALL Global VPN Client window and disables any active VPN connections.

Moving the mouse pointer over the SonicWALL Global VPN Client icon in the system tray displays the number of enabled VPN connections.

The Global VPN Client icon in the system tray also acts as a visual indicator of data passing between the Global VPN Client and the SonicWALL gateway.

Adding VPN Connections

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 from the Global VPN Client user. VPN connections can be created using three methods:

- Download the VPN policy from the SonicWALL VPN Gateway to the Global VPN Client using the **New Connection Wizard**. This wizard walks you through the process of locating the source of your configuration information and automatically downloads the VPN configuration information over a secure IPSec VPN tunnel.
- Import a VPN policy file into the SonicWALL Global VPN Client. The VPN policy is sent to you as a **.rcf** file, which you install using the **Import Connection** dialog box.
- Install the **default.rcf** file as part of the Global VPN Client software installation or add it after installing the Global VPN Client. If the SonicWALL VPN Gateway administrator included the **default.rcf** file as part of the Global VPN Client software, when the program is installed, one or more preconfigured VPN connections are automatically created.

Note! *Creating a **Default.rcf** file and distributing it with the Global VPN Client software allows the SonicWALL VPN Gateway administrator to streamline VPN client deployment and allow users to quickly establish VPN connections. When the Global VPN Client software is installed, the VPN policy created by the SonicWALL VPN Gateway administrator is automatically created. For more information on creating the **Default.rcf** file, see "Appendix A - Using the Default.rcf File for Global VPN Clients" on page 41.*

Alert! *Your SonicWALL must be configured with GroupVPN to facilitate the automatic provisioning of Global VPN Clients. For instructions on configuring your SonicWALL with GroupVPN, see your SonicWALL Administrator's Guide.*

Note! *For instructions on importing a certificate into the Global VPN Client, see "Using Certificates" on page 31.*

Understanding VPN Connections

The Global VPN Client allows multiple connections to be configured at the same time, whether they are provisioned from multiple gateways or imported from one or more files. Because connections may be provisioned from multiple gateways, each connection explicitly states allowed behavior in the presence of any connection policy conflicts. You may have VPN connections that don't allow other VPN connections or Internet and network connections while the VPN policy is enabled.

The VPN connection policy includes all the parameters necessary to establish secure IPSec tunnels to the gateway. A connection policy includes Phase 1 and Phase 2 Security Associations (SA) parameters including:

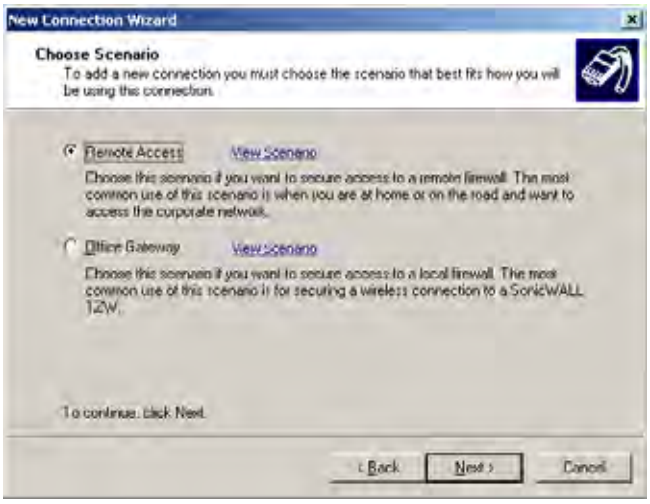
- Encryption and authentication proposals
- Phase 1 identity payload type
- Phase 2 proxy IDs (traffic selectors)
- Client Phase 1 credential
- Allowed behavior of connection in presence of other active connections
- Client caching behavior

Creating a VPN Connection Using the New Connection Wizard

The following instructions explain how to use the **New Connection Wizard** to automatically download a VPN connection policy for the Global VPN Client from a local or remote SonicWALL VPN gateway.

1. Choose **Start>Programs>SonicWALL Global VPN Client**. The first time you open the SonicWALL Global VPN Client, the **New Connection Wizard** automatically launches.

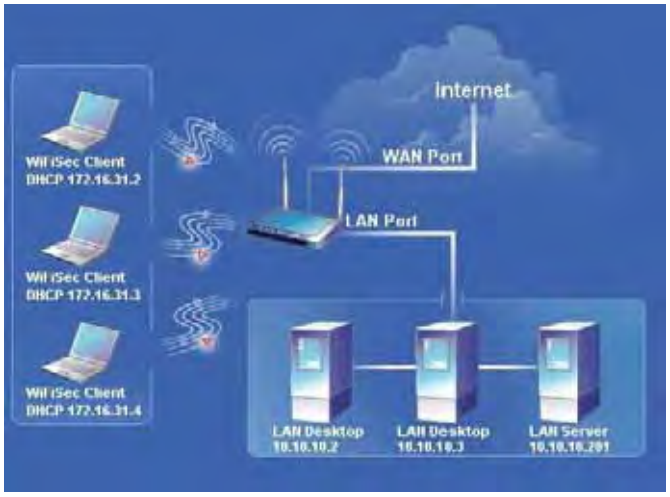
2. If the **New Connection Wizard** does not display, click the **New Connection Wizard** icon to launch the **New Connection Wizard**. Click **Next**.
3. In the **Choose Scenario** page, you can click on **View Scenario** to view a diagram of each type of VPN connection.



- **Remote Access** - You choose this scenario if you want secure access to a remote VPN gateway from any wired or wireless network. The most common use of this scenario is when you are at home or on the road and want access to the corporate network. You enter the IP address or FQDN (gateway.yourcompany.com) of the VPN gateway and the Global VPN Client automatically downloads the VPN connection policy from the remote SonicWALL VPN gateway.

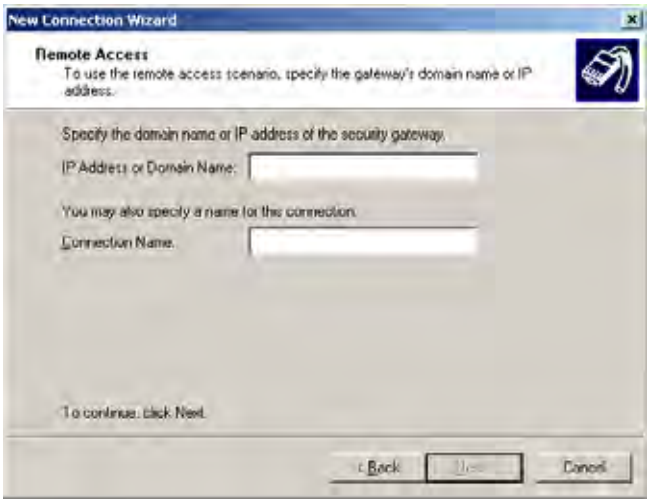
Clicking on the **Remote Access View Scenario** links displays the diagram for this type of VPN connection.

- **Office Gateway** - You choose this scenario if you want secure access to a local SonicWALL Secure Wireless appliance network. When you create an **Office Gateway** VPN connection, it appears as the **Peer** entry of **<Default Gateway>** in the **SonicWALL Global VPN Client** window. You can use this single **Office Gateway** VPN connection to roam securely across SonicWALL Secure Wireless appliance networks.
  Clicking on the **Office Gateway View Scenario** link displays the diagram for this type of VPN connection.



4. Select **Remote Access** or **Office Gateway** and then click **Next**.

5. If you selected **Remote Access** in the **Choose Scenario page**, the **Remote Access** page is displayed. Type 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. If you want a different name for your connection, type the new name for your VPN connection in the **Connection Name** field. Click **Next**. The **Completing the New Connection Wizard** page is displayed.



6. If you selected Office Gateway in the Choose Scenario page, the **Completing the New Connection Wizard** page is displayed.

7. In the **Completing the New Connection Wizard** page select any of the following options:

   Select **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.

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

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

Note! *You can change the default name by right-clicking the **Office Gateway** entry and selecting **Properties** from the menu. In the **General** tab of the **Properties** dialog box, enter the new name in the **Name** field.*

Importing a VPN Configuration File

A VPN connection can be created as a file and sent to you by the SonicWALL VPN gateway administrator. This VPN configuration file has the filename extension **.rcf**. If you received a VPN connection file from your administrator, you can install it using the **Import Connection** dialog box.

The VPN policy file is in the XML format to provide more efficient encoding of policy information. Because the file can be encrypted, pre-shared keys can also be exported in the file. The encryption method is specified in the PKCS#5 Password-Based Cryptography Standard from RSA Laboratories and uses Triple-DES encryption and SHA-1 message digest algorithms.

Alert! *If the **.rcf** file exported from the SonicWALL appliance is encrypted, you must have the password to import the configuration file into the Global VPN Client.*

The following instructions explain how to add a VPN connection by importing a connection file provided by your gateway administrator.

1. Choose **Start>Programs>SonicWALL Global VPN Client**.
2. Select **File>Import**. The **Import Connection** dialog box is displayed.

3. Type the file path for the configuration file in the **Specify the name of the configuration file to import** field or click the browse **...** button to locate the file. If the file is encrypted, enter the password in the **If the file is encrypted, specify the password** field.
4. Click **OK**.

Configuring a Dial-Up VPN Connection

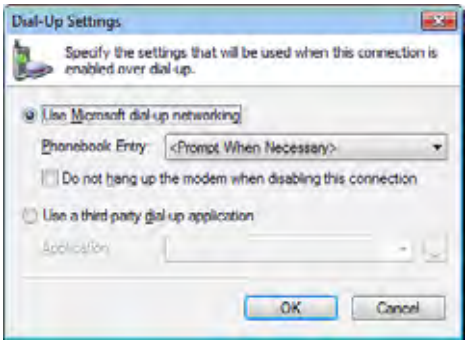
You can use a dial-up Internet connection to establish your VPN connection. You can create a **Remote Access** VPN connection using the **Make New Connection** wizard or use an existing VPN connection, and then configure the VPN connection to use a Microsoft Dial-Up Networking phone book entry or a third-party dial-up application. You can also use a dial-up connection as an automatic backup for your VPN connection in the event your broadband Internet connection is disabled.

Alert! *Make sure you create your dial-up connection profile using Microsoft Dial-up Networking or your third-party dial-up application **before** configuring your dial-up VPN connection.*

1. Create a VPN connection using the **New Connection Wizard** or use an existing VPN connection.
2. Right-click the VPN connection and select **Properties** from the menu. The **Properties** dialog box is displayed.
3. Click the **Peers** tab.

4. Click **Edit**. The **Peer Information** dialog box is displayed.

5. Use the default **Automatic** option in the **Interface Selection** menu, if you want the Global VPN Client to automatically determine whether to use the LAN or Dial-Up interface based on availability. If the LAN interface is active, the Global VPN Client uses this interface first. If the LAN interface is not available, the Global VPN Client uses the dial-up connection. If you want this VPN connection to use a dial-up connection, select **Dial-Up Only** from the **Interface Selection** menu.
6. Click **Dial-Up Settings**. The **Dial-Up Settings** dialog box is displayed.



7. If you're using Microsoft Dial-Up Networking, check **Use Microsoft dial-up networking** and select the dial-up networking profile from the **Phonebook Entry** list. Select **Do not hang up the modem when disabling this connection**, if you want to remain connected to the Internet after disabling the Global VPN Client connection.
8. If you're using a third-party dial-up application, select **Use a third-party dial-up application**, and then enter the path for the program in the **Application** field or click browse **...** to locate the program.
9. Click OK three times to return to the **SonicWALL Global VPN Client** window.

Using SonicWALL Global VPN Client from a Different Workstation

Using the SonicWALL Global VPN Client to connect to a Microsoft Network has certain limitations. Typically, when a computer is attached to a Microsoft Network it has a persistent network connection to the domain controller that is used to verify the user credentials. When the user credentials have been verified by the domain controller, the computer then creates a locally cached profile that is used when the

domain controller is not available. However, the SonicWALL Global VPN Client provides an ad hoc secure network connection over the Internet back to the Microsoft Network containing the domain controller and thus is not a persistent connection. Since the remote computer cannot connect to the domain controller to verify the logon credentials until the connection is provided by the SonicWALL Global VPN Client, the logon fails unless a locally cached profile is available.

The following steps illustrate the classic problem:

1. A SonicWALL Global VPN Client session must be established to communicate remotely with a Microsoft domain controller.
2. SonicWALL Global VPN Client can only be launched after you have logged on to the workstation. Because there is no way for the SonicWALL Global VPN Client to connect before you log on, you cannot use it for domain logon when initially logging on.
3. If you have logged on to the workstation before, there will be a locally cached profile that is used to log on.
   a) You can then start the SonicWALL Global VPN Client, and a connection to the domain is established.
   b) After connecting to the domain, you can run logon scripts, change password, access domain resources, etc.
   c) When you log off, the SonicWALL Global VPN Client terminates, preventing domain communications.
4. If you have never logged on to the workstation before, there will not be a locally cached profile, so logon will not be possible.

