SONICWALL GLOBAL VPN CLIENT 1.0

USER'S GUIDE

SONICWALL

SonicWALL Global VPN Client 1.0 User's Guide

Table of Contents

SonicWALL Global VPN Client User Guide

Introduction

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 secure, encrypted access through the Internet or corporate dial-up facilities for remote users such as mobile employees or telecommuters. The Global VPN Client also provides secure wireless (WiFiSec) networking for SonicWALL SOHO TZW clients.

The SonicWALL Global VPN Client combined with GroupVPN on SonicWALL Internet Security Appliances streamlines VPN deployment and management. Using SonicWALL's Client Policy Provisioning technology, the SonicWALL administrator establishes the VPN connection policies for the SonicWALL Global VPN Clients, removing the burden of provisioning VPN connections from the VPN client user. The VPN configuration data is transparently downloaded from the SonicWALL VPN Gateway (SonicWALL Internet Security Appliance) to Global VPN Clients or exported as a file for importing by Global VPN Clients.

SonicWALL Global VPN Client Features

The SonicWALL Global VPN Client delivers a robust IPSec VPN solution designed for quick and easy deployment with these features:

- **Ease of Use** - Provides an easy-to-follow Installation Wizard to quickly install the product and an easy-to-follow Configuration Wizard to easily configure a VPN connection.
- **Easy User Interface** - Offers a point-and-click activation of VPN and streamlined management tools to minimize support requirements.
- **Simple Client Policy Provisioning -** Using only the IP address or Fully Qualified Domain Name (FQDN) of the SonicWALL VPN gateway, the VPN connection gets established after automatically downloading the VPN configuration data from the SonicWALL VPN gateway via a secure IPSec tunnel. This removes 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.
- **Redundant Gateway Support** - Allows automatic redirect in case of SonicWALL VPN gateway failure. If the SonicWALL VPN gateway A is down, then the Global VPN Client can go through SonicWALL VPN gateway B.
- **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.

- **NAT Traversal -** Global VPN Client connections can 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.
- **DHCP Relay 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.
- **3DES Encryption** - Uses a 168-bit key for dramatically increased security than DES.
- **GMS Management** - Global VPN Client connections can be managed by SonicWALL's award-winning Global Management System (GMS).
- **Multi-Platform Client Support** - Supports Windows 98 SE, Windows ME, Windows NT 4.0 (service pack 3 or later), Windows 2000 Professional (service pack 3 or later), Windows XP Professional, and Windows XP Home Edition.

About this Guide

This guide explains installing, configuring, and managing the SonicWALL Global VPN Client. It also describes how to configure the SonicWALL gateway to automatically provision SonicWALL Global VPN Clients. This guide is updated and released with Global VPN Client version 1.0 and SonicWALL Internet Security Appliance firmware version 6.4.2.0 and SonicOS 1.0.0.0 (SOHO TZW). Always check www.sonciwall.com/support/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.

Copyright Notice

Installing the SonicWALL Global VPN Client

The Global VPN Client uses an easy-to-use wizard to guide you through the installation process. The SonicWALL Global VPN Client supports Windows 98 SE, Windows ME, Windows NT 4.0 (service pack 6 or later), Windows 2000 Professional (service pack 6 or later), Windows XP Professional, and Windows XP Home Edition.

Alert! The SonicWALL Global VPN Client requires a SonicWALL gateway running firmware version 6.4.2.0 (or higher) or SonicOS 1.0.0.0 (or higher) and a 3rd generation SonicWALL Internet Security Appliance.

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 page 44.

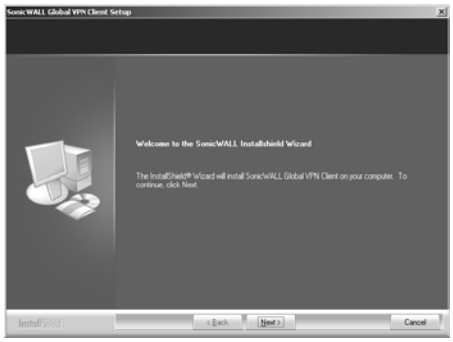
Using the Setup Wizard

The following steps explain how to install the SonicWALL Global VPN Client program using the **Setup Wizard**.

Alert! Remove any installed VPN client program before installing the SonicWALL Global VPN Client.

Alert! You must use a Zip program to unzip the SonicWALL Global VPN Client program files before installing it.

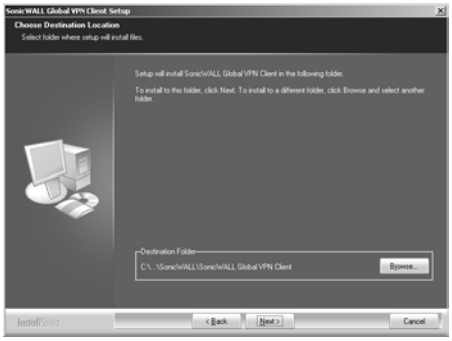
1. Unzip **SonicWALLGlobalVPNC1000.zip**.
2. Double-click **setup.exe**. The **Setup Wizard** launches.



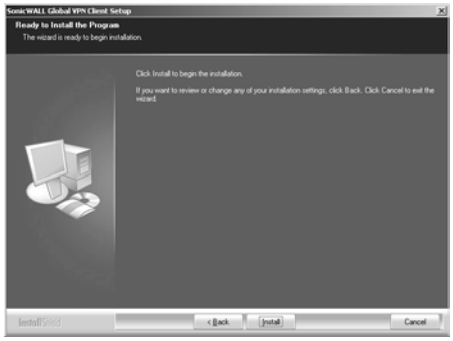
3. Click **Next** to continue installation of the VPN Client.

4. Close all applications and disable any disk protection and personal firewall software running on your computer. Click **Next**.

5. Select **I accept the terms of the license agreement**. Click **Next**.



6. Click **Next** to accept the default location and continue installation or click **Browse** to specify a different location.



7. Click **Install**. The **Setup Wizard** installs the Global VPN Client files on your computer.

8. Select **Start VPN Global Client Automatically when users log in** to automatically launch the VPN Global Client when you log onto the computer, if desired.
9. Select **Launch program now** to automatically launch the Global VPN Client after finishing the installation, if desired.
10. Click **Finish**.

Adding VPN Connection Policies

Adding a new VPN connection policy for the Global VPN Client is easy because SonicWALL's Client Policy Provisioning provides all the information necessary to make the VPN connection to the remote network. This information is transparently downloaded from the SonicWALL VPN Gateway via a secure IPSec VPN tunnel to your SonicWALL Global VPN Client or provided as a file for importing into SonicWALL Global VPN Client.

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 page 32.

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

The Global VPN Client allows multiple connection policies to be configured at the same time, whether they are provisioned from multiple gateways or imported from one or more files. Because connection policies may be provisioned from multiple gateways, each connection policy explicitly states allowed behavior in the presence of any connection policy conflicts.

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. For instructions on importing a certificate into the Global VPN Client, see page 25.

New Connection Wizard

The Global VPN Client's **New Connection Wizard** walks you through the process of locating the source of your configuration information. You can configure your Global VPN Client by downloading the VPN policy from a remote SonicWALL VPN gateway (SonicWALL Internet Security Appliance) or import the VPN policy from a local file.

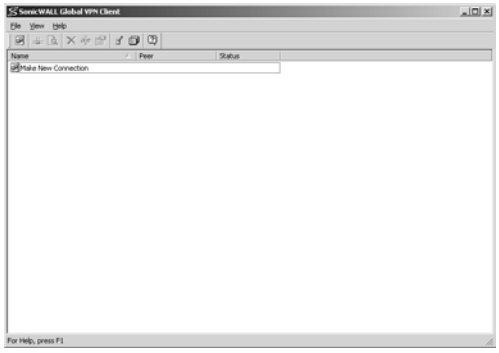
- **Downloading a VPN Policy from the SonicWALL VPN Gateway** - Downloading the Global VPN Client provisioning information is performed via a secure IPSec VPN tunnel to the SonicWALL VPN gateway. This configuration data is automatically downloaded when you use the **New Connection Wizard**. All you need for this configuration is the IP address or the Fully Qualified Domain Name (FQDN) of the SonicWALL Internet Security Appliance.
- **Importing a VPN Policy File** - If your SonicWALL VPN Gateway administrator provides you with a VPN connection policy file, you import the file into the Global VPN Client using the **New Connection Wizard**.

Downloading a VPN Policy from the SonicWALL VPN Gateway

The following instructions explain how to configure the SonicWALL Global VPN Client by downloading the connection policy from a SonicWALL VPN gateway using the **New Connection Wizard**.

⚠ **Alert!** You must have the IP address or FQDN of the remote SonicWALL VPN gateway and an active Internet connection before using the **New Connection Wizard**.

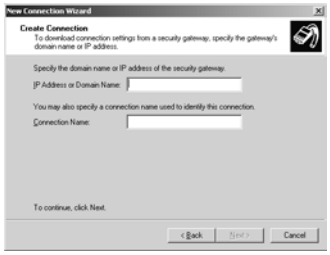
1. Choose **Start>Programs>SonicWALL Global VPN Client**.



2. Double-click the **Make New Connection** icon to launch the **New Connection Wizard**. Click **Next**.

3. **Download from a Gateway** is selected by default in the **Create or Import Connection** page. Click **Next.**

4. Type the IP address or FQDN of the gateway in the **IP Address or Domain Name** box.



5. Type a name for your VPN connection policy in the **Connection Name** field. Click **Next**.

6. 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.
7. 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 policy appears in the SonicWALL Global VPN Client window.

Importing a VPN Policy File

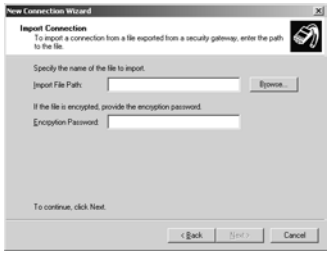
The VPN policy file is in the XML format to provide more efficient encoding of policy information. Because the file can be encrypted, pre-shared keys can also be exported in the file. The encryption method is specified in the PKCS#5 Password-Based Cryptography Standard from RSA Laboratories and uses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

The VPN policy file has filename extension **.rcf**.

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

1. Choose **Start>Programs>SonicWALL Global VPN Client**.
2. Double-click the **Make New Connection** icon to launch the **New Connection Wizard**. Click **Next**.
3. Select **Import from a File.** Click **Next**.

4. Type the file path in the **Import File Path** field or click **Browse** to locate the file. If the file is encrypted, enter the password in the **Encryption Password** field.

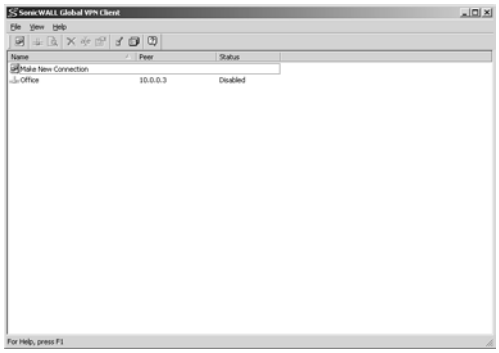


5. Click **Next** to continue.

6. 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.
7. 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 policy appears in the SonicWALL Global VPN Client window.

