SonicWall™ Global VPN Client 4.10

Administration Guide

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal/.

Legend

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

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

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

Global VPN Client Administration Guide
Updated - March 2017
Software Version - 4.10
232-003830-00 Rev A

Contents

1

Introduction to Global VPN Client

Global VPN Client Overview

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

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

For configuring your SonicWall security appliance to support Global VPN Clients using SonicOS GroupVPN, see the *SonicOS Administration Guide* for the firmware version running on your SonicWall security appliance (your VPN gateway appliance).

Topics:

- Global VPN Client Features on page 6
- Global VPN Client Enterprise on page 8

Global VPN Client Features

The SonicWall Global VPN Client delivers a robust IPsec VPN solution with these features:

- **Easy to Use** - Provides an easy-to-follow Installation Wizard to quickly install the product, an easy-to-follow Configuration Wizard with point-and-click activation of VPN connections, and streamlined management tools to minimize support requirements.
- **Multiple Language Support** - The Global VPN Client user interface supports English, Simplified Chinese, Japanese, Korean, and Brazilian Portuguese. The UI automatically displays in the Windows display language.

- **Client Policy Provisioning** - Using only the IP address or Fully Qualified Domain Name (FQDN) of the SonicWall VPN gateway, the VPN configuration data is automatically downloaded from the SonicWall VPN gateway via a secure IPsec tunnel, removing the burden from the remote user of provisioning VPN connections.
- **XAUTH Authentication with RADIUS** - Provides added security with user authentication after the client has been authenticated via a RADIUS server.
- **VPN Session Reliability** - Allows automatic redirect in case of a SonicWall VPN gateway failure. If a SonicWall VPN gateway is down then the Global VPN Client can go through another SonicWall VPN gateway.
- **Multiple Subnet Support** - Allows Global VPN Client connections to more than one subnet in the configuration to increase networking flexibility.
- **Third-Party Certificate Support** - Supports VeriSign, Entrust, Microsoft, and Netscape Certificate Authorities (CAs) for enhanced user authentication.
- **Tunnel All Support** - Provides enhanced security by blocking all traffic not directed to the VPN tunnel to prevent Internet attacks from entering the corporate network through a VPN connection.
- **DHCP over VPN Support** - Allows IP address provisioning across a VPN tunnel for the corporate network while allowing WAN DHCP for Internet Access from the ISP.
- **Secure VPN Configuration** - Critical Global VPN Client configuration information is locked from the user to prevent tampering.
- **AES and 3DES Encryption** - Supports 168-bit key 3DES (Data Encryption Standard) and AES (Advanced Encryption Standard) for increased security. AES requires SonicOS 2.0 or higher on the SonicWall VPN gateway appliance.
- **GMS Management** - Allows Global VPN Client connections to be managed by SonicWall's award-winning Global Management System (GMS).
- **Multi-Platform Client Support** - Supports 32-bit and 64-bit versions of Windows: Windows 10, Windows 8, Windows 8.1, and Windows 7.
- **NAT Traversal -** Enables Global VPN Client connections to be initiated from behind any device performing NAT (Network Address Translation). The SonicWall Global VPN Client encapsulates IPsec VPN traffic to pass through NAT devices, which are widely deployed to allow local networks to use one external IP address for an entire network.
- **Automatic Reconnect When Error Occurs** - Allows the Global VPN Client to keep retrying a connection if it encounters a problem connecting to a peer. This feature allows the Global VPN Client to automatically make a connection to a SonicWall VPN gateway that is temporarily disabled, without manual intervention.
- **Ghost Installation for Large Scale Installations** - Enables the Global VPN Client's virtual adapter to get its default address after installation and then create a ghost image.
- **NT Domain Logon Script Support** - Allows Global VPN Clients to perform Windows NT domain authentication after establishing a secure IPsec tunnel. The SonicWall VPN gateway passes the logon script as part of the Global VPN Client configuration. This feature allows the VPN user to have access to mapped network drives and other network services.
- **Dual Processor Support** - Enables the Global VPN Client to operate on dual-processor computers.
- **Group Policy Management** - Global VPN Clients access can be customized and restricted to specific subnet access (Requires SonicOS Enhanced).
- **Hub and Spoke VPN Access** - Allows IP addressing from SonicWall VPN gateway's DHCP Server to Global VPN Client for configuring a different subnet for all remote Global VPN Clients than the subnet of the LAN. Makes hub-and-spoke VPN access simpler. When a Global VPN Client successfully authenticates with the central site, it receives a virtual IP address that also grants it access to other trusted VPN sites.

- **Default VPN Connections File** - Enables the SonicOS administrator to configure and distribute the corporate VPN connections with the Global VPN Client software to streamline VPN client deployment.
- **Single VPN Connection to any SonicWall Secure Wireless Appliance for Roaming** - Allows users to use a single VPN connection to access the networks of multiple SonicWall Secure Wireless appliances.
- **Automatic Configuration of Redundant Gateways from DNS** - When an IPsec gateway domain name resolves to multiple IP addresses, the Global VPN Client uses the IP addresses in the list as failover gateways.
- **Tunnel State Display Enhancement** - The Global VPN Client provides information about the state of VPN tunnels. In addition to the states of enabled, disabled, and connected, the Global VPN Client indicates when tunnels are authenticating, provisioning, and connecting.
- **Tunnel Status Pop-Up Window** - The Global VPN Client alerts users when tunnels are connected or disconnected by displaying a small pop-up window.
- **Smart Card and USB Token Authentication -** The Global VPN Client is integrated with the Microsoft Cryptographic Application Program (MS CryptoAPI or MSCAPI), which enables the Global VPN Client to support user authentication using digital certificates on Smart cards and USB tokens.
- **NAT-T RFC 3947 Support** - Allows for automatic detection of NAT along the path between two IKE peers during IKE Phase 1 negotiation. On detection of NAT in middle, packets are UDP encapsulated using port 4500.
- **DNS Redirect** - DNS queries to DNS suffix associated with Virtual Adapter are not sent on the physical adapter.
- **Tunnel All Support Enhancement** - Provides the ability to route clear traffic to directly connected network interfaces that are configured with the Route All policy, which is generally used in the WLAN zone.
- **Program Auto-Start on VPN Connection** - Automatically launches a program, with optional arguments, when successful VPN connections are established, as specified in the **Connection Properties** dialog.

Global VPN Client Enterprise

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

About this Guide

The *SonicWall Global VPN Client Administration Guide* provides complete documentation on installing, configuring, and managing the SonicWall Global VPN Client. This guide also provides instructions for SonicWall Global VPN Client Enterprise.

For configuring your SonicWall security appliance to support Global VPN Clients using SonicOS GroupVPN, see the *SonicOS Administration Guide* for the firmware version running on your SonicWall security appliance (your VPN gateway appliance).

Topics:

- Text Conventions on page 9
- Message Icons on page 9

Text Conventions

Convention	Use
Bold	Highlights items you can select on the Global VPN Client interface or the SonicOS management interface.
Menu Item > Menu Item	Indicates a multiple step menu choice. For example, “select **File > Open**” means “select the **File** menu, and then select the **Open** item from the **File** menu.
`Screen Text`	Indicates text as you would see it on a computer screen or would enter on a command line. For example, `myDevice> show alerts`

Message Icons

These special messages refer to noteworthy information, and include a symbol for quick identification:

WARNING: Important information that warns about a potential for property damage, personal injury, or death

CAUTION: Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWall appliance.

TIP: Useful information about security features and configurations on your SonicWall appliance.

IMPORTANT: Important information on a feature that requires callout for special attention.

NOTE: Supporting information on a feature.

MOBILE: Useful information about mobile apps for your SonicWall appliance.

VIDEO: Links to videos containing further information about a feature on your SonicWall appliance.

2

Getting Started with Global VPN Client

This section provides information about installing, upgrading, and launching the SonicWall Global VPN Client.

Installing the Global VPN Client

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

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

The SonicWall Global VPN Client operates on 32-bit and 64-bit versions of Windows 10, Windows 8.1, Windows 8, and Windows 7 client operating systems.

The Global VPN Client is supported on all SonicWall security appliances running Gen5 (5.0 and higher) and Gen6 (6.1 and higher) SonicOS firmware versions.

> **NOTE:** For information on the number of SonicWall Global VPN Client connections supported by your SonicWall appliance and Global VPN Client licensing for your appliance, see Global VPN Client Licenses on page 50.

Using the Setup Wizard

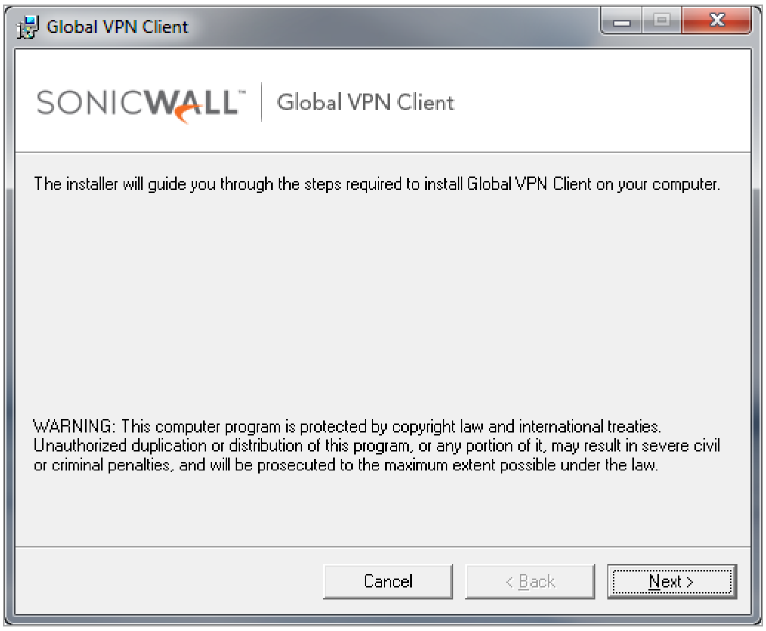
This section explains how to install the SonicWall Global VPN Client program using the **Setup Wizard**.

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

To use the Setup Wizard:

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

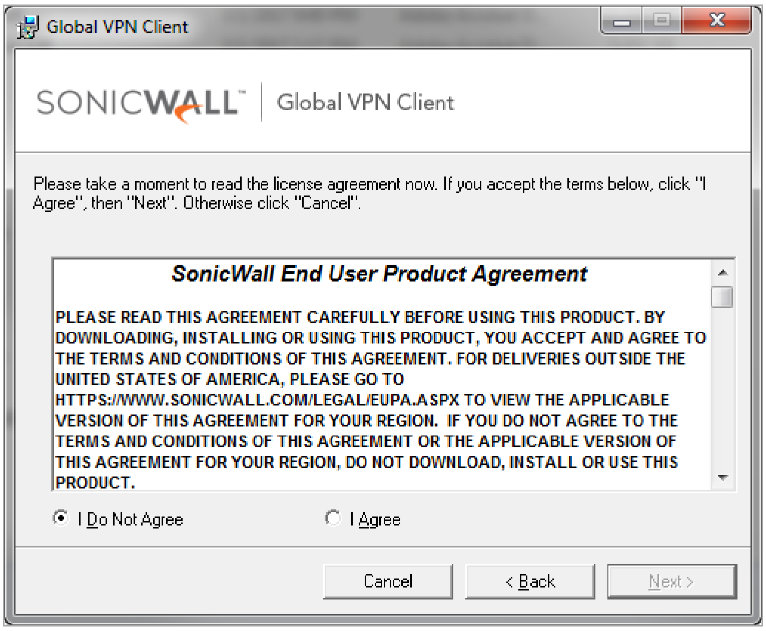
2 Double-click **GVCSetupXX.exe**. The **Setup Wizard** launches.



The installer will guide you through the steps required to install Global VPN Client on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

3 Click **Next** to continue installation of the VPN Client. The **License Agreement** page displays.



Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".

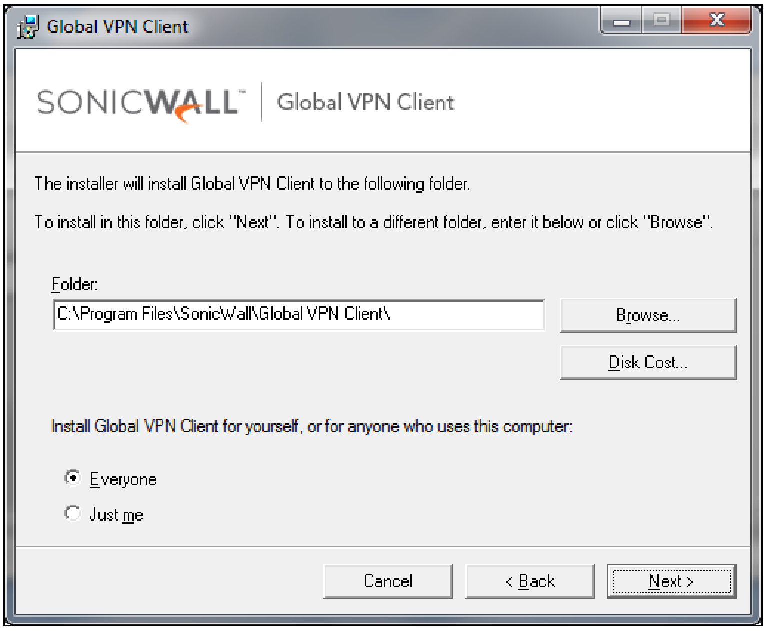
SonicWall End User Product Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA.ASPX TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THE THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

● I Do Not Agree ○ I Agree

4 Select the **I Agree** radio button.

5 Click **Next**. The **Installation Folder Selection** page displays.



Global VPN Client

The installer will install Global VPN Client to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\SonicWall\Global VPN Client\

Install Global VPN Client for yourself, or for anyone who uses this computer:

● Everyone

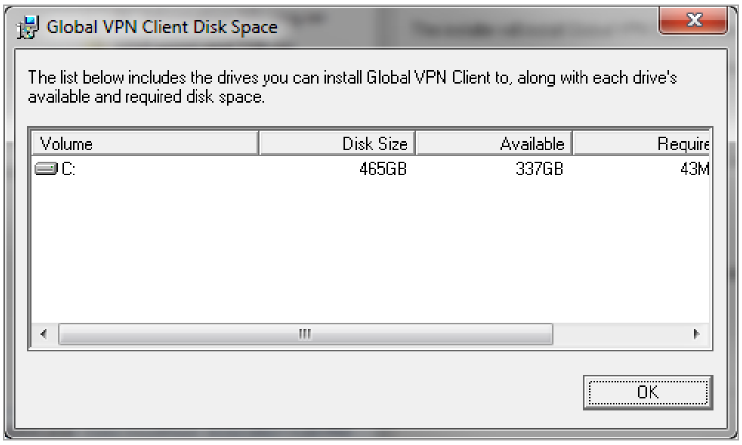
○ Just me

6 Optionally, to specify a custom installation location, click **Browse**.

   a Select the location.

   b Click **OK**.

7 Optionally, click the **Disk Cost** button to see the disk space requirements.



Global VPN Client Disk Space

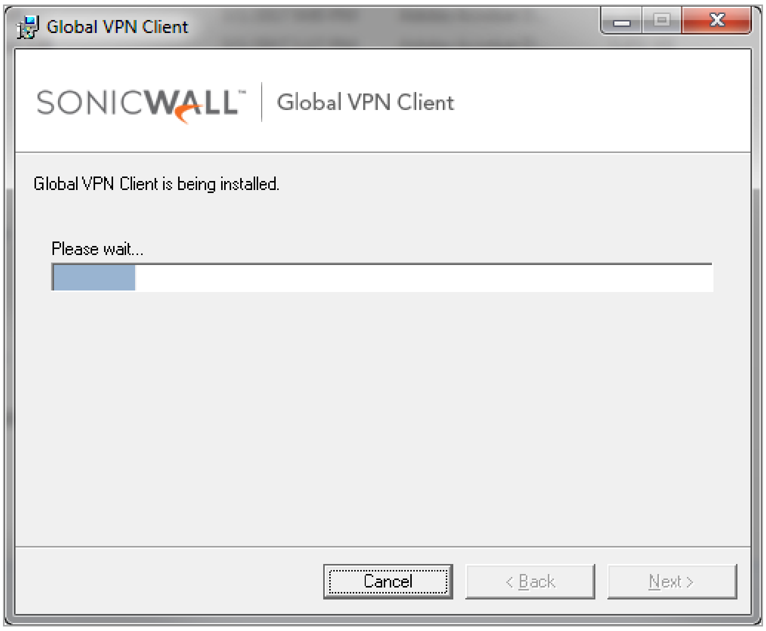
The list below includes the drives you can install Global VPN Client to, along with each drive's available and required disk space.

Volume	Disk Size	Available	Require
C:	465GB	337GB	43M

8 Under **Install SonicWall Global VPN Client for yourself, or for anyone who uses this computer**, select either **Everyone** or **Just me**.

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

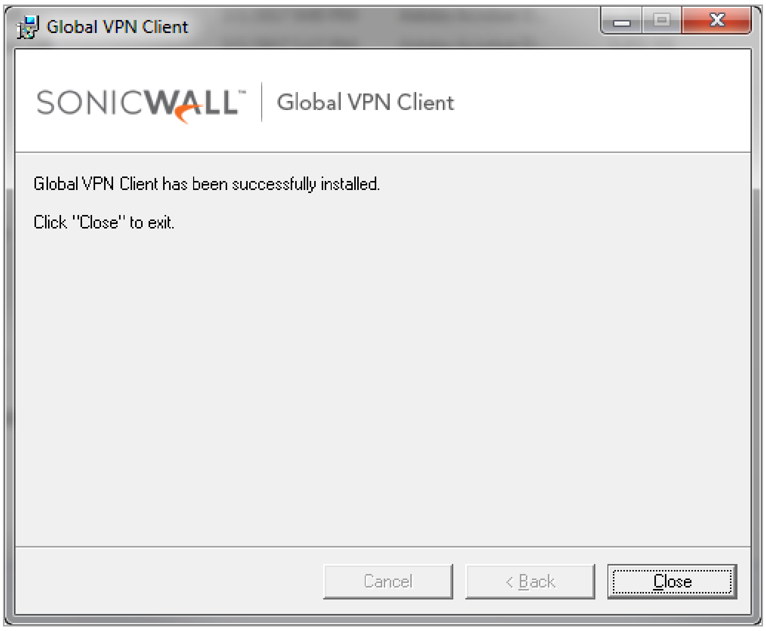
10 Click **Next**. The **Global VPN Client is being installed** page displays, which indicates the status of the installation.



Global VPN Client is being installed.

Please wait...

11 Wait while the SonicWall Global VPN Client files are installed on your computer. When the installation is complete, the **Global VPN Client has been successfully installed** page displays.



Global VPN Client has been successfully installed.

Click "Close" to exit.