Because logging off (step 3c) terminates the SonicWALL Global VPN Client, it has historically precluded a different user from logging on and creating a new locally cached profile. This has the undesirable effect that only a user with a pre-existing (locally cached) profile can log on over the SonicWALL Global VPN Client.

The standard workaround for this is to first connect locally to the domain controller and logon with each account expected to use the SonicWALL Global VPN Client. This creates a locally cached profile for each account and enables client logon without connection to the Domain Controller.

The unfortunate result of this workaround is that a user without a cached profile on the computer cannot logon without a sojourn to the network containing the domain controller. This can be extremely cumbersome in certain situations such as being located at the Dumont d' Urville research station and trying to get back to your main office in Svalbard.

Workaround – Forced Creation of a New Locally Cached Profile

The workaround is to create an induced local profile, and then log on to the Microsoft domain using the SonicWALL Global VPN Client. To do this, perform the following steps:

1. Log on to the workstation with any locally cached profile (e.g. mydomain\user1, or a local machine account). The locally cached profiles are usually stored in the C:\Documents and Settings directory. You should see a folder called user1 in this path containing user1's profile.
2. Launch the SonicWALL Global VPN Client.
3. After the SonicWALL Global VPN Client establishes a connection and the workstation can communicate with the domain controller, you can create another locally cached profile. You can use the **runas** command to create a locally cached profile for a new user (e.g. mydomain\user2) while using the SonicWALL Global VPN Client connection provided by user1.
4. From a command prompt, type: **runas /user:mydomain\user2 explorer.exe** (substitute your actual domain for mydomain and actual username for user2). You can use notepad.exe instead of explorer.exe if you prefer.
5. At the prompt, enter the domain password for user2.

6. It will take anywhere from a few seconds to a few minutes to create the local profile for user2, and to launch the explorer.exe program. You may quit the explorer.exe program after it launches.
7. The C:\Documents and Settings directory should now contain a folder for user2.
8. Close the SonicWALL Global VPN Client, and log off as user1 from the workstation. You will see the familiar **Log On to Windows** dialog box.
9. Log onto the workstation as user2 using the newly created locally cached profile.
10. Launch the SonicWALL Global VPN Client. The user2 profile will now provide the credentials for all domain access (including running logon scripts).
11. You can repeat this procedure as many times as necessary to create additional profiles.
12. It is also possible to change an expired user password with this procedure if you have another account available to make the SonicWALL Global VPN Client connection back to the domain controller. A simple way to change passwords is from the Windows Security dialog box, accessed by pressing **Ctrl+Alt+Delete**. In the dialog box, click **Change Password….** This brings up the Change Password dialog box, from which you can change the expired password.

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 SonicWALL administrator sets the parameters for what is allowed and not allowed with the VPN connection. For example, for security reasons, the SonicWALL VPN Gateway 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 and 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.

Accessing Redundant VPN Gateways

The Global VPN Client supports redundant VPN gateways by manually adding the peer in the **Peers** page of the VPN connection **Properties** dialog box. The Global VPN Client version 2.1.0.0 (or higher) adds automatic support for redundant VPN gateways if the IPSec gateway's domain name resolves to multiple IP address. For example, if *gateway.yourcompany.com* resolves to 67.115.118.7, 67.115.118.8 and 67.115.118.9, the Global VPN Client cycles through these resolved IP addresses until it finds a gateway that responds, allowing multiple IP addresses to be used as failover gateways. If all the resolved IP addresses fail to respond, Global VPN Client switches to the next peer, if another peer is specified in the **Peers** page of the VPN connection **Properties** dialog box. See “Peers” on page 27 for more information.

Note! *When configuring redundant VPN gateways, the Group VPN policy attributes (such as pre-shared keys and the attributes on the Peer Information window) must be the same for every gateway if the gateway's FQDN resolves to multiple IP addresses. However, if you set up multiple peers on the Peers page, then each peer gateway can have its own settings.*

Enabling a VPN Connection

Enabling a VPN connection with the SonicWALL Global VPN Client is a transparent two phase process. Phase 1 enables the connection, which completes the ISAKMP (Internet Security Association and Key

Management Protocol) negotiation. Phase 2 is IKE (Internet Key Exchange) negotiation, which establishes the VPN tunnel for sending and receiving data.

When you enable a VPN connection, the following information is displayed in the Status column of the **SonicWALL Global VPN Client** window:

1. **Disabled** changes to **Connecting**.
2. **Connecting** changes to **Authenticating** when the **Enter Username/Password** dialog box is displayed.
3. **Authenticating** changes to **Connecting** when the user enters the username and password.
4. **Connecting** changes to **Provisioning**.
5. **Provisioning** changes to **Connected** once the VPN connection is fully established. A green checkmark is displayed on the VPN connection icon.

Once the VPN connection is established, a pop-up notification is displayed from the Global VPN Client system tray icon. It displays the **Connection Name**, **Connected to IP address** and the **Virtual IP Address**.

If an error occurs during the VPN connection, **Error** appears in the **Status** column and an error mark (red x) appears on the VPN connection icon. A VPN connection that doesn't successfully complete all phase 2 connections displays a yellow warning symbol on the connection icon.

Note! *If the Global VPN Client doesn't establish the VPN connection, you can use the **Log Viewer** to view the error messages to troubleshoot the problem. See "Understanding the Global VPN Client Log" on page 32 for more information.*

To establish a VPN connection using the Global VPN Client, follow these instructions.

1. Enable a VPN connection using one of the following methods:

- If you selected **Enable this connection when the program is launched** in the **New Connection Wizard**, the VPN connection is automatically established when you launch the SonicWALL Global VPN Client.
- If your VPN connection isn't 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 **SonicWALL Global VPN Client** window.

2. Depending on how the VPN connection is configured, the **Cannot Enable Connection**, **Enter Pre-Shared Secret**, **Enter Username and Password**, and **Connection Warning** dialog boxes may be displayed, which are explained in the following sections.

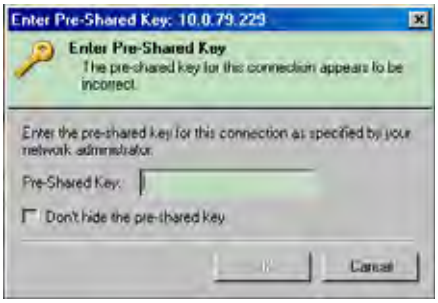
Establishing Multiple Connections

You can have more than one connection enabled at a time but it depends on the connection parameters established at the VPN gateway. If you attempt to enable a subsequent VPN connection with a currently enabled VPN connection policy that does not allow multiple VPN connections, the **Cannot Enable Connection** message appears informing you the VPN connection cannot be made because the currently

active VPN policy does not allow multiple active VPN connection. The currently enabled VPN connection must be disabled before enabling the new VPN connection.

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 in order to make your VPN connection. If the default Pre-Shared Key is not included as part of the connection policy download or file, the **Enter Pre-Shared Key** dialog box appears to prompt you for the Pre-Shared key before establishing the VPN connection.

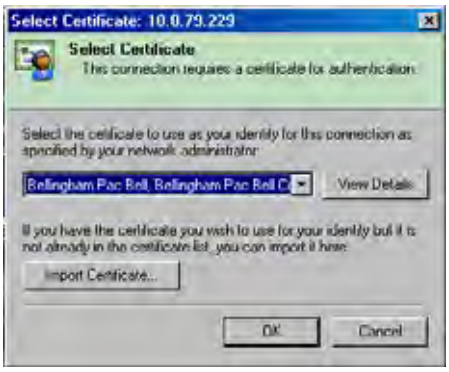


1. Type your Pre-Shared Key in the **Pre-shared Key** field. The Pre-Shared Key is masked for security purposes.
2. If you want to make sure you're entering the correct Pre-Shared Key, check **Don't hide the pre-shared key**. The Pre-Shared Key you enter appears unmasked in the **Pre-shared Key** field.
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 box appears. This dialog box lists all the available certificates installed on your Global VPN Client. Select the certificate from the menu, then click **OK**. If you have a

certificate that has not been imported into the Global VPN Client using **Certificate Manager**, click **Import Certificate**.



Note! *See "Managing Certificates" on page 31 for more information on using the* ***Certificate Manager****.*

Username and Password Authentication

The VPN gateway typically specifies the use of XAUTH for determining GroupVPN policy membership by requiring a username and password either for authentication against the gateway's internal user database or via an external RADIUS service.

If the SonicWALL VPN gateway is provisioned to prompt you for the username and password to enter the remote network, the **Enter Username and Password** dialog box appears. Type your username and password. If permitted by the gatewa y, check **Remember Username and Password** to cache your username and password to automatically log in for future VPN connections. Click **OK** to continue with establishing your VPN connection.

Creating a Connection Shortcut

To streamline enabling a VPN connection, you can place a VPN connection on the desktop, taskbar, or Start menu. You can also place the connection at any other location on your system.

To create a shortcut:

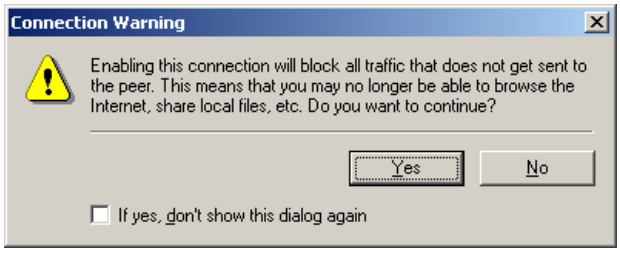
1. Select the VPN connection you want to create a shortcut for in the SonicWALL Global VPN Client window.
2. Choose **File>Create Shortcut** and select the shortcut option you want. You can select from **On the Desktop**, **On the Task Bar**, **In the Start Menu**, or **Select a Location**.

You can also right-click the VPN connection and then choose **Create Shortcut>***shortcut option*.

Tip! *You can also create a Desktop shortcut for the SonicWALL Global VPN Client program for easy access to all your connections.*

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 checking **If yes, don't show this dialog box again**. Click **Yes** to continue with establishing your VPN connection.

Managing Current VPN Connections

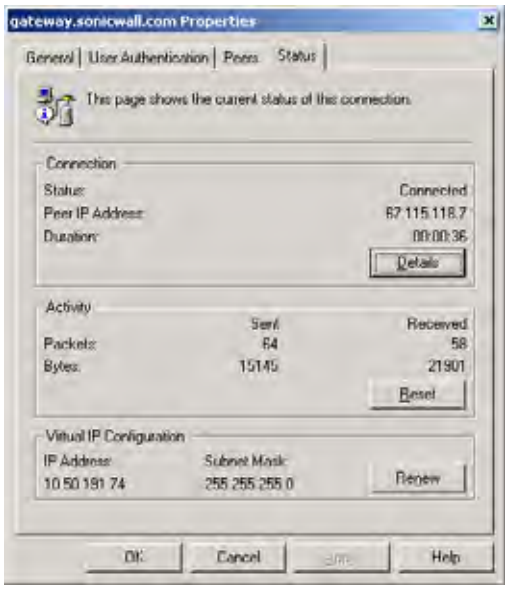
The SonicWALL Global VPN Client allows you to check the status of current VPN connections or to disable a current VPN connection.

Checking the Status of a VPN Connection

The SonicWALL Global VPN Client includes a variety of indicators to determine the status of your VPN connections. The main SonicWALL Global VPN Client window lists your VPN connections and their respective status: **Disabled**, **Enabled**, **Connected**, or **Error**.

- A successfully connected VPN policy is indicated by a green check mark on the policy icon.
- A VPN policy that doesn't successfully complete all phase 2 connections displays a yellow warning on the policy icon.
- A VPN policy that cannot be successfully connected displays an error mark (red **x)** on the policy icon.
- The SonicWALL Global VPN Client icon in the system tray displays a visual indicator of data passing between the Global VPN Client and the gateway.
- The **Status** page in the **Properties** dialog box displays more detailed information about the status of an active VPN connection. To display the **Status** tab for any VPN connection, use one of the following methods:
  - Double-click the active VPN connection.
  - Select the VPN connection, then press **Ctrl+T**.
  - Select the VPN connection, then click the **Status** button on the toolbar.

- Right-click the VPN connection in the SonicWALL Global VPN Client window and select **Status**.