Launching the SonicWALL Global VPN Client

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



The default setting for the SonicWALL Global VPN Client window is **Hide the window (reopen it from the tray icon)**. 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.

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 page 18 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 page 17 for more information

Enabling a Pre-Shared Key VPN Connection

A Pre-Shared Key (also called a Shared Secret) is a predefined filed 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.

To establish a VPN connection using a VPN connection policy you created using the **New Connection Wizard**, follow these instructions:

1. Launch **SonicWALL Global VPN Client.** 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.

Tip! Right-clicking the SonicWALL Global VPN Client icon on the system tray, then selecting **Enable>***connection policy* establishes the VPN connection without opening the **SonicWALL Global VPN Client** window.

2. 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 policy in the SonicWALL Global VPN Client window.

   Right-click the VPN connection policy icon in the SonicWALL Global VPN Client window and select **Enable**.

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

   Select the VPN connection policy, and click the **Enable** button on the toolbar in the SonicWALL Global VPN Client window.

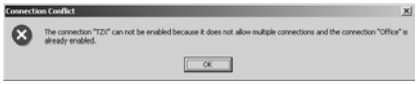
   Select the VPN connection policy, then choose **Enable>***connection policy*.

Establishing 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 connection for sending and receiving data.

When the SonicWALL VPN Client enables the VPN connection using the default settings, **Enable** appears in the **Status** column. When phase 1 completes, **Connected** appears in the **Status** Column. If an error occurs during phase 1, **Error** appears in the **Status** column. When phase 2 completes, the connection policy icon changes to include a green checkmark. If any of the phase 2 SAs (Security Associations) fail, the connection policy icon changes to include a warning icon. If all the phase 2 SAs fail, the connection policy icon changes to include a stop icon.

Establishing Multiple Connections

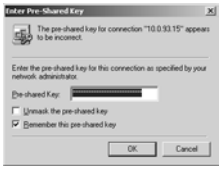
You can have more than one connection enabled at a time but it depends on the connection policy parameters established at the gateway. If you attempt to enable a subsequent VPN connection with a currently enabled VPN connection policy that does not allow multiple VPN connections, the **Connection Conflict**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



Entering a Pre-Shared Key

Depending on the attributes for the VPN connection policy, 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. Type in the Pre-Shared Secret provided by your SonicWALL administrator.



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 **Unmask the pre-shared key**. The Pre-Shared Key you enter appears unmasked in the **Pre-shared Key** field.
3. By default, the **Remember this Pre-shared Key** setting is checked allowing the Global VPN Client to save the key in an encrypted file to automatically send when enabling the VPN connection. Unchecking this setting displays the **Enter Pre-Shared Key** dialog box every time you enable the VPN connection to enter the Pre-Shared Key.
4. Click **OK**.

Username and Password Authentication

The gateway may specify 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 gateway, 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.

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 interface and 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.

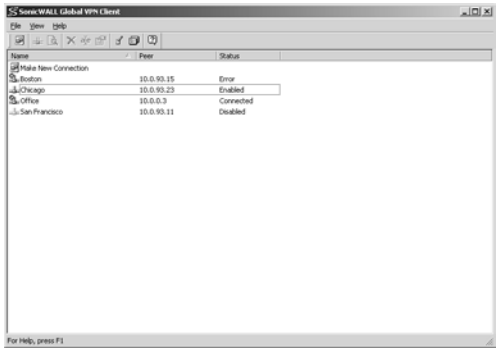
Disabling a VPN Connection

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

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 default **Details** view lists your VPN connection policies 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 policy.

  Select the VPN connection policy, then press **Ctrl+T**.

  Select the VPN connection policy, then click the **Status** button on the toolbar.

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

Tip! For more information on the **Status** page, see page 23.

Creating a VPN Connection Policy Shortcut

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

To create a shortcut:

1. Select the VPN connection policy 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 also right-click the VPN connection policy and then choose **Create Shortcut>***shortcut option*.

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.
- **When closing the connections window** - Specifies how the Global VPN Client window behaves after closing. 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.

SonicWALL 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 connection policies.
- **Disable** - Allows you to disable active VPN connections.
- **Open Log Viewer** - Opens the Log Viewer to view informational and error messages. See page 26 for more information on the Log Viewer.
- **Open Certificate Manager** - Opens the Certificate Manager. See page 25 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.

Managing VPN Connection Policy 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 policy and choose **File>Properties**.
- Right click the connection policy and select **Properties**.
- Select the connection policy 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 includes the following settings:

Name - Displays the name of your VPN connection policy.

Description - Displays a pop-up text about the connection policy. The text appears when your mouse pointer moves over the VPN connection policy.

Attributes - Defines the status of Tunnel All support. These settings are controlled at the SonicWALL VPN gateway.

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

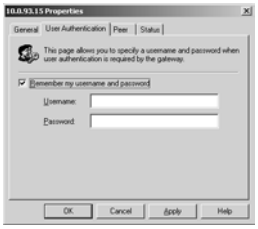
Enable this connection when the program is launched - Establishes the VPN connection policy as the default VPN connection when you launch the SonicWALL Global VPN Client.

Allow this connection to be re-enabled when waking from sleep or hibernation - Automatically re-enables the VPN connection policy after the computer wakes from a sleep or hibernation state. This setting is disabled by default.

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.

User Authentication

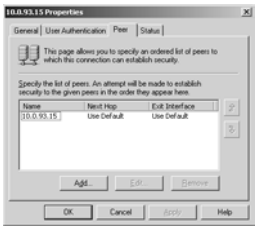
The **User Authentication** page allows you to specify a username and password when user authentication is required by the gateway. If the SonicWALL VPN gateway does not support the saving (caching) of a username and password, the settings in this page are not active and the message **The peer does not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

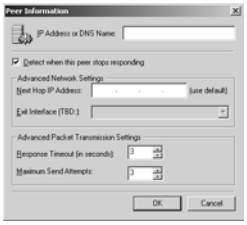
The **Peers** page allows you to specify an ordered list of VPN gateway peers that this connection policy can use (multiple entries allow a VPN connection to be established through multiple VPN gateways). An attempt is made to establish a VPN connection to the given VPN gateway peers in the order they 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.
- **Detect when this peer stops responding** - Automatically initiates VPN connection again if the VPN gateway does not respond for four consecutive heart beats. The Global VPN Client
  exchanges “heart beat” packets to detect if the peer gateway is alive. This setting is enabled by default.
- **Force the use of NAT traversal when connecting to this peer** - Forces the use of UDP encapsulation of IPSec packets even when there is no NAPT/NAT device in between the peers.
- **Advanced Network Settings -** Allows the user to manually configure the next hop IP address, if it needs to be something other than the default route.

  Next Hop IP Address (use default) - Specifies the IP address of next hop.
- **Advanced Packet Transmission Settings -** Allows manual configuration of the timeout value and retries for IKE negotiations.

  Response Timeout (in seconds) - Specifies timeout value.

  Maximum Send Attempts - Specifies the number of IKE negotiation retries.

Status

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

- **Connection**

  Status - Indicates whether VPN connection policy is enabled or disabled.

  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.

  Renew - Renews DHCP lease information.

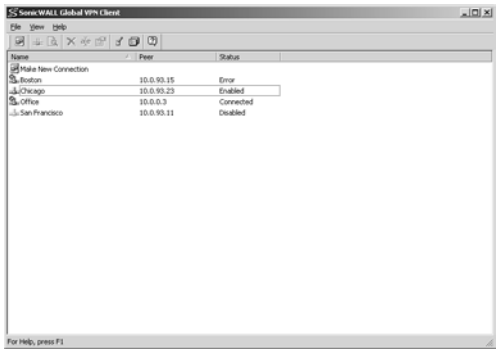
Managing VPN Connection Policies

The SonicWALL Global VPN Client supports as many VPN connection policies as you need. To help you manage these connection policies, the Global VPN Client provides the following connection policy management tools.

Displaying Connection Policies

You can display VPN connection policy icons using standard Windows icon display modes by choosing **Large Icons**, **Small Icons**, **List**, or **Details** from the **View** menu in the SonicWALL Global VPN Client window.

The default **Details** view provides a handy view of your VPN connection profiles including their gateway IP addresses or FQDNs as well as the status of the connection policies (**Disabled**, **Enabled**, **Connected**, or **Error**).



Arranging Connection Policies

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

Name - Sorts connection policies by name.

Gateway - Sorts connection policies by gateway IP address.

Status - Sorts connection policies by connection status.

Ascending - Sorts Name, Gateway, or Status arrangements in ascending order. If unchecked, policy arrangements are sorted in descending order.

The default arrangement is by **Name** in **Ascending** order**.**

Renaming a Connection Policy

To rename a connection policy, select the policy 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 policy and choose **Rename** from the menu.

Deleting a Connection Policy

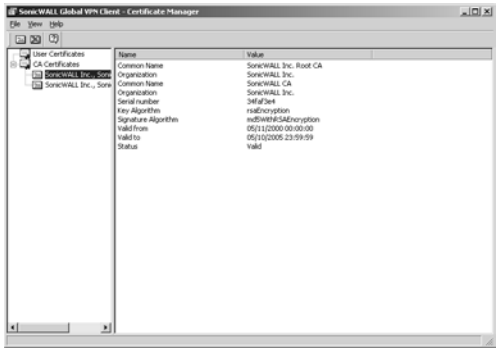
To delete a connection policy, select the policy, press **Del** or choose **File>Delete**. You can also right-click the policy name and choose **Delete**. You cannot delete an active VPN connection. Disable the VPN connection, then delete it.

Selecting All Connection Policies

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

Managing Certificates

The **Certificate Manager** allows you to manage your digital certificates. To open the Certificate Manager, click the **Certificate Manager** button on the SonicWALL Global VPN Client window toolbar, choose **View>Certificate Manager**, or press **Ctrl+M**.



The left pane of the **Certificate Manager** window lists the active certificates currently used for your VPN connections. User Certificates list digital certificates assigned to your computer. CA Certificates list the digital certificates assigned to the SonicWALL VPN Gateway.

- Click on the certificate in the left pane to display the certificate information in the right pane.
- Click the **Import** button on the toolbar, press **Ctrl+I**, or choose **File>Import Certificate** from the to display the **Import Certificate** window to import a certificate file.
- Click the **Delete** button on the toolbar, press **Del**, or choose **File>Delete Certificate** to delete the selected certificate.
- Choose **View>Toolbar** to hide the toolbar.
- Choose **View>Status Bar** to hide the status bar.