12 Click **Close** to exit the wizard. After a successful installation, what happens next depends on whether you had saved connections:

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

- If no previous connections exist, the **New Connection Wizard** launches automatically. This only occurs the first time the Global VPN Client starts up. For more information, see Creating a VPN Connection Using the New Connection Wizard on page 19,

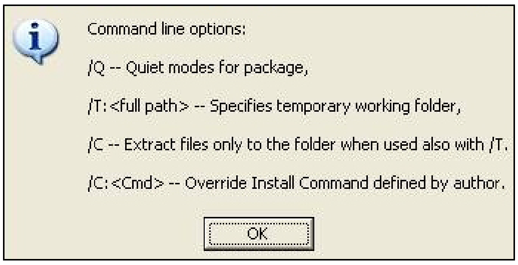
> ⓘ **TIP:** You can configure the Global VPN Client to launch automatically every time you log onto your computer, on the **General** tab in the **View > Options** page. For more information, see Specifying Global VPN Client Launch Options on page 16

Upgrading Global VPN Client from a Previous Version

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

Command-Line Options for Installation

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



Command line options:

/Q -- Quiet modes for package,

/T:<full path> -- Specifies temporary working folder,

/C -- Extract files only to the folder when used also with /T.

/C:<Cmd> -- Override Install Command defined by author.

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

- **/Q** – Quiet mode. A normal (non-silent) installation of the SonicWall Global VPN Client receives the necessary input from the user in the form of responses to dialogs. However, a silent installation does not prompt the user for any input, but instead, uses the defaults for every option. Simply type in the following where **XX** is either **32** for 32-bit Windows platforms or **64** for 64-bit Windows platforms:

  ```
  GVCSetupXX.exe /q
  ```

- **/T** – Specify a temporary working folder in which to place any temporary files generated during the installation process. The T option must be followed by a colon (**:**) and the full path to the folder that you want to use. For example, type in the following:

  ```
  GVCSetupXX.exe /t:C:\TemporaryFiles
  ```

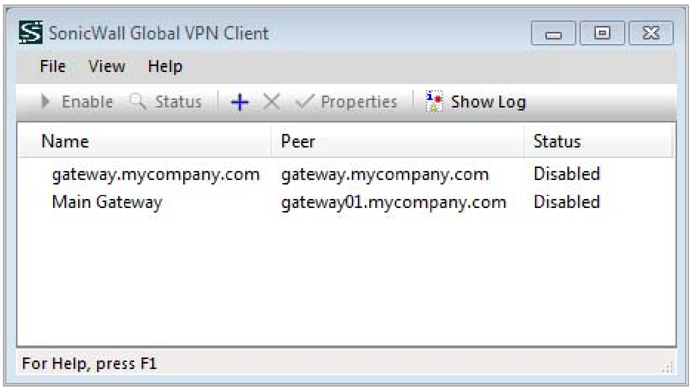
- **/C** – Place all files extracted (MSI Installer file) from the install package into the folder specified in the **T** option. The **C** option is only valid when used together with the **T** option. For example, type one of the following:

  ```
  GVCSetupXX.exe /c /t:C:\TemporaryFiles
  GVCSetupXX.exe /T:C:\TemporaryFiles /c
  ```

Launching the Global VPN Client

To launch the SonicWall Global VPN Client:

1 Select **Start > Programs > Global VPN Client**.



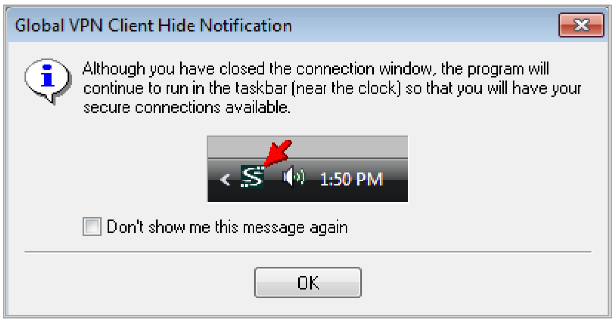
Name	Peer	Status
gateway.mycompany.com	gateway.mycompany.com	Disabled
Main Gateway	gateway01.mycompany.com	Disabled

For Help, press F1

2 You can do any of the following:

- To close the Global VPN Client dialog, but have your established VPN connections remain active, click **X,** press **Alt+F4,** or choose **File > Close**.

  A message appears notifying you that the Global VPN Client program and any enabled connections remain active after the dialog is closed.

  Although you have closed the connection window, the program will continue to run in the taskbar (near the clock) so that you will have your secure connections available.

  □ Don't show me this message again

  If you don't want this notification message to display every time you close the Global VPN Client dialog:

  a) Select the **Don't show me this message again** checkbox.

  b) Click **OK**.

- To open the Global VPN Client dialog:
  - Double-click the Global VPN Client icon in the system tray.
  - Right-click the icon, and the select **Open Global VPN Client**.

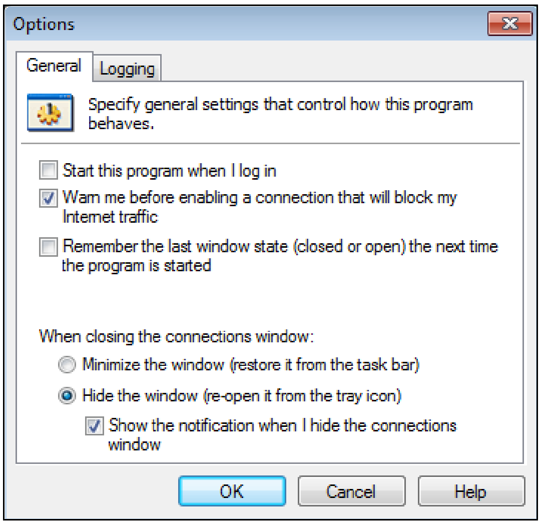
CAUTION: Exiting the SonicWall Global VPN Client from the system tray icon menu disables any active VPN connections.

ⓘ **TIP:** You can:

- Change the default launch setting for SonicWall Global VPN Client; see Specifying Global VPN Client Launch Options on page 16 for more information.
- Create a shortcut to automatically launch the Global VPN Client dialog and make the VPN connection from the desktop, taskbar, or **Start** menu. See Global VPN Client Licenses on page 50 for more information.
- Launch the Global VPN Client from the command line, See Using the Global VPN Client CLI on page 60 for more information.

Specifying Global VPN Client Launch Options

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



Options

General | Logging

Specify general settings that control how this program behaves.

☐ Start this program when I log in

☑ Warn me before enabling a connection that will block my Internet traffic

☐ Remember the last window state (closed or open) the next time the program is started

When closing the connections window:

○ Minimize the window (restore it from the task bar)

● Hide the window (re-open it from the tray icon)

☑ Show the notification when I hide the connections window

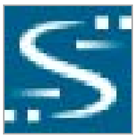
The **General** tab includes the following settings to control the launch of the Global VPN Client:

- **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 a **Connection Warning** message notifying you that the VPN connection will block local Internet and network traffic.
- **Remember the last window state (closed or open) the next time the program is started** - Allows the Global VPN Client to remember the last window state (open or closed) the next time the program is started. For example, a user can launch the Global VPN Client from the system tray without opening a window on the desktop.
- **When closing the connections window** - Specifies how the Global VPN Client behaves when the window is closed:
  - **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 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** - Selecting this checkbox activates the **SonicWall Global VPN Client Hide Notification** window whenever you close

the **Global VPN Client** window while the program is still running. The message tells you that the Global VPN Client program continues to run after you close (hide) the window.

Managing the Global VPN Client System Tray Icon

When you launch the **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 **Global VPN Client** icon in the system tray displays a menu of options for managing the program.

- **Open Global VPN Client** - Opens the program window.
- **Enable** - Displays a menu of VPN connections that can be enabled.
- **Disable** - Displays a menu of VPN connections that can be disabled.
- **Open Log Viewer** - Opens the Log Viewer to view informational and error messages. See Understanding the Global VPN Client Log on page 43 for more information on the Log Viewer.
- **Open Certificate Manager** - Opens the Certificate Manager. See Managing Certificates on page 41 for more information on the Certificate Manager.
- **Exit** - Exits the **Global VPN Client** window and disables any active VPN connections.

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

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

3

Adding VPN Connections

Understanding VPN Connections

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

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

- 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

Adding a new VPN connection is easy because SonicWall's Client Policy Provisioning automatically provides all the necessary configuration information to make a secure connection to the local or remote network. The burden of configuring the VPN connection parameters is removed from the Global VPN Client user. VPN connections can be created using three methods:

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

default.rcf file as part of the Global VPN Client software, one or more preconfigured VPN connections are automatically created when the program is installed.

ⓘ **NOTE:** Creating a default.rcf file and distributing it with the Global VPN Client software allows the SonicWall VPN Gateway administrator to streamline VPN client deployment and allows users to quickly establish VPN connections. If a default.rcf file is included with the downloaded Global VPN Client software, the VPN policy configured by the SonicWall VPN Gateway administrator is used to create a connection automatically when the client software is installed. For more information on creating the default.rcf file, see Using the default.rcf File on page 52.

ⓘ **NOTE:** To facilitate the automatic provisioning of Global VPN Clients, configure your SonicWall appliance be configured with GroupVPN . For instructions on configuring your appliance with GroupVPN, see the *SonicOS Administration Guide*.

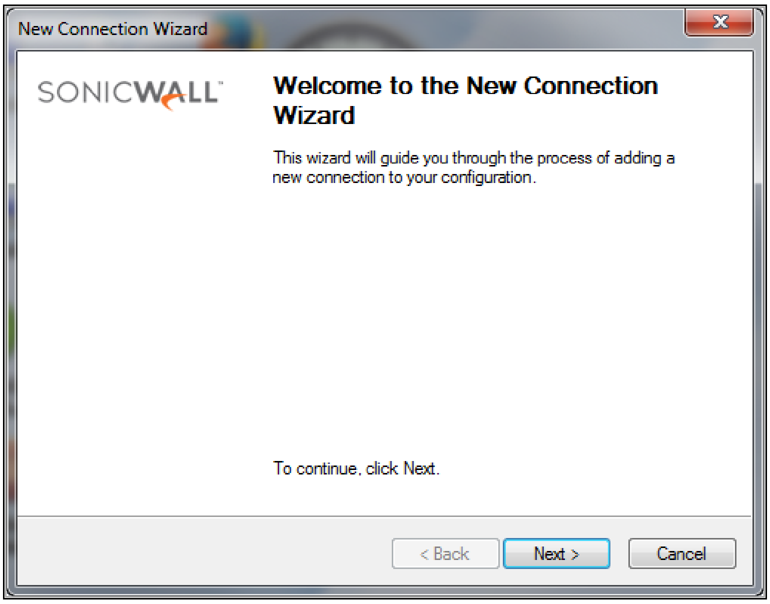
ⓘ **NOTE:** For instructions on importing a certificate into the Global VPN Client, see Using Certificates on page 41.

Creating a VPN Connection Using the New Connection Wizard

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

To use the New Connection Wizard:

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



New Connection Wizard

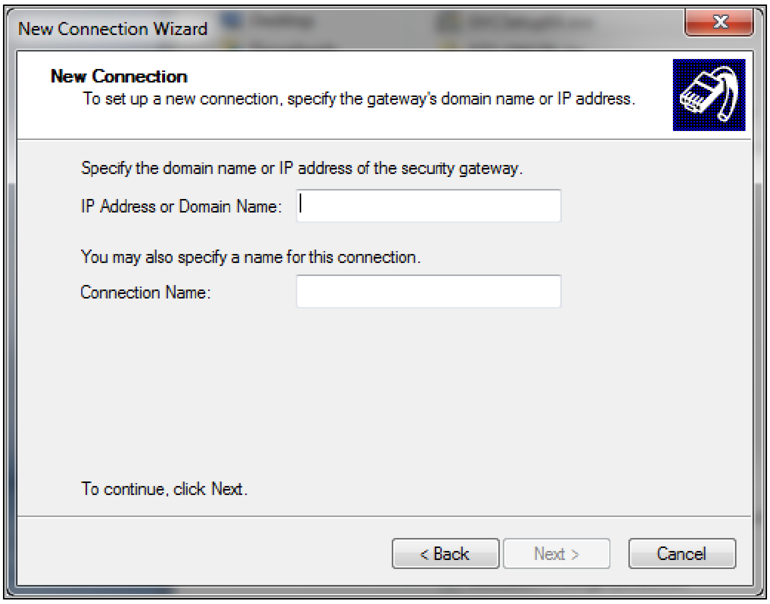
Welcome to the New Connection Wizard

This wizard will guide you through the process of adding a new connection to your configuration.

To continue, click Next.

2 If the **New Connection Wizard** does not display, to launch it, click the **New Connection** ➕ button.

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



New Connection Wizard

New Connection

To set up a new connection, specify the gateway's domain name or IP address.

Specify the domain name or IP address of the security gateway.

IP Address or Domain Name:

You may also specify a name for this connection.

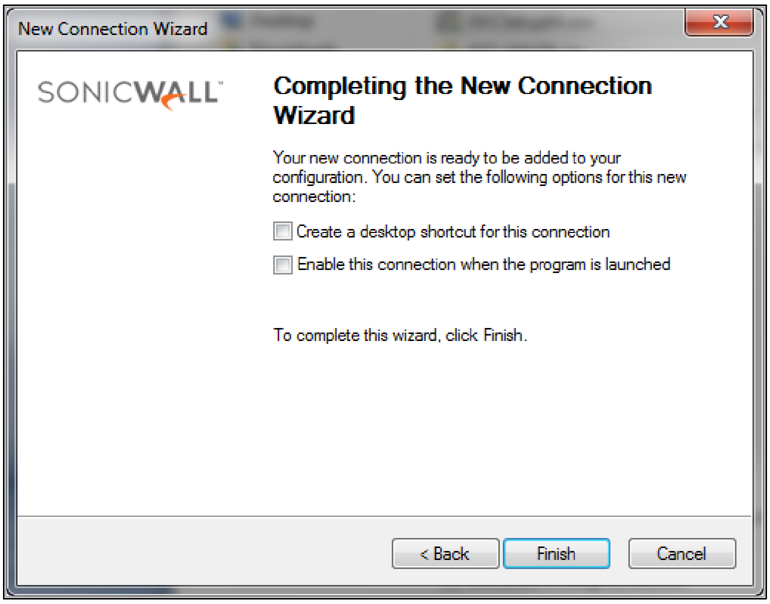
Connection Name:

To continue, click Next.

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

5 Optionally, if you want a different name for your connection, type the new name for your VPN connection in the **Connection Name** field.

6 Click **Next**. The **Completing the New Connection Wizard** page displays.



New Connection Wizard

Completing the New Connection Wizard

Your new connection is ready to be added to your configuration. You can set the following options for this new connection:

□ Create a desktop shortcut for this connection

□ Enable this connection when the program is launched

To complete this wizard, click Finish.

7 Optionally, select either or both:

- **Create a desktop shortcut for this connection** if you want to create a shortcut icon on your desktop for this VPN connection.
- **Enable this connection when the program is launched** if you want to automatically establish this VPN connection when you launch the SonicWall Global VPN Client.

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

Importing a VPN Configuration File

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

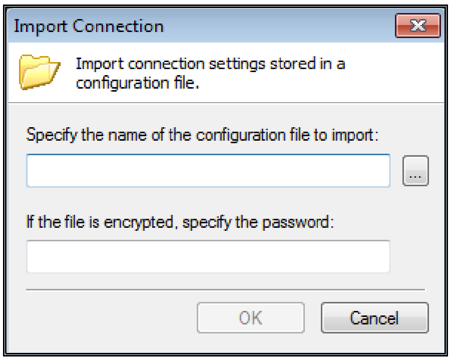
The VPN policy file is in the XML format to provide more efficient encoding of policy information. Because the file can be encrypted, pre-shared keys can also be exported in the file. The encryption method is specified in the PKCS#5 Password-Based Cryptography Standard from RSA Laboratories and uses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

ⓘ **NOTE:** If the `.rcf` file exported from the SonicWall appliance is encrypted, you must have the password to import the configuration file into the Global VPN Client.

To add a VPN connection by importing a connection file provided by your gateway administrator:

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

2 Select **File** > **Import**. The **Import Connection** dialog displays.



Import Connection

Import connection settings stored in a configuration file.

Specify the name of the configuration file to import:

If the file is encrypted, specify the password:

3 Either:

- Type the file path for the configuration file in the **Specify the name of the configuration file to import** field.
- Click the **Browse** ... button to locate the file.

4 If the file is encrypted, enter the password in the **If the file is encrypted, specify the password** field.

5 Click **OK**.

Using Global VPN Client from a Different Workstation

Using the SonicWall Global VPN Client to connect to a Microsoft Network has certain limitations. Typically, when a computer is attached to a Microsoft Network it has a persistent network connection to the domain controller that is used to verify the user credentials. When the user credentials have been verified by the domain controller, the computer then creates a locally cached profile that is used when the domain controller is not available. However, the SonicWall Global VPN Client provides an ad hoc secure network connection over the Internet back to the Microsoft Network containing the domain controller and thus is not a persistent connection. Since the remote computer cannot connect to the domain controller to verify the logon credentials until the connection is provided by the SonicWall Global VPN Client, the logon fails unless a locally cached profile is available.

The following steps illustrate the classic problem:

1 A Global VPN Client session must be established to communicate remotely with a Microsoft domain controller.

2 Global VPN Client can only be launched after you have logged on to the workstation. Because there is no way for the Global VPN Client to connect before you log on, you cannot use it for domain logon when initially logging on.

3 If you have logged on to the workstation before, there will be a locally cached profile that is used to log on.

   a You can then start the Global VPN Client, and a connection to the domain is established.

   b After connecting to the domain, you can run logon scripts, change password, access domain resources, etc.

   c When you log off, the Global VPN Client terminates, preventing domain communications.

4 If you have never logged on to the workstation before, there will not be a locally cached profile, so logon will not be possible.

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

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

The unfortunate result of this workaround is that a user without a cached profile on the computer cannot logon without a sojourn to the network containing the domain controller. This can be extremely cumbersome in certain situations such as being located in a distant satellite office and trying to get back to the main office.

Workaround — Forced Creation of a New Locally Cached Profile

The workaround is to create an induced local profile, and then log on to the Microsoft domain using the SonicWall Global VPN Client.

To create an induced local profile:

1 Log on to the workstation with any locally cached profile (for example, `mydomain\user1` or a local machine account). The locally cached profiles are usually stored in the `C:\Documents and Settings` directory. You should see a folder, called `user1`, in this path, which contains user1's profile.

2 Launch the SonicWall Global VPN Client.

3 After the SonicWall Global VPN Client establishes a connection and the workstation can communicate with the domain controller, you can create another locally cached profile. You can use the `runas` command to create a locally cached profile for a new user (for example, `mydomain\user2`) while using the Global VPN Client connection provided by user1.

4 From a command prompt, type `runas /user:`*`mydomain`*`\`*`user2`*` explorer.exe` (substitute your actual domain for *`mydomain`* and actual username for *`user2`*). You can use `notepad.exe` instead of `explorer.exe` if you prefer.

5 At the prompt, enter the domain password for user2.

6 It will take anywhere from a few seconds to a few minutes to create the local profile for user2, and to launch the `explorer.exe` program. You may quit the `explorer.exe` program after it launches.

7 The `C:\Documents and Settings` directory should now contain a folder for user2.

8 Close the Global VPN Client.

9 Log off as user1 from the workstation. You will see the familiar **Log On to Windows** dialog.

10 Log onto the workstation as user2 using the newly created locally cached profile.

11 Launch the SonicWall Global VPN Client. The user2 profile will now provide the credentials for all domain access (including running logon scripts).