Tip! *For more information on the **Status** page, see "Status" on page 29.*

Disabling a VPN Connection

Disabling a VPN connection terminates the VPN tunnel. You can disable a VPN connection using any of the following methods:

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

Managing VPN Connection Properties

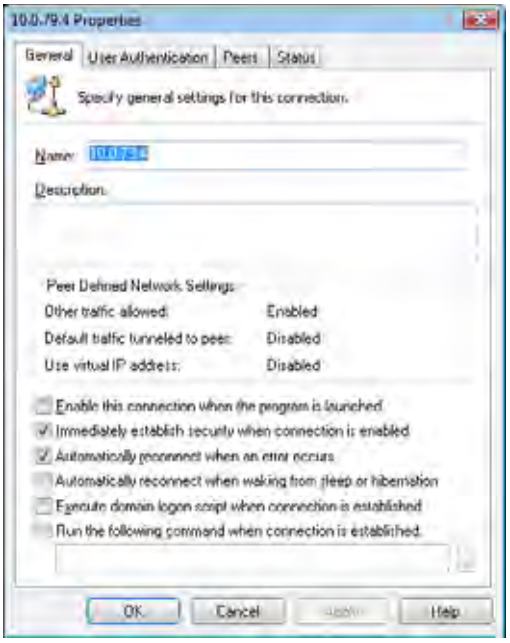
The **Connection Properties** dialog box includes the controls for configuring a specific VPN connection profile. To open the **Connection Properties** dialog box, choose one of the following methods:

- Select the connection and choose **File>Properties**.
- Right click the connection and select **Properties**.
- Select the connection and click the **Properties** button on the SonicWALL Global VPN Client window toolbar.

The **Connection Properties** dialog box includes the **General**, **User Authentication**, **Peers** and **Status** tabs.

General

The **General** page in the **Connection Properties** dialog box includes the following settings:



- **Name** - Displays the name of your VPN connection.
- **Description** - Displays a pop-up text about the connection. The text appears when your mouse pointer moves over the VPN connection.
- **Peer Defined Network Settings** - Defines the status of Tunnel All support. These settings are controlled at the SonicWALL VPN gateway.

  Other traffic allowed - If enabled, your computer can access the local network or Internet connection while the VPN connection is active.

  Default traffic tunneled to peer - If activated, all network traffic not routed to the SonicWALL VPN gateway is blocked. When you enable the VPN connection with this feature active, the **Connection Warning** message appears.

  Use virtual IP address - Allows the VPN Client to get its IP address via DHCP through the VPN tunnel from the gateway.

- **Enable this connection when the program is launched** - Establishes the VPN connection as the default VPN connection when you launch the SonicWALL Global VPN Client.
- **Immediately establish security when connection is enabled** - Negotiates the first phase of IKE as soon as the connection is enabled instead of waiting for network traffic transmission to begin. This setting is enabled by default.
- **Automatically reconnect when an error occurs** - With this feature enabled, if the Global VPN Client encounters a problem connecting to the peer, it keeps retrying to make the connection. This feature allows a Global VPN Client to make a connection to a VPN connection that is temporarily disabled, without manual intervention. If the connection error is due to an incorrect configuration, such as the DNS or IP address of the peer gateway, then the connection must be manually corrected. Check the Log Viewer to determine the problem and then edit the connection. This option is enabled by default. If an error occurs with this option disabled during an attempted connection, the Global VPN Client logs the error, displays an error message dialog box, and stops the connection attempt.
- **Automatically reconnect when waking from sleep or hibernation** - Automatically re-enables the VPN connection after the computer wakes from a sleep or hibernation state. This setting is disabled by default.

- **Execute logon script when connected** - After logging into the SonicWALL VPN Gateway and establishing a secure tunnel, performs any action configured in the logon script.
- **Run the following command when connection is established** - Allows a program to be automatically executed, with optional arguments, when successful VPN connections are established.

User Authentication

The **User Authentication** page allows you to specify a username and password when user authentication is required by the gateway. If the SonicWALL VPN gateway does not support the saving (caching) of a username and password, the settings in this page are not active and the message **The peer does not allow saving of username and password** appears at the bottom of the page.

- **Remember my username and password** - Enables the saving of your username and password for connecting to the SonicWALL VPN gateway.
- **Username** - Enter the username provided by your gateway administrator.
- **Password** - Enter the password provided by your gateway administrator.

Peers

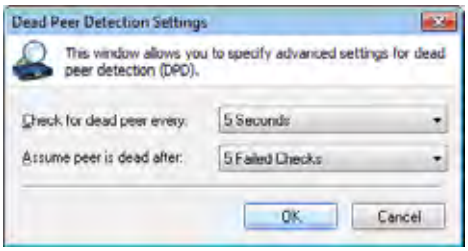
The **Peers** page allows you to specify an ordered list of VPN gateway peers that this connection can use (multiple entries allow a VPN connection to be established through multiple VPN gateways). An attempt is made to establish a VPN connection to the given VPN gateway peers in the order they appear in the list.

- To add a peer, click **Add**. In the **Peer Information** dialog box, enter the IP address or DNS Name in the **IP Address or DNS Name** box, then click **OK**.
- To edit a peer entry, select the peer name and click **Edit**. In the **Peer Information** dialog box, make your changes, then click **OK**.
- To delete a peer entry, select the peer entry and click **Remove**.

Peer Information Dialog Box

The **Peer Information** dialog box allows you to add or edit peer information.

- **IP Address or DNS Name** - Specifies the peer VPN gateway IP address or DNS name.
- **Use the default gateway as the peer IP address** - Specifies the default gateway as the peer IP address.
- **Dead Peer Detection - Automatic** - This is traffic based DPD. If Global VPN Client does not receive response data (one way traffic), then Global VPN Client exchanges heartbeat packets to detect if the peer gateway is alive. If there is no heartbeat packet response for the configured number of failed checks in **DPD Settings**, then Global VPN Client will try to re-initiate IKE negotiations. This setting is enabled by default.
- **Dead Peer Detection - Forced On** - Performs DPD periodically. The Global VPN Client exchanges heartbeat packets to detect if the peer gateway is alive. If there is no heartbeat packet response for the configured number of failed checks in **DPD Settings**, then Global VPN Client will try to re-initiate IKE negotiations.
- **Dead Peer Detection - Disabled** - DPD is disabled. No heartbeat packets are exchanged. This will prevent Global VPN Client from detecting when the gateway is unavailable.
- **DPD Settings** - Displays the **Dead Peer Detection** Settings dialog box.



Check for dead peer every - choose from 5, 10, 15, 20, 25, or 30 seconds.

Assume peer is dead after - choose from 3, 4, or 5 Failed Checks.

- **NAT Traversal** - Choose one of the following three menu options:

  Automatic - Automatically determines whether or not to use UDP encapsulation of IPSec packets between the peers.

  Forced On - Forces the use of UDP encapsulation of IPSec packets even when there is no NAPT/NAT device in between the peers.

  Disabled - Disables use of UDP encapsulation of IPSec packets between the peers.

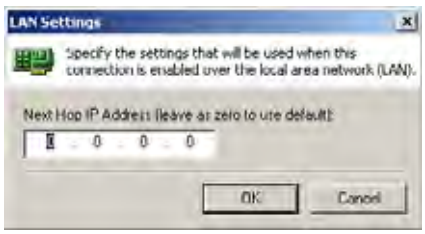
- **Interface Selection** - Defines the interface used by this VPN connection.

  Automatic - Automatically determines the availability of each interface beginning with the LAN interface. If the LAN interface is not available, the Global VPN Client uses the Dial-Up interface.

  LAN Only - Defaults to the LAN interface only.

  Dial-Up Only - Defaults to the Dial-Up interface only.

- **LAN Settings** - Displays **LAN Settings** dialog box for specifying the setting used when this connection is enabled over the LAN. Type the IP address in the **Next Hop IP Address** field to specify the next hop IP address of a different route than the default route. Leaving the setting as zeros instructs the Global VPN Client to use the default route.



- **Dial-Up Settings** - Displays the **Dial-Up Settings** dialog box, which allows you to select the dial-up profile to use making a dial-up VPN connection.

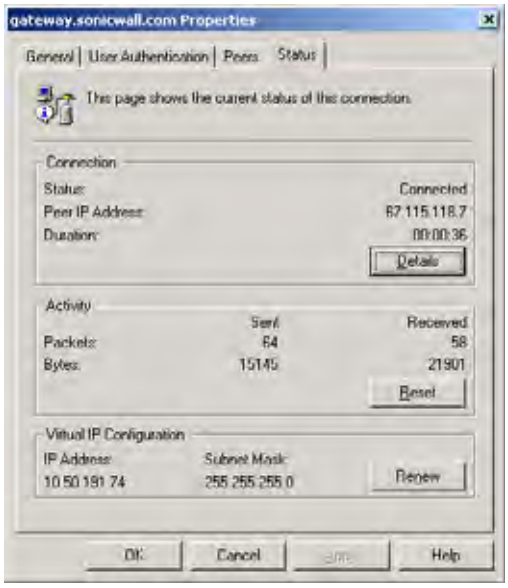
  Use Microsoft dial-up networking - Uses the Microsoft dial-up networking profile you specify for making the VPN connection. Select the Dial-up networking profile from the **Phonebook Entry** list. Check the **Do not hang up the modem when disabling this connection** to keep the dial-up network connection active after disabling the VPN connection.

  Use a third-party dial-up application - Select this option to use a third party dial-up program. Type the path in the **Application** field or use the browse **...** button to locate the program.

- **Response Timeout (in seconds)** - Specifies the maximum amount of time to wait for a response to a sent packet. After this time expires, the sent packet will be considered to be lost and the packet will be retransmitted.
- **Maximum Send Attempts** - Specifies the maximum number of times the same packet will be sent before determining that the peer is not responding.

Status

The **Status** page shows the current status of the connection.



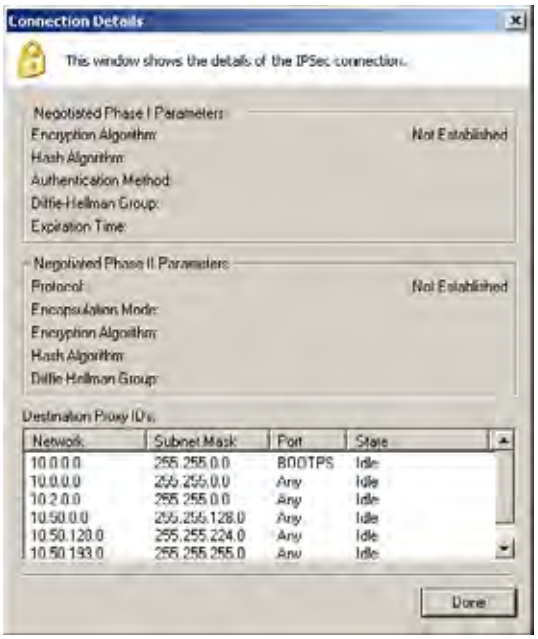
- **Connection**

  Status - Indicates whether VPN connection is enabled or disabled.

  Peer IP Address - Displays the IP address of the VPN connection peer.

  Duration - Displays connection time.

Details - Displays the **Connection Status Details** dialog box, which specifies the negotiated phase 1 and phase 2 parameters as well as the status of all individual phase 2 SAs.



- **Activity**
  Packets - Displays number of packets sent and received through VPN tunnel.

  Bytes - Displays number of bytes sent and received through VPN tunnel.

  Reset - Resets the status information.
- **Virtual IP Configuration**
  IP Address - The IP address assigned via DHCP through the VPN tunnel from the VPN gateway.

  Subnet Mask - The subnet of the peer.

  Renew - Renews DHCP lease information.

Managing VPN Connections

The SonicWALL Global VPN Client supports as many VPN connections as you need. To help you manage these connections, the Global VPN Client provides the connection management tools described in this section.

Arranging Connections

Over time, as the number of VPN connections can increase in the SonicWALL Global VPN Client window, you may want to arrange them for quicker access. You can arrange your VPN connections in the SonicWALL Global VPN Client window by choosing **View>Sort by**. You can arrange VPN connection profiles by:

Name - Sorts the connections by connection name.

Peer - Sorts the connections by peer name.

Status - Sorts the connections by connection status.

Ascending - Sorts the connections in ascending order, such as A-Z, if enabled, and in descending order, such as Z-A, if disabled. The default sorting is by **Name** in **Ascending** order.

Renaming a Connection

To rename a connection, select the connection and click on the **Rename** button on the toolbar or choose **File>Rename**, then type in the new name. You can also right-click the connection and choose **Rename** from the menu.

Deleting a Connection

To delete a connection, select the connection, press **Del** or choose **File>Delete**. You can also right-click the connection name and choose **Delete**. You cannot delete an active VPN connection. Disable the VPN connection, then delete it.

Selecting All Connections

Choosing **View>Select All** or pressing **Ctrl+A** selects all the connections in the SonicWALL Global VPN Client window.