Troubleshooting SonicWALL Global VPN Client

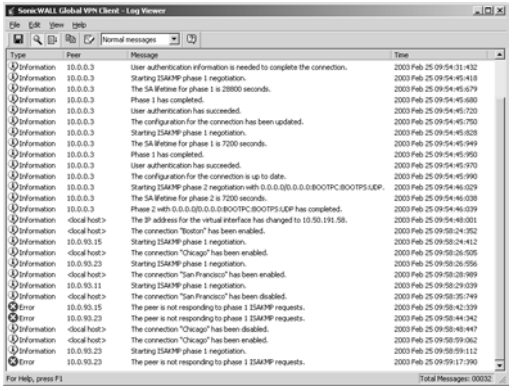
The SonicWALL Global VPN Client provides tools for troubleshooting your VPN connections. This section explains using Log Viewer, generating a Help Report, accessing SonicWALL's Support site, using SonicWALL Global VPN Client help system, and uninstalling the Global VPN Client.

Log Viewer

The **SonicWALL Global VPN Client Log Viewer** window displays messages about Global VPN Client activities. The Log Viewer window displays the type of message (**Information**, **Error**, or **Warning**) the peer IP address or FQDN, and the date and time the message was generated.

Tip! See **Appendix A** for complete listing of Log Viewer messages.

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**.



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**.
- To enable or disable message capturing, click the **Capture** button on the toolbar, press **Ctrl+M**, or choose **View>Stop Capturing Messages** or **View>Start Capturing Messages**.
- To start or stop automatic scrolling of messages to the latest message, click the **Auto Scroll** button on the toolbar, press **Ctrl+T**, or choose **View>Start Auto Scroll** or **View>Stop Auto Scroll**.
- 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 specify the message display level from **All Messages** to **Normal Messages**, click the drop-down list box on the toolbar, or choose **View>Message Level**.
- To remove redundant messages from displaying, choose **View>Ignore Redundant Messages** or press **Ctrl+I**.
- 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**.

Setting Up Log Files

The **Auto-Logging** tab in the **Options** dialog box specifies the settings to use when automatically logging messages to a file. Log files are saved as text files (**.txt**). To access Auto-Logging from the SonicWALL Global VPN Client window, choose **View>Options**, then click the **Auto-Logging** tab.

Enable auto-logging - Enables auto-logging to a file.

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.

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 - Instructs Auto-logging what to do when log file size is reached.

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

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

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

Generating a Help Report

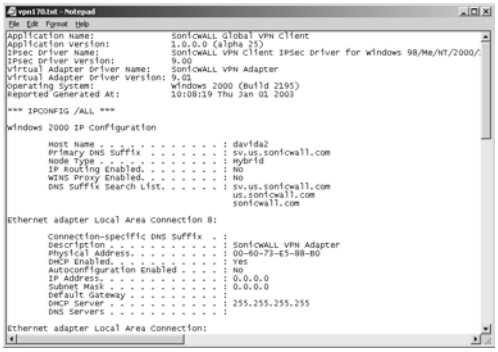
Choosing **Help>Generate Report** in the SonicWALL Global VPN Client window displays the **SonicWALL Global VPN Client Report** dialog box.

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**.



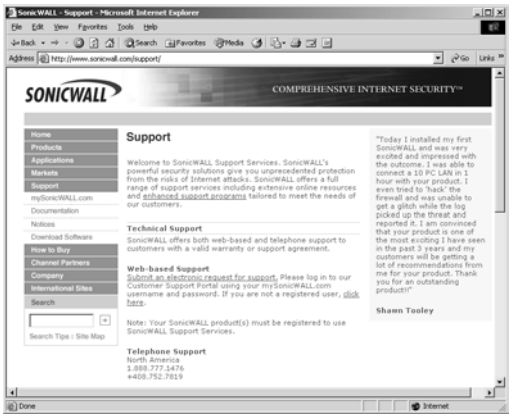
To save the report to a text file, click **Save As**.

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

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

Technical Support

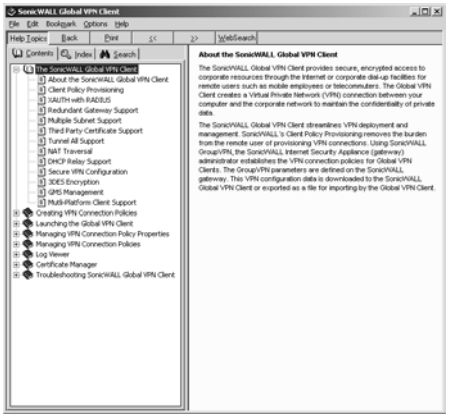
Selecting **Help**>**Technical Support** accesses the SonicWALL Support site (www.sonicwall.com/support). The SonicWALL Support site offer a full range of support services including extensive online resources and information on SonicWALL's enhanced support programs.



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 connection policies as part of the uninstall process. To uninstall the SonicWALL Global VPN Client:

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

1. Launch the Windows Control Panel
2. Double-click **Add/Remove Programs**
3. Select SonicWALL Global VPN Client 1.0, then click **Change/Remove**. The SonicWALL Global VPN Client Setup Wizard appears.
4. Select **Remove** and **Click** Next. The **Confirm File Deletion** message appears.
5. Click **OK** to proceed with program removal. The **Confirm Delete User Profiles** message appears.
6. Click **Yes** to delete your VPN connection policies or click **No** to save the policies. If you select **No**, the VPN connection policies are saved and appear again when you install the SonicWALL Global VPN Client.
7. After the SonicWALL Global VPN Client is removed, select **Yes, I want to restart my computer now**, then click **Finish**.

Configuring the SonicWALL for Global VPN Clients

SonicWALL's GroupVPN Security Association (SA) provides the automatic provisioning of SonicWALL Global VPN Client from the SonicWALL Internet Security Appliance. The GroupVPN security association (SA) is only available for SonicWALL Global VPN Clients. SonicWALL GroupVPN supports three IPSec keying modes: **IKE using shared secret**, **IKE using SonicWALL Certificates**, and **IKE using 3rd Party Certificates**.

Once you create the GroupVPN SA, 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.

The following instructions explain how to configure GroupVPN with **IKE using Preshared Secret** on 3rd generation SonicWALLs running firmware version 6.4.2.0 and the SonicWALL TZW running SonicOS version 1.0.0.0. For more detailed information on setting up GroupVPN, see the Administrator's Guide for your SonicWALL.

Tip! For information on configuring GroupVPN using **IKE using SonicWALL Certificates** or **IKE using 3rd Party Certificates**, see the Administrator's Guide for your SonicWALL.

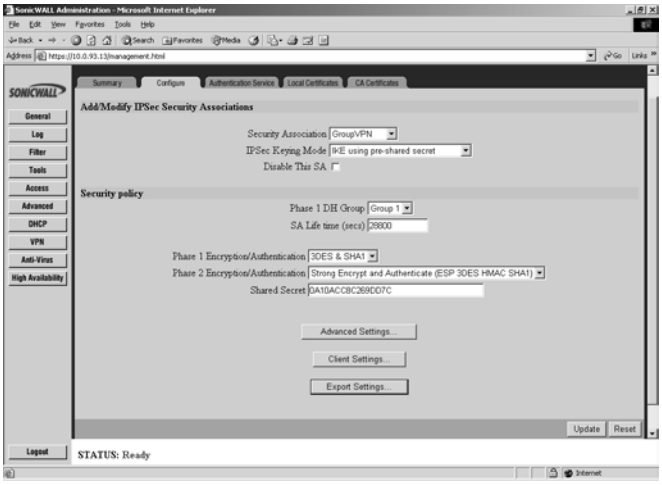
Alert! Your SonicWALL Internet Security Appliance must be a 3rd generation product using firmware version 6.4.2.0.0 (or higher) or SonicOS 1.0.0.0 (SOHO TZW) to support SonicWALL Global VPN Clients.

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 page 44.

Configuring GroupVPN (Firmware v6.4.2.0)

The following instructions explain how to configure GroupVPN on SonicWALL Internet Security Appliances running firmware version 6.4.2.0

1. Log into your SonicWALL's Management Interface.
2. Click **VPN** on the left side of the SonicWALL management interface.
3. Click on the **Configure** tab.

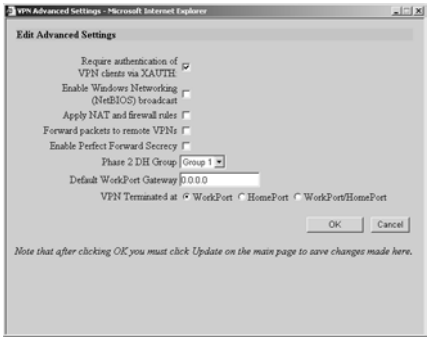


4. Select **GroupVPN** from the **Security Association** drop-down list.
5. Select **IKE using pre-shared secret** from the **IPSec Keying Mode** drop-down list box.
6. If the **Disable This SA** box is checked, uncheck it.
7. Select **Group 2** from the **Phase 1 DH Group** menu.
8. Type the **SA Life Time** value in seconds. The default value of 28800 seconds (8 hours) is recommended.
9. Select **3DES & SHA1** from the **Phase 1 Encryption/Authentication** drop-down list box.
10. Select **Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)** from the **Phase 2 Encryption/Authentication** drop-down list box.
11. Type a Shared Secret in the **Shared Secret** box or use the **Shared Secret** automatically generated by the SonicWALL. If you enter a Shared Secret, the value should consist of a combination of letters and numbers. A Shared Secret is case-sensitive.
12. Click **Update** to enable the changes.

Configuring Advanced Settings (Optional)

All the advanced settings for GroupVPN connections are configured in the **Advanced Settings** window. These settings are optional. To configure GroupVPN advanced settings:

1. Click **Advanced Settings** to open the **VPN Advanced Settings** window.



2. Select any of the following boxes in the **Advanced Settings** window that apply to your GroupVPN SA:

   Require authentication of VPN clients via XAUTH - All Global VPN Client users will be authenticated via XAUTH using the authentication service specified on the **Access>Users** page.

   Enable Windows Networking (NetBIOS) broadcast - Select this setting if you want to allow Global VPN Client access to network resources by browsing the Windows Network Neighborhood.

   Apply NAT and firewall rules - Allows a remote site's LAN subnet to be hidden from the corporate site. It is most useful when a remote office's network traffic is initiated to the corporate office.

   Forward packets to remote VPNs - Allows the remote VPN tunnel to participate in the SonicWALL routing table.

   Enable Perfect Forward Secrecy - Adds an additional layer of security using a second Diffie-Hellman key exchange.

   Phase 2 DH Group - Generates an additional key exchange if you select **Enable Perfect Forward Secrecy**.

   Default LAN/WorkPort Gateway - Allows the network administrator to specify the next hop IP address on the gateway network. Required only if the Global VPN Client has a tunnel all policy.