12 You can repeat this procedure as many times as necessary to create additional profiles.

It is also possible to change an expired user password with this procedure if you have another account available to make the Global VPN Client connection back to the domain controller. A simple way to change passwords is from the Windows Security dialog, accessed by:

1 Pressing **Ctrl+Alt Delete**.

2 Select **Change a password …**.

3 Enter the old password.

4 Enter the new password.

5 Confirm the new password.

6 Click the **Arrow** button.

4

Making VPN Connections

Overview

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

The Global VPN Client supports two IPsec authentication modes:

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

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

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

Accessing Redundant VPN Gateways

The Global VPN Client supports redundant VPN gateways by manually adding the peer in the **Peers** page of the VPN connection **Properties** window. The Global VPN Client adds automatic support for redundant VPN gateways if the IPsec gateway’s domain name resolves to multiple IP addresses. For example, if `gateway.yourcompany.com` resolves to `67.115.118.7`, `67.115.118.8`, and `67.115.118.9`, the

Global VPN Client cycles through these resolved IP addresses until it finds a gateway that responds, allowing multiple IP addresses to be used as failover gateways. If all the resolved IP addresses fail to respond, Global VPN Client switches to the next peer, if another peer is specified in the **Peers** page of the VPN connection **Properties** dialog. See Connection Properties Peers Settings on page 33 for more information.

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

Enabling a VPN Connection

Enabling a VPN connection with the SonicWall Global VPN Client is a transparent two phase process. Phase 1 enables the connection, which completes the ISAKMP (Internet Security Association and Key Management Protocol) negotiation. Phase 2 is IKE (Internet Key Exchange) negotiation, which establishes the VPN tunnel for sending and receiving data.

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

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

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

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

> ⓘ **NOTE:** f the Global VPN Client does not establish the VPN connection, you can use the **Log Viewer** to view the error messages to troubleshoot the problem. See Understanding the Global VPN Client Log on page 43 for more information.

To establish a VPN connection using the Global VPN Client:

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

  - If you selected **Enable this connection when the program is launched** in the **New Connection Wizard**, the VPN connection is automatically established when you launch the SonicWall Global VPN Client.
  - If your VPN connection is not automatically established when you launch the Global VPN Client, choose one of the following methods to enable a VPN connection:
    - Double-click the VPN connection.
    - Right-click the VPN connection icon and select **Enable** from the menu.
    - Select the VPN connection and press **Ctrl+B**.
    - Select the VPN connection, and click the **Enable** button on the toolbar
    - Select the VPN connection, and then choose **File > Enable**.

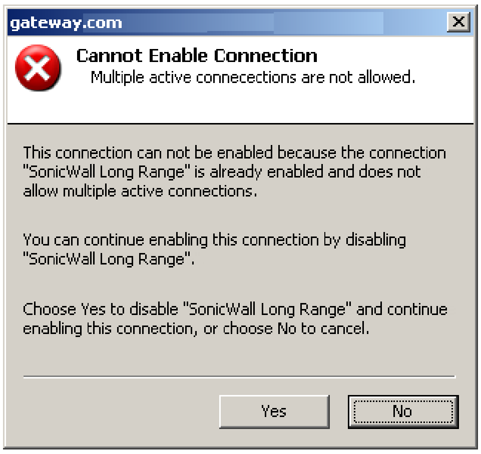
- If the **Global VPN Client** icon is displayed in the system tray, right-click the icon and then select **Enable >** `connection name`. Global VPN Client enables the VPN connection without opening the **Global VPN Client** window.

2 Depending on how the VPN connection is configured, these dialogs may be displayed:

- **Cannot Enable Connection** – see Establishing Multiple Connections on page 26
- **Enter Pre-Shared Secret** – see Entering a Pre-Shared Key on page 26
- **Enter Username and Password** – see Providing Username and Password Authentication on page 28
- **Connection Warning** – see Connection Warning on page 29

Establishing Multiple Connections

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



gateway.com

Cannot Enable Connection

Multiple active connecections are not allowed.

This connection can not be enabled because the connection "SonicWall Long Range" is already enabled and does not allow multiple active connections.

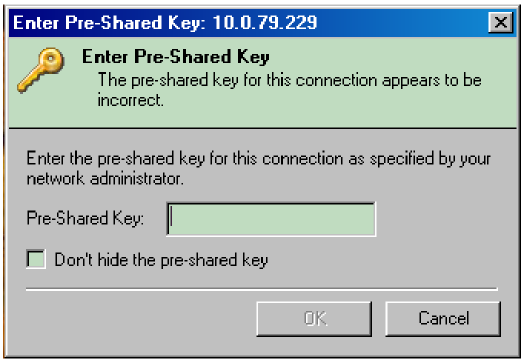
You can continue enabling this connection by disabling "SonicWall Long Range".

Choose Yes to disable "SonicWall Long Range" and continue enabling this connection, or choose No to cancel.

Entering a Pre-Shared Key

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

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



Enter Pre-Shared Key: 10.0.79.229

Enter Pre-Shared Key

The pre-shared key for this connection appears to be incorrect.

Enter the pre-shared key for this connection as specified by your network administrator.

Pre-Shared Key:

□ Don't hide the pre-shared key

To enter a Pre-Shared Key:

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

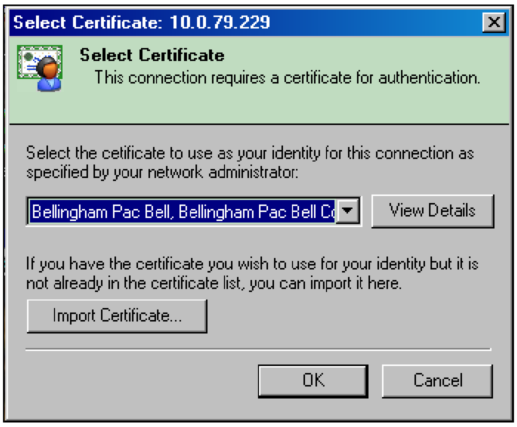
2 Optionally, if you want to make sure you are entering the correct Pre-Shared Key, select **Don't hide the pre-shared key**. The Pre-Shared Key you enter appears unmasked in the **Pre-shared Key** field.

   ⓘ | **TIP:** If you select this option, be sure to unselect it when you've verified the Pre-Shared Key.

3 Click **OK**.

Selecting a Certificate

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



Select Certificate: 10.0.79.229

Select Certificate

This connection requires a certificate for authentication.

Select the cetificate to use as your identity for this connection as specified by your network administrator:

Bellingham Pac Bell, Bellingham Pac Bell C

If you have the certificate you wish to use for your identity but it is not already in the certificate list, you can import it here.

ⓘ | **NOTE:** For more information on using the **Certificate Manager,** see Managing Certificates on page 41.

To select a certificate:

1 Do one of the following:

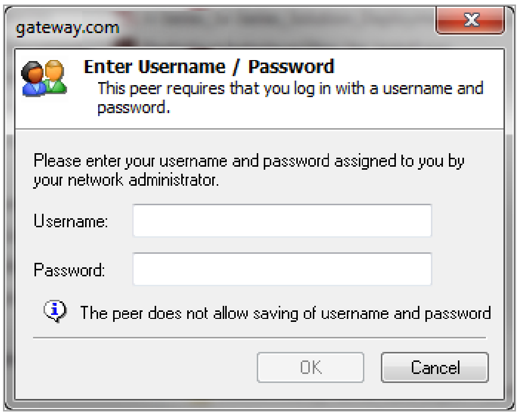
   - Select the certificate from the menu.
   - If you have a certificate that has not been imported into the Global VPN Client using **Certificate Manager**, click **Import Certificate**.

2 Click **OK**.

Providing Username and Password Authentication

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

If the SonicWall VPN gateway is provisioned to prompt you for the username and password to enter the remote network, the **Enter Username and Password** dialog appears.



gateway.com

Enter Username / Password

This peer requires that you log in with a username and password.

Please enter your username and password assigned to you by your network administrator.

Username:

Password:

The peer does not allow saving of username and password

To enter a username and password:

1 Type your username and password.

2 Optionally, if permitted by the gateway, select **Remember Username and Password** to cache your username and password to automatically log in for future VPN connections.

3 Click **OK** to continue with establishing your VPN connection.

Creating a Connection Shortcut

TIP: Create a Desktop shortcut for the SonicWall Global VPN Client program for easy access to all your connections.

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

To create a shortcut:

1 Select the VPN connection for which to create a shortcut in the Global VPN Client window.

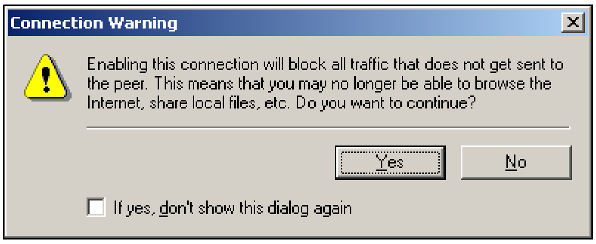
2 Choose **File > Create Shortcut**.

3 Select the shortcut option you want: **On the Desktop**, **On the Task Bar**, **In the Start Menu**, or **Select a Location**.

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

Connection Warning

If the VPN connection policy allows only traffic to the gateway, the **Connection Warning** message appears, warning you that only network traffic destined for the remote network at the other end of the VPN tunnel is allowed. Any network traffic destined for local network interfaces and the Internet is blocked.



Connection Warning

Enabling this connection will block all traffic that does not get sent to the peer. This means that you may no longer be able to browse the Internet, share local files, etc. Do you want to continue?

□ If yes, don't show this dialog again

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 again**.

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

5

Configuring VPN Connection Properties

Displaying the Connections Properties Dialog

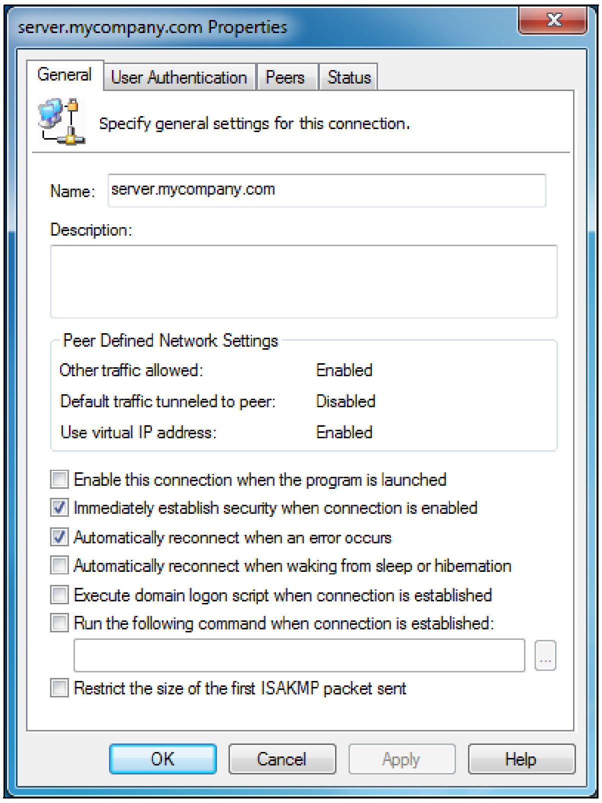
The **Connection Properties** dialog includes the controls for configuring a specific VPN connection profile. To open the **Connection Properties** dialog, choose one of the following methods:

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

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

Connection Properties General Settings

The **General** tab in the **Connection Properties** dialog displays the following settings:



server.mycompany.com Properties

Specify general settings for this connection.

Name: server.mycompany.com

Description:

Peer Defined Network Settings

Other traffic allowed:	Enabled
Default traffic tunneled to peer:	Disabled
Use virtual IP address:	Enabled

□ Enable this connection when the program is launched
☑ Immediately establish security when connection is enabled
☑ Automatically reconnect when an error occurs
□ Automatically reconnect when waking from sleep or hibernation
□ Execute domain logon script when connection is established
□ Run the following command when connection is established:
□ Restrict the size of the first ISAKMP packet sent

- **Name** - Displays the name of your VPN connection.
- **Description** - Displays a pop-up text about the connection. The text appears when your mouse pointer moves over the VPN connection.
- **Peer Defined Network Settings** - Defines the status of Tunnel All support. These settings are controlled at the SonicWall VPN gateway.
  - **Other traffic allowed** - If enabled, your computer can access the local network or Internet connection while the VPN connection is active.
  - **Default traffic tunneled to peer** - If activated, all network traffic not routed to the SonicWall VPN gateway is blocked. When you enable the VPN connection with this feature active, the **Connection Warning** message appears.
  - **Use virtual IP address** - Allows the VPN Client to get its IP address via DHCP through the VPN tunnel from the gateway.
- **Enable this connection when the program is launched** - Establishes the VPN connection as the default VPN connection when you launch the SonicWall Global VPN Client.
- **Immediately establish security when connection is enabled** - Negotiates the first phase of IKE as soon as the connection is enabled instead of waiting for network traffic transmission to begin. This setting is enabled by default.
- **Automatically reconnect when an error occurs** - With this feature enabled, if the Global VPN Client encounters a problem connecting to the peer, it keeps retrying to make the connection. This feature allows a Global VPN Client to make a connection to a VPN connection that is temporarily disabled, without manual intervention.

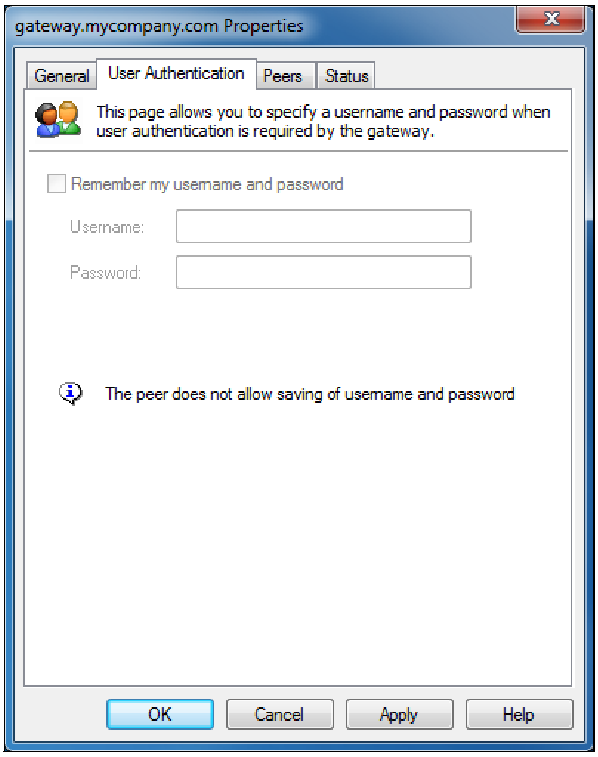
If the connection error is due to an incorrect configuration, such as the DNS or IP address of the peer gateway, then the connection must be manually corrected. Check the Log Viewer to determine the problem and then edit the connection.

This option is enabled by default. If an error occurs with this option disabled during an attempted connection, the Global VPN Client logs the error, displays an error message dialog, and stops the connection attempt.

- **Automatically reconnect when waking from sleep or hibernation** - Automatically re-enables the VPN connection after the computer wakes from a sleep or hibernation state. This setting is disabled by default.
- **Execute logon script when connected** - After logging into the SonicWall VPN Gateway and establishing a secure tunnel, performs any action configured in the logon script.
- **Run the following command when connection is established** - Allows a program to be automatically executed, with optional arguments, when successful VPN connections are established.
- **Restrict the size of the first ISAKMP packet sent** - This option can be used when the Global VPN Client gets an error such as, “The peer is not responding to phase 1 ISAKMP requests” when attempting to connect. This error can occur when the ISAKMP packet is fragmented due to its size, but the network device (router) does not allow a fragmented packet when establishing the VPN connection.

Connection Properties User Authentication Settings

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.


gateway.mycompany.com Properties

This page allows you to specify a username and password when user authentication is required by the gateway.

☐ Remember my username and password

Username:

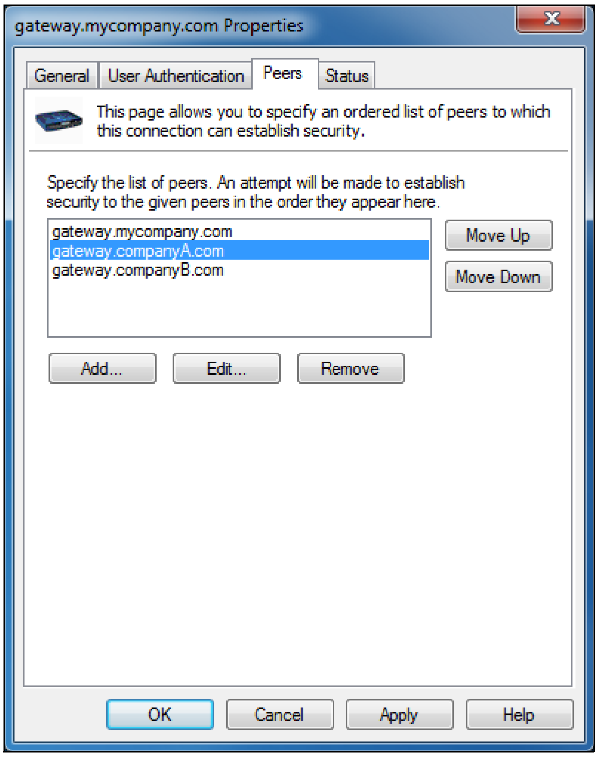
Password:

The peer does not allow saving of username and password

- **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.

Connection Properties Peers Settings

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



gateway.mycompany.com Properties

This page allows you to specify an ordered list of peers to which this connection can establish security.

Specify the list of peers. An attempt will be made to establish security to the given peers in the order they appear here.

gateway.mycompany.com
gateway.companyA.com
gateway.companyB.com

To add a peer:

1 Click **Add**.

2 In the **Peer Information** dialog, enter the IP address or DNS Name in the **IP Address or DNS Name** field.

3 Click **OK**.

To edit a peer entry:

1 Select the peer name.

2 Click **Edit**.

3 In the **Peer Information** dialog, make your changes. See Peer Information Dialog on page 34.

4 Click **OK**.

To change the order of the peer list:

1 Select a peer name

2 Click **Move Up** or **Move Down**.

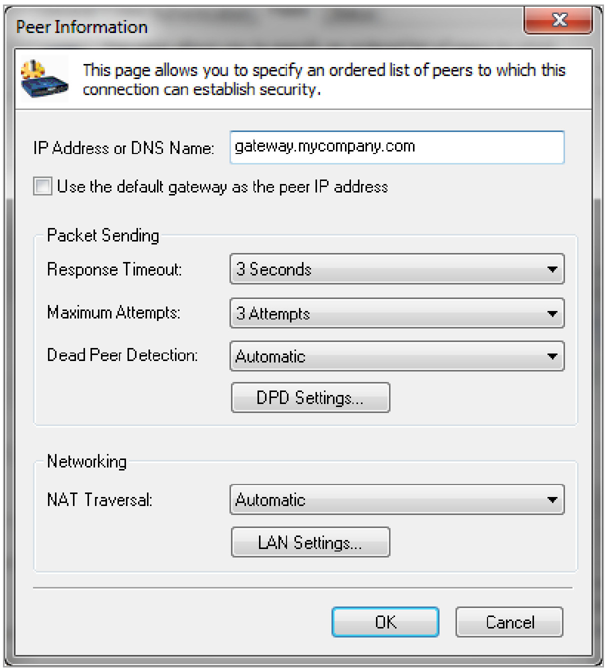
To delete a peer entry:

1 Select the peer entry.

2 Click **Remove**.

Peer Information Dialog

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



Peer Information

This page allows you to specify an ordered list of peers to which this connection can establish security.