Using Certificates

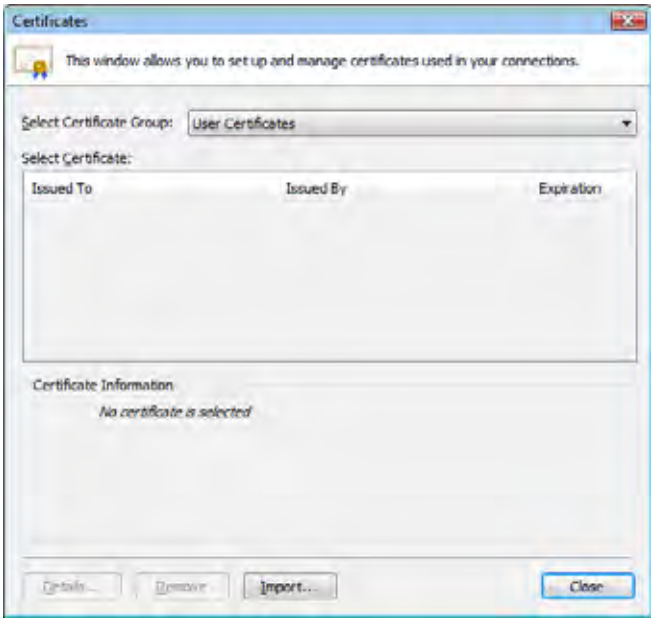
If digital certificates are required as part of your VPN connection policy, your gateway administrator must provide you with the required information to import the certificate. You then need to import the certificate in the Global VPN Client using the Certificate Manager.

Alert! *If digital certificates are required as part of your VPN connection policy, your VPN gateway administrator must provide you with the required certificates.*

Managing Certificates

The **Certificate Manager** allows you to manage digital certificates used by the SonicWALL Global VPN Client for VPN connections. If your VPN gateway uses digital certificates, you must import the CA and Local Certificates into the **Certificate Manager**.

To open the Certificate Manager, click the **View** menu and select **Certificates** in the SonicWALL Global VPN Client window.



The **Select Certificate Group** drop-down list in the **Certificate Manager** window lists the **User**, **CA**, and **Trusted Root CA** certificates currently available for your VPN policies. User Certificates list the local digital certificates used to establish the VPN Security Association. CA Certificates list the digital certificates used to validate the user certificates. Trusted Root CA is used to validate the CA Certificates.

- Click the **Import** button in the **Certificate Manager** window to display the **Import Certificate** window to import a certificate file.
- Click the **Remove** button to delete the selected certificate.
- Click the **Details button** to view the selected certificate details.

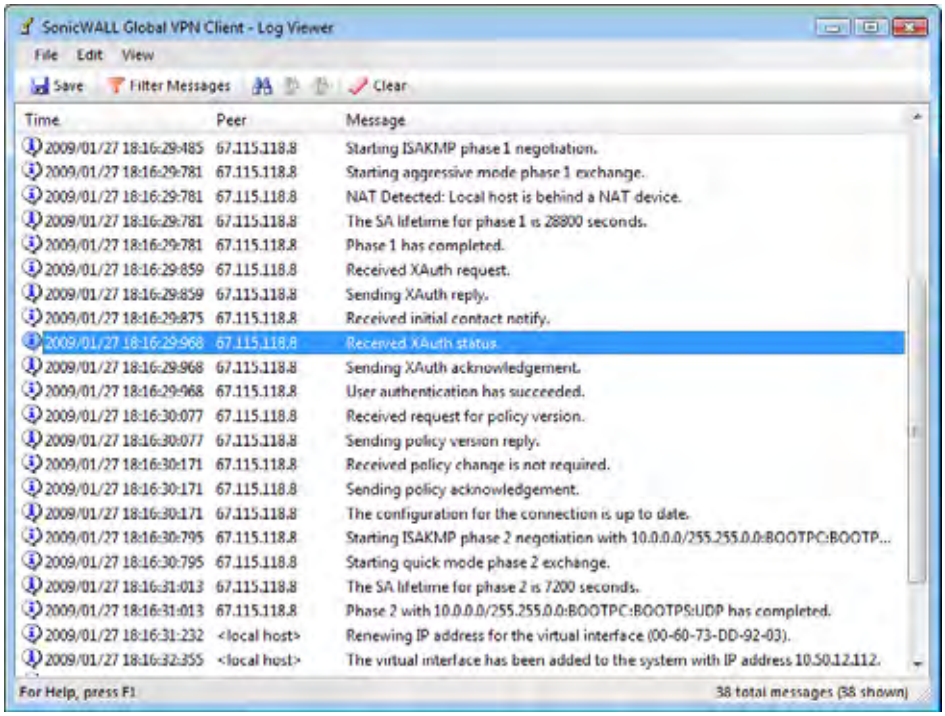
Tip! *For more information on using certificates for your VPN on the SonicWALL, see the SonicOS Administrator's Guide.*

Troubleshooting the SonicWALL Global VPN Client

The SonicWALL Global VPN Client provides tools for troubleshooting your VPN connections. This section explains using Log Viewer, generating a Help Report, accessing SonicWALL's Support site, using SonicWALL Global VPN Client help system, and uninstalling the Global VPN Client.

Understanding the Global VPN Client Log

The **SonicWALL Global VPN Client Log** window displays messages about Global VPN Client activities. To open the **Log Viewer** window, click the **Log Viewer** button on the Global VPN Client window toolbar, or choose **View>Log Viewer**, or press **Ctrl+L**.



Type - The icon indicating the type of message (**Information**, **Warning**, or **Error**). The icons for the three types are:

- **Information** - A blue 'i' in a bubble
- **Warning** - An exclamation point in a yellow triangle
- **Error** - A white 'X' in a red circle

Time - Date and time the message was generated.

Peer - The IP address or FQDN of the peer.

Message - Text of the message describing the event.

You can save a current log to a **.txt** file. When you save the current log to a file, the Global VPN Client automatically adds a **Help Report** containing useful information regarding the condition of the SonicWALL Global VPN Client as well as the system it's running on for troubleshooting. The **Help Report** information is inserted at the beginning of the log file. See "Generating a Help Report" on page 35 for more information.

Tip! *See "Appendix C - Log Viewer Messages" on page 50 for complete listing of Log Viewer messages.*

The Log Viewer provides the following features to help you manage log messages:

- To save a current log to a **.txt** file, click the **Save** button on the toolbar, press **Ctrl+S**, or choose **File>Save**. When you save a Log Viewer file, the Global VPN Client automatically adds a report containing useful information regarding the condition of the SonicWALL Global VPN Client as well as the system it is running on.
- To select all messages, press **Ctrl+A** or choose **Edit>Select All**.
- To copy log contents for pasting into another application, select the messages you want to copy, then click the **Copy** button on the toolbar, press **Ctrl+C**, or choose **Edit>Copy**.
- To clear current log information, click the **Clear** button on the toolbar, press **Crtl+X**, or choose **Edit>Clear**.
- To display less detailed information in the log viewer, choose **View>Filter Messages**.
- To hide the toolbar in the **Log Viewer** window, choose **View>Toolbar**.
- To hide the status bar in the **Log Viewer** window, choose **View>Status Bar**.

Configuring the Log

The Logging page in the **Options** dialog box specifies the settings for configuring the Global VPN Client Log behavior.

Maximum number of log messages to keep - Specifies the maximum number of log messages kept in the log file.

Log ISAKMP header information - Enables the logging of ISAKMP header information.

Log dead peer detection packets - Enables the logging of dead peer detection packets.

Log NAT keep-alive packets - Enables the logging of NAT keep-alive packets.

Enable automatic logging of messages to file - Enables automatic logging of messages to a file as specified in the **Auto-Logging** window.

Settings - Clicking on **Settings** displays the **Auto-Logging** window.

Configuring Auto-Logging

Clicking on **Settings** displays the **Auto-Logging** window for specifying settings for auto-logging of messages to a file. Log files are saved as text files (**.txt**).

Enter the name of the auto-log file - Specifies the file to save the logging messages. Clicking on the **...** button allows you to specify the location of your auto-log file. If only a file name is specified (no path is given in the file name), the log file will be created in the user's TEMP directory.

View Auto-Log File - Displays the entire log file up to 71,000 lines.

Overwrite existing file when auto-logging starts - Overwrites the existing auto-log file when auto-logging is started.

Set size limit on auto-log file - Activates a maximum size limit for the log file.

Maximum auto-log file size - Specifies the maximum file size in KB or MB.

When auto-log size limit is reached - Specifies the action to take when the auto-log file reaches the maximum size.

Ask me what to do - Prompts the user when the log file reaches the maximum size to choose either **Stop auto-logging** or **Overwrite auto-log file**.

Stop auto-logging - Stops auto-logging when the maximum file size is reached.

Overwrite auto-log file - Overwrites existing auto-log file after the maximum file size is reached.

Generating a Help Report

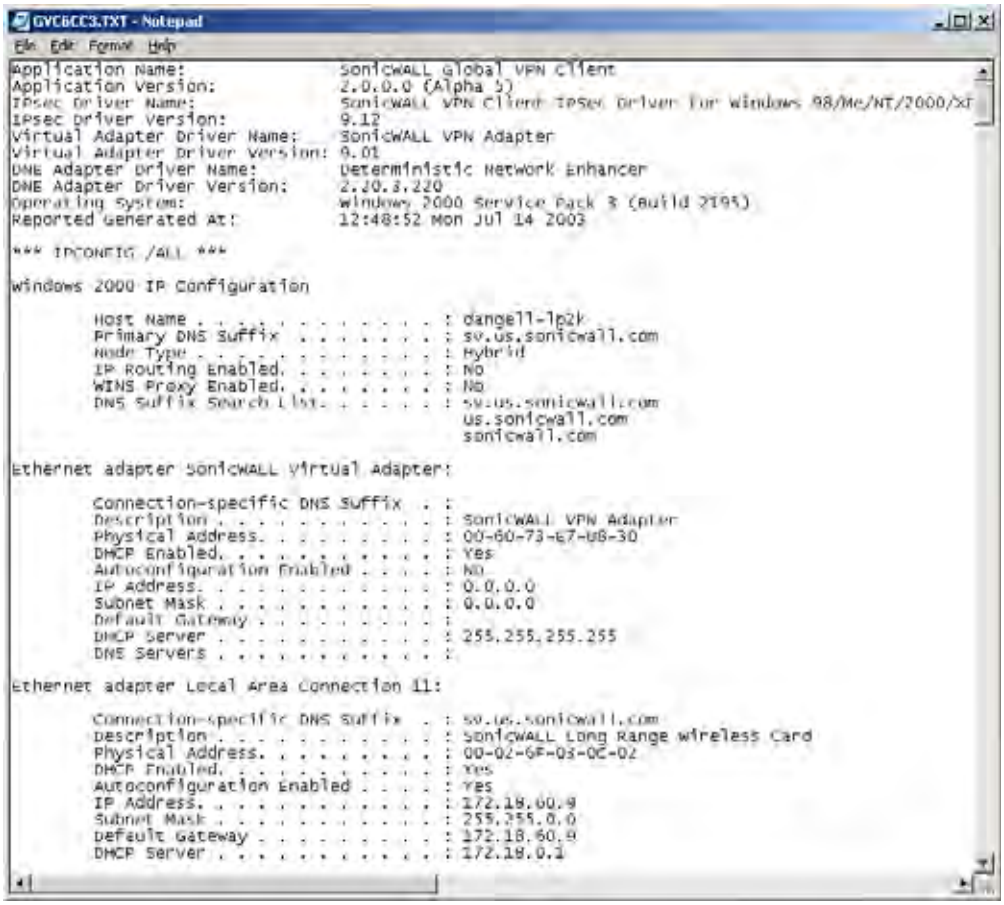
Choosing **Help>Generate Report** in the SonicWALL Global VPN Client window displays the **SonicWALL Global VPN Client Report** dialog box.

Generate Report creates a report containing useful information for getting help in solving any problems you may be experiencing. The report contains information regarding the condition of the SonicWALL Global VPN Client as well as the system it's running on.

Information in this report includes:

- Version information
- Drivers
- System information
- IP addresses
- route table
- Current log messages.

To view the report in the default text editor window, click **View**.



To save the report to a text file, click **Save As**.

To send the report via e-mail, click **Send**.

To close the report window without taking any action, click **Don't Send**.

Accessing SonicWALL Global VPN Client Technical Support

SonicWALL's comprehensive support services protect your network security investment and offer the support you need - when you need it. SonicWALL Global VPN Client support is included as part of the support program of your SonicWALL Internet Security Appliance.

Selecting **Help**>**Technical Support** accesses the SonicWALL Support site at *http://www.sonicwall.com/us/Support.html*

The SonicWALL Support site offer a full range of support services including extensive online resources and information on SonicWALL's enhanced support programs. You can purchase/activate SonicWALL Support Services through your MySonicWALL account at: *http://www.mysonicwall.com*

For Web-based technical support, please visit:
http://www.sonicwall.com/us/Support.html

Viewing Help Topics

Selecting **Help**>**Help Topics** displays SonicWALL Global VPN Client help system window. You can access help topics using the following options:

- **Contents** - displays help in a table of contents view.
- **Index** - displays help in an alphabetical topic view.
- **Search** - allows you to search the help system using keywords.