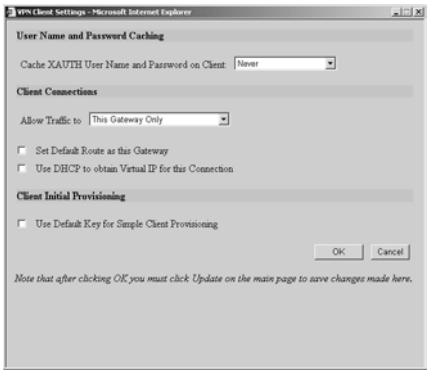
   VPN Terminated at - Select **LAN** (**WorkPort**), **DMZ** (**Home Port**), or **LAN/DMZ** (**WorkPort**/**HomePort**) to terminate a VPN tunnel at a specific destination rather than the entire network to restrict access only to specified resources.

3. Click **OK**.
4. Click **Update** to enable the changes.

Configuring VPN Client Settings

Clicking the **Client Settings** button in the **Configure** tab displays the **VPN Client Settings** window. The controls in this window allows configuration of Global VPN Client authentication requirements, username and password caching, use of DHCP Relay, and multi-connection behavior.

1. Click **Client Settings**. The **VPN Client Settings** window appears.



2. Select any of the following boxes that you want to apply to Global VPN Client provisioning:

- **Cache XAUTH User Name and Password** - Allows Global VPN Client to cache any username and password required for XAUTH user authentication. The drop-down list provides the following
  options:

  Never - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.

  Single Session - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.

  Always - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Allow Traffic to** - Specifies single or multiple VPN connections. The drop-down list provides the following options:

  This Gateway Only - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of this gateway is sent through the VPN tunnel. All other traffic is blocked. If this option is selected along with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked.

All Secured Gateways - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.

Any Destination - Same as the All Secured Gateways option but Internet traffic is sent through the VPN tunnel when the **Set Default Route as this Gateway** is not enabled.

- **Set Default Route as this Connection** - If checked, Global VPN Client traffic that does not match selectors for the gateway's protected subnets must also be tunneled. In effect, this changes the Global VPN Client's default gateway to the gateway tunnel endpoint. If unchecked, the Global VPN Client must drop all non-matching traffic if **Allow traffic to This Gateway Only** or **All Secured Gateways** is selected.
- **Use DHCP to Obtain Virtual IP for this Connection** - If set, this allows the Global VPN Client to obtain the IP address and other attributes like DNS and WINS from an external DHCP server on the LAN side of the gateway.
- **Use Default Key for Simple Client Provisioning** - If set, authentication of initial Aggressive mode exchange uses a default Pre-Shared Key by gateway and all Global VPN Clients. This allows for the control of the use of the default registration key. If not set, then Pre-Shared Key must be distributed out of band.

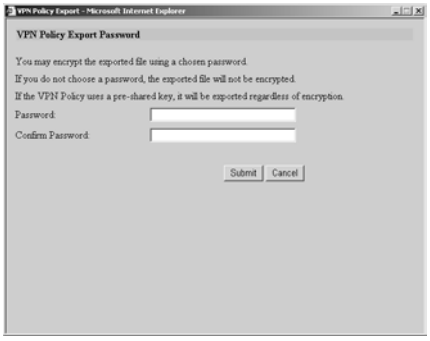
3. Click **OK**.
4. Click **Update** to enable the changes.

Exporting GroupVPN Settings to a File

To export the **GroupVPN** settings to a file, click on the **Export Settings** button in the **Configure** tab to display the **Export Security Association** window. The controls in this window allow you to export the SA to a file. SonicWALL Global VPN Client users import this file using the **New Connection Wizard**.

To export the GroupVPN SA to a file,

1. Click the **Export Settings** button in the **Configure** tab to display the **Export Security Association** window.
2. Select **rcf format is required for SonicWALL Global VPN Clients**. Files saved in the rcf format can be password encrypted.
3. Click **Yes**. The **VPN Policy Export** window appears**.**



4. Type a password in the **Password** text box and re-enter it in the **Confirm Password** text box, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.
5. Click **Submit**. If you did not enter a password, a message window appears confirming your choice.
6. Click **OK.** The **File Download** window appears showing the default filename.
7. Save the file.
8. Click **Close**.

The security file can be saved to a floppy disk or e-mailed to a remote VPN client. The SA must be enabled on the SonicWALL to export the configuration file.

Authenticating VPN Users with Username and Password

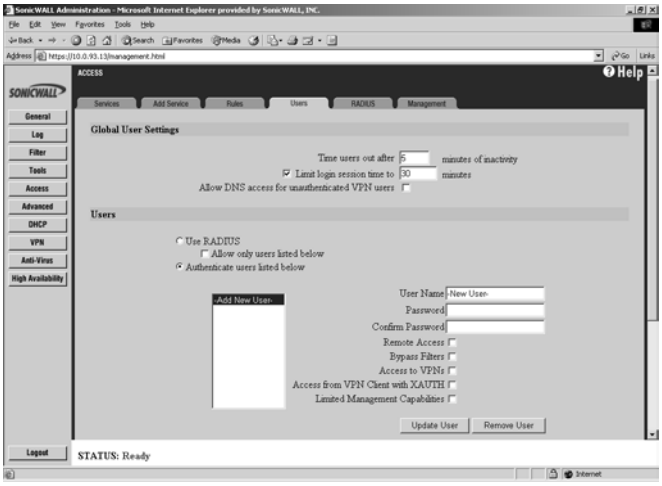
Authenticating users provides added security for your VPN by requiring Global VPN Client users to log into your VPN using a username and password. User level authentication can be performed using a database on the SonicWALL, a RADIUS server, or a combination of the two methods. The local database on the SonicWALL supports up to 100 users.

The following instructions explain how to set up user level authentication for your Global VPN Clients using the local database on the SonicWALL.

Note For more information on authenticating Global VPN Clients using an external RADIUS server for authentication of SonicWALL Global VPN Clients, see the Administrator's Guide for your SonicWALL.

To require Global VPN Clients to authenticate with XAUTH using the internal SonicWALL user database,

1. Navigate to the **Access>Users** page.



2. Select **Authenticate users listed below**.
3. Type the username in the **User Name** text box.
4. Type the password in the **Password** text box.
5. Type the password again in the **Confirm Password** text box.
6. Select **Access from VPN Client with XAUTH**.
7. Click **Update User**.
8. Repeat steps 3 - 7 for each additional user up to 100 users.
9. Click **Update**.

Alert! You must provide the Global VPN Client user with the XAUTH username and password entered in the SonicWALL user database to allow access to your VPN.

Configuring GroupVPN on the SOHO TZW (SonicOS v1.0.0.0)

GroupVPN is automatically configured on the SOHO TZW to support secure (WiFiSec) wireless networking using SonicWALL Global VPN Clients installed on WLAN clients. The Global VPN Client software is available on the SOHO TZW Product CD.

For remote VPN connections using the SonicWALL Global VPN Client, you must purchase an upgrade license to enable VPN connectivity from the Internet through the SOHO TZW WAN port. For more information on SonicWALL Global VPN Client Licenses, see page 44.

Configuring GroupVPN using Preshared Secret

The following instructions explain how to configure GroupVPN on the SOHO TZW to support Global VPN Clients.

1. To configure Group VPN on the SonicWALL TZW, in the **VPN>Settings** page click the **Notepad** icon under **Configure**. The **VPN Policy** window is displayed.
2. On the **General** tab, in the **Security Policy** section, **IKE using Preshared Secret** is selected by default from the **IPSec Keying Mode** menu. The SA name is **GroupVPN** by default and cannot be changed.
3. Use the SonicWALL generated Shared Secret or type your own shared secret in the **Shared Secret** field. If you create you own shared secret, use a combination of letters, numbers, and symbols. Remember a shared secret is case-sensitive.

Proposals

4. Click on the **Proposals** tab.
5. In the **IKE (Phase 1) Proposal** section, select the following settings:

   Group 2 from the **DH Group** menu

   3DES from the **Encryption** menu

   SHA1 from the **Authentication** menu
6. Leave the default setting, 28800, in the **Life Time (secs)** field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.
7. In the **IPSec (Phase 2) Proposal** section, select the following settings:

   ESP from the **Protocol** menu

   3DES from the **Encryption** menu

   MD5 from the **Authentication** menu
8. Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Then select **Group 2** from the **DH Group** menu.
9. Leave the default setting, 28800, in the Life Time (secs) field. This setting forces the tunnel to renegotiate and exchange keys every 8 hours.

Advanced (Optional)

10. Click on the **Advanced** tab and select any of the following settings that you want to apply to your GroupVPN SA:

    Enable Windows Networking (NetBIOS) broadcast - allows access to remote network resources by browsing the Windows® Network Neighborhood.

    Apply NAT and Firewall Rules - allows a remote site's LAN subnet to be hidden from the corporate site, and is most useful when a remote office's network traffic is initiated to the corporate office. The IPSec tunnel is located between the SonicWALL WAN interface and the LAN segment of the corporation. To protect the traffic, NAT (Network Address Translation) is performed on the outbound packet before it is sent through the tunnel, and in turn, NAT is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the SonicWALL public address) from the corporate LAN. If the SonicWALL uses the **Standard** network configuration, using this check box applies the firewall access rules and checks for attacks, but not does not apply NAT.

⚠ **Alert!** You cannot use this feature if you have selected **Route all Internet traffic through this SA** in the **Advanced** window.

⚠ **Alert!** Offices can have overlapping LAN IP ranges if the **Apply NAT and Firewall Rules** feature is selected.

Forward Packets to Remote VPNs - allows the remote VPN tunnel to participate in the SonicWALL routing table. Inbound traffic is decrypted and can be forwarded to a remote site via another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the SonicWALL LAN or a specific route on the LAN configured on the **Routing** page located in the **Network** section. Enabling this feature allows a network administrator to create a "hub and spoke" network configuration by forwarding inbound traffic to a remote site via a VPN security association. To create a "hub and spoke" network, select the **Forward Packets to Remote VPNs** check box. Traffic can travel from a branch office to a branch office via the corporate office.

Default LAN Gateway - used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. **Default LAN Gateway** allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a **Default LAN Gateway**. If a **Default LAN Gateway** is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

VPN Terminated at the LAN, WLAN, or LAN/WLAN - Selecting this option allows you to terminate a VPN tunnel on a specific destination instead of allowing the VPN tunnel to terminate on the entire SonicWALL network. By terminating the VPN tunnel to a specific

destination, the VPN tunnel has access to a specific portion of the destination LAN or WLAN network.

Require Authentication of VPN Clients via XAUTH - requires that all inbound traffic on this SA is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

Client

11. Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:

Cache XAUTH User Name and Password - Allows Global VPN Client to cache any username and password required for XAUTH user authentication. The drop-down list provides the following options:

- **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
- **Single Session** - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
- **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.

Allow Traffic to - Specifies single or multiple VPN connections. The drop-down list provides the following options:

- **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of this gateway is sent through the VPN tunnel. All other traffic is blocked. If this option is selected along with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked.
- **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set **Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
- **Any Destination** - Same as the All Secured Gateways option but Internet traffic is sent through the VPN tunnel when the Set Default Route as this Gateway is not enabled.