IP Address or DNS Name: gateway.mycompany.com

□ Use the default gateway as the peer IP address

Packet Sending

Response Timeout: 3 Seconds

Maximum Attempts: 3 Attempts

Dead Peer Detection: Automatic

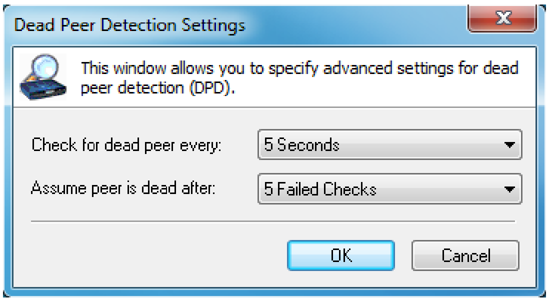
Networking

NAT Traversal: Automatic

- **IP Address or DNS Name** - Specifies the peer VPN gateway IP address or DNS name.
- **Use the default gateway as the peer IP address** - Specifies the default gateway as the peer IP address. The Global VPN Client gets the default gateway from the routing table.
- **Response Timeout** - Specifies the maximum amount of time to wait for a response to a sent packet. After this time expires, the sent packet is considered lost and the packet is retransmitted. The valid range is 1-10 seconds.
- **Maximum Attempts** - Specifies the maximum number of times the same packet is sent before determining that the peer is not responding. The valid range is 1-10 attempts.
- **Dead Peer Detection** - Select from:
  - **Automatic** - This is traffic-based DPD. If Global VPN Client does not receive response data (one-way traffic), then Global VPN Client exchanges heartbeat packets to detect if the peer gateway is alive. If there is no heartbeat packet response for the configured number of failed checks in **DPD Settings**, then Global VPN Client tries to re-initiate IKE negotiations. This setting is enabled by default.
  - **Forced On** - Performs DPD periodically. The Global VPN Client exchanges heartbeat packets to detect if the peer gateway is alive. If there is no heartbeat packet response for the configured number of failed checks in **DPD Settings**, then Global VPN Client tries to re-initiate IKE negotiations.

    - **Disabled** - DPD is disabled. No heartbeat packets are exchanged. This prevents Global VPN Client from detecting when the gateway is unavailable.

- **DPD Settings** - Displays the **Dead Peer Detection Settings** dialog.



Dead Peer Detection Settings

This window allows you to specify advanced settings for dead peer detection (DPD).

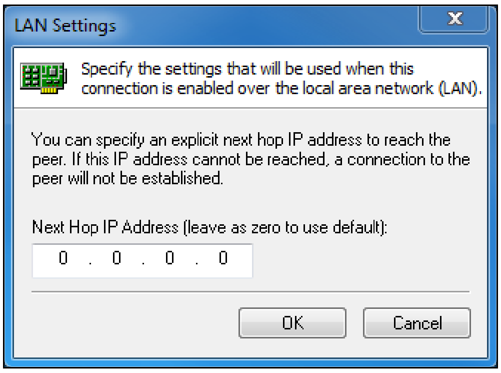
Check for dead peer every: 5 Seconds

Assume peer is dead after: 5 Failed Checks

    - **Check for dead peer every** - choose from 3, 5, 10, 15, 20, 25, or 30 seconds.
    - **Assume peer is dead after** - choose from 3, 4, or 5 Failed Checks.

- **NAT Traversal** - Choose one of the following three options:
    - **Automatic** - Automatically determines whether to use UDP encapsulation of IPsec packets between the peers.
    - **Forced On** - Forces the use of UDP encapsulation of IPsec packets even when there is no NAPT/NAT device in between the peers.
    - **Disabled** - Disables use of UDP encapsulation of IPsec packets between the peers.

- **LAN Settings** - Displays the **LAN Settings** dialog for specifying the setting used when this connection is enabled over the LAN.



LAN Settings

Specify the settings that will be used when this connection is enabled over the local area network (LAN).

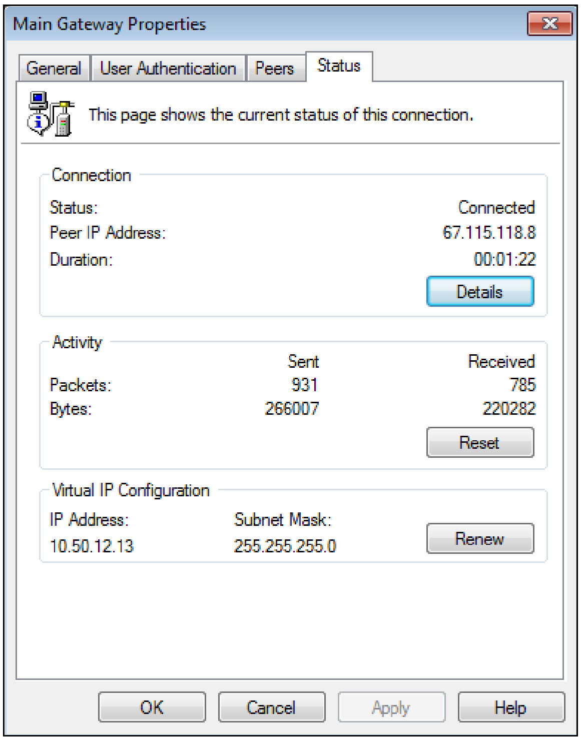
You can specify an explicit next hop IP address to reach the peer. If this IP address cannot be reached, a connection to the peer will not be established.

Next Hop IP Address (leave as zero to use default): 0 . 0 . 0 . 0

Type the IP address in the **Next Hop IP Address** field to specify the next hop IP address of a different route than the default route. Leaving the setting as zeros instructs the Global VPN Client to use the default route.

Connection Properties Status Settings

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



Main Gateway Properties

This page shows the current status of this connection.

Connection

Status: Connected
Peer IP Address: 67.115.118.8
Duration: 00:01:22

Activity

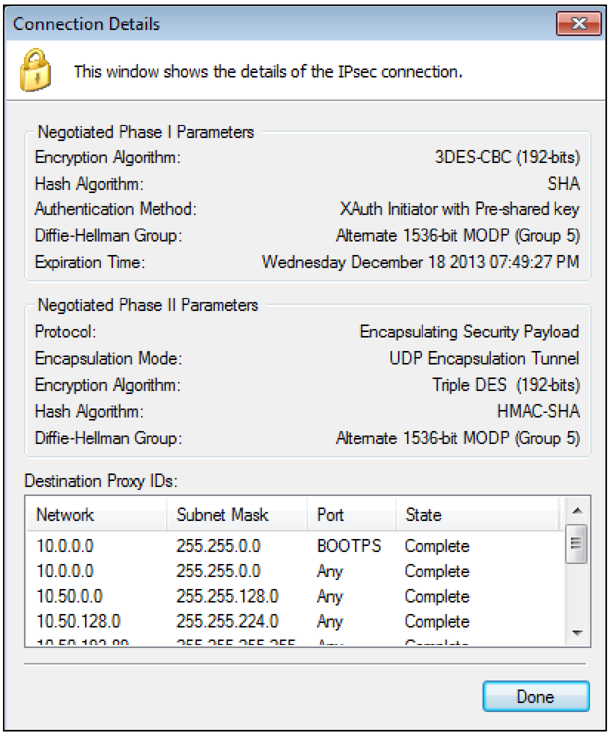
	Sent	Received
Packets:	931	785
Bytes:	266007	220282

Virtual IP Configuration

IP Address: 10.50.12.13
Subnet Mask: 255.255.255.0

- **Connection**:
  - **Status** - Indicates whether VPN connection is enabled or disabled.
  - **Peer IP Address** - Displays the IP address of the VPN connection peer.
  - **Duration** - Displays connection time.

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



Connection Details

This window shows the details of the IPsec connection.

Negotiated Phase I Parameters

Encryption Algorithm: 3DES-CBC (192-bits)
Hash Algorithm: SHA
Authentication Method: XAuth Initiator with Pre-shared key
Diffie-Hellman Group: Alternate 1536-bit MODP (Group 5)
Expiration Time: Wednesday December 18 2013 07:49:27 PM

Negotiated Phase II Parameters

Protocol: Encapsulating Security Payload
Encapsulation Mode: UDP Encapsulation Tunnel
Encryption Algorithm: Triple DES (192-bits)
Hash Algorithm: HMAC-SHA
Diffie-Hellman Group: Alternate 1536-bit MODP (Group 5)

Destination Proxy IDs:

Network	Subnet Mask	Port	State
10.0.0.0	255.255.0.0	BOOTPS	Complete
10.0.0.0	255.255.0.0	Any	Complete
10.50.0.0	255.255.128.0	Any	Complete
10.50.128.0	255.255.224.0	Any	Complete

- **Activity**:
  - **Packets** - Displays number of packets sent and received through the VPN tunnel.
  - **Bytes** - Displays number of bytes sent and received through the VPN tunnel.
  - **Reset** - Resets the Packets and Bytes values to zero, from which these counts immediately resume.
- **Virtual IP Configuration**:
  - **IP Address** - The IP address assigned via DHCP through the VPN tunnel from the VPN gateway.
  - **Subnet Mask** - The subnet mask for the virtual IP address.
  - **Renew** - Renews the DHCP lease.

6

Managing VPN Connections

About VPN Connections

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

Arranging Connections

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

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

Renaming a Connection

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

Deleting a Connection

ⓘ **IMPORTANT:** You cannot delete an active VPN connection. Disable the VPN connection first, then delete it.

To delete a connection, do one of these:

- Select the connection and then press the **Delete** key.
- Choose **File > Delete**.
- Right-click the connection name and choose **Delete**.

Selecting All Connections

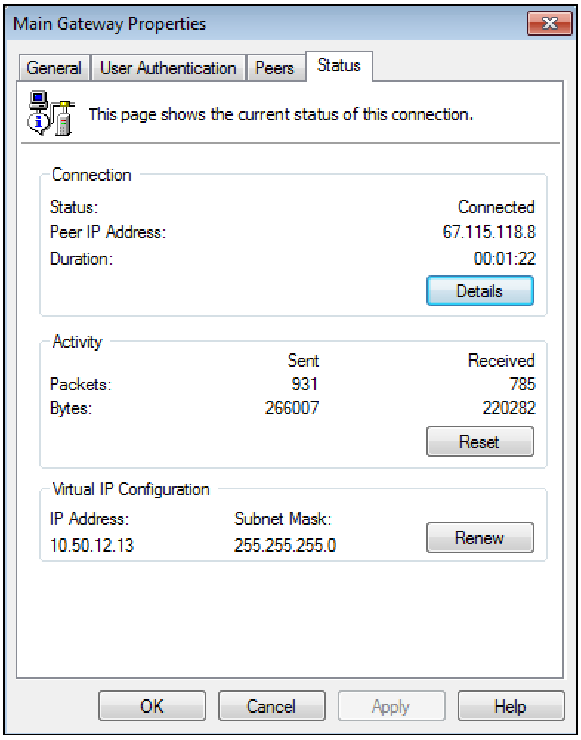
Choosing **View > Select All** or pressing **Ctrl+A** selects all the connections in the **Global VPN Client** window.

Checking the Status of VPN Connections

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

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

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



This page shows the current status of this connection.

Connection

Status:	Connected
Peer IP Address:	67.115.118.8
Duration:	00:01:22

Activity

	Sent	Received
Packets:	931	785
Bytes:	266007	220282

Virtual IP Configuration

IP Address:	Subnet Mask:
10.50.12.13	255.255.255.0

TIP: For more information on the **Status** page, see Connection Properties Status Settings on page 36.

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

7

Using Certificates

Obtaining Certificate Information

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.

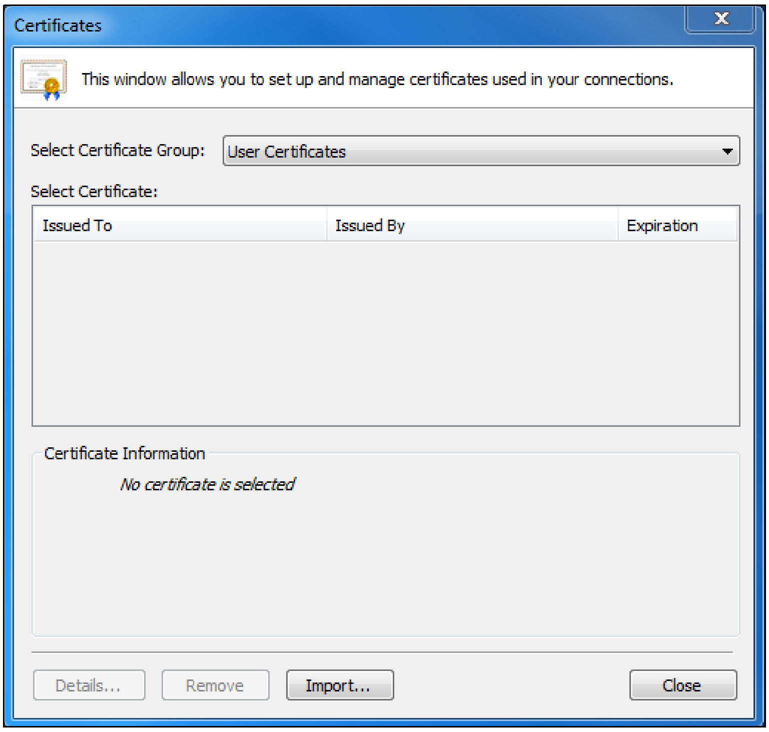
△ CAUTION: **If digital certificates are required as part of your VPN connection policy, your VPN gateway administrator must provide you with the required certificates.**

Managing Certificates

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

To open the Certificate Manager for managing certificates:

1 Click the **View** menu.



Certificates

This window allows you to set up and manage certificates used in your connections.

Select Certificate Group: User Certificates

Select Certificate:

Issued To	Issued By	Expiration

Certificate Information

No certificate is selected

2 Select **Certificates** in the **Global VPN Client** window.

3 In the **Select Certificate Group** drop-down menu, select one of these types of certificates:

- **User** – The local digital certificates used to establish the VPN Security Association.
- **CA** – The digital certificates used to validate the user certificates.
- **Trusted Root CA** – Is used to validate the CA Certificates.

4 Select the certificate in the list and then do one of these:

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

ⓘ **TIP:** For more information on using certificates for your VPN on the SonicWall appliance, see the *SonicOS Administration Guide.*

8

Troubleshooting the Global VPN Client

Tools for Troubleshooting

The SonicWall Global VPN Client provides tools for troubleshooting your VPN connections:

- Log Viewer – Understanding the Global VPN Client Log on page 43
- Help Report – Configuring the Log on page 46
- SonicWall's Support site – Accessing SonicWall Global VPN Client Technical Support on page 48
- SonicWall Global VPN Client help system – Accessing SonicWall Global VPN Client Technical Support on page 48
- Global VPN Client uninstall – Uninstalling the Global VPN Client on page 49

Understanding the Global VPN Client Log

The **Global VPN Client Log** window displays messages about Global VPN Client activities. You can save the messages as well as manage them.

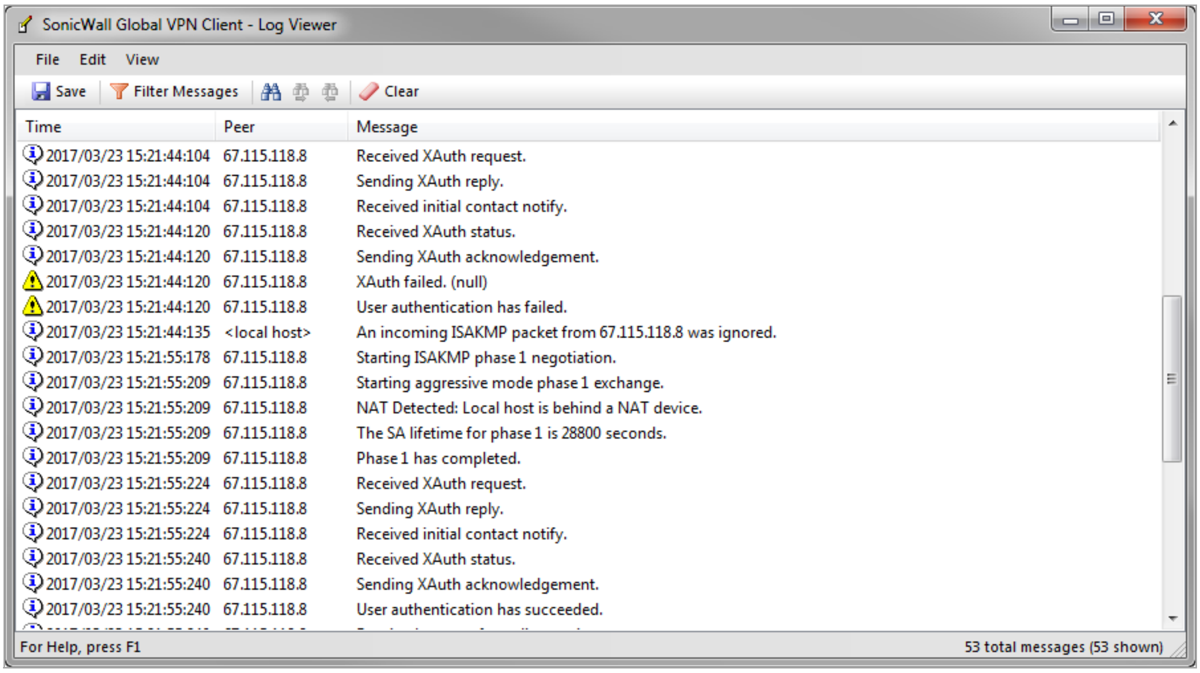
Topics:

Opening the Log Viewer Window

To open the Log Viewer window:

1 Do one of the following:

- Click the **Show Log** button on the **Global VPN Client** window toolbar.
- Choose **View > Log Viewer**.
- Press **Ctrl+L**.