Uninstalling the SonicWALL Global VPN Client

You can easily uninstall the SonicWALL Global VPN Client and choose to save or delete your VPN connections as part of the uninstall process.

Alert! *You must exit the SonicWALL Global VPN Client before uninstalling the program.*

Alert! *If you are upgrading SonicWALL Global VPN Client from an earlier version to 4.6, you must uninstall the earlier version before installing Global VPN Client 4.6.*

To uninstall the SonicWALL Global VPN Client:

1. Launch the Windows Control Panel
2. Double-click **Add/Remove Programs.**
3. Select SonicWALL Global VPN Client and then click **Remove**.
4. In the **Confirm File Deletion dialog box,** click **Yes** or **OK** to confirm the removal of the SonicWALL Global VPN Client.
5. Choose **Delete all individual user profiles** if you want to delete all you existing VPN connection profiles. If you leave this setting unchecked, the VPN connection profiles are saved and appear again when you install the SonicWALL Global VPN Client at another time.
6. Choose **Retain MAC Address** if you want to retain the same SonicWALL VPN Adapter MAC address the next time you install the Global VPN Client. Click **Next**.
7. After the Global VPN Client is removed, restart your computer when prompted to do so.

Configuring SonicWALL Appliances for Global VPN Clients

SonicWALL's GroupVPN policy provides the automatic provisioning of SonicWALL Global VPN Client from the SonicWALL security appliance. The GroupVPN policy is only available for SonicWALL Global VPN Clients. SonicWALL GroupVPN supports two IPSec keying modes: **IKE using shared secret** and **IKE using 3rd Party Certificates**.

Once you create the GroupVPN policy, you configure GroupVPN to automatically provision SonicWALL Global VPN Clients by downloading the policy, or exporting the policy file for manual installation in the SonicWALL Global VPN Client.

Note! *For information on configuring GroupVPN on the SonicWALL to support SonicWALL Global VPN Client, refer to the Administrator's Guide for your SonicWALL. All SonicWALL product documentation is available at http://www.sonicwall.com/support/documentation.html*

SonicWALL Global VPN Client Licenses

Global VPN Client Licensing is based on the number of simultaneous Global VPN Client connections to a SonicWALL. If the number of simultaneous Global VPN Client connections is exceeded, the SonicWALL does not allow any additional Global VPN Client connections. Once the number of simultaneous Global VPN Client drops below the license limit, new Global VPN connections can be established.

Group VPN Connections Supported by Each SonicWALL Model

Each SonicWALL appliance model supports a different number of Global VPN Client licenses. You can purchase Global VPN Client software and Global VPN Client Licenses from your reseller or online at mysonicwall.com.

Activating Your SonicWALL Global VPN Clients

In order to activate and download your SonicWALL Global VPN Client software, you must have a valid mysonicwall.com account and your SonicWALL product must be registered to your account. If you do not have a mysonicwall.com account, or if you have not registered your product to your account, create an account and then follow the registration instructions at *http://www.mysonicwall.com.*

To activate your Global VPN Client license,

1. Log in to your mysonicwall.com account:
2. Select the registered SonicWALL Internet Security Appliance.
3. Select **Global VPN Client** from the **Applicable Services** menu.
4. Select **Activate**.
5. Type in your activation key in the Activation Key field.
6. Click **Submit**.

Upon successful activation, a confirmation message will be displayed. For future reference, record the Serial Number of the SonicWALL product. Your license activation is now complete.

Downloading Global VPN Client Software and Documentation

1. In the My Products page, click the name of your SonicWALL on which the Global VPN Client license is activated.
2. Select **Software Download**. If this service is not already activated, click on **Agree** to activate it.
3. Download the SonicWALL Global VPN Client software and documentation.

SOFTWARE LICENSE AGREEMENT FOR THE SONICWALL GLOBAL VPN CLIENT

This Software License Agreement (SLA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this SLA. If you do not agree to the terms of this SLA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE PRODUCT to your place of purchase for a full refund.

- The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as by other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
- Title to the SOFTWARE PRODUCT licensed to you and all copies thereof are retained by SonicWALL or third parties from whom SonicWALL has obtained a licensing right. You acknowledge and agree that all right, title, and interest in and to the SOFTWARE PRODUCT, including all associated intellectual property rights, are and shall remain with SonicWALL. This SLA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this SLA.
- The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.

- You may install and use one copy of the SOFTWARE PRODUCT, or any prior version for the same operating system, on a single computer.
- You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on your other computers over an internal network. However, you must acquire and dedicate a license for each separate computer on which the SOFTWARE PRODUCT is installed or run from the storage device. A license for the SOFTWARE PRODUCT may not be shared or used concurrently on different computers.
- You may not resell, or otherwise transfer for value, the SOFTWARE PRODUCT.
- You may not rent, lease, or lend the SOFTWARE PRODUCT.
- You may permanently transfer all of your rights under this SLA, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, and this SLA); the recipient agrees to the terms of this SLA; and you obtain prior written consent from SonicWALL. If the SOFTWARE PRODUCT is an upgrade, any transfer must include all prior versions of the SOFTWARE PRODUCT.
- The SOFTWARE PRODUCT is trade secret or confidential information of SonicWALL or its licensors. You shall take appropriate action to protect the confidentiality of the SOFTWARE PRODUCT. You shall not reverse-engineer, de-compile, or disassemble the SOFTWARE PRODUCT, in whole or in part. The provisions of this section will survive the termination of this SLA.

LICENSE

SonicWALL grants you a non-exclusive license to use the SOFTWARE PRODUCT for SonicWALL

Internet Security Appliances.

OEM - If the SOFTWARE PRODUCT is modified and enhanced for a SonicWALL OEM partner, you must adhere to the software license agreement of the SonicWALL OEM partner.

EXPORTS LICENSE

Licensee will comply with, and will, at SonicWALL's request, demonstrate such compliance with all applicable export laws, restrictions, and regulations of the U.S. Department of Commerce, the U.S. Department of Treasury and any other any U.S. or foreign agency or authority. Licensee will not export or re-export, or allow the export or re-export of any product, technology or information it obtains or learns pursuant to this Agreement (or any direct product thereof) in violation of any such law, restriction or regulation, including, without limitation, export or re-export to Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country subject to applicable U.S. trade embargoes or restrictions, or to any party on the U.S. Export Administration Table of Denial Orders or the U.S. Department of Treasury List of Specially Designated Nationals, or to any other prohibited destination or person pursuant to U.S. law, regulations or other provisions.

SUPPORT SERVICES

SonicWALL may provide you with support services related to the SOFTWARE PRODUCT (“Support Services”). Use of Support Services is governed by the SonicWALL policies and programs described in the user manual, in “online” documentation, and/or in other SonicWALL-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to terms and conditions of this SLA. With respect to technical information you provide to SonicWALL as part of the Support Services, SonicWALL may use such information for its business purposes, including for product support and development. SonicWALL shall not utilize such technical information in a form that identifies its source.

UPGRADES

If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by SonicWALL as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this SLA. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

COPYRIGHT

All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and “applets” incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by SonicWALL or its suppliers/licensors. The SOFTWARE PRODUCT is protected by copyrights laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

U.S. GOVERNMENT RESTRICTED RIGHTS

If you are acquiring the Software including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense (“DOD”), the Software is subject to “Restricted Rights”, as that term is defined in the DOD Supplement to the Federal Acquisition Regulations (“DFAR”) in paragraph 252.227 7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government's rights in the Software will be as defined in paragraph 52.227 19(c) (2) of the Federal Acquisition Regulations (“FAR”). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions.

MISCELLANEOUS

This SLA represents the entire agreement concerning the subject matter hereof between the parties and supersedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This SLA shall be governed by and construed under the laws of the State of California as if entirely performed within the State and without regard for conflicts of laws. Should any term of this SLA be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

TERMINATION

This SLA is effective upon your opening of the sealed package(s), installing or otherwise using the SOFTWARE PRODUCT, and shall continue until terminated. Without prejudice to any other rights, SonicWALL may terminate this SLA if you fail to comply with the terms and conditions of this SLA. In such event, you agree to return or destroy the SOFTWARE PRODUCT (including all related documents and components items as defined above) and any and all copies of same.

LIMITED WARRANTY

SonicWALL warrants that a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and b) any Support Services provided by SonicWALL shall be substantially as described in applicable written materials provided to you by SonicWALL. Any implied warranties on the SOFTWARE PRODUCT are limited to ninety (90) days. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES

SonicWALL's and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the SOFTWARE PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside of the United States, neither these remedies nor any product Support Services offered by SonicWALL are available without proof of purchase from an authorized SonicWALL international reseller or distributor.

NO OTHER WARRANTIES

To the maximum extent permitted by applicable law, SonicWALL and its suppliers/licensors disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE PRODUCT, and the provision of or failure to provide Support Services. This Limited Warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

LIMITATION OF LIABILITY

To the maximum extent permitted by applicable law, in no event shall SonicWALL or its suppliers/licensors be liable for any damages (including without limitation special, incidental, indirect, or consequential) whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of or failure to provide Support Services, even if SonicWALL has been advised of the possibility of such damages. In any case, SonicWALL's entire liability under any provision of this SLA shall be limited to the greater of the amount actually paid by you for the SOFTWARE PRODUCT or U.S. $10.00; provided, however, if you have entered into a SonicWALL Support Services Agreement, SonicWALL's entire liability regarding Support Services shall be governed by the terms of that agreement. Because some states and jurisdiction do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

Appendix A - Using the Default.rcf File for Global VPN Clients

The **default.rcf** file allows the SonicWALL VPN Gateway administrator to create and distribute preconfigured VPN connections for SonicWALL Global VPN Clients. The SonicWALL VPN Gateway administrator can distribute the **default.rcf** file with the Global VPN Client software to automatically create preconfigured VPN connections for streamlined deployment.

The VPN connections created from the **default.rcf** file appear in the SonicWALL Global VPN Client window. The Global VPN Client user simply enables the VPN connection and after XAUTH authentication with a username and password, the policy download is automatically completed.

How the Global VPN Client uses the default.rcf File

When the Global VPN Client starts up, the program always looks for the configuration file, **SonicWALL Global VPN Client.rcf**, in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory. If this file does not exist the Global VPN Client looks for the **default.rcf** file in the program install directory, *C:\Program Files\SonicWALL\SonicWALL Global VPN Client*.

The Global VPN Client reads the **default.rcf** file, if it exists and creates the configuration file, **SonicWALL Global VPN Client.rcf**, in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory. The **SonicWALL Global VPN Client.rcf** file contains all the VPN connection configuration information for the SonicWALL Global VPN Client, with sensitive data (user names and passwords) encrypted.

Deploying the default.rcf File

There are three ways to deploy the **default.rcf** file for your SonicWALL Global VPN Clients:

- Include the **default.rcf** file along with the installer software **GVCInstallXX.MSI**, where **XX** is either **32** for 32-bit Windows platforms or **64** for 64-bit Windows platforms, prior to running the installer. See “Including the default.rcf File with the Installer Software GVCInstallXX.MSI” on page 42.
- Add the **default.rcf** file to the program install directory before opening the SonicWALL Global VPN Client application for the first time. See “Adding the default.rcf file to the Installed Global VPN Client Directory” on page 43.
- If the **SonicWALL Global VPN Client.rcf** configuration file exists in the user’s configuration file folder, replace it using settings from the **default.rcf** file in the program install directory. See “Replacing an Existing SonicWALL Global VPN Client.rcf with default.rcf Settings” on page 43.

Including the default.rcf File with the Installer Software GVCInstallXX.MSI

After you create the **default.rcf** file, you can include it in the same folder as the MSI installer (**GVCInstallXX.MSI** where **XX** is either **32** for 32-bit Windows platforms or **64** for 64-bit Windows platforms) prior to running the installer. The installation process now copies the **default.rcf** to the program install directory. After this installation, when the user launches the Global VPN Client program, the connection(s) defined in **default.rcf** are used to create the configuration file **SonicWALL Global VPN Client.rcf** in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory. This is the easiest method for Global VPN Client users.

Perform the following steps to get the same profile (from default.rcf) to all the users during install:

1. Export the WAN groupVPN configuration from your UTM or create **default.rcf** if you want multiple connections.
2. Rename the exported configuration file to **default.rcf**.
3. Extract the **GVCInstallXX.MSI** from **GVCSetupXX.exe** (where **XX** is either **32** for 32-bit Windows platforms or **64** for 64-bit Windows platforms) by typing the command line as follows:
   GVCSetupXX.exe /T:<Path where you want MSI to be extracted> /C
4. Copy the **default.rcf** file to same directory where you have the **GVCInstallXX.MSI** (installer file).
5. Launch the installer (**GVCInstallXX.MSI**).
   The installation process will copy **default.rcf** to the GVC Install directory.
6. After the install is complete and you start the Global VPN Client, it reads the **default.rcf** and creates the defined connections from it.