Set Default Route as this Gateway - If checked, Global VPN Client traffic that does not match selectors for the gateway's protected subnets must also be tunneled. In effect, this changes the Global VPN Client's default gateway to the gateway tunnel endpoint. If unchecked, the Global VPN Client must drop all non-matching traffic if Allow traffic to This Gateway Only or All Secured Gateways is selected.

Use DHCP to Obtain Virtual IP for this Connection - If set, this allows the Global VPN Client to obtain the IP address and other attributes like DNS and WINS from an external DHCP server on the LAN side of the gateway.

Use Default Key for Simple Client Provisioning - If set, authentication of initial Aggressive mode exchange uses a default Preshared Key by gateway and all Global VPN Clients. This allows for the control of the use of the default registration key. If not set, then Preshared Key must be distributed out of band.

12. Click **OK**.
13. Click **Apply** to enable the changes.

Export VPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:

Alert! The GroupVPN SA must be enabled on the SonicWALL to export a configuration file.

1. Click the **Disk** icon under **Configure** for the GroupVPN Security Association. The **Export VPN Client Policy** window appears.
2. **rcf format is required for SonicWALL Global Clients** is selected by default. Files saved in the rcf format can be password encrypted.
3. Click **Yes**. The VPN Policy Export window appears.
4. Type a password in the **Password** field and re-enter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.
5. Click **Submit**. If you did not enter a password, a message appears confirming your choice.
6. Click **OK**. The **File Download** window appears showing the default file name.
7. Save the file.
8. Click **Close**.

The file can be saved to a floppy disk or sent electronically to remote users to configure their Global VPN Clients.

Authenticating VPN Users with Username and Password

Authenticating users provides added security for your VPN by requiring Global VPN Client users to log into your VPN using a username and password. User level authentication can be performed using a database on the SonicWALL, a RADIUS server, or a combination of the two methods. The local database on the SonicWALL supports up to 100 users.

The following instructions explain how to set up user level authentication for your Global VPN Clients using the local database on the SonicWALL.

Note For more information on authenticating Global VPN Clients using an external RADIUS server for authentication of SonicWALL Global VPN Clients, see the Administrator's Guide for your SonicWALL.

1. Select **Users>Settings** in the SonicWALL Management Interface.
2. Select **Authenticate users listed below**.
3. Click the **Add** button in the **Users** section. The **Add User** window is displayed.
4. Type the username in the **User Name** field.
5. Select **Access from VPN client with XAUTH** to require the Global VPN Client user to login before accessing VPN.
6. Click **OK**.
7. Repeat steps 3 - 6 for each additional user.
8. Click **Apply**.

Alert! You must provide the Global VPN Client user with the XAUTH username and password entered in the SonicWALL user database to allow access to your VPN.

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 additonal Global VPN Client connections. Once the number of simultaneous Global VPN Client drops below the license limit, new Global VPN connections can be established.

VPN Connections Supported by Each SonicWALL Model

The number of Security Associations each SonicWALL model supports. An SA refers to all the settings needed to create a single VPN tunnel. A VPN tunnel can be a Global VPN Client to SonicWALL VPN connection or a SonicWALL to SonicWALL connection for LAN to LAN connections. The SAs supported by each SonicWALL Internet Security Appliance model are the maximum number of simultaneous VPN connections that can be supported at any one time.

You can purchase Global VPN Client software from SonicWALL, your reseller, or online at mysonicwall.com. For more information on purchasing the Global VPN Client www.sonicwall.com/products/vpnglobal.html.

.

Table 1: IPSec VPN and Global VPN Client Support by SonicWALL Model

SonicWALL Model	**SAs Supported**	**IPSec VPN and Global VPN Clients**
TELE3 TELE3 TZ TELE TZX	5	Includes IPSec VPN Requires Global VPN Client license.
TELE3 SP	10	Includes IPSec VPN Requires Global VPN Client license.
SOHO3/10 SOHO3/25 SOHO3/50	10	Requires IPSec VPN Upgrade (SOHO 3/10 Only) Requires Global VPN Client license.
SOHO TZW	50	Includes IPSec VPN and Global VPN Clients for WLAN. Requires Global VPN Client license for WAN VPN access.
PRO 100	50	Includes IPSec VPN and 1 Global VPN Client license.
PRO200/230	500	Includes IPSec VPN and 10 Global VPN Client licenses.
PRO 300/330	1,000	Includes IPSec VPN and 200 Global VPN Client licenses.
GX250	5,000	Includes IPSec VPN and 5,000 Global VPN Client licenses.
GX650	10,000	Includes IPSec VPN and 10,000 Global VPN Client licenses.

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 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 supercedes 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.

SonicWALL Global VPN Client Support

SonicWALL's comprehensive support services protect your network security investment and offer the support you need - when you need it.

Knowledge Base - All SonicWALL customers have immediate, 24X7 access to our state-of-the-art electronic support tools. Power searching technologies on our Web site allow customers to locate information quickly and easily from our robust collection of technical information - including manuals, product specifications, operating instructions, FAQs, Web pages, and known solutions to common customer questions and challenges.

Expertise - Technical Support is only as good as the people providing it to you. SonicWALL support professionals are Certified Internet Security Administrators with years of experience in networking and Internet security. They are also supported by the best in class tools and processes that ensure a quick and accurate solution to your problem.

Warranty Support - North America and International

SonicWALL products are recognized as extremely reliable as well as easy to configure, install, and manage. SonicWALL Warranty Support enhances these features with

- 1 year, factory replacement for defective hardware
- 90 days of advisory support for installation and configuration assistance during local business hours
- 90 days of software and firmware updates
- Access to SonicWALL's electronic support and Knowledge Base system.

SonicWALL Support 8X5

Designed for customers who need advanced technical support and the additional benefits of ongoing software updates, SonicWALL Support 8X5 is an annual service that includes

- Telephone or electronic technical support during local business hours
- Access to SonicWALL's electronic support and Knowledge Base systems
- All software updates and upgrades

SonicWALL Support 24X7

For customers with mission-critical network requirements who cannot afford downtime, SonicWALL Support 24X7 is an annual subscription service that offers

- Telephone or electronic support, 24 hours, seven days a week
- Enhanced escalation for high priority problems
- Access to SonicWALL's electronic support and Knowledge Base systems
- All software updates and upgrades

All of SonicWALL Support Services offer a variety of support services to meet your unique needs including fast, responsive service, instant access to electronic support tools, and high quality technical support.

SonicWALL Support Services Features and Benefits

Telephone or Web-based Technical Support. SonicWALL's technical support experts help solve your problems or answer your questions quickly, reducing your risk of Internet attack.

Knowledge Base. Instant access to solutions and documentation provides answers to questions and solves problems electronically.

Firmware/Software Upgrades. Automatic firmware and software upgrades give instant access to new features and capabilities, allowing you to extend your Internet security investment.

Annual Support Agreement. Low, fixed prices for support services allow you to budget accurately and protect you from unexpected technical support expenses.

Table 2:

	SonicWALL Warranty	SonicWALL Support 8X5	Super SonicWALL Support
Telephone/Web-based technical support	90 days 8:00 a.m. - 5:00 p.m., local time, Monday - Friday	1-year 8:00 a.m. - 5:00 p.m., local time, Monday - Friday	1-year 24 hours by 7 days a week
Hardware Replace-ment	1 year, return to factory	1 year, return to factory	1 year, advanced exchange
Software/Firmware Updates	90 days	1-year	1-year
Enhanced Escalation			Yes

Warranty Support - *North America*

Included with all SonicWALL products, SonicWALL warranty support includes return-to-factory hardware replacement for one year. Warranty Support also includes technical support and software/firmware updates for 90 days. Coverage is provided during normal business hours.

Coverage Hours

Support is provided during standard business hours, 24 hours per day local time, seven days per week, including locally-recognized SonicWALL holidays.

Telephone and Web-based Support

SonicWALL provides technical assistance during standard coverage hours by telephone or through Web-based support tools for 90 days after the date of purchase. A SonicWALL technical specialist works with you to remotely diagnose and identify firmware and hardware not performing to documented specifications. Web-based support includes interactive communication with a SonicWALL technical specialist. SonicWALL also provides general assistance regarding usage and documentation on a limited basis.

Software/Firmware Support

SonicWALL logs, tracks, prioritizes, and resolves software, firmware and/or documentation bug reports and enhancement requests for software support for a period of 90 days after the date of purchase.

Software/Firmware Updates

All software and firmware maintenance releases and updates are included for 90 days after the date of purchase. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

Warranty Support provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

This warranty is available only in the United States and Canada.

Warranty Support - *International*

Included with all SonicWALL products, SonicWALL warranty support includes return-to-factory hardware replacement for one year. Warranty Support also includes technical support and software/firmware updates for 90 days. Coverage is provided during normal business hours.

Coverage Hours

Support is provided during standard business hours, 24 hours per day local time, seven days per week, including locally-recognized SonicWALL holidays.

Software/Firmware Updates

All software and firmware maintenance releases and updates are included for 90 days after the date of purchase. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

Warranty Support provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

This warranty applied to products sold in Europe, the Middle East, Africa, Asia, Central and South America.

SonicWALL Support 24X7

Available for all SonicWALL products, **SonicWALL Support 24X7** includes software/firmware technical support, and factory replacement of defective hardware. Coverage is provided 24 hours a day, seven days a week.

Coverage Hours

Support is provided during standard business hours, 24 hours per day local time, seven days per week, including locally-recognized SonicWALL holidays.

Telephone and Web-based Support

SonicWALL provides technical assistance during standard coverage hours by telephone or through Web-based support tools. A SonicWALL technical specialist works with you to remotely diagnose and identify firmware and hardware not performing to documented specifications. Web-based support includes interactive communication with a SonicWALL technical specialist. SonicWALL also provides general assistance regarding usage and documentation on a limited basis.

Software/Firmware Support

SonicWALL logs, tracks, prioritizes, and resolves software, firmware and/or documentation bug reports and enhancement requests for software support under this agreement.

SonicWALL Support 24X7 includes priority escalation based on problem severity.

Support for software, firmware, and documentation is limited to the most current version and the immediate prior revision.

Software/Firmware Updates

All software and firmware maintenance releases and updates are included with this agreement. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

SonicWALL Support 24X7 provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

SonicWALL Support 24X7 is an annual service available for sale at the time of product purchase or anytime before warranty expiration.

SonicWALL Support 8X5

Available for all products, **SonicWALL Support 8X5** includes software/firmware technical support and factory hardware replacement. Coverage is provided during standard business hours.

Coverage Hours

Support is provided during standard business hours, 8:00 a.m. - 5:00 p.m. local time, Monday through Friday, excluding locally-recognized SonicWALL holidays.

Telephone and Web-based Support

SonicWALL provides technical assistance during standard coverage hours by telephone or through Web-based support tools. A SonicWALL technical specialist works with you to remotely diagnose and identify firmware and hardware not performing to documented specifications. Web-based support includes interactive communication with a SonicWALL technical specialist. SonicWALL also provides general assistance regarding usage and documentation on a limited basis.