SonicWall Global VPN Client - Log Viewer
File
Edit
View
Save
Filter Messages
Clear
For Help, press F1
53 total messages (53 shown)

```
   Time                     Peer           Message
ⓘ 2017/03/23 15:21:44:104  67.115.118.8   Received XAuth request.
ⓘ 2017/03/23 15:21:44:104  67.115.118.8   Sending XAuth reply.
ⓘ 2017/03/23 15:21:44:104  67.115.118.8   Received initial contact notify.
ⓘ 2017/03/23 15:21:44:120  67.115.118.8   Received XAuth status.
ⓘ 2017/03/23 15:21:44:120  67.115.118.8   Sending XAuth acknowledgement.
⚠ 2017/03/23 15:21:44:120  67.115.118.8   XAuth failed. (null)
⚠ 2017/03/23 15:21:44:120  67.115.118.8   User authentication has failed.
ⓘ 2017/03/23 15:21:44:135  <local host>   An incoming ISAKMP packet from 67.115.118.8 was ignored.
ⓘ 2017/03/23 15:21:55:178  67.115.118.8   Starting ISAKMP phase 1 negotiation.
ⓘ 2017/03/23 15:21:55:209  67.115.118.8   Starting aggressive mode phase 1 exchange.
ⓘ 2017/03/23 15:21:55:209  67.115.118.8   NAT Detected: Local host is behind a NAT device.
ⓘ 2017/03/23 15:21:55:209  67.115.118.8   The SA lifetime for phase 1 is 28800 seconds.
ⓘ 2017/03/23 15:21:55:209  67.115.118.8   Phase 1 has completed.
ⓘ 2017/03/23 15:21:55:224  67.115.118.8   Received XAuth request.
ⓘ 2017/03/23 15:21:55:224  67.115.118.8   Sending XAuth reply.
ⓘ 2017/03/23 15:21:55:224  67.115.118.8   Received initial contact notify.
ⓘ 2017/03/23 15:21:55:240  67.115.118.8   Received XAuth status.
ⓘ 2017/03/23 15:21:55:240  67.115.118.8   Sending XAuth acknowledgement.
ⓘ 2017/03/23 15:21:55:240  67.115.118.8   User authentication has succeeded.
```

The **Log Viewer** window displays this information:

- **Type** - The icon indicating the type of message:
  - **Information** - ⓘ
  - **Warning** - ⚠
  - **Error** - ⊗
- **Time** - Date and time the message was generated.
- **Peer** - The IP address or FQDN of the peer.
- **Message** - Text of the message describing the event.

Saving the Current Log

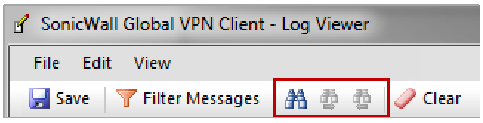
Click the **Save** button to save the current log to a `.txt` file. When you save the current log to a file, the Global VPN Client automatically adds a **Help Report** containing useful information regarding the condition of the SonicWall Global VPN Client as well as the system it's running on for troubleshooting. The **Help Report** information is inserted at the beginning of the log file. See Generating a Help Report on page 47 for more information.

ⓘ | **TIP:** For a complete listing of Log Viewer messages, see Log Viewer Messages on page 62 .

Managing Log Messages

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

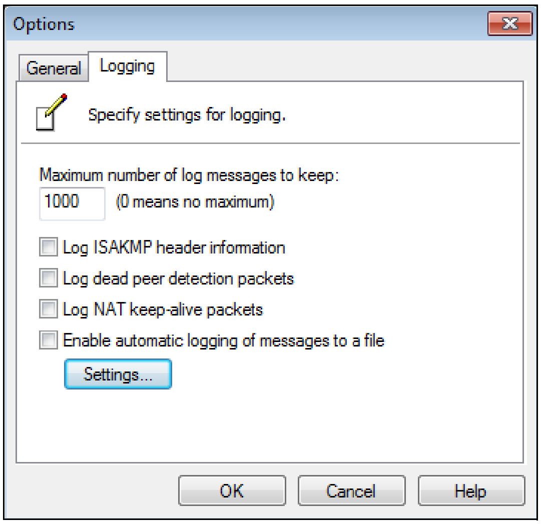
- To save a current log to a `.txt` file, click the **Save** button on the toolbar, press **Ctrl+S**, or choose **File > Save**. When you save a Log Viewer file, the Global VPN Client automatically adds a report containing useful information regarding the condition of the SonicWall Global VPN Client as well as the system it is running on.
- To select all messages, press **Ctrl+A** or choose **Edit > Select All**.
- To copy log contents for pasting into another application, select the messages you want to copy, then press **Ctrl+C** or choose **Edit > Copy**.
- To display less detailed information in the log viewer, click the **Filter Messages** button on the toolbar or choose **View > Filter Messages**.
- To search the log messages for a character string, do one of the following:
  - Click the **Find** icon on the toolbar.
  - Choose **Edit > Find** and enter the string in the **Find** dialog.

    In the dialog, you can select **Match Whole Word Only**, **Match Case**, and **Up** or **Down** for the search direction.
  - Click the **Find Next** icon to search. Once a string is entered in the **Find** dialog, you can click the **X** to close the dialog, then use the **Find Next** and **Find Previous** icons in the toolbar.
- To clear current log information, do one of these:
  - Click **Clear** on the toolbar.
  - Press **Crtl+X**.
  - Choose **Edit > Clear**.
- To hide or show the toolbar in the **Log Viewer** window, choose **View > Toolbar** to toggle the toolbar on or off.
- To hide or show the status bar in the **Log Viewer** window, choose **View > Status Bar** to toggle the status bar on or off.

Configuring the Log

The **Logging** tab in the **View > Options** dialog specifies the settings for configuring the Global VPN Client Log behavior.



Options

General | Logging

Specify settings for logging.

Maximum number of log messages to keep:
1000 (0 means no maximum)

□ Log ISAKMP header information
□ Log dead peer detection packets
□ Log NAT keep-alive packets
□ Enable automatic logging of messages to a file

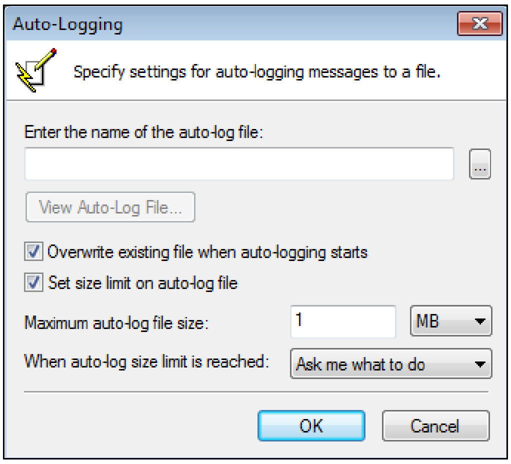
Settings...

OK | Cancel | Help

- **Maximum number of log messages to keep** - Specifies the maximum number of log messages kept in the log file.
- **Log ISAKMP header information** - Enables the logging of ISAKMP header information.
- **Log dead peer detection packets** - Enables the logging of dead peer detection packets.
- **Log NAT keep-alive packets** - Enables the logging of NAT keep-alive packets.
- **Enable automatic logging of messages to file** - Enables automatic logging of messages to a file as specified in the **Auto-Logging** window.
- **Settings** - Displays the **Auto-Logging** dialog; see Configuring Auto-Logging on page 46.

Configuring Auto-Logging

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



Auto-Logging

Specify settings for auto-logging messages to a file.

Enter the name of the auto-log file:

View Auto-Log File...

☑ Overwrite existing file when auto-logging starts
☑ Set size limit on auto-log file

Maximum auto-log file size: 1 MB

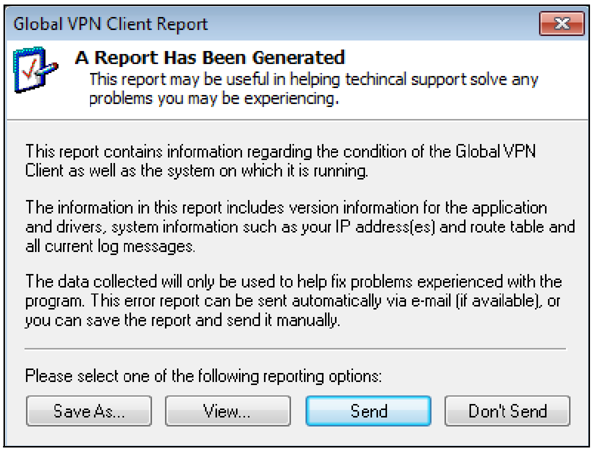
When auto-log size limit is reached: Ask me what to do

OK | Cancel

- **Enter the name of the auto-log file** - Specifies the file in which to save the logging messages. Clicking on the **Browse** button allows you to specify the location of your auto-log file. If only a file name is specified (no path is given in the file name), the log file is created in the user's TEMP directory.
- **View Auto-Log File** - Displays the entire log file up to 71,000 lines.
- **Overwrite existing file when auto-logging starts** - Overwrites the existing auto-log file when auto-logging is started.
- **Set size limit on auto-log file** - Limits the maximum size of the log file.
- **Maximum auto-log file size** - Specifies the maximum file size in KB or MB.
- **When auto-log size limit is reached** - Specifies the action to take when the auto-log file reaches the maximum size:
    - **Ask me what to do** - When the log file reaches the maximum size, prompts to choose either **Stop auto-logging or Overwrite auto-log file**.
    - **Stop auto-logging** - Stops auto-logging when the maximum file size is reached.
    - **Overwrite auto-log file** - Overwrites the existing auto-log file after the maximum file size is reached.

Generating a Help Report

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



Global VPN Client Report

A Report Has Been Generated

This report may be useful in helping techincal support solve any problems you may be experiencing.

This report contains information regarding the condition of the Global VPN Client as well as the system on which it is running.

The information in this report includes version information for the application and drivers, system information such as your IP address(es) and route table and all current log messages.

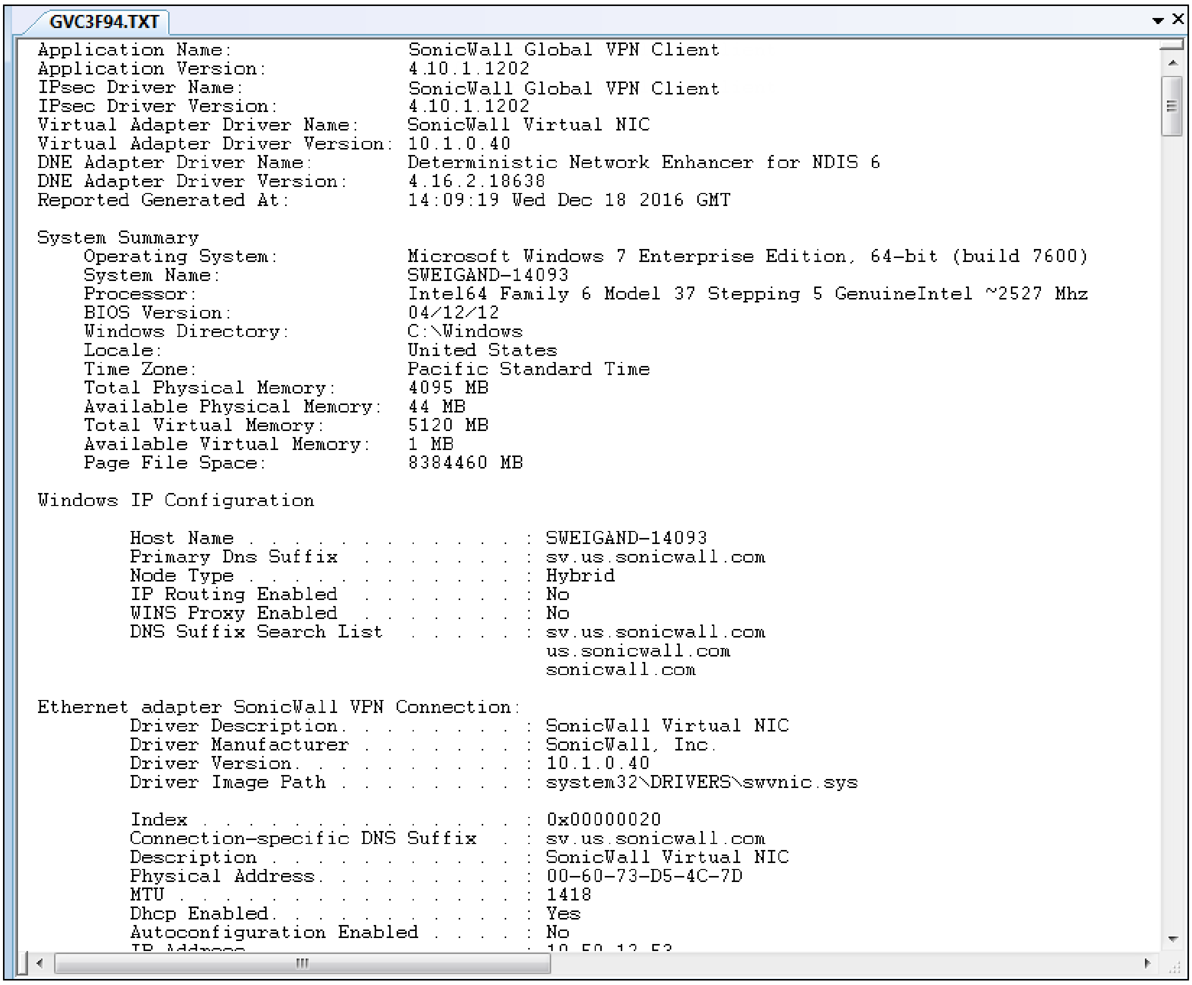
The data collected will only be used to help fix problems experienced with the program. This error report can be sent automatically via e-mail (if available), or you can save the report and send it manually.

Please select one of the following reporting options:

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 is running on:

- Version information
- Drivers
- System information
- IP addresses
- Route table
- Current log messages

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



```
Application Name:                SonicWall Global VPN Client
Application Version:             4.10.1.1202
IPsec Driver Name:               SonicWall Global VPN Client
IPsec Driver Version:            4.10.1.1202
Virtual Adapter Driver Name:     SonicWall Virtual NIC
Virtual Adapter Driver Version:  10.1.0.40
DNE Adapter Driver Name:         Deterministic Network Enhancer for NDIS 6
DNE Adapter Driver Version:      4.16.2.18638
Reported Generated At:           14:09:19 Wed Dec 18 2016 GMT

System Summary
    Operating System:            Microsoft Windows 7 Enterprise Edition, 64-bit (build 7600)
    System Name:                 SWEIGAND-14093
    Processor:                   Intel64 Family 6 Model 37 Stepping 5 GenuineIntel ~2527 Mhz
    BIOS Version:                04/12/12
    Windows Directory:           C:\Windows
    Locale:                      United States
    Time Zone:                   Pacific Standard Time
    Total Physical Memory:       4095 MB
    Available Physical Memory:   44 MB
    Total Virtual Memory:        5120 MB
    Available Virtual Memory:    1 MB
    Page File Space:             8384460 MB

Windows IP Configuration

        Host Name . . . . . . . . . . . . : SWEIGAND-14093
        Primary Dns Suffix  . . . . . . . : sv.us.sonicwall.com
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : sv.us.sonicwall.com
                                            us.sonicwall.com
                                            sonicwall.com

Ethernet adapter SonicWall VPN Connection:
        Driver Description. . . . . . . . : SonicWall Virtual NIC
        Driver Manufacturer . . . . . . . : SonicWall, Inc.
        Driver Version. . . . . . . . . . : 10.1.0.40
        Driver Image Path . . . . . . . . : system32\DRIVERS\swvnic.sys

        Index . . . . . . . . . . . . . . : 0x00000020
        Connection-specific DNS Suffix  . : sv.us.sonicwall.com
        Description . . . . . . . . . . . : SonicWall Virtual NIC
        Physical Address. . . . . . . . . : 00-60-73-D5-4C-7D
        MTU . . . . . . . . . . . . . . . : 1418
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : No
        IP Address. . . . . . . . . . . . : 10.50.12.53
```

- To save the report to a text file, click **Save As**.
- To send the report via email, click **Send**.
- To close the report window without taking any action, click **Don’t Send**.

Accessing SonicWall Global VPN Client Technical Support

SonicWall’s comprehensive support services protect your network security investment and offer the support you need — when you need it. SonicWall Global VPN Client support is included as part of the support program of your SonicWall network security appliance.

- Selecting **Help > Technical Support** accesses the SonicWall Support site at:

  https://support.sonicwall.com

- The SonicWall Support site offer a full range of support services including extensive online resources and information on SonicWall’s enhanced support programs. You can purchase/activate SonicWall Support Services through your MySonicWall account at:

  http://www.mysonicwall.com

Viewing Help Topics

Selecting **Help > Help Topics** displays the 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 Global VPN Client

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

ⓘ **NOTE:** You must exit the SonicWall Global VPN Client before uninstalling the program.

To uninstall the SonicWall Global VPN Client:

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

9

Configuring SonicWall Appliances for Global VPN Clients

About GroupVPN Policies

The SonicOS GroupVPN policy provides the automatic provisioning of SonicWall Global VPN Client from the SonicWall security appliance. The GroupVPN policy is only available for SonicWall Global VPN Clients. SonicOS GroupVPN supports two IPsec keying modes:

- **IKE using shared secret**
- **IKE using 3rd Party Certificates**

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

> **NOTE:** For information on configuring GroupVPN on the SonicWall appliance to support SonicWall Global VPN Client, refer to the *SonicOS Administration Guide*. All SonicWall product documentation is available from the Support page at:
>
> https://support.sonicwall.com

Global VPN Client Licenses

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

Group VPN Connections Supported by Platform

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

Activating Your Global VPN Client

To activate and download your SonicWall Global VPN Client software, you must have a valid MySonicWall account and your SonicWall appliance must be registered to your account. If you do not have a MySonicWall account, or if you have not registered your appliance 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 account.
2. Select the registered SonicWall network 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 is displayed.

ⓘ **TIP:** For future reference, record the Serial Number of the SonicWall appliance. Your license activation is now complete.

Downloading Global VPN Client Software and Documentation

1. In a web browser, log into your MySonicWall account.
2. In the My Products page, click the name of your SonicWall appliance on which the Global VPN Client license is activated.
3. Select **Software Download**. If this service is not already activated, click on **Agree** to activate it.
4. Download the SonicWall Global VPN Client software and documentation.

Using the default.rcf File

About the default.rcf File

The **default.rcf** file allows you to create and distribute preconfigured VPN connections for SonicWall Global VPN Client. You can distribute the **default.rcf** file with the Global VPN Client software to automatically create preconfigured VPN connections for streamlined deployment.

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

How Global VPN Client Uses default.rcf

When the Global VPN Client starts up, the program always looks for the configuration file, **Connections.rcf**, in the `C:\Users\<user>\AppData\Roaming\SonicWall\Global VPN Client\` directory. If this file does not exist, the Global VPN Client looks for the **default.rcf** file in the program install directory, `C:\Program Files\SonicWall\Global VPN Client\`.

The Global VPN Client reads the **default.rcf** file, if it exists, and creates the configuration file, **Connections.rcf**, in the `C:\Users\<user>\AppData\Roaming\SonicWall\Global VPN Client\` directory. The **Connections.rcf** file contains all the VPN connection configuration information for the SonicWall Global VPN Client, with sensitive data (user names and passwords) encrypted.

Deploying the default.rcf File

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

- Include the **default.rcf** file along with the installer software **GVCInstall*XX*.MSI**, where ***XX*** is either **32**, for 32-bit Windows platforms or **64,** for 64-bit Windows platforms, before running the installer. See Including the default.rcf File with the MSI Installer on page 53.
- Add the **default.rcf** file to the program install directory before opening the SonicWall Global VPN Client application for the first time. See Adding the default.rcf File to the Installation Directory on page 54.
- If the **Connections.rcf** configuration file exists in the user's configuration file folder, replace it using settings from the **default.rcf** file in the program install directory. See Replacing an Existing .rcf File with the default.rcf File on page 54.