Alert! *The **default.rcf** file must be included in the Global VPN Client installation directory C:\Program Files\SonicWALL\SonicWALL Global VPN Client\ for the program to write the **SonicWALL Global VPN Client.rcf** file based on the settings defined in the default.rcf file.*

Adding the default.rcf file to the Installed Global VPN Client Directory

After the Global VPN Client software is installed and prior to running the program, the user can add the **default.rcf** file to the Global VPN Client installation directory *C:\Program Files\SonicWALL\SonicWALL Global VPN Client*.

When the user launches the Global VPN Client program, the configuration file **SonicWALL Global VPN Client.rcf** is created in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory based on the **default.rcf** file settings.

Replacing an Existing SonicWALL Global VPN Client.rcf with default.rcf Settings

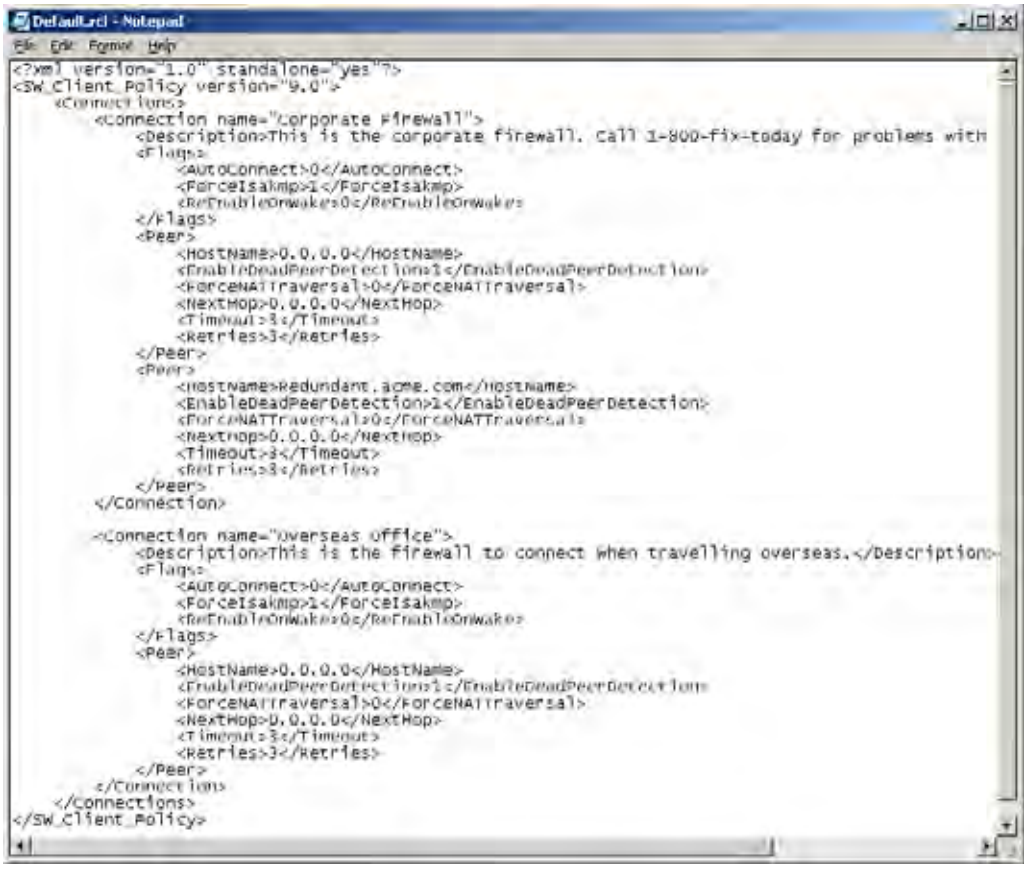
If the configuration file **SonicWALL Global VPN Client.rcf** already exists in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory, the user can remove this file and add the **default.rcf** file to the Global VPN Client installation directory *C:\Program Files\SonicWALL\SonicWALL Global VPN Client*. The next time the user launches the Global VPN Client, the **SonicWALL Global VPN Client.rcf** file is created in the *C:\Documents and Settings\<user>\Application Data\SonicWALL\SonicWALL Global VPN Client* directory based on the **default.rcf** file settings.

Alert! *The **SonicWALL Global VPN Client.rcf** file is user-specific and in most cases will not work for another user running the SonicWALL Global VPN Client, even on the same machine.*

Alert! *Removing an existing **SonicWALL Global VPN Client.rcf** file will remove the VPN connections created in the Global VPN Client. These VPN connections can be added again from the Global VPN Client into the new **SonicWALL Global VPN Client.rcf** file.*

Creating the default.rcf File

You can create your custom **default.rcf** file from any text editor, such as Windows Notepad.



default.rcf File Tag Descriptions

Tag that you do not explicitly list in the default.rcf are set to the default setting (which is the same behavior as when you configure a New VPN Connection within the Global VPN Client manually). The default setting for each tag is highlighted in bracketed bold text, like **[default]**.

<SW_Client_Policy version =”9.0”>

<Connections> Defines the connection profiles in the **default.rcf** configuration file. There is no hard limit defined on the number of connection profiles allowed.

<Connection name = *connection name***>** Provides a name for the VPN connection that appears in the **Global VPN Client** window.

<Description> *description text***</Description>** Provides a description for each connection profile that appears when the user moves the mouse pointer over the VPN Policy in the Global VPN Client window. The maximum number of characters for the <Description> tag is 1023.

<Flags>

<AutoConnect>*[Off=0]*/*On=1*</AutoConnect> Enables this connection when program is launched.

<ForceIsakmp>*Off=0/***[On=1]</ForceIsakmp>** Starts IKE negotiation as soon as the connection is enabled without waiting for network traffic. If disabled then only traffic to the destination network(s) will initiate IKE negotiations.

<ReEnableOnWake>*[Off=0]*/*On=1*</ReEnableOnWake> Enables the connection when computer is coming out of sleep or hibernation.

<ReconnectOnError>*Off=0/***[On=1]</ReconnectOnError>** Automatically keeps trying to enable the connection when an error occurs.

<ExecuteLogonScript>*[Disable=0]*/*Enable=1*</ExecuteLogonScript> Forces launch login script.

</Flags>

<Peer> Defines the peer settings for a VPN connection. A VPN connection can support up to 5 peers.

Alert! *A special case of Host Name is for an Office Gateway scenario. If you want to use the Default Gateway as the host name use the exact text,* ***<Default Gateway>*** *including the semicolons and &s. In this case, you must also set the tag,* ***<UseDefaultGWAsPeerIP>=1****.*

<HostName>*IP Address/Domain Name***</HostName>** The IP address or Domain name of the SonicWALL gateway.

<EnableDeadPeerDetection>*Off=0/On=1***</EnableDeadPeerDetection>** Enables detection if the Peer stops responding to traffic. This will send Vendor ID to the SonicWALL during IKE negotiation to enable Dead peer detection heart beat traffic.

Alert! NAT Traversal - The implementation options for NAT Traversal were changed in Global VPN Client 2.x. In Global VPN Client releases prior to 2.x, there were checkboxes for Forcing or Disabling NAT Traversal. With Global VPN Client 2.x and later, there is now a drop down selection list containing the following three items:

- Automatic - Detects if NAT Traversal is on or off.
- Forced On - Forces NAT Traversal On.
- Disabled - Forces NAT Traversal Off.

To specify Automatic in a custom **default.rcf** file, set ForceNATTraversal and DisableNATTraversal to 0, or do not list these tags at all.

<ForceNATTraversal>*[Off=0]*/*On=1*</ForceNATTraversal> Forces NAT traversal even without a NAT device in the middle. Normally NAT devices in the middle are automatically detected and UDP encapsulation of IPSEC traffic starts after IKE negotiation is complete.

<DisableNATTraversal>[*Off=0]*/On=1</**DisableNATTraversal>** Disables NAT traversal even without a NAT device in the middle. Normally NAT devices in the middle are automatically detected and UDP encapsulation of IPSEC traffic starts after IKE negotiation is complete.

<NextHop>*IP Address***</NextHop>**The IP Address of the next hop for this connection. This is ONLY used if there is a need to use a next hop that is different from the default gateway.

<Timeout>*3***<Timeout>** Defines **t**imeout value in seconds for packet retransmissions. The minimum <Timeout> value is 1 second and the maximum value is 10 seconds.

<Retries>*3***<Retries>**Number of times to retry packet retransmissions before the connection is considered as dead. The minimum <Retries>value is 1 and the maximum value is 10.

<UseDefaultGWAsPeerIP>[*Off=0]*/On=1</**UseDefaultGWAsPeerIP>** Specifies that the PC's Default Gateway IP Address is used as the Peer IP Address.

<InterfaceSelection> Automatically selects the connection based on link and IP detection=0/ Connection always uses LAN=1/Connection always uses Dial-Up=2**</InterfaceSelection>** Forces the interface selection for the VPN connection.

<WaitForSourceIP>*Off=0/***[*On=1]<**/**WaitForSourceIP>** Specifies that packets are to be sent when a local source IP address is available.

<DialupUseMicrosoftDUN>*3rd Party=0/***[*Microsoft=1]<**/**DialupUseMicrosoftDUN>** Instructs the Global VPN Client to use either Microsoft or a third party Dialup connection.

<DialupApp>*c:\Program Files\Windows NT\dialer.exe***</DialupApp>** Specifies the directory path to a third party Dialup connection application, including the application name.

<DialupPhonebook>*MSN Office Network/***[Prompt When Necessary]</DialupPhonebook>** Specifies the name of the Microsoft Dialup connection as listed in Network and Dial-up Connections for the local computer.

<DialupLeaveConnected>[*Off=0]*/On=1</**DialupLeaveConnected>** Instructs the Global VPN Client to leave the dialup connection logged in when the Global VPN Client is not connected.

<DPDInterval>[**[*5]***-30]<**/**DPDInterval>** Specifies the duration of time (in seconds) to wait before declaring a peer as dead. The interval times listed are incremented by 5, and the allowed values are 5, 10, 15, 20, 25 and 30 seconds.

<DPDAttempts>[3-**[*5]]<**/**DPDAttempts>** Specifies number of unsuccessful attempts to contact a peer before declaring it as dead. The allowed values are 3, 4 or 5 times.

<DPDAlwaysSend>[*Off=0]*/On=1</**DPDAlwaysSend>** Instructs the Global VPN Client to send a DPD packet based on network traffic received from the peer.

</Peer> For redundant gateways on this connection, repeat all the tags under <Peer>. There can be up to 5 redundant gateways for each connection.

</Connection> Defines the end of each connection profile in the configuration file.

</Connections> Defines the end of all connection profiles in the **Default.rcf** file.

<SW_Client_Policy>

Sample default.rcf File

The following is an example of a default.rcf file. This file includes two VPN connections: **Corporate Firewall** and **Office Gateway**. The **Corporate Firewall** connection configuration includes two peer entries for redundant VPN connectivity.