Software/Firmware Support

SonicWALL logs, tracks, prioritizes, and resolves software, firmware and/or documentation bug reports and enhancement requests for software support under this agreement.

SonicWALL Support 8X5 includes priority escalation based on problem severity.

Support for software, firmware, and documentation is limited to the most current version and the immediate prior revision.

Software/Firmware Updates

All software and firmware maintenance releases and updates are included with this agreement. SonicWALL notifies administrators via electronic mail of new updates. The updates are delivered exclusively via the Web.

Support Tools

SonicWALL Support 8X5 provides access to SonicWALL's Web-based support tools, including FAQs, documentation, and Knowledge Base systems.

Availability

SonicWALL Support 8X5 is an annual service available for sale at the time of product purchase or anytime before warranty expiration.

Appendix A - Log Viewer Messages

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

Table 3: Log Viewer Messages

ERROR	"Invalid DOI in notify message,"
ERROR	"Invalid DOI in notify message,"
ERROR	: called with invalid parameters.
ERROR	:called with invalid parameters.
ERROR	A phase 2 IV has already been created.
ERROR	A phase 2 IV has already been created.
ERROR	An error occurred.
ERROR	An error occurred.
ERROR	Attributes were specified but not offered.
ERROR	Attributes were specified but not offered.
ERROR	Authentication algorithm is not supported.

Table 3: Log Viewer Messages

ERROR	Authentication algorithm is not supported.
ERROR	CA certificate not found in list.
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 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	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 change the Diffie-Hellman group for PFS.
ERROR	Can not process packet that does not have at least one payload.
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 mode config type.
ERROR	Can not process unsupported XAuth type.
ERROR	Can not process unsupported XAuth type.
ERROR	Can not set IPSEC proposals into empty SA list.
ERROR	Can not set IPSEC proposals into empty SA list.
ERROR	Cannot do quick mode: no SA's to negotiate.
ERROR	Cannot do quick mode: no SA's to negotiate.
ERROR	certificate error.
ERROR	certificate error.
ERROR	Certificate ID not specified.
ERROR	Certificate ID not specified.

Table 3: Log Viewer Messages

ERROR	Deallocation of event publisher context failed.
ERROR	Deallocation of event publisher context failed.
ERROR	Diffie-Hellman group generator length has not been set.
ERROR	Diffie-Hellman group generator length has not been set.
ERROR	Diffie-Hellman group prime 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	DSS signature processing failed - signature is not valid.
ERROR	Encryption algorithm is not supported.
ERROR	Encryption algorithm is not supported.
ERROR	ESP transform 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 AH entry to the phase 2 SA list.
ERROR	Failed to add a new ESP entry to the phase 2 SA list.
ERROR	Failed to add a new ESP entry to the phase 2 SA list.
ERROR	Failed to add IPSEC encapsulation mode into the payload.
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 group description into the payload.
ERROR	Failed to add IPSEC HMAC algorithm 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 duration into the payload.
ERROR	Failed to add IPSEC life type into the payload.
ERROR	Failed to add IPSEC life type into the payload.

Table 3: Log Viewer Messages

ERROR	Failed to add OAKLEY authentication algorithm 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 encryption algorithm into the payload.
ERROR	Failed to add OAKLEY generator G1 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 description into the payload.
ERROR	Failed to add OAKLEY group type 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 hash algorithm into the payload.
ERROR	Failed to add OAKLEY life duration 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 life type into the payload.
ERROR	Failed to add OAKLEY prime P 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 INI format into the payload.
ERROR	Failed to add policy configuration version 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 password '' into the payload.
ERROR	Failed to add XAuth status into the payload.
ERROR	Failed to add XAuth status into the payload.

Table 3: Log Viewer Messages

ERROR	Failed to add XAuth type into the payload.
ERROR	Failed to add XAuth type into the payload.
ERROR	Failed to add XAuth username '' into the payload.
ERROR	Failed to add XAuth username '' into the payload.
ERROR	Failed to allocate bytes.
ERROR	Failed to allocate bytes.
ERROR	Failed to allocate memory.
ERROR	Failed to allocate memory.
ERROR	Failed to begin phase 1 exchange.
ERROR	Failed to begin phase 1 exchange.
ERROR	Failed to begin quick mode exchange.
ERROR	Failed to begin quick mode exchange.
ERROR	Failed to build a DSS object.
ERROR	Failed to build a DSS object.
ERROR	Failed to build dead peer detection packet.
ERROR	Failed to build dead peer detection packet.
ERROR	Failed to build dead peer detection reply message.
ERROR	Failed to build dead peer detection reply message.
ERROR	Failed to build dead peer detection request message.
ERROR	Failed to build dead peer detection request message.
ERROR	Failed to build phase 1 delete message.
ERROR	Failed to build phase 1 delete message.
ERROR	Failed to calculate DES mode from ESP transfor.
ERROR	Failed to calculate DES mode from ESP transform.
ERROR	Failed to calculate policy configuration attributes length.
ERROR	Failed to calculate policy configuration attributes length.

Table 3: Log Viewer Messages

ERROR	Failed to calculate XAuth attributes length.
ERROR	Failed to calculate XAuth attributes length.
ERROR	Failed to compute IV for connection entry.
ERROR	Failed to compute IV for connection entry.
ERROR	Failed to construct certificate payload.
ERROR	Failed to construct certificate payload.
ERROR	Failed to construct certificate request payload.
ERROR	Failed to construct certificate request payload.
ERROR	Failed to construct certificate.
ERROR	Failed to construct certificate.
ERROR	Failed to construct destination proxy ID payload.
ERROR	Failed to construct destination proxy ID payload.
ERROR	Failed to construct DSS signature.
ERROR	Failed to construct DSS signature.
ERROR	Failed to construct hash payload.
ERROR	Failed to construct hash payload.
ERROR	Failed to construct IPSEC nonce payload.
ERROR	Failed to construct IPSEC nonce payload.
ERROR	Failed to construct IPSEC SA payload.
ERROR	Failed to construct IPSEC SA payload.
ERROR	Failed to construct ISAKMP blank hash payload.
ERROR	Failed to construct ISAKMP blank hash payload.
ERROR	Failed to construct ISAKMP delete hash payload.
ERROR	Failed to construct ISAKMP delete hash payload.
ERROR	Failed to construct ISAKMP DPD notify payload.
ERROR	Failed to construct ISAKMP DPD notify payload.

Table 3: Log Viewer Messages

ERROR	Failed to construct ISAKMP ID payload.
ERROR	Failed to construct ISAKMP ID payload.
ERROR	Failed to construct ISAKMP info hash payload.
ERROR	Failed to construct ISAKMP info hash payload.
ERROR	Failed to construct ISAKMP key exchange payload.
ERROR	Failed to construct ISAKMP key exchange payload.
ERROR	Failed to construct ISAKMP nonce payload.
ERROR	Failed to construct ISAKMP nonce payload.
ERROR	Failed to construct ISAKMP notify payload.
ERROR	Failed to construct ISAKMP notify payload.
ERROR	Failed to construct ISAKMP packet header.
ERROR	Failed to construct ISAKMP packet header.
ERROR	Failed to construct ISAKMP phase 1 delete payload.
ERROR	Failed to construct ISAKMP phase 1 delete payload.
ERROR	Failed to construct ISAKMP phase 1 delete payload.
ERROR	Failed to construct ISAKMP phase 1 delete payload.
ERROR	Failed to construct ISAKMP SA payload.
ERROR	Failed to construct ISAKMP SA payload.
ERROR	Failed to construct ISAKMP vendor ID payload (ID =).
ERROR	Failed to construct ISAKMP vendor ID payload (ID =).
ERROR	Failed to construct mode config hash payload.
ERROR	Failed to construct mode config hash payload.
ERROR	Failed to construct NAT discovery payload.
ERROR	Failed to construct NAT discovery payload.
ERROR	Failed to construct PFS key exchange payload.
ERROR	Failed to construct PFS key exchange payload.

Table 3: Log Viewer Messages

ERROR	Failed to construct policy provisioning payload.
ERROR	Failed to construct policy provisioning payload.
ERROR	Failed to construct quick mode hash payload.
ERROR	Failed to construct quick mode hash payload.
ERROR	Failed to construct quick mode packet.
ERROR	Failed to construct quick mode packet.
ERROR	Failed to construct responder lifetime payload.
ERROR	Failed to construct responder lifetime payload.
ERROR	Failed to construct RSA signature.
ERROR	Failed to construct RSA signature.
ERROR	Failed to construct signature payload.
ERROR	Failed to construct signature payload.
ERROR	Failed to construct source proxy ID payload.
ERROR	Failed to construct source proxy ID payload.
ERROR	Failed to construct XAuth payload.
ERROR	Failed to construct XAuth payload.
ERROR	Failed to convert the peer name to an IP address.
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 a new connection entry: an entry already exists with ID.
ERROR	Failed to create connection entry with message ID.
ERROR	Failed to create connection entry with message ID.
ERROR	Failed to decrypt buffer.
ERROR	Failed to decrypt buffer.

Table 3: Log Viewer Messages

ERROR	Failed to decrypt mode config payload.
ERROR	Failed to decrypt mode config payload.
ERROR	Failed to decrypt notify payload.
ERROR	Failed to decrypt notify payload.
ERROR	Failed to decrypt packet.
ERROR	Failed to decrypt packet.
ERROR	Failed to decrypt quick mode payload.
ERROR	Failed to decrypt quick mode payload.
ERROR	Failed to encrypt mode config payload.
ERROR	Failed to encrypt mode config payload.
ERROR	Failed to encrypt notify payload.
ERROR	Failed to encrypt notify payload.
ERROR	Failed to encrypt packet.
ERROR	Failed to encrypt packet.
ERROR	Failed to encrypt quick mode payload.
ERROR	Failed to encrypt quick mode payload.
ERROR	Failed to expand packet to size bytes.
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_AH.
ERROR	Failed to find an SA list for PROTO_IPSEC_ESP.
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 an SA list given the protocol.
ERROR	Failed to find certificate with ID.
ERROR	Failed to find certificate with ID.

Table 3: Log Viewer Messages

ERROR	Failed to find connection entry for message ID.
ERROR	Failed to find connection entry for message ID.
ERROR	Failed to find exit interface to reach.
ERROR	Failed to find exit interface to reach.
ERROR	Failed to find MAC address in the system interfaces table.
ERROR	Failed to find MAC address in the system interfaces table.
ERROR	Failed to find matching SA list.
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 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 connection entry list.
ERROR	Failed to find message ID in the SA 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 OAKLEY group specified in the SA payload.
ERROR	Failed to find private key for certificate with ID.
ERROR	Failed to find private key for certificate with ID.
ERROR	Failed to find protocol ID in the SA list.
ERROR	Failed to find protocol ID in the SA list.
ERROR	Failed to find route to reach.
ERROR	Failed to find route to reach.
ERROR	Failed to find sequence number .
ERROR	Failed to find sequence number.