Including the default.rcf File with the MSI Installer

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

To get the same profile (from default.rcf) to all the users during installation:

1. Export the WAN groupVPN configuration from your SonicWall network security appliance (the VPN Gateway) or create **default.rcf** if you want multiple connections.
2. Rename the exported configuration file to **default.rcf**.
3. Extract the **GVCInstall*XX*.MSI** from **GVCSetup*XX*.exe** (where ***XX*** is either **32** for 32-bit Windows platforms or **64** for 64-bit Windows platforms) by typing this command line:

   ```
   GVCSetupXX.exe /T:<Path where you want MSI to be extracted> /C
   ```
4. Copy the **default.rcf** file to same directory where you have the **GVCInstall*XX*.MSI** (installer file).
5. Launch the installer (**GVCInstallXX.MSI**). The installation process copies **default.rcf** to the GVC Install directory.
6. After the install is complete and you start the Global VPN Client, it reads the **default.rcf** and creates the defined connections from it.

△ CAUTION: **The default.rcf file must be included in the Global VPN Client installation directory** `C:\Program Files\SonicWall\Global VPN Client\` **for the program to write the Connections.rcf file based on the settings defined in the default.rcf file.**

Adding the default.rcf File to the Installation Directory

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

When the user launches the Global VPN Client program, the configuration file **Global VPN Client.rcf** is created in the `C:\Users\<user>\AppData\Roaming\SonicWall\Global VPN Client\` directory based on the **default.rcf** file settings.

Replacing an Existing .rcf File with the default.rcf File

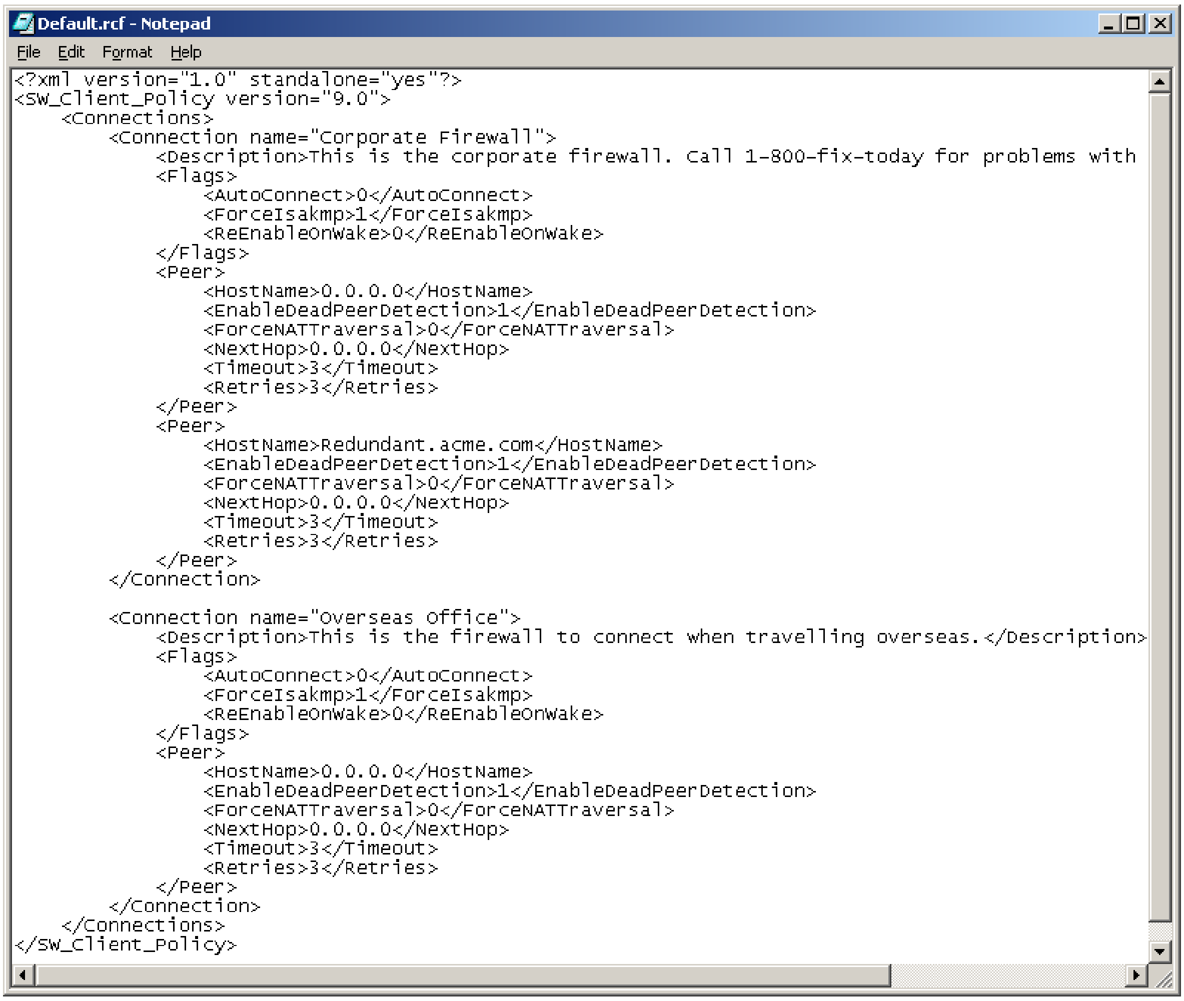
If the configuration file, **Connections.rcf**, already exists in the `C:\Users\<user>\AppData\Roaming\SonicWall\Global VPN Client\` directory, the user can remove this file and add the **default.rcf** file to the Global VPN Client installation directory `C:\Program Files\SonicWall\Global VPN Client\`. The next time the user launches the Global VPN Client, the **Connections.rcf** file is created in the `C:\Users\<user>\AppData\Roaming\SonicWall\Global VPN Client\` directory based on the **default.rcf** file settings.

△ **CAUTION: The Connections.rcf file is user-specific and in most cases will not work for another user running the SonicWall Global VPN Client, even on the same machine.**

△ **CAUTION: Removing an existing Connections.rcf file removes the VPN connections created in the Global VPN Client. These VPN connections can be added again from the Global VPN Client into the new Connections.rcf file.**

Creating the default.rcf File

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



```
<?xml version="1.0" standalone="yes"?>
<SW_Client_Policy version="9.0">
    <Connections>
        <Connection name="Corporate Firewall">
            <Description>This is the corporate firewall. Call 1-800-fix-today for problems with
            <Flags>
                <AutoConnect>0</AutoConnect>
                <ForceIsakmp>1</ForceIsakmp>
                <ReEnableOnWake>0</ReEnableOnWake>
            </Flags>
            <Peer>
                <HostName>0.0.0.0</HostName>
                <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
                <ForceNATTraversal>0</ForceNATTraversal>
                <NextHop>0.0.0.0</NextHop>
                <Timeout>3</Timeout>
                <Retries>3</Retries>
            </Peer>
            <Peer>
                <HostName>Redundant.acme.com</HostName>
                <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
                <ForceNATTraversal>0</ForceNATTraversal>
                <NextHop>0.0.0.0</NextHop>
                <Timeout>3</Timeout>
                <Retries>3</Retries>
            </Peer>
        </Connection>

        <Connection name="Overseas Office">
            <Description>This is the firewall to connect when travelling overseas.</Description>
            <Flags>
                <AutoConnect>0</AutoConnect>
                <ForceIsakmp>1</ForceIsakmp>
                <ReEnableOnWake>0</ReEnableOnWake>
            </Flags>
            <Peer>
                <HostName>0.0.0.0</HostName>
                <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
                <ForceNATTraversal>0</ForceNATTraversal>
                <NextHop>0.0.0.0</NextHop>
                <Timeout>3</Timeout>
                <Retries>3</Retries>
            </Peer>
        </Connection>
    </Connections>
</SW_Client_Policy>
```

default.rcf File Tag Descriptions

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

<SW_Client_Policy version =”9.0”>

> **<Connections>** – Defines the connection profiles in the default.rcf configuration file. There is no hard limit defined on the number of connection profiles allowed.
>
> > **<Connection name =** *connection name***>** – Provides a name for the VPN connection that appears in the Global VPN Client window.
> >
> > > **<Description>** *description text***</Description>** – Provides a description for each connection profile that appears when the user moves the mouse pointer over the VPN Policy in the Global VPN Client window. The maximum number of characters for the `<Description>` tag is 1023.
> > >
> > > **`<Flags>`**

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

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

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

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

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

</Flags>

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

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

<EnableDeadPeerDetection>*Off=0/On=1***</EnableDeadPeerDetection> –** Enables detection if the Peer stops responding to traffic. This sends Vendor ID to the SonicWall appliance during IKE negotiation to enable Dead peer-detection heart beat traffic.

NOTE: NAT Traversal - There is a drop down selection list containing the following three items:

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

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

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

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

<NextHop>*IP Address***</NextHop>** – The IP Address of the next hop for this connection.

IMPORTANT: `<NextHop>` is ONLY used if there is a need to use a next hop that is different from the default gateway.

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

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

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

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

<DPDInterval>*[***[3]***-30]***</DPDInterval>** – Specifies the duration of time (in seconds) to wait before declaring a peer as dead. The allowed values for the interval times are **3**, 5, 10, 15, 20, 25 and 30 seconds.

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

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

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

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

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

</SW_Client_Policy>

Sample default.rcf File

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

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

```
<?xml version="1.0" standalone="yes"?>

<SW_Client_Policy version="9.0">

    <Connections>

        <Connection name="Corporate Firewall">

            <Description>This is the corporate firewall. Call 1-800-fix-today for connection
            problems.</Description>

            <Flags>

                <AutoConnect>0</AutoConnect>

                <ForceIsakmp>1</ForceIsakmp>

                <ReEnableOnWake>0</ReEnableOnWake>

                <ReconnectOnError>1</ReconnectOnError>

                <ExecuteLogonScript>0</ExecuteLogonScript>

            </Flags>

            <Peer>

                <HostName>CorporateFW</HostName>
        <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
        <ForceNATTraversal>0</ForceNATTraversal>
        <DisableNATTraversal>0</DisableNATTraversal>
        <NextHop>0.0.0.0</NextHop>
        <Timeout>3</Timeout>
        <Retries>3</Retries>
        <UseDefaultGWAsPeerIP>0</UseDefaultGWAsPeerIP>
        <InterfaceSelection>0</InterfaceSelection>
        <WaitForSourceIP>0</WaitForSourceIP>
        <DPDInterval>3</DPDInterval>
        <DPDAttempts>3</DPDAttempts>
        <DPDAlwaysSend>0</DPDAlwaysSend>
    </Peer>
    <Peer>
        <HostName>1.2.3.4</HostName>
        <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
        <ForceNATTraversal>0</ForceNATTraversal>
        <DisableNATTraversal>0</DisableNATTraversal>
        <NextHop>0.0.0.0</NextHop>
        <Timeout>3</Timeout>
        <Retries>3</Retries>
        <UseDefaultGWAsPeerIP>0</UseDefaultGWAsPeerIP>
        <InterfaceSelection>0</InterfaceSelection>
        <WaitForSourceIP>0</WaitForSourceIP>
        <DPDInterval>3</DPDInterval>
        <DPDAttempts>3</DPDAttempts>
        <DPDAlwaysSend>0</DPDAlwaysSend>
    </Peer>
</Connection>
<Connection name="Overseas Gateway">
    <Description>This is the firewall to connect when traveling overseas.</Description>
    <Flags>
        <AutoConnect>0</AutoConnect>
        <ForceIsakmp>1</ForceIsakmp>
        <ReEnableOnWake>0</ReEnableOnWake>
        <ReconnectOnError>1</ReconnectOnError>
        <ExecuteLogonScript>0</ExecuteLogonScript>
```

```
                </Flags>
                <Peer>
                    <HostName>&lt;Default Gateway&gt;</HostName>
                    <EnableDeadPeerDetection>1</EnableDeadPeerDetection>
                    <ForceNATTraversal>0</ForceNATTraversal>
                    <DisableNATTraversal>0</DisableNATTraversal>
                    <NextHop>0.0.0.0</NextHop>
                    <Timeout>3</Timeout>
                    <Retries>3</Retries>
                    <UseDefaultGWAsPeerIP>1</UseDefaultGWAsPeerIP>
                    <InterfaceSelection>0</InterfaceSelection>
                    <WaitForSourceIP>0</WaitForSourceIP>
                    <DPDInterval>3</DPDInterval>
                    <DPDAttempts>3</DPDAttempts>
                    <DPDAlwaysSend>0</DPDAlwaysSend>
                </Peer>
            </Connection>
        </Connections>
</SW_Client_Policy>
```

Troubleshooting the default.rcf File

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

B

Using the Global VPN Client CLI

About the Global VPN Client CLI

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

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

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

Command Line Options

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

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

Command Line Examples

- **<*path*>\swgvpnclient** - runs/starts application. If application is already running, it does not create another instance.
- **<*path*>\swgvpnclient /E <*connection name*> /U <*username*> and /P <*password*>** - runs/starts the application and enables the named connection and use the `<username>` and `<password>` for user

authentication. If you do not include a username and password. the Global VPN Client presents a dialog asking for the information in order to continue.

- **<*path*>\swgvpnclient /A <*path\filename*> -** runs/starts the application and enables auto logging of all events to a log file. If the filename is not specified, then the log file is created with the default name `<gvcauto.log>`. If you want to save the autolog for each Global VPN Client session, you can use the filename option and specify a different filename each time the application is started. If the path is not specified, this file is created in the same directory where the Global VPN Client application is started.

Log Viewer Messages

This section provides information about SonicWall Global VPN Client log messages. The following tables list the **Error**, **Info**, and **Warning** messages that can appear in the Global VPN Client Log Viewer:

- Error Messages on page 62
- Info Messages on page 67
- Warning Messages on page 71

Error Messages

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

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

Type	Message
ERROR	Failed to construct IPSEC nonce payload.
ERROR	Failed to construct IPSEC SA payload.
ERROR	Failed to construct ISAKMP blank hash payload.
ERROR	Failed to construct ISAKMP delete hash payload.
ERROR	Failed to construct ISAKMP DPD notify payload.
ERROR	Failed to construct ISAKMP ID payload.
ERROR	Failed to construct ISAKMP info hash payload.
ERROR	Failed to construct ISAKMP key exchange payload.
ERROR	Failed to construct ISAKMP nonce payload.
ERROR	Failed to construct ISAKMP notify payload.
ERROR	Failed to construct ISAKMP packet header.
ERROR	Failed to construct ISAKMP phase 1 delete payload.
ERROR	Failed to construct ISAKMP SA payload.
ERROR	Failed to construct ISAKMP vendor ID payload (ID =).
ERROR	Failed to construct mode config hash payload.
ERROR	Failed to construct NAT discovery payload.
ERROR	Failed to construct PFS key exchange payload.
ERROR	Failed to construct policy provisioning payload.
ERROR	Failed to construct quick mode hash payload.
ERROR	Failed to construct quick mode packet.
ERROR	Failed to construct responder lifetime payload.
ERROR	Failed to construct RSA signature.
ERROR	Failed to construct signature payload.
ERROR	Failed to construct source proxy ID payload.
ERROR	Failed to construct XAuth payload.
ERROR	Failed to convert the peer name to an IP address.
ERROR	Failed to create a new connection entry: an entry already exists with ID.
ERROR	Failed to create connection entry with message ID.
ERROR	Failed to decrypt buffer.
ERROR	Failed to decrypt mode config payload.
ERROR	Failed to decrypt notify payload.
ERROR	Failed to decrypt packet.
ERROR	Failed to decrypt quick mode payload.
ERROR	Failed to encrypt mode config payload.
ERROR	Failed to encrypt notify payload.
ERROR	Failed to encrypt packet.
ERROR	Failed to encrypt quick mode payload.
ERROR	Failed to expand packet to size bytes.
ERROR	Failed to find an SA list for PROTO_IPSEC_AH.
ERROR	Failed to find an SA list for PROTO_IPSEC_ESP.
ERROR	Failed to find an SA list given the protocol.

Type	Message
ERROR	Failed to find certificate with ID.
ERROR	Failed to find connection entry for message ID.
ERROR	Failed to find exit interface to reach.
ERROR	Failed to find MAC address in the system interfaces table.
ERROR	Failed to find matching SA list.
ERROR	Failed to find message ID and matching cookies in the connection entry list.
ERROR	Failed to find message ID in the connection entry list.
ERROR	Failed to find message ID in the SA list.
ERROR	Failed to find OAKLEY group specified in the SA payload.
ERROR	Failed to find private key for certificate with ID.
ERROR	Failed to find protocol ID in the SA list.
ERROR	Failed to find route to reach.
ERROR	Failed to find sequence number.
ERROR	Failed to find source IP address to reach.
ERROR	Failed to flush the system ARP cache.
ERROR	Failed to generate Diffie-Hellman parameters.
ERROR	Failed to generate quick mode initiator key.
ERROR	Failed to generate quick mode responder key.
ERROR	Failed to generate SKEYID.
ERROR	Failed to get the size of the system interfaces table.
ERROR	Failed to get the size of the system IP address table.
ERROR	Failed to get the system interface table.
ERROR	Failed to get the system IP address table.
ERROR	Failed to get transforms from SA list.
ERROR	Failed to match initiator cookie.
ERROR	Failed to match responder cookie.
ERROR	Failed to parse certificate data.
ERROR	Failed to parse configuration file.
ERROR	Failed to read the size of an incoming ISAKMP packet.
ERROR	Failed to re-allocate bytes.
ERROR	Failed to receive an incoming ISAKMP packet.
ERROR	Failed to receive an incoming ISAKMP packet. The length is incorrect.
ERROR	Failed to send an outgoing ISAKMP packet.
ERROR	Failed to set policy configuration attributes into payload.
ERROR	Failed to set proposals into phase 1 SA payload.
ERROR	Failed to set proposals into phase 2 SA payload.
ERROR	Failed to set responder lifetype attributes.
ERROR	Failed to set the ESP attributes from the SA payload into the SA.
ERROR	Failed to set the IPSEC AH attributes into the phase 2 SA.
ERROR	Failed to set the IPSEC ESP attributes into the phase 2 SA.
ERROR	Failed to set the OAKLEY attributes into the phase 1 SA.

Type	Message
ERROR	Failed to set vendor ID into packet payload.
ERROR	Failed to set XAuth attributes into payload.
ERROR	Failed to sign hash.
ERROR	Failed to verify certificate signature.
ERROR	Failed to verify informational message hash payload.
ERROR	Failed to verify mode config message hash payload.
ERROR	Hash algorithm is not supported.
ERROR	Hash Payload does not match.
ERROR	Hash size invalid:
ERROR	Header invalid (verified)!
ERROR	Invalid certificate: ASN sequence is not correct.
ERROR	Invalid certificate: payload length is too small.
ERROR	Invalid hash payload.
ERROR	Invalid payload. Possible overrun attack!
ERROR	Invalid SA state:
ERROR	Invalid signature payload.
ERROR	Invalid SPI size.
ERROR	is not a supported Diffie-Hellman group type.
ERROR	is not a supported DOI.
ERROR	is not a supported exchange type.
ERROR	is not a supported ID payload type.
ERROR	is not a supported IPSEC protocol.
ERROR	is not a supported notify message type.
ERROR	is not a supported payload type.
ERROR	is not a supported policy configuration attribute type.
ERROR	is not a supported policy configuration message type.
ERROR	is not a supported proxy ID payload type.
ERROR	is not a supported XAuth attribute type.
ERROR	is not a valid quick mode state.
ERROR	is not a valid XAuth message type.
ERROR	is not a valid XAuth status.
ERROR	ISAKMP SA delete msg for a different SA!
ERROR	No certificate for CERT authentication.
ERROR	No entry in the system IP address table was found with index.
ERROR	No KE payload while PFS configured mess_id.
ERROR	Out of memory.
ERROR	Phase 1 authentication algorithm is not supported.
ERROR	Phase 1 encryption algorithm is not supported.
ERROR	Protocol ID has already been added to the SA list.
ERROR	Protocol mismatch: expected PROTO_IPSEC_AH but got.
ERROR	Protocol mismatch: expected PROTO_IPSEC_ESP but got.