Alert! *If you attempt to directly copy this sample file to an ASCII text editor, you may have to remove all of the paragraph marks at the end of each line before saving it. Verify the file can be imported into the Global VPN Application before distributing it.*

```
<?xml version="1.0" standalone="yes"?>
<SW_Client_Policy version="9.0">
<Connections>
 <Connection name="Corporate Firewall">
  <Description>This is the corporate firewall. Call 1-800-fix-today for connection problems.</Description>
  <Flags>
   <AutoConnect>0</AutoConnect>
   <ForceIsakmp>1</ForceIsakmp>
   <ReEnableOnWake>0</ReEnableOnWake>
   <ReconnectOnError>1</ReconnectOnError>
   <ExecuteLogonScript>0</ExecuteLogonScript>
  </Flags>
  <Peer>
   <HostName>CorporateFW</HostName>
   <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
   <ForceNATTraversal>0</ForceNATTraversal>
   <DisableNATTraversal>0</DisableNATTraversal>
   <NextHop>0.0.0.0</NextHop>
   <Timeout>3</Timeout>
   <Retries>3</Retries>
   <UseDefaultGWAsPeerIP>0</UseDefaultGWAsPeerIP>
   <InterfaceSelection>0</InterfaceSelection>
   <WaitForSourceIP>0</WaitForSourceIP>
   <DialupUseMicrosoftDUN>1</DialupUseMicrosoftDUN>
   <DialupApp>c:\program files\aol\aol.exe</DialupApp>
   <DialupPhonebook>text</DialupPhonebook>
   <DialupLeaveConnected>0</DialupLeaveConnected>
   <DPDInterval>5</DPDInterval>
   <DPDAttempts>3</DPDAttempts>
   <DPDAlwaysSend>0</DPDAlwaysSend>
  </Peer>
  <Peer>
   <HostName>1.2.3.4</HostName>
   <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
   <ForceNATTraversal>0</ForceNATTraversal>
   <DisableNATTraversal>0</DisableNATTraversal>
   <NextHop>0.0.0.0</NextHop>
```

```
    <Timeout>3</Timeout>
    <Retries>3</Retries>
    <UseDefaultGWAsPeerIP>0</UseDefaultGWAsPeerIP>
    <InterfaceSelection>0</InterfaceSelection>
    <WaitForSourceIP>0</WaitForSourceIP>
    <DialupUseMicrosoftDUN>1</DialupUseMicrosoftDUN>
    <DialupApp>c:\program files\aol\aol.exe</DialupApp>
    <DialupPhonebook>text</DialupPhonebook>
    <DialupLeaveConnected>0</DialupLeaveConnected>
    <DPDInterval>5</DPDInterval>
    <DPDAttempts>3</DPDAttempts>
    <DPDAlwaysSend>0</DPDAlwaysSend>
  </Peer>
 </Connection>
<Connection name="Office Gateway">
  <Description>This is the firewall to connect when traveling overseas.</Description>
  <Flags>
   <AutoConnect>0</AutoConnect>
   <ForceIsakmp>1</ForceIsakmp>
   <ReEnableOnWake>0</ReEnableOnWake>
   <ReconnectOnError>1</ReconnectOnError>
   <ExecuteLogonScript>0</ExecuteLogonScript>
  </Flags>
  <Peer>
   <HostName>&lt;Default Gateway&gt;</HostName>
   <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
   <ForceNATTraversal>0</ForceNATTraversal>
   <DisableNATTraversal>0</DisableNATTraversal>
   <NextHop>0.0.0.0</NextHop>
   <Timeout>3</Timeout>
   <Retries>3</Retries>
   <UseDefaultGWAsPeerIP>1</UseDefaultGWAsPeerIP>
   <InterfaceSelection>0</InterfaceSelection>
   <WaitForSourceIP>0</WaitForSourceIP>
   <DialupUseMicrosoftDUN>1</DialupUseMicrosoftDUN>
   <DialupApp>c:\program files\aol\aol.exe</DialupApp>
   <DialupPhonebook>text</DialupPhonebook>
```

```
    <DialupLeaveConnected>0</DialupLeaveConnected>
    <DPDInterval>5</DPDInterval>
    <DPDAttempts>3</DPDAttempts>
    <DPDAlwaysSend>0</DPDAlwaysSend>
  </Peer>
 </Connection>
</Connections>
</SW_Client_Policy>
```

Troubleshooting the default.rcf File

.

Table 1: Troubleshooting the default.rcf File

Issue	Solution
If there are any incorrect entries or typos in your **default.rcf** file, the settings in the **default.rcf** file will not be incorporated into the Global VPN Client, and no connection profiles will appear in the Global VPN Client window. The error message ***Failed to parse configuration <file>*** will appear in the Global VPN Client Log Viewer, or the following error message will be displayed when attempting to import the file: "**Could not import the specified configuration file. The file appears to be corrupt."**	Ensure that the file does not contain any non-ASCII characters. The **SonicWALL Global VPN Client.rcf** file created by the **default.rcf** file must be deleted from the **** directory and the **default.rcf** file edited to correct the errors.
The **default.rcf** file cannot have an attribute of READ Only.	The **SonicWALL Global VPN Client.rcf** file created by the **default.rcf** file must be deleted from the **** directory and the **default.rcf** file Read Only attribute removed to correct the error.
The Peer Name, <Default Gateway> displays the following error message when attempting to connect: "**Failed to convert the Peer name <Default Gateway> to an IP address"**.	When setting the Peer Name to the special case of <Default Gateway>, the tag for **<UseDefaultGWAsPeerIP>** must be set to **1**. The **SonicWALL Global VPN Client.rcf** file created by the **default.rcf** file must be deleted from the **** directory.

Appendix B - Running the Global VPN Client from the CLI

The SonicWALL Global VPN Client can run from the Command Line Interface (CLI). This interface allows for the programmatic or script-based initiation of certain Global VPN Client functions without requiring the user to directly act in the Global VPN Client application. The Global VPN Client CLI enables the setting up of scripts that automatically initiate a secure tunnel anytime a particular application or connection method is started.

The CLI commands require the use of a complete path name to the Global VPN Client application followed by various flags and variable information such as username or password.

Alert! *Embedding a user's password directly in a script is a security risk. Anyone who can gain access to the script can read the password to circumvent security. It is recommended that scripts or programmatic dashboards ask for the password before initiating a connection and then clear the variable.*

Command Line Options

You can use the following options to perform a variety of Global VPN Client actions from the command line.

- **/E "*Connection Name*"** Enables the specific connection.
- **/D "*Connection Name*"** Disables the specific connection.
- **/Q** - Quits a running an instance of the program. Ignored if program is not already running.
- **/A [*filename*]** - Starts the program and sends all messages to the specified log file. If no log file is specified, the default file name is **gvcauto.log**. If the program is already running, this option is ignored.
- **/U "Username"** - Username to pass to XAUTH. Must be used in conjunction with **/E**.
- **/P "Password"** - Password to pass to XAUTH. Must be used in conjunction with **/E**.

Command Line Examples

- **<path>\swgvpnclient** - runs/starts application. If application is already running, it does not create another instance.
- **<path>\swgvpnclient /E <connection name> /U <username> and /P <password>** - runs/starts the application and enables the named connection and use the <username> and <password> for user authentication. If you do not include a username and password. the Global VPN Client presents a dialog box asking for the information in order to continue.
- **<path>\swgvpnclient /A <path\filename> -** runs/starts the application and enables auto logging of all events to a log file. If the filename is not specified, then the log file is created with the default name <gvcauto.log>. If you want to save the autolog for each Global VPN Client session, you can use the filename option and specify a different filename each time the application is stated. This file is created in the same directory where the Global VPN Client application is started, if the path is not specified.

Appendix C - Log Viewer Messages

The following sections list the **Error**, **Info**, and **Warning** messages that can appear in the Global VPN Client Log Viewer.

Log Viewer Error Messages

The following table lists possible Error messages.

Table 2: Log Viewer Messages

ERROR	"Invalid DOI in notify message,"
ERROR	: called with invalid parameters.
ERROR	A phase 2 IV has already been created.
ERROR	An error occurred.
ERROR	Attributes were specified but not offered.
ERROR	Authentication algorithm is not supported.
ERROR	CA certificate not found in list.
ERROR	Calculated policy configuration attributes length does not match length of attributes set into policy configuration payload.
ERROR	Calculated XAuth attributes length does not match length of attributes set into XAuth payload.
ERROR	Can not change the Diffie-Hellman group for PFS.
ERROR	Can not process packet that does not have at least one payload.
ERROR	Can not process unsupported mode config type.
ERROR	Can not process unsupported XAuth type.
ERROR	Can not set IPSEC proposals into empty SA list.
ERROR	Cannot do quick mode: no SA's to negotiate.
ERROR	certificate error.
ERROR	Certificate ID not specified.
ERROR	Deallocation of event publisher context failed.
ERROR	Diffie-Hellman group generator length has not been set.
ERROR	Diffie-Hellman group prime length has not been set.
ERROR	DSS signature processing failed - signature is not valid.
ERROR	Encryption algorithm is not supported.
ERROR	ESP transform algorithm is not supported.
ERROR	Failed to add a new AH entry to the phase 2 SA list.
ERROR	Failed to add a new ESP entry to the phase 2 SA list.

Table 2: Log Viewer Messages

ERROR	Failed to add IPSEC encapsulation mode into the payload.
ERROR	Failed to add IPSEC group description into the payload.
ERROR	Failed to add IPSEC HMAC algorithm into the payload.
ERROR	Failed to add IPSEC life duration into the payload.
ERROR	Failed to add IPSEC life type into the payload.
ERROR	Failed to add OAKLEY authentication algorithm into the payload.
ERROR	Failed to add OAKLEY encryption algorithm into the payload.
ERROR	Failed to add OAKLEY generator G1 into the payload.
ERROR	Failed to add OAKLEY group description into the payload.
ERROR	Failed to add OAKLEY group type into the payload.
ERROR	Failed to add OAKLEY hash algorithm into the payload.
ERROR	Failed to add OAKLEY life duration into the payload.
ERROR	Failed to add OAKLEY life type into the payload.
ERROR	Failed to add OAKLEY prime P into the payload.
ERROR	Failed to add policy configuration INI format into the payload.
ERROR	Failed to add policy configuration version into the payload.
ERROR	Failed to add XAuth password '' into the payload.
ERROR	Failed to add XAuth status into the payload.
ERROR	Failed to add XAuth type into the payload.
ERROR	Failed to add XAuth username '' into the payload.
ERROR	Failed to allocate bytes.
ERROR	Failed to allocate memory.
ERROR	Failed to begin phase 1 exchange.
ERROR	Failed to begin quick mode exchange.
ERROR	Failed to build a DSS object.
ERROR	Failed to build dead peer detection packet.
ERROR	Failed to build dead peer detection reply message.
ERROR	Failed to build dead peer detection request message.
ERROR	Failed to build phase 1 delete message.
ERROR	Failed to calculate DES mode from ESP transfer.
ERROR	Failed to calculate policy configuration attributes length.
ERROR	Failed to calculate XAuth attributes length.

Table 2: Log Viewer Messages

ERROR	Failed to compute IV for connection entry.
ERROR	Failed to construct certificate payload.
ERROR	Failed to construct certificate request payload.
ERROR	Failed to construct certificate.
ERROR	Failed to construct destination proxy ID payload.
ERROR	Failed to construct DSS signature.
ERROR	Failed to construct hash payload.
ERROR	Failed to construct IPSEC nonce payload.
ERROR	Failed to construct IPSEC SA payload.
ERROR	Failed to construct ISAKMP blank hash payload.
ERROR	Failed to construct ISAKMP delete hash payload.
ERROR	Failed to construct ISAKMP DPD notify payload.
ERROR	Failed to construct ISAKMP ID payload.
ERROR	Failed to construct ISAKMP info hash payload.
ERROR	Failed to construct ISAKMP key exchange payload.
ERROR	Failed to construct ISAKMP nonce payload.
ERROR	Failed to construct ISAKMP notify payload.
ERROR	Failed to construct ISAKMP packet header.
ERROR	Failed to construct ISAKMP phase 1 delete payload.
ERROR	Failed to construct ISAKMP SA payload.
ERROR	Failed to construct ISAKMP vendor ID payload (ID =).
ERROR	Failed to construct mode config hash payload.
ERROR	Failed to construct NAT discovery payload.
ERROR	Failed to construct PFS key exchange payload.
ERROR	Failed to construct policy provisioning payload.
ERROR	Failed to construct quick mode hash payload.
ERROR	Failed to construct quick mode packet.
ERROR	Failed to construct responder lifetime payload.
ERROR	Failed to construct RSA signature.
ERROR	Failed to construct signature payload.
ERROR	Failed to construct source proxy ID payload.
ERROR	Failed to construct XAuth payload.

Table 2: Log Viewer Messages

ERROR	Failed to convert the peer name to an IP address.
ERROR	Failed to create a new connection entry: an entry already exists with ID.
ERROR	Failed to create connection entry with message ID.
ERROR	Failed to decrypt buffer.
ERROR	Failed to decrypt mode config payload.
ERROR	Failed to decrypt notify payload.
ERROR	Failed to decrypt packet.
ERROR	Failed to decrypt quick mode payload.
ERROR	Failed to encrypt mode config payload.
ERROR	Failed to encrypt notify payload.
ERROR	Failed to encrypt packet.
ERROR	Failed to encrypt quick mode payload.
ERROR	Failed to expand packet to size bytes.
ERROR	Failed to find an SA list for PROTO_IPSEC_AH.
ERROR	Failed to find an SA list for PROTO_IPSEC_ESP.
ERROR	Failed to find an SA list given the protocol.
ERROR	Failed to find certificate with ID.
ERROR	Failed to find connection entry for message ID.
ERROR	Failed to find exit interface to reach.
ERROR	Failed to find MAC address in the system interfaces table.
ERROR	Failed to find matching SA list.
ERROR	Failed to find message ID and matching cookies in the connection entry list.
ERROR	Failed to find message ID in the connection entry list.
ERROR	Failed to find message ID in the SA list.
ERROR	Failed to find OAKLEY group specified in the SA payload.
ERROR	Failed to find private key for certificate with ID.
ERROR	Failed to find protocol ID in the SA list.
ERROR	Failed to find route to reach.
ERROR	Failed to find sequence number.
ERROR	Failed to find source IP address to reach.
ERROR	Failed to flush the system ARP cache.
ERROR	Failed to generate Diffie-Hellman parameters.