Table 3: Log Viewer Messages

ERROR	Failed to find source IP address to reach.
ERROR	Failed to find source IP address to reach.
ERROR	Failed to flush the system ARP cache.
ERROR	Failed to flush the system ARP cache.
ERROR	Failed to generate Diffie-Hellman parameters.
ERROR	Failed to generate Diffie-Hellman parameters.
ERROR	Failed to generate quick mode initiator key.
ERROR	Failed to generate quick mode initiator key.
ERROR	Failed to generate quick mode responder key.
ERROR	Failed to generate quick mode responder key.
ERROR	Failed to generate SKEYID.
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 interfaces table.
ERROR	Failed to get the size of the system IP address 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 interface table.
ERROR	Failed to get the system IP address table.
ERROR	Failed to get the system IP address table.
ERROR	Failed to get transforms from SA list.
ERROR	Failed to get transforms from SA list.
ERROR	Failed to match initiator cookie.
ERROR	Failed to match initiator cookie.
ERROR	Failed to match responder cookie.
ERROR	Failed to match responder cookie.

Table 3: Log Viewer Messages

ERROR	Failed to parse certificate data.
ERROR	Failed to parse certificate data.
ERROR	Failed to parse configuration file.
ERROR	Failed to parse configuration file.
ERROR	Failed to read the size of an incoming ISAKMP packet.
ERROR	Failed to read the size of an incoming ISAKMP packet.
ERROR	Failed to re-allocate bytes.
ERROR	Failed to re-allocate bytes.
ERROR	Failed to receive an incoming ISAKMP packet.
ERROR	Failed to receive an incoming ISAKMP packet.
ERROR	Failed to receive an incoming ISAKMP packet. The length is incorrect.
ERROR	Failed to receive an incoming ISAKMP packet. The length is incorrect.
ERROR	Failed to send an outgoing ISAKMP packet.
ERROR	Failed to send an outgoing ISAKMP packet.
ERROR	Failed to set policy configuration attributes into payload.
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 1 SA payload.
ERROR	Failed to set proposals into phase 2 SA payload.
ERROR	Failed to set proposals into phase 2 SA payload.
ERROR	Failed to set responder lifetype attributes.
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 ESP attributes from the SA payload into the SA.

Table 3: Log Viewer Messages

ERROR	Failed to set the IPSEC AH attributes into the phase 2 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 IPSEC ESP attributes into the phase 2 SA.
ERROR	Failed to set the OAKLEY attributes into the phase 1 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 vendor ID into packet payload.
ERROR	Failed to set vendor ID into packet payload.
ERROR	Failed to set vendor ID into packet payload.
ERROR	Failed to set XAuth attributes into payload.
ERROR	Failed to set XAuth attributes into payload.
ERROR	Failed to sign hash.
ERROR	Failed to sign hash.
ERROR	Failed to verify certificate signature.
ERROR	Failed to verify certificate signature.
ERROR	Failed to verify informational message hash payload.
ERROR	Failed to verify informational message hash payload.
ERROR	Failed to verify mode config message hash payload.
ERROR	Failed to verify mode config message hash payload.
ERROR	Hash algorithm is not supported.
ERROR	Hash algorithm is not supported.
ERROR	Hash Payload does not match.
ERROR	Hash Payload does not match.
ERROR	Hash size invalid:
ERROR	Hash size invalid:

Table 3: Log Viewer Messages

ERROR	Header invalid (verified)!
ERROR	Header invalid (verified)!
ERROR	Invalid certificate: ASN sequence is not correct.
ERROR	Invalid certificate: ASN sequence is not correct.
ERROR	Invalid certificate: payload length is too small.
ERROR	Invalid certificate: payload length is too small.
ERROR	Invalid hash payload.
ERROR	Invalid hash payload.
ERROR	Invalid payload. Possible overrun attack!
ERROR	Invalid payload. Possible overrun attack!
ERROR	Invalid SA state:
ERROR	Invalid SA state:
ERROR	Invalid signature payload.
ERROR	Invalid signature payload.
ERROR	Invalid SPI size.
ERROR	Invalid SPI size.
ERROR	is not a supported Diffie-Hellman group type.
ERROR	is not a supported Diffie-Hellman group type.
ERROR	is not a supported DOI.
ERROR	is not a supported DOI.
ERROR	is not a supported exchange type.
ERROR	is not a supported exchange type.
ERROR	is not a supported ID payload type.
ERROR	is not a supported ID payload type.
ERROR	is not a supported IPSEC protocol.
ERROR	is not a supported IPSEC protocol.

Table 3: Log Viewer Messages

ERROR	is not a supported notify message type.
ERROR	is not a supported notify message type.
ERROR	is not a supported payload type.
ERROR	is not a supported payload type.
ERROR	is not a supported policy configuration attribute type.
ERROR	is not a supported policy configuration attribute type.
ERROR	is not a supported policy configuration message type.
ERROR	is not a supported policy configuration message type.
ERROR	is not a supported proxy ID payload type.
ERROR	is not a supported proxy ID payload type.
ERROR	is not a supported XAuth attribute type.
ERROR	is not a supported XAuth attribute type.
ERROR	is not a valid quick mode state.
ERROR	is not a valid quick mode state.
ERROR	is not a valid XAuth message type.
ERROR	is not a valid XAuth message type.
ERROR	is not a valid XAuth status.
ERROR	is not a valid XAuth status.
ERROR	ISAKMP SA delete msg for a different SA!
ERROR	ISAKMP SA delete msg for a different SA!
ERROR	No certificate for CERT authentication.
ERROR	No certificate for CERT authentication.
ERROR	No entry in the system IP address table was found with index.
ERROR	No entry in the system IP address table was found with index.
ERROR	No KE payload while PFS configured mess_id.
ERROR	No KE payload while PFS configured mess_id.

Table 3: Log Viewer Messages

ERROR	Out of memory.
ERROR	Out of memory.
ERROR	Phase 1 authentication algorithm is not supported.
ERROR	Phase 1 authentication algorithm is not supported.
ERROR	Phase 1 encryption algorithm is not supported.
ERROR	Phase 1 encryption algorithm is not supported.
ERROR	Protocol ID has already been added to the SA list.
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_AH but got.
ERROR	Protocol mismatch: expected PROTO_IPSEC_ESP but got.
ERROR	Protocol mismatch: expected PROTO_IPSEC_ESP but got.
ERROR	Publisher deregistration failed.
ERROR	Publisher deregistration failed.
ERROR	Responder cookie is not zero.
ERROR	Responder cookie is not zero.
ERROR	RSA signature processing failed - signature is not valid.
ERROR	RSA signature processing failed - signature is not valid.
ERROR	SA hash function has not been set in.
ERROR	SA hash function has not been set in.
ERROR	Signature Algorithm mismatch is X.509 certificate.
ERROR	Signature Algorithm mismatch is X.509 certificate.
ERROR	Signature verification failed!
ERROR	Signature verification failed!
ERROR	The certificate is not valid at this time.
ERROR	The certificate is not valid at this time.

Table 3: Log Viewer Messages

ERROR	The current state is not valid for processing mode config payload.
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 current state is not valid for processing signature payload.
ERROR	The first payload is not a hash payload.
ERROR	The first payload is not a hash payload.
ERROR	The following error occurred while trying to open the configuration file:
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 state flag indicates that the IPSEC SA payload has not been processed.
ERROR	The system interface table is empty.
ERROR	The system interface table is empty.
ERROR	The system IP address table is empty.
ERROR	The system IP address table is empty.
ERROR	Unable to compute hash!
ERROR	Unable to compute hash!
ERROR	Unable to compute shared secret for PFS in phase 2!
ERROR	Unable to compute shared secret for PFS in phase 2!
ERROR	Unable to read configuration file.
ERROR	Unable to read configuration file.
ERROR	User did not enter XAuth next pin.

Table 3: Log Viewer Messages

ERROR	User did not enter XAuth next pin.
ERROR	XAuth CHAP requests are not supported at this time.
ERROR	XAuth CHAP requests are not supported at this time.
ERROR	XAuth failed.
ERROR	XAuth failed.
ERROR	XAuth has requested a password but one has not yet been specified.
ERROR	XAuth has requested a password but one has not yet been specified.
INFO	"The connection """" has been disabled."
INFO	"The connection """" has been disabled."
INFO	"The connection """" has been enabled."
INFO	"The connection """" has been enabled."
INFO	A certificate is needed to complete phase 1.
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 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	A pre-shared key is needed to complete phase 1.
INFO	AG failed. SA state unknown. Peer:
INFO	AG failed. SA state unknown. Peer:
INFO	An incoming ISAKMP packet from was ignored.
INFO	An incoming ISAKMP packet from was ignored.
INFO	DSS g value:
INFO	DSS g value:

Table 3: Log Viewer Messages

INFO	DSS p value:
INFO	DSS p value:
INFO	DSS q value:
INFO	DSS q value:
INFO	Event publisher deregistered.
INFO	Event publisher deregistered.
INFO	Event publisher registered for.
INFO	Event publisher registered for.
INFO	Failed to negotiate configuration information with.
INFO	Failed to negotiate configuration information with.
INFO	Found CA certificate in CA certificate list.
INFO	Found CA certificate in CA certificate list.
INFO	Ignoring unsupported payload.
INFO	Ignoring unsupported payload.
INFO	Ignoring unsupported vendor ID.
INFO	Ignoring unsupported vendor ID.
INFO	ISAKMP phase 1 proposal is not acceptable.
INFO	ISAKMP phase 1 proposal is not acceptable.
INFO	ISAKMP phase 2 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_KEY_EXCH. Peer:
INFO	MM failed. Payload processing failed: OAK_MM_NO_STATE. Peer:

Table 3: Log Viewer Messages

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. 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 auth. Peer:
INFO	MM failed. SA state not matching mask process key. 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 not matching mask process sa. Peer:
INFO	MM failed. SA state unknown. Peer:
INFO	MM failed. SA state unknown. Peer:
INFO	NAT Detected: Local host is behind a NAT device.
INFO	NAT Detected: Local host is behind a NAT device.
INFO	NAT Detected: Peer is behind a NAT device.
INFO	NAT Detected: Peer is behind a NAT device.
INFO	peer certificate missing key value.
INFO	peer certificate missing key value.
INFO	Phase 1 has completed.
INFO	Phase 1 has completed.
INFO	Phase 1 SA lifetime set to.
INFO	Phase 1 SA lifetime set to.
INFO	Phase 2 negotiation has failed.
INFO	Phase 2 negotiation has failed.
INFO	Phase 2 SA lifetime set to.