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

Info Messages

Type	Message
INFO	"The connection """" has been disabled."
INFO	A certificate is needed to complete phase 1.
INFO	A phase 2 SA can not be established with until a phase 1 SA is established.
INFO	A pre-shared key is needed to complete phase 1.
INFO	AG failed. SA state unknown. Peer:
INFO	An incoming ISAKMP packet from was ignored.
INFO	DSS g value:
INFO	DSS p value:
INFO	DSS q value:
INFO	Event publisher deregistered.
INFO	Event publisher registered for.
INFO	Failed to negotiate configuration information with.
INFO	Found CA certificate in CA certificate list.

Type	Message
INFO	Ignoring unsupported payload.
INFO	Ignoring unsupported vendor ID.
INFO	ISAKMP phase 1 proposal is not acceptable.
INFO	ISAKMP phase 2 proposal is not acceptable.
INFO	MM failed. Payload processing failed. OAK_MM_KEY_EXCH. Peer:
INFO	MM failed. Payload processing failed: OAK_MM_NO_STATE. Peer:
INFO	MM failed. Payload processing failed: OAK_MM_SA_SETUP. Peer:
INFO	MM failed. SA state not matching mask process auth. Peer:
INFO	MM failed. SA state not matching mask process key. Peer:
INFO	MM failed. SA state not matching mask process sa. Peer:
INFO	MM failed. SA state unknown. Peer:
INFO	NAT Detected: Local host is behind a NAT device.
INFO	NAT Detected: Peer is behind a NAT device.
INFO	peer certificate missing key value.
INFO	Phase 1 has completed.
INFO	Phase 1 SA lifetime set to.
INFO	Phase 2 negotiation has failed.
INFO	Phase 2 SA lifetime set to.
INFO	Phase 2 with has completed.
INFO	Proposal not acceptable: not authentication algorithm specified.
INFO	Proposal not acceptable: not Diffie-Hellman group specified.
INFO	Proposal not acceptable: not encryption algorithm specified.
INFO	Proposal not acceptable: not hash algorithm specified.
INFO	Proposal not acceptable: proposal not found in list.
INFO	QM failed. Load SA failed. Peer:
INFO	Reading configuration file.
INFO	Ready to negotiate phase 2 with.
INFO	Received address notification notify.
INFO	Received attributes not supported notify.
INFO	Received authentication failed notify.
INFO	Received bad syntax notify.
INFO	Received certificate unavailable notify.
INFO	Received dead peer detection acknowledgement.
INFO	Received dead peer detection request.
INFO	Received initial contact notify.
INFO	Received invalid certificate authentication notify.
INFO	Received invalid certificate encoding notify.
INFO	Received invalid certificate notify.
INFO	Received invalid certificate request syntax notify.
INFO	Received invalid cookie notify.
INFO	Received invalid exchange type notify.

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

Type	Message
INFO	Signature Verified!
INFO	SonicWall Global VPN Client version.
INFO	SonicWall VPN Client.
INFO	Starting aggressive mode phase 1 exchange.
INFO	Starting authentication negotiation.
INFO	Starting configuration negotiation.
INFO	Starting ISAKMP phase 1 negotiation.
INFO	Starting ISAKMP phase 2 negotiation with.
INFO	Starting main mode phase 1 exchange.
INFO	Starting quick mode phase 2 exchange.
INFO	The configuration for the connection has been updated.
INFO	The configuration for the connection is up to date.
INFO	The configuration has been updated and must be reloaded.
INFO	The connection has entered an unknown state.
INFO	The connection is idle.
INFO	The hard lifetime has expired for phase 1.
INFO	The hard lifetime has expired for phase 2 with.
INFO	The IP address for the virtual interface has been released.
INFO	The IP address for the virtual interface has changed to.
INFO	The ISAKMP port (500) is already in use. Port will be used as the ISAKMP source port.
INFO	The peer is not responding to phase 2 ISAKMP requests to.
INFO	The phase 1 SA has been deleted.
INFO	The phase 1 SA has died.
INFO	The phase 2 SA has been deleted.
INFO	The phase 2 SA has died.
INFO	The SA lifetime for phase 1 is seconds.
INFO	The SA lifetime for phase 2 is seconds.
INFO	The soft lifetime has expired for phase 1.
INFO	The soft lifetime has expired for phase 2 with.
INFO	The system ARP cache has been flushed.
INFO	Unable to encrypt payload!
INFO	User authentication has failed.
INFO	User authentication has succeeded.
INFO	User authentication information is needed to complete the connection.
INFO	XAuth has requested a username but one has not yet been specified.

Warning Messages

Type	Message
WARNING	A password must be entered.
WARNING	AG failed. SA state not matching mask process auth. Peer:
WARNING	AG failed. SA state not matching mask process key. Peer:
WARNING	AG failed. State OAK_AG_INIT_EXCH is invalid when responder. Peer:
WARNING	AG failed. State OAK_AG_NO_STATE is invalid when initiator. Peer:
WARNING	Failed to process aggressive mode packet.
WARNING	Failed to process final quick mode packet.
WARNING	Failed to process informational exchange packet.
WARNING	Failed to process main mode packet.
WARNING	Failed to process mode configuration packet.
WARNING	Failed to process packet payloads.
WARNING	Failed to process payload.
WARNING	Failed to process quick mode packet.
WARNING	Ignoring AUTH message when aggressive mode already complete. Peer:
WARNING	Invalid DOI in delete message:
WARNING	Invalid IPSEC SA delete message.
WARNING	Invalid ISAKMP SA delete message.
WARNING	is not a supported OAKLEY attribute class.
WARNING	Protocol ID is not supported in SA payloads.
WARNING	Received an encrypted packet when not crypto active!
WARNING	Received an unencrypted packet when crypto active!
WARNING	Responder lifetime protocol is not supported.
WARNING	The password is incorrect. Please re-enter the password.
WARNING	The pre-shared key dialog was cancelled by the user. The connection will be disabled.
WARNING	The select certificate dialog was cancelled by the user. The connection will be disabled.
WARNING	The username/password dialog was cancelled by the user. The connection will be disabled.
WARNING	Unable to decrypt payload!

SonicWall End User Product Agreement

Revised 10 February 2017

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA.ASPX TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

This SonicWall End User Product Agreement (the "***Agreement***") is made between you, the Customer ("**Customer**" or "**You**") and the Provider, as defined below.

1. **Definitions**. Capitalized terms not defined in context shall have the meanings assigned to them below:

(a) "**Affiliate**" means any legal entity controlling, controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists.

(b) "**Appliance**" means a computer hardware product upon which Software is pre-installed and delivered.

(c) "**Documentation**" means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.

(d) "**Maintenance Services**" means Provider's maintenance and support offering for the Products as identified in the Maintenance Services Section below.

(e) "**Partner**" means the reseller or distributor that is under contract with Provider or another Partner and is authorized via such contract to resell the Products and/or Maintenance Services.

(f) "**Provider**" means, (i) for the US, Europe, Middle East, Africa, Latin America, and Taiwan, SonicWall Inc., with its principal place of business located at 4 Polaris Way, Aliso Viejo, CA 92656 USA and (ii) for Asia (other than Taiwan) SonicWall International Ltd. City Gate Park Mahon, Cork, Ireland.

(g) "**Products**" means the Software and Appliance(s) provided to Customer under this Agreement.

(h) "**Software**" means the object code version of the software that is delivered on the Appliance and any other software that is later provided to Customer as well as any new versions and releases to such software that are made available to Customer pursuant to this Agreement, and all copies of the foregoing.

2. **Software License.**

(a) **General**. Subject to the terms of this Agreement, Provider grants to Customer, and Customer accepts from Provider, a non-exclusive, non-transferable (except as otherwise set forth herein) and non-sublicensable license to access and use the quantities of each item of Software purchased from Provider or a Partner within the parameters of the license type ("**License Type(s)**") described below in the quantities purchased ("License"). Except for MSP Licenses (as defined below), Customer shall only use the Software to support the internal business operations of itself and its worldwide Affiliates.

(b) **License Types.** The License Type for the Software initially delivered on the Appliance is "***per Appliance***". Software licensed per Appliance may be used only on the Appliance on which it is delivered, but without any other quantitative limitations. Software that is purchased on a subscription, or periodic basis is licensed by User or by Managed Node. A "**User**" is each person with a unique login identity to the Software. A "**Managed Node**" is any object managed by the Software including, but not limited to firewalls, devices, and other items sold by Provider.

(c) **Software as a Service.** When Customer purchases a right to access and use Software installed on equipment operated by Provider or its suppliers (the "***SaaS Software***"), (i) the License for such SaaS Software shall be granted for the duration of the term stated in the order (the "***SaaS Term***"), as such SaaS Term may be extended by automatic or agreed upon renewals, and (ii) the terms set forth in the SaaS Provisions Section of this Agreement shall apply to all access to and use of such Software. If any item of Software to be installed on Customer's equipment is provided in connection with SaaS Software, the License duration for such Software shall be for the corresponding SaaS Term, and Customer shall promptly install any updates to such Software as may be provided by Provider.

(d) **MSP License.**

"***Management Services***" include, without limitation, application, operating system, and database implementation, performance tuning, and maintenance services provided by Customer to its customers (each, a "***Client***") where Customer installs copies of the Software on its Clients' equipment or provides its Clients access to the Products. Customer shall be granted a License to use the Software and the associated Documentation to provide Management Services (the "***MSP License***"). Each MSP License is governed by the terms of this Agreement and any additional terms agreed to by the parties.

If the Product is to be used by Customer as a managed service provider, then Customer shall ensure that (i) Customer makes no representations or warranties related to the Products in excess of SonicWall's representations or warranties contained in this Agreement, (ii) each Client only uses the Products and Documentation as part of the Management Services provided to it by Customer, (iii) such use is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section of this Agreement, and (iv) each Client cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent. At the conclusion of any Management Services engagement with a Client, Customer shall promptly remove any Appliance and Software installed on its Client's computer equipment or require the Client to do the same. Customer agrees that it shall be jointly and severally liable to Provider for the acts and omissions of its Clients in connection with their use of the Software and Documentation and shall, at its expense, defend Provider against any action, suit, or claim brought against Provider by a Client in connection with or related to Customer's Management Services and pay any final judgments or settlements as well as Provider's expenses in connection with such action, suit, or claim.

(e) **Evaluation/Beta License.** If Software is obtained from Provider for evaluation purposes or in beta form, Customer shall be granted a License to use such Software and the associated Documentation solely for Customer's own non-production, internal evaluation purposes (an "***Evaluation License***"). Each Evaluation License shall be granted for an evaluation period of up to thirty (30) days beginning (i) five (5) days after the Appliance is shipped or (ii) from the date that access is granted to the beta Software or the SaaS Software, plus any extensions granted by Provider in writing (the "Evaluation Period"). There is no fee for an Evaluation License during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Beta Software licensed hereunder may include pre-release features and capabilities which may not be available in SonicWall's generally available commercial versions of the Software. SonicWall retains the right during the term of the Evaluation License to modify, revise, or remove SonicWall beta software from Customer's premises. Customer acknowledges that SonicWall owns all modifications, derivative works, changes, expansions or improvements to beta software, as well as all reports, testing data or results, feedback, benchmarking or other analysis completed in whole or in part in conjunction with usage of beta software. NOTWITHSTANDING ANYTHING OTHERWISE SET FORTH IN THIS AGREEMENT, CUSTOMER UNDERSTANDS AND AGREES THAT EVALUATION AND BETA SOFTWARE IS PROVIDED "AS IS", WHERE IS, WITH ALL FAULTS AND THAT SONICWALL DOES NOT PROVIDE A WARRANTY OR MAINTENANCE SERVICES FOR EVALUATION OR BETA LICENSES, AND SONICWALL BEARS NO LIABILITY FOR

ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE (OR ATTEMPTED USE) OF THE EVALUATION OR BETA SOFTWARE THROUGH AND AFTER THE EVALUATION PERIOD AND HAS NO DUTY TO PROVIDE SUPPORT TO CUSTOMER FOR SUCH SOFTWARE. BETA SOFTWARE MAY CONTAIN DEFECTS AND A PRIMARY PURPOSE OF LICENSING THE BETA SOFTWARE IS TO OBTAIN FEEDBACK ON THE BETA SOFTWARE'S PERFORMANCE AND THE IDENTIFICATION OF DEFECTS. CUSTOMER IS ADVISED TO SAFEGUARD IMPORTANT DATA, TO USE CAUTION AND NOT TO RELY IN ANY WAY ON THE CORRECT FUNCTIONING OR PERFORMANCE OF THE BETA SOFTWARE AND/OR ACCOMPANYING MATERIALS.

(f) **Use by Third Parties.** Customer may allow its services vendors and contractors (each, a "**Third Party User**") to access and use the Products and Documentation provided to Customer hereunder solely for purposes of providing services to Customer, provided that Customer ensures that (i) the Third Party User's access to or use of the Products and Documentation is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section, (ii) the Third Party User cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent, and (iii) the Third Party Users promptly removes any Software installed on its computer equipment upon the completion of the Third Party's need to access or use the Products as permitted by this Section. Customer agrees that it shall be liable to Provider for those acts and omissions of its Third Party Users which, if done or not done by Customer, would be a breach of this Agreement.

3. **Restrictions**. Customer may not reverse engineer, decompile, disassemble, or attempt to discover or modify in any way the underlying source code of the Software, or any part thereof unless and to the extent (a) such restrictions are prohibited by applicable law and (b) Customer has requested interoperability information in writing from Provider and Provider has not provided such information in a timely manner. In addition, Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Products, Documentation or any part thereof, (ii) resell, sublicense or distribute the Products or Documentation, (iii) provide, make available to, or permit use of the Products, in whole or in part, by any third party (except as expressly set forth herein), (iv) use the Products or Documentation to create or enhance a competitive offering or for any other purpose which is competitive to Provider, (v) remove Software that was delivered on an Appliance from the Appliance on which it was delivered and load such Software onto a different appliance without Provider's prior written consent, or (vi) perform or fail to perform any other act which would result in a misappropriation or infringement of Provider's intellectual property rights in the Products or Documentation. Each permitted copy of the Software and Documentation made by Customer hereunder must contain all titles, trademarks, copyrights and restricted rights notices as in the original. Customer understands and agrees that the Products may work in conjunction with third party products and Customer agrees to be responsible for ensuring that it is properly licensed to use such third party products. Notwithstanding anything otherwise set forth in this Agreement, the terms and restrictions set forth herein shall not prevent or restrict Customer from exercising additional or different rights to any open source software that may be contained in or provided with the Products in accordance with the applicable open source software licenses which shall be either included with the Products or made available to Customer upon request. Customer may not use any license keys or other license access devices not provided by Provider, including but not limited to "pirate keys", to install or access the Software.

4. **Proprietary Rights.** Customer understands and agrees that (i) the Products are protected by copyright and other intellectual property laws and treaties, (ii) Provider, its Affiliates and/or its licensors own the copyright, and other intellectual property rights in the Products, (iii) the Software is licensed, and not sold, (iv) this Agreement does not grant Customer any rights to Provider's trademarks or service marks, and (v) Provider reserves any and all rights, implied or otherwise, which are not expressly granted to Customer in this Agreement.

5. **Title.** Provider, its Affiliates and/or its licensors own the title to all Software.

6. **Payment.** Customer agrees to pay to Provider (or, if applicable, the Partner) the fees specified in each order, including any applicable shipping fees. Customer will be invoiced promptly following delivery of the Products or prior to the commencement of any Renewal Maintenance Period and Customer shall make all payments due to Provider in full within thirty (30) days from the date of each invoice or such other period (if any) stated in an order. Provider reserves the right to charge Customer a late penalty of 1.5% per month (or the maximum rate permitted by law, whichever is the lesser) for any amounts payable to Provider by Customer that are not subject to a good faith dispute and that remain unpaid after the due date until such amount is paid.

7. **Taxes.** The fees stated in an order from Provider or a Partner may not include taxes. If Provider is required to pay sales, use, property, value-added or other taxes based on the Products or Maintenance Services provided under this Agreement or on Customer's use of Products or Maintenance Services, then such taxes shall be billed to and paid by Customer. This Section does not apply to taxes based on Provider's or a Partner's income.

8. **Termination.**

(a) This Agreement or the Licenses granted hereunder may be terminated (i) by mutual written agreement of Provider and Customer or (ii) by either party for a breach of this Agreement by the other party (or a Third Party User) that the breaching party fails to cure to the non-breaching party's reasonable satisfaction within thirty (30) days following its receipt of notice of the breach. Notwithstanding the foregoing, in the case of MSP Licenses, if Customer or its Client breaches this Agreement two (2) times in any twelve (12) consecutive month period, the breaching party shall not have a cure period for such breach and Provider may terminate this Agreement immediately upon providing written notice to the breaching party.

(b) Upon termination of this Agreement or expiration or termination of a License for any reason, all rights granted to Customer for the applicable Software shall immediately cease and Customer shall immediately: (i) cease using the applicable Software and Documentation, (ii) remove all copies, installations, and instances of the applicable Software from all Appliances, Customer computers and any other devices on which the Software was installed, and ensure that all applicable Third Party Users and Clients do the same, (iii) return the applicable Software to Provider together with all Documentation and other materials associated with the Software and all copies of any of the foregoing, or destroy such items, (iv) cease using the Maintenance Services associated with the applicable Software, (v) pay Provider or the applicable Partner all amounts due and payable up to the date of termination, and (vi) give Provider a written certification, within ten (10) days, that Customer, Third Party Users, and Clients, as applicable, have complied with all of the foregoing obligations.

(c) Any provision of this Agreement that requires or contemplates execution after (i) termination of this Agreement, (ii) a termination or expiration of a License, or (iii) the expiration of a SaaS Term, is enforceable against the other party and their respective successors and assignees notwithstanding such termination or expiration, including, without limitation, the Restrictions, Payment, Taxes, Termination, Survival, Warranty Disclaimer, Infringement Indemnity, Limitation of Liability, Confidential Information, Compliance Verification, and General Sections of this Agreement. Termination of this Agreement or a License shall be without prejudice to any other remedies that the terminating party or a Partner may have under law, subject to the limitations and exclusions set forth in this Agreement.