Table 2: Log Viewer Messages

ERROR	Failed to generate quick mode initiator key.
ERROR	Failed to generate quick mode responder key.
ERROR	Failed to generate SKEYID.
ERROR	Failed to get the size of the system interfaces table.
ERROR	Failed to get the size of the system IP address table.
ERROR	Failed to get the system interface table.
ERROR	Failed to get the system IP address table.
ERROR	Failed to get transforms from SA list.
ERROR	Failed to match initiator cookie.
ERROR	Failed to match responder cookie.
ERROR	Failed to parse certificate data.
ERROR	Failed to parse configuration file.
ERROR	Failed to read the size of an incoming ISAKMP packet.
ERROR	Failed to re-allocate bytes.
ERROR	Failed to receive an incoming ISAKMP packet.
ERROR	Failed to receive an incoming ISAKMP packet. The length is incorrect.
ERROR	Failed to send an outgoing ISAKMP packet.
ERROR	Failed to set policy configuration attributes into payload.
ERROR	Failed to set proposals into phase 1 SA payload.
ERROR	Failed to set proposals into phase 2 SA payload.
ERROR	Failed to set responder lifetype attributes.
ERROR	Failed to set the ESP attributes from the SA payload into the SA.
ERROR	Failed to set the IPSEC AH attributes into the phase 2 SA.
ERROR	Failed to set the IPSEC ESP attributes into the phase 2 SA.
ERROR	Failed to set the OAKLEY attributes into the phase 1 SA.
ERROR	Failed to set vendor ID into packet payload.
ERROR	Failed to set XAuth attributes into payload.
ERROR	Failed to sign hash.
ERROR	Failed to verify certificate signature.
ERROR	Failed to verify informational message hash payload.
ERROR	Failed to verify mode config message hash payload.

Table 2: Log Viewer Messages

ERROR	Hash algorithm is not supported.
ERROR	Hash Payload does not match.
ERROR	Hash size invalid:
ERROR	Header invalid (verified)!
ERROR	Invalid certificate: ASN sequence is not correct.
ERROR	Invalid certificate: payload length is too small.
ERROR	Invalid hash payload.
ERROR	Invalid payload. Possible overrun attack!
ERROR	Invalid SA state:
ERROR	Invalid signature payload.
ERROR	Invalid SPI size.
ERROR	is not a supported Diffie-Hellman group type.
ERROR	is not a supported DOI.
ERROR	is not a supported exchange type.
ERROR	is not a supported ID payload type.
ERROR	is not a supported IPSEC protocol.
ERROR	is not a supported notify message type.
ERROR	is not a supported payload type.
ERROR	is not a supported policy configuration attribute type.
ERROR	is not a supported policy configuration message type.
ERROR	is not a supported proxy ID payload type.
ERROR	is not a supported XAuth attribute type.
ERROR	is not a valid quick mode state.
ERROR	is not a valid XAuth message type.
ERROR	is not a valid XAuth status.
ERROR	ISAKMP SA delete msg for a different SA!
ERROR	No certificate for CERT authentication.
ERROR	No entry in the system IP address table was found with index.
ERROR	No KE payload while PFS configured mess_id.
ERROR	Out of memory.
ERROR	Phase 1 authentication algorithm is not supported.
ERROR	Phase 1 encryption algorithm is not supported.

Table 2: Log Viewer Messages

ERROR	Protocol ID has already been added to the SA list.
ERROR	Protocol mismatch: expected PROTO_IPSEC_AH but got.
ERROR	Protocol mismatch: expected PROTO_IPSEC_ESP but got.
ERROR	Publisher deregistration failed.
ERROR	Responder cookie is not zero.
ERROR	RSA signature processing failed - signature is not valid.
ERROR	SA hash function has not been set in.
ERROR	Signature Algorithm mismatch is X.509 certificate.
ERROR	Signature verification failed!
ERROR	The certificate is not valid at this time.
ERROR	The current state is not valid for processing mode config payload.
ERROR	The current state is not valid for processing signature payload.
ERROR	The first payload is not a hash payload.
ERROR	The following error occurred while trying to open the configuration file:
ERROR	The peer is not responding to phase 1 ISAKMP requests.
ERROR	The peer is not responding to phase 1 ISAKMP requests.
ERROR	The state flag indicates that the IPSEC SA payload has not been processed.
ERROR	The system interface table is empty.
ERROR	The system IP address table is empty.
ERROR	Unable to compute hash!
ERROR	Unable to compute shared secret for PFS in phase 2!
ERROR	Unable to read configuration file.
ERROR	User did not enter XAuth next pin.
ERROR	XAuth CHAP requests are not supported at this time.
ERROR	XAuth failed.
ERROR	XAuth has requested a password but one has not yet been specified.

Log Viewer Info Messages

The following table lists possible Information messages.

Table 3: Log Viewer Info Messages

INFO	"The connection """" has been disabled."
INFO	A certificate is needed to complete phase 1.
INFO	A phase 2 SA can not be established with until a phase 1 SA is established.
INFO	A pre-shared key is needed to complete phase 1.
INFO	AG failed. SA state unknown. Peer:
INFO	An incoming ISAKMP packet from was ignored.
INFO	DSS g value:
INFO	DSS p value:
INFO	DSS q value:
INFO	Event publisher deregistered.
INFO	Event publisher registered for.
INFO	Failed to negotiate configuration information with.
INFO	Found CA certificate in CA certificate list.
INFO	Ignoring unsupported payload.
INFO	Ignoring unsupported vendor ID.
INFO	ISAKMP phase 1 proposal is not acceptable.
INFO	ISAKMP phase 2 proposal is not acceptable.
INFO	MM failed. Payload processing failed. OAK_MM_KEY_EXCH. Peer:
INFO	MM failed. Payload processing failed: OAK_MM_NO_STATE. Peer:
INFO	MM failed. Payload processing failed: OAK_MM_SA_SETUP. Peer:
INFO	MM failed. SA state not matching mask process auth. Peer:
INFO	MM failed. SA state not matching mask process key. Peer:
INFO	MM failed. SA state not matching mask process sa. Peer:
INFO	MM failed. SA state unknown. Peer:
INFO	NAT Detected: Local host is behind a NAT device.
INFO	NAT Detected: Peer is behind a NAT device.
INFO	peer certificate missing key value.
INFO	Phase 1 has completed.
INFO	Phase 1 SA lifetime set to.
INFO	Phase 2 negotiation has failed.

Table 3: Log Viewer Info Messages

INFO	Phase 2 SA lifetime set to.
INFO	Phase 2 with has completed.
INFO	Proposal not acceptable: not authentication algorithm specified.
INFO	Proposal not acceptable: not Diffie-Hellman group specified.
INFO	Proposal not acceptable: not encryption algorithm specified.
INFO	Proposal not acceptable: not hash algorithm specified.
INFO	Proposal not acceptable: proposal not found in list.
INFO	QM failed. Load SA failed. Peer:
INFO	Reading configuration file.
INFO	Ready to negotiate phase 2 with.
INFO	Received address notification notify.
INFO	Received attributes not supported notify.
INFO	Received authentication failed notify.
INFO	Received bad syntax notify.
INFO	Received certificate unavailable notify.
INFO	Received dead peer detection acknowledgement.
INFO	Received dead peer detection request.
INFO	Received initial contact notify.
INFO	Received invalid certificate authentication notify.
INFO	Received invalid certificate encoding notify.
INFO	Received invalid certificate notify.
INFO	Received invalid certificate request syntax notify.
INFO	Received invalid cookie notify.
INFO	Received invalid exchange type notify.
INFO	Received invalid flags notify.
INFO	Received invalid ID information notify.
INFO	Received invalid key info notify.
INFO	Received invalid major version notify.
INFO	Received invalid message ID notify.
INFO	Received invalid minor version notify.
INFO	Received invalid payload notify.
INFO	Received invalid protocol ID notify.

Table 3: Log Viewer Info Messages

INFO	Received invalid signature notify.
INFO	Received invalid SPI notify.
INFO	Received invalid transform ID notify.
INFO	Received malformed payload notify.
INFO	Received no proposal chosen notify.
INFO	Received notify SA lifetime notify.
INFO	Received phase 1 delete message.
INFO	Received phase 2 delete message for SPI.
INFO	Received policy provisioning acknowledgement.
INFO	Received policy provisioning OK.
INFO	Received policy provisioning update.
INFO	Received policy provisioning version reply.
INFO	Received policy provisioning version request.
INFO	Received responder lifetime notify.
INFO	Received situation not supported notify.
INFO	Received unequal payload length notify.
INFO	Received unknown notify.
INFO	Received unsupported DOI notify.
INFO	Received unsupported exchange type notify.
INFO	Received XAuth request.
INFO	Received XAuth status.
INFO	Re-evaluating ID info after INVALID_ID_INFO message.
INFO	Releasing IP address for the virtual interface ().
INFO	Renewing IP address for the virtual interface ().
INFO	Saving configuration file.
INFO	Sending dead peer detection acknowledgement.
INFO	Sending dead peer detection request.
INFO	Sending phase 1 delete.
INFO	Sending phase 2 delete for.
INFO	Sending policy provisioning acknowledgement.
INFO	Sending policy provisioning version reply.
INFO	Sending XAuth acknowledgement.

Table 3: Log Viewer Info Messages

INFO	Sending XAuth reply.
INFO	Signature Verified!
INFO	SonicWALL Global VPN Client version.
INFO	SonicWALL VPN Client.
INFO	Starting aggressive mode phase 1 exchange.
INFO	Starting authentication negotiation.
INFO	Starting configuration negotiation.
INFO	Starting ISAKMP phase 1 negotiation.
INFO	Starting ISAKMP phase 2 negotiation with.
INFO	Starting main mode phase 1 exchange.
INFO	Starting quick mode phase 2 exchange.
INFO	The configuration for the connection has been updated.
INFO	The configuration for the connection is up to date.
INFO	The configuration has been updated and must be reloaded.
INFO	The connection has entered an unknown state.
INFO	The connection is idle.
INFO	The hard lifetime has expired for phase 1.
INFO	The hard lifetime has expired for phase 2 with.
INFO	The IP address for the virtual interface has been released.
INFO	The IP address for the virtual interface has changed to.
INFO	The ISAKMP port (500) is already in use. Port will be used as the ISAKMP source port.
INFO	The peer is not responding to phase 2 ISAKMP requests to.
INFO	The phase 1 SA has been deleted.
INFO	The phase 1 SA has died.
INFO	The phase 2 SA has been deleted.
INFO	The phase 2 SA has died.
INFO	The SA lifetime for phase 1 is seconds.
INFO	The SA lifetime for phase 2 is seconds.
INFO	The soft lifetime has expired for phase 1.
INFO	The soft lifetime has expired for phase 2 with.
INFO	The system ARP cache has been flushed.

Table 3: Log Viewer Info Messages

INFO	Unable to encrypt payload!
INFO	User authentication has failed.
INFO	User authentication has succeeded.
INFO	User authentication information is needed to complete the connection.
INFO	XAuth has requested a username but one has not yet been specified.

Log Viewer Warning Messages

The following table lists possible Warning messages.

Table 4: Log Viewer Warning Messages

WARNING	A password must be entered.
WARNING	AG failed. SA state not matching mask process auth. Peer:
WARNING	AG failed. SA state not matching mask process key. Peer:
WARNING	AG failed. State OAK_AG_INIT_EXCH is invalid when responder. Peer:
WARNING	AG failed. State OAK_AG_NO_STATE is invalid when initiator. Peer:
WARNING	Failed to process aggressive mode packet.
WARNING	Failed to process final quick mode packet.
WARNING	Failed to process informational exchange packet.
WARNING	Failed to process main mode packet.
WARNING	Failed to process mode configuration packet.
WARNING	Failed to process packet payloads.
WARNING	Failed to process payload.
WARNING	Failed to process quick mode packet.
WARNING	Ignoring AUTH message when aggressive mode already complete. Peer:
WARNING	Invalid DOI in delete message:
WARNING	Invalid IPSEC SA delete message.
WARNING	Invalid ISAKMP SA delete message.
WARNING	is not a supported OAKLEY attribute class.
WARNING	Protocol ID is not supported in SA payloads.
WARNING	Received an encrypted packet when not crypto active!
WARNING	Received an unencrypted packet when crypto active!
WARNING	Responder lifetime protocol is not supported.

Table 4: Log Viewer Warning Messages

WARNING	The password is incorrect. Please re-enter the password.
WARNING	The pre-shared key dialog box was cancelled by the user. The connection will be disabled.
WARNING	The select certificate dialog box was cancelled by the user. The connection will be disabled.
WARNING	The username/password dialog box was cancelled by the user. The connection will be disabled.
WARNING	Unable to decrypt payload!

Index

SonicWALL, Inc.

2001 Logic Drive
San Jose, CA 95124-3452

T +1 408.745.9600 www.sonicwall.com
F +1 408.745.9300

P/N: 232-002016-00
Rev A, 2/11

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™