Table 3: Log Viewer Messages

INFO	Phase 2 SA lifetime set to.
INFO	Phase 2 with has completed.
INFO	Phase 2 with has completed.
INFO	Proposal not acceptable: not authentication algorithm specified.
INFO	Proposal not acceptable: not authentication algorithm specified.
INFO	Proposal not acceptable: not Diffie-Hellman group specified.
INFO	Proposal not acceptable: not Diffie-Hellman group specified.
INFO	Proposal not acceptable: not encryption algorithm specified.
INFO	Proposal not acceptable: not encryption algorithm specified.
INFO	Proposal not acceptable: not hash algorithm specified.
INFO	Proposal not acceptable: not hash algorithm specified.
INFO	Proposal not acceptable: proposal not found in list.
INFO	Proposal not acceptable: proposal not found in list.
INFO	QM failed. Load SA failed. Peer:
INFO	QM failed. Load SA failed. Peer:
INFO	Reading configuration file.
INFO	Reading configuration file.
INFO	Ready to negotiate phase 2 with.
INFO	Ready to negotiate phase 2 with.
INFO	Received address notification notify.
INFO	Received address notification notify.
INFO	Received attributes not supported notify.
INFO	Received attributes not supported notify.
INFO	Received authentication failed notify.
INFO	Received authentication failed notify.
INFO	Received authentication failed notify.

Table 3: Log Viewer Messages

INFO	Received authentication failed notify.
INFO	Received bad syntax notify.
INFO	Received bad syntax notify.
INFO	Received certificate unavailable notify.
INFO	Received certificate unavailable notify.
INFO	Received dead peer detection acknowledgement.
INFO	Received dead peer detection acknowledgement.
INFO	Received dead peer detection request.
INFO	Received dead peer detection request.
INFO	Received initial contact notify.
INFO	Received initial contact notify.
INFO	Received invalid certificate authentication notify.
INFO	Received invalid certificate authentication notify.
INFO	Received invalid certificate encoding notify.
INFO	Received invalid certificate encoding notify.
INFO	Received invalid certificate notify.
INFO	Received invalid certificate notify.
INFO	Received invalid certificate request syntax notify.
INFO	Received invalid certificate request syntax notify.
INFO	Received invalid cookie notify.
INFO	Received invalid cookie notify.
INFO	Received invalid exchange type notify.
INFO	Received invalid exchange type notify.
INFO	Received invalid flags notify.
INFO	Received invalid flags notify.
INFO	Received invalid ID information notify.

Table 3: Log Viewer Messages

INFO	Received invalid ID information notify.
INFO	Received invalid key info notify.
INFO	Received invalid key info notify.
INFO	Received invalid major version notify.
INFO	Received invalid major version notify.
INFO	Received invalid message ID notify.
INFO	Received invalid message ID notify.
INFO	Received invalid minor version notify.
INFO	Received invalid minor version notify.
INFO	Received invalid payload notify.
INFO	Received invalid payload notify.
INFO	Received invalid protocol ID notify.
INFO	Received invalid protocol ID notify.
INFO	Received invalid signature notify.
INFO	Received invalid signature notify.
INFO	Received invalid SPI notify.
INFO	Received invalid SPI notify.
INFO	Received invalid transform ID notify.
INFO	Received invalid transform ID notify.
INFO	Received malformed payload notify.
INFO	Received malformed payload notify.
INFO	Received no proposal chosen notify.
INFO	Received no proposal chosen notify.
INFO	Received notify SA lifetime notify.
INFO	Received notify SA lifetime notify.
INFO	Received phase 1 delete message.

Table 3: Log Viewer Messages

INFO	Received phase 1 delete message.
INFO	Received phase 2 delete message for SPI.
INFO	Received phase 2 delete message for SPI.
INFO	Received policy provisioning acknowledgement.
INFO	Received policy provisioning acknowledgement.
INFO	Received policy provisioning OK.
INFO	Received policy provisioning OK.
INFO	Received policy provisioning update.
INFO	Received policy provisioning update.
INFO	Received policy provisioning version reply.
INFO	Received policy provisioning version reply.
INFO	Received policy provisioning version request.
INFO	Received policy provisioning version request.
INFO	Received responder lifetime notify.
INFO	Received responder lifetime notify.
INFO	Received situation not supported notify.
INFO	Received situation not supported notify.
INFO	Received unequal payload length notify.
INFO	Received unequal payload length notify.
INFO	Received unknown notify.
INFO	Received unknown notify.
INFO	Received unsupported DOI notify.
INFO	Received unsupported DOI notify.
INFO	Received unsupported exchange type notify.
INFO	Received unsupported exchange type notify.
INFO	Received XAuth request.

Table 3: Log Viewer Messages

INFO	Received XAuth request.
INFO	Received XAuth status.
INFO	Received XAuth status.
INFO	Re-evaluating ID info after INVALID_ID_INFO message.
INFO	Re-evaluating ID info after INVALID_ID_INFO message.
INFO	Releasing IP address for the virtual interface ().
INFO	Releasing IP address for the virtual interface ().
INFO	Renewing IP address for the virtual interface ().
INFO	Renewing IP address for the virtual interface ().
INFO	Saving configuration file.
INFO	Saving configuration file.
INFO	Sending dead peer detection acknowledgement.
INFO	Sending dead peer detection acknowledgement.
INFO	Sending dead peer detection request.
INFO	Sending dead peer detection request.
INFO	Sending phase 1 delete.
INFO	Sending phase 1 delete.
INFO	Sending phase 2 delete for.
INFO	Sending phase 2 delete for.
INFO	Sending policy provisioning acknowledgement.
INFO	Sending policy provisioning acknowledgement.
INFO	Sending policy provisioning version reply.
INFO	Sending policy provisioning version reply.
INFO	Sending XAuth acknowledgement.
INFO	Sending XAuth acknowledgement.
INFO	Sending XAuth reply.

Table 3: Log Viewer Messages

INFO	Sending XAuth reply.
INFO	Signature Verified!
INFO	Signature Verified!
INFO	SonicWALL Global VPN Client version.
INFO	SonicWALL VPN Client.
INFO	SonicWALL VPN Client.
INFO	Starting aggressive mode phase 1 exchange.
INFO	Starting aggressive mode phase 1 exchange.
INFO	Starting authentication negotiation.
INFO	Starting authentication negotiation.
INFO	Starting configuration negotiation.
INFO	Starting configuration negotiation.
INFO	Starting ISAKMP phase 1 negotiation.
INFO	Starting ISAKMP phase 1 negotiation.
INFO	Starting ISAKMP phase 2 negotiation with.
INFO	Starting ISAKMP phase 2 negotiation with.
INFO	Starting main mode phase 1 exchange.
INFO	Starting main mode phase 1 exchange.
INFO	Starting quick mode phase 2 exchange.
INFO	Starting quick mode phase 2 exchange.
INFO	The configuration for the connection has been updated.
INFO	The configuration for the connection has been updated.
INFO	The configuration for the connection is up to date.
INFO	The configuration for the connection is up to date.
INFO	The configuration has been updated and must be reloaded.
INFO	The configuration has been updated and must be reloaded.

Table 3: Log Viewer Messages

INFO	The connection has entered an unknown state.
INFO	The connection has entered an unknown state.
INFO	The connection is idle.
INFO	The connection is idle.
INFO	The hard lifetime has expired for phase 1.
INFO	The hard lifetime has expired for phase 1.
INFO	The hard lifetime has expired for phase 2 with.
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 been released.
INFO	The IP address for the virtual interface has changed to.
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 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 peer is not responding to phase 2 ISAKMP requests to.INFO SonicWALL Global VPN Client version.
INFO	The phase 1 SA has been deleted.
INFO	The phase 1 SA has been deleted.
INFO	The phase 1 SA has died.
INFO	The phase 1 SA has died.
INFO	The phase 2 SA has been deleted.
INFO	The phase 2 SA has been deleted.
INFO	The phase 2 SA has died.
INFO	The phase 2 SA has died.

Table 3: Log Viewer Messages

INFO	The SA lifetime for phase 1 is seconds.
INFO	The SA lifetime for phase 1 is seconds.
INFO	The SA lifetime for phase 2 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 1.
INFO	The soft lifetime has expired for phase 2 with.
INFO	The soft lifetime has expired for phase 2 with.
INFO	The system ARP cache has been flushed.
INFO	The system ARP cache has been flushed.
INFO	Unable to encrypt payload!
INFO	Unable to encrypt payload!
INFO	User authentication has failed.
INFO	User authentication has failed.
INFO	User authentication has succeeded.
INFO	User authentication has succeeded.
INFO	User authentication information is needed to complete the connection.
INFO	User authentication information is needed to complete the connection.
INFO	XAuth has requested a username but one has not yet been specified.
INFO	XAuth has requested a username but one has not yet been specified.
WARNING	A password must be entered.
WARNING	A password must be entered.
WARNING	AG failed. SA state not matching mask process auth. Peer:

Table 3: Log Viewer Messages

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. 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_INIT_EXCH is invalid when responder. Peer:
WARNING	AG failed. State OAK_AG_NO_STATE is invalid when initiator. 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 aggressive mode packet.
WARNING	Failed to process final quick mode packet.
WARNING	Failed to process final quick mode packet.
WARNING	Failed to process informational exchange packet.
WARNING	Failed to process informational exchange packet.
WARNING	Failed to process main mode packet.
WARNING	Failed to process main mode packet.
WARNING	Failed to process mode configuration packet.
WARNING	Failed to process mode configuration packet.
WARNING	Failed to process packet payloads.
WARNING	Failed to process packet payloads.
WARNING	Failed to process payload.
WARNING	Failed to process payload.
WARNING	Failed to process quick mode packet.
WARNING	Failed to process quick mode packet.

Table 3: Log Viewer Messages

WARNING	Ignoring AUTH message when aggressive mode already complete. Peer:
WARNING	Ignoring AUTH message when aggressive mode already complete. Peer:
WARNING	Invalid DOI in delete message:
WARNING	Invalid DOI in delete message:
WARNING	Invalid IPSEC SA delete message.
WARNING	Invalid IPSEC SA delete message.
WARNING	Invalid ISAKMP SA delete message.
WARNING	Invalid ISAKMP SA delete message.
WARNING	is not a supported OAKLEY attribute class.
WARNING	is not a supported OAKLEY attribute class.
WARNING	Protocol ID is not supported in SA payloads.
WARNING	Protocol ID is not supported in SA payloads.
WARNING	Received an encrypted packet when not crypto active!
WARNING	Received an encrypted packet when not crypto active!
WARNING	Received an unencrypted packet when crypto active!
WARNING	Received an unencrypted packet when crypto active!
WARNING	Responder lifetime protocol is not supported.
WARNING	Responder lifetime protocol is not supported.
WARNING	The password is incorrect. Please re-enter the password.
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 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.

Table 3: Log Viewer Messages

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	The username/password dialog box was cancelled by the user. The connection will be disabled.
WARNING	Unable to decrypt payload!
WARNING	Unable to decrypt payload!

SonicWALL,Inc.
1143 Borregas Avenue
Sunnyvale,CA 94089-1306
T: 408.745.9600
F: 408.745.9300
www.sonicwall.com

P/ N 232-000333-00
Rev B 6/03