9. **Export.** Customer acknowledges that the Products and Maintenance Services are subject to the export control laws, rules, regulations, restrictions and national security controls of the United States and other applicable foreign agencies (the "Export Controls") and agrees to abide by the Export Controls. Customer hereby agrees to use the Products and Maintenance Services in accordance with the Export Controls, and shall not export, re-export, sell, lease or otherwise transfer the Products or any copy, portion or direct product of the foregoing in violation of the Export Controls. Customer is solely responsible for obtaining all necessary licenses or authorizations relating to the export, re-export, sale, lease or transfer of the Products and for ensuring compliance with the requirements of such licenses or authorizations. Customer hereby (i) represents that Customer, and if Customer is providing services under the MSP License herein each of its Clients, is not an entity or person to which shipment of Products, or provision of Maintenance Services, is prohibited by the Export Controls; and (ii) agrees that it shall not export, re-export or otherwise transfer the Products to (a) any country subject to a United States trade embargo, (b) a national or resident of any country subject to a United States trade embargo, (c) any person or entity to which shipment of Products is prohibited by the Export Controls, or (d) anyone who is engaged in activities related to the design, development, production, or use of nuclear materials, nuclear facilities, nuclear weapons, missiles or chemical or biological weapons. Customer shall, at its expense, defend Provider and its Affiliates from any third party claim or action arising out of any inaccurate representation made by Customer regarding the existence of an export license, Customer's failure to provide information to Provider to obtain an export license, or any allegation made against Provider due to Customer's violation or alleged violation of the Export Controls (an "Export Claim") and shall pay any judgments or settlements reached in connection with the Export Claim as well as Provider's costs of responding to the Export Claim.

10. **Maintenance Services.**

(a) **Description.** During any Maintenance Period, Provider shall:

(i) Make available to Customer new versions and releases of the Software, if and when Provider makes them generally available without charge as part of Maintenance Services.

(ii) Respond to communications from Customer that report Software failures not previously reported to Provider by Customer. Nothing in the foregoing shall operate to limit or restrict follow up communication by Customer regarding Software failures.

(iii) Respond to requests from Customer's technical coordinators for assistance with the operational/technical aspects of the Software unrelated to a Software failure. Provider shall have the right to limit such responses if Provider reasonably determines that the volume of such non-error related requests for assistance is excessive or overly repetitive in nature.

(iv) Provide access to Provider's software support web site at https://support.sonicwall.com (the "***Support Site***").

(v) For Customers that have purchased Maintenance Services continuously since the purchase of such License, provide the repair and return program described on the Support Site for the Appliance on which the Software is delivered.

Maintenance Services are available during regional business support hours ("Business Hours") as indicated on the Support Site, unless Customer has purchased 24x7 Support. The list of Software for which 24x7 Support is available and/or required is listed in the Global Support Guide on the Support Site.

The Maintenance Services for Software that Provider has obtained through an acquisition or merger may, for a period of time following the effective date of the acquisition or merger, be governed by terms other than those in this Section. The applicable different terms, if any, shall be stated on the Support Site.

(b) **Maintenance Period.** The first period for which Customer is entitled to receive Maintenance Services begins on the date of the registration of the Product at Provider's registration portal (the "Registration") and ends twelve (12) months thereafter (the "***Initial Maintenance Period***"). Following the Initial Maintenance Period, Maintenance Services for the Product(s) may then be renewed for additional terms of twelve (12) or more months (each, a "***Renewal Maintenance Period***") For purposes of this Agreement, the Initial Maintenance Period and each Renewal Maintenance Period shall be considered a "***Maintenance Period.***" For the avoidance of doubt, this Agreement shall apply to each Renewal Maintenance Period. Cancellation of Maintenance Services will not terminate Customer's rights to continue to otherwise use the Products. Maintenance fees shall be due in advance of each Renewal Maintenance Period and shall be subject to the payment requirements set forth in this Agreement. The procedure for reinstating Maintenance Services for the Products after it has lapsed is posted at https://support.sonicwall.com/essentials/support-guide. Maintenance Services are optional and only provided if purchased separately.

For SaaS Software, the Maintenance Period is equal to the duration of the applicable SaaS Term. For non-perpetual Licenses or for non-perpetual MSP Licenses, the Maintenance Period is equal to the duration of the License.

11. **Warranties and Remedies.**

(a) **Software Warranties.** Provider warrants that, during the applicable Warranty Period (as defined in subsection (c) below),

(i) the operation of the Software, as provided by Provider, will substantially conform to its Documentation (the "***Operational Warranty***");

(ii) the Software, as provided by Provider, will not contain any viruses, worms, Trojan Horses, or other malicious or destructive code designed by Provider to allow unauthorized intrusion upon, disabling of, or erasure of the Software, except that the Software may contain a key limiting its use to the scope of the License granted, and license keys issued by Provider for temporary use are time-sensitive (the "***Virus Warranty***");

(iii) it will make commercially reasonable efforts to make the SaaS Software available twenty-four hours a day, seven days a week except for scheduled maintenance, the installation of updates, those factors that are beyond the reasonable control of Provider, Customer's failure to meet any minimum system requirements communicated to Customer by Provider, and any breach of this Agreement by Customer that impacts the availability of the SaaS Software (the "***SaaS Availability Warranty***").

(b) **Appliance Warranties.** Provider warrants that, during the applicable Warranty Period, the Appliance will operate in a manner which allows the SNWL Software, respectively, to be used in substantial conformance with the Documentation (the ""***Appliance Warranty***",).

(c) **Warranty Periods.** The "***Warranty Period***" for each of the above warranties (except for E-class appliances which do not include a Software warranty, shall be as follows: (i) for the Operational Warranty as it applies to Software and the Virus Warranty, ninety (90) days following the initial Registration of the Software; (ii) for the Operational Warranty as it applies to SaaS Software and the SaaS Availability Warranty, the duration of the SaaS Term; and (iv) for the Appliance Warranty, one (1) year following the date the Appliance is registered with Provider.

(d) **Remedies.** Any breach of the foregoing warranties must be reported by Customer to Provider during the applicable Warranty Period. Customer's sole and exclusive remedy and Provider's sole obligation for any such breach shall be as follows:

(i) For a breach of the *Operational Warranty* that impacts the use of Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach within a reasonable time considering the severity of the error and its effect on Customer or, at Provider's option, refund the license fees paid for the nonconforming Software upon return of such Software to Provider and termination of the related License(s) hereunder.

(ii) For a breach of the *Operational Warranty* that impacts the use of SaaS Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach and provide a credit or refund of the fees allocable to the period during which the Software was not operating in substantial conformance with the applicable Documentation.

(iii) For a breach of the *Virus Warranty*, Provider shall replace the Software with a copy that is in conformance with the Virus Warranty.

(v) For a breach of the *SaaS Availability Warranty*, Provider shall provide a credit or refund of the fees allocable to the period during which the SaaS Software was not available for use.

(e) **Warranty Exclusions.** The warranties set forth in this Section shall not apply to any non-conformance (i) that Provider cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the applicable Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; or (iii) arising from the modification of the Product by anyone other than Provider.

(f) **Third Party Products.** Certain Software may contain features designed to interoperate with third-party products. If the third-party product is no longer made available by the applicable provider, Provider may discontinue the related product feature. Provider shall notify Customer of any such discontinuation, however Customer will not be entitled to any refund, credit or other compensation as a result of the discontinuation.

(g) **Warranty Disclaimer.** THE EXPRESS WARRANTIES AND REMEDIES SET FORTH IN THIS SECTION ARE THE ONLY WARRANTIES AND REMEDIES PROVIDED BY PROVIDER HEREUNDER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ALL OTHER WARRANTIES OR REMEDIES ARE EXCLUDED, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, AND ANY WARRANTIES ARISING FROM USAGE OF TRADE OR COURSE OF DEALING OR PERFORMANCE. PROVIDER DOES NOT WARRANT UNINTERRUPTED OR ERROR-FREE OPERATION OF THE PRODUCTS.

(h) **High-Risk Disclaimer.** CUSTOMER UNDERSTANDS AND AGREES THAT THE PRODUCTS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HIGH-RISK OR HAZARDOUS ENVIRONMENT, INCLUDING WITHOUT LIMITATION, THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION WHERE THE FAILURE OR MALFUNCTION OF ANY PRODUCT CAN REASONABLY BE EXPECTED TO RESULT IN DEATH, PERSONAL INJURY, SEVERE PROPERTY DAMAGE OR SEVERE ENVIRONMENTAL HARM (A "***HIGH RISK ENVIRONMENT***"). ACCORDINGLY, (I) CUSTOMER SHOULD NOT USE THE PRODUCTS IN A HIGH RISK ENVIRONMENT, (II) ANY USE OF THE PRODUCTS BY CUSTOMER IN A HIGH RISK ENVIRONMENT IS AT CUSTOMER'S OWN RISK, (III) PROVIDER, ITS AFFILIATES AND SUPPLIERS SHALL NOT BE LIABLE TO CUSTOMER IN ANY WAY FOR USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT, AND (IV) PROVIDER MAKES NO WARRANTIES OR ASSURANCES, EXPRESS OR IMPLIED, REGARDING USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT.

12. **Infringement Indemnity.** Provider shall indemnify Customer from and against any claim, suit, action, or proceeding brought against Customer by a third party to the extent it is based on an allegation that the Software directly infringes any patent, copyright, trademark, or other proprietary right enforceable in the country in which Provider has authorized Customer to use the Software, including, but not limited to the country to which the Software is delivered to Customer, or misappropriates a trade secret in such country (a "***Claim***"). Indemnification for a Claim shall consist of the following: Provider shall (a) defend or settle the

Claim at its own expense, (b) pay any judgments finally awarded against Customer under a Claim or any amounts assessed against Customer in any settlements of a Claim, and (c) reimburse Customer for the reasonable administrative costs or expenses, including without limitation reasonable attorneys' fees, it necessarily incurs in responding to the Claim. Provider's obligations under this *Infringement Indemnity* Section are conditioned upon Customer (i) giving prompt written notice of the Claim to Provider, (ii) permitting Provider to retain sole control of the investigation, defense or settlement of the Claim, and (iii) providing Provider with cooperation and assistance as Provider may reasonably request in connection with the Claim. Provider shall have no obligation hereunder to defend Customer against any Claim (a) resulting from use of the Software other than as authorized by this Agreement, (b) resulting from a modification of the Software other than by Provider, (c) based on Customer's use of any release of the Software after Provider recommends discontinuation because of possible or actual infringement and has provided a non-infringing version at no charge, or (d) to the extent the Claim arises from or is based on the use of the Software with other products, services, or data not supplied by Provider if the infringement would not have occurred but for such use. If, as a result of a Claim or an injunction, Customer must stop using any Software ("***Infringing Software***"), Provider shall at its expense and option either (1) obtain for Customer the right to continue using the Infringing Software, (2) replace the Infringing Software with a functionally equivalent non-infringing product, (3) modify the Infringing Software so that it is non-infringing, or (4) terminate the License for the Infringing Software and (A) for non-SaaS Software, accept the return of the Infringing Software and refund the license fee paid for the Infringing Software, pro-rated over a sixty (60) month period from the date of initial delivery of such Software, or (B) for SaaS Software, discontinue Customer's right to access and use the Infringing Software and refund the unused pro-rated portion of any license fees pre-paid by Customer for such Software. This Section states Provider's entire liability and its sole and exclusive indemnification obligations with respect to a Claim and Infringing Software.

13. **Limitation of Liability**. EXCEPT FOR (A) ANY BREACH OF THE *RESTRICTIONS* OR *CONFIDENTIAL INFORMATION* SECTIONS OF THIS AGREEMENT, (B) AMOUNTS CONTAINED IN JUDGMENTS OR SETTLEMENTS WHICH PROVIDER OR CUSTOMER IS LIABLE TO PAY TO A THIRD PARTY UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER IS LIABLE TO PAY ON BEHALF OF OR TO PROVIDER UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES SECTIONS* OF THIS AGREEMENT, OR (C) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, IN NO EVENT SHALL CUSTOMER OR ITS AFFILIATES, OR PROVIDER, ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR (X) ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND OR (Y) LOSS OF REVENUE, LOSS OF ACTUAL OR ANTICIPATED PROFITS, LOSS OF BUSINESS, LOSS OF CONTRACTS, LOSS OF GOODWILL OR REPUTATION, LOSS OF ANTICIPATED SAVINGS, LOSS OF, DAMAGE TO OR CORRUPTION OF DATA, HOWSOEVER ARISING, WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE OR IN THE CONTEMPLATION OF THE PARTIES AND WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE.

EXCEPT FOR (A) ANY BREACH OF THE *SOFTWARE LICENSE*, *RESTRICTIONS*, OR CONFIDENTIAL INFORMATION SECTIONS OF THIS AGREEMENT, OR ANY OTHER VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (B) PROVIDER'S EXPRESS OBLIGATIONS UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER'S EXPRESS OBLIGATIONS UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES* SECTIONS OF THIS AGREEMENT, (C) PROVIDER'S COSTS OF COLLECTING DELINQUENT AMOUNTS WHICH ARE NOT THE SUBJECT OF A GOOD FAITH DISPUTE; (D) A PREVAILING PARTY'S LEGAL FEES PURSUANT TO THE *LEGAL FEES* SECTION OF THIS AGREEMENT; OR (E) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY OF CUSTOMER AND ITS AFFILIATES, AND PROVIDER, ITS AFFILIATES AND SUPPLIERS, FOR DAMAGES UNDER THIS AGREEMENT, WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE, SHALL BE AN AMOUNT EQUAL TO (Y) THE GREATER OF THE FEES PAID AND/OR OWED (AS APPLICABLE) BY CUSTOMER OR ITS AFFILIATES FOR THE PRODUCTS THAT ARE THE SUBJECT OF THE BREACH OR FIVE HUNDRED DOLLARS ($500.00),EXCEPT FOR (Z) MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, FOR WHICH THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY SHALL BE THE GREATER OF THE AMOUNT PAID AND/OR OWED (AS APPLICABLE) FOR SUCH MAINTENANCE SERVICE OR PRODUCT DURING THE TWELVE (12) MONTHS PRECEDING THE BREACH OR FIVE HUNDRED DOLLARS ($500.00). THE PARTIES AGREE THAT THESE LIMITATIONS OF LIABILITY ARE AGREED ALLOCATIONS OF RISK CONSTITUTING IN PART THE CONSIDERATION FOR PROVIDER PROVIDING PRODUCTS AND SERVICES TO CUSTOMER, AND SUCH LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITIES OR FAILURES.

Provider's Affiliates and suppliers and Customer's Affiliates shall be beneficiaries of this Limitation of Liability Section and Customer's Clients and Third Party Users are entitled to the rights granted under the MSP License and Use by Third Parties Sections of this Agreement; otherwise, no third party beneficiaries exist under this Agreement. Provider expressly excludes any and all liability to Third Party Users, Clients and to any other third party.

14. **Confidential Information.**

(a) **Definition.** "***Confidential Information***" means information or materials disclosed by one party (the "***Disclosing Party***") to the other party (the "***Receiving Party***") that are not generally available to the public and which, due to their character and nature, a reasonable person under like circumstances would treat as confidential, including, without limitation, financial, marketing, and pricing information, trade secrets, know-how, proprietary tools, knowledge and methodologies, the Software (in source code and/or object code form), information or benchmark test results regarding the functionality and performance of the Software, any Software license keys provided to Customer, and the terms and conditions of this Agreement.

Confidential Information shall not include information or materials that (i) are generally known to the public, other than as a result of an unpermitted disclosure by the Receiving Party after the date that Customer accepts the Agreement (the "***Effective Date***"); (ii) were known to the Receiving Party without an obligation of confidentiality prior to receipt from the Disclosing Party; (iii) the Receiving Party lawfully received from a third party without that third party's breach of agreement or obligation of trust; (iv) are protected by Provider in accordance with its obligations under the Protected Data Section below, or (v) are or were independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information.

(b) **Obligations.** The Receiving Party shall (i) not disclose the Disclosing Party's Confidential Information to any third party, except as permitted in subsection (c) below and (ii) protect the Disclosing Party's Confidential Information from unauthorized use or disclosure by exercising at least the same degree of care it uses to protect its own similar information, but in no event less than a reasonable degree of care. The Receiving Party shall promptly notify the Disclosing Party of any known unauthorized use or disclosure of the Disclosing Party's Confidential Information and will cooperate with the Disclosing Party in any litigation brought by the Disclosing Party against third parties to protect its proprietary rights. For the avoidance of doubt, this Section shall apply to all disclosures of the parties' Confidential Information as of the Effective Date, whether or not specifically arising from a party's performance under this Agreement.

(c) **Permitted Disclosures.** Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent to any of its Affiliates, directors, officers, employees, consultants, contractors or representatives (collectively, the "***Representatives***"), but only to those Representatives that (i) have a "need to know" in order to carry out the purposes of this Agreement or to provide professional advice in connection with this Agreement, (ii) are legally bound to the Receiving Party to protect information such as the Confidential Information under terms at least as restrictive as those provided herein, and (iii) have been informed by the Receiving Party of the confidential nature of the Confidential Information and the requirements regarding restrictions on disclosure and use as set forth in this Section. The Receiving Party shall be liable to the Disclosing Party for the acts or omissions of any Representatives to which it discloses Confidential Information which, if done by the Receiving Party, would be a breach of this Agreement.

Additionally, it shall not be a breach of this Section for the Receiving Party to disclose the Disclosing Party's Confidential Information as may be required by operation of law or legal process, provided that the Receiving Party provides prior notice of such disclosure to the Disclosing Party unless expressly prohibited from doing so by a court, arbitration panel or other legal authority of competent jurisdiction.

15. **Protected Data.** For purposes of this Section, "***Protected Data***" means any information or data that is provided by Customer to Provider during this Agreement that alone or together with any other information relates to an identified or identifiable natural person or data considered to be personal data as defined under Privacy Laws, and "***Privacy Laws***" means any applicable law, statute, directive or regulation regarding privacy, data protection, information security obligations and/or the processing of Protected Data.

Except as permitted herein or to the extent required by Privacy Laws or legal process, Provider shall implement reasonable technical and organizational measures to prevent unauthorized disclosure of or access to Protected Data by third parties, and shall only store and process Protected Data as may be required to fulfill its obligations under this Agreement. If Provider complies with Customer's written instructions with respect to the Protected Data, Provider shall have no liability to Customer for any breach of this Section resulting from such compliance. Provider shall promptly notify Customer of any disclosure of or access to the Protected Data by a third party in breach of this Section and shall cooperate with Customer to reasonably remediate the effects of such disclosure or access. Provider further affirms to Customer that it has adequate agreements in place incorporating the EU standard contractual clauses for the transfer of Protected Data from the European Union ("EU") to a country outside the EU.

Customer hereby (i) represents that it has the right to send the Protected Data to Provider, (ii) consents for Provider to store and use the Protected Data worldwide for the sole purpose of performing its obligations under this Agreement, (iii) agrees that the Protected Data may be accessed and used by Provider and its Representatives worldwide as may be needed to support Provider's standard business operations, and (iv) agrees that Protected Data consisting of Customer contact information (e.g., email addresses, names) provided as part of Maintenance Services may be sent to Provider's third party service providers as part of Provider's services improvement processes.

16**. Compliance Verification.** Customer agrees to maintain and use systems and procedures to accurately track, document, and report its installations, acquisitions and usage of the Software. Such systems and procedures shall be sufficient to determine if Customer's deployment of the Software or, if applicable, use of the SaaS Software is within the quantities, terms, and maintenance releases to which it is entitled. Provider or its designated auditing agent shall have the right to audit Customer's deployment of the Software or, if applicable, use of the SaaS Software for compliance with the terms and conditions of this Agreement. Any such audits shall be scheduled at least ten (10) days in advance and shall be conducted during normal business hours at Customer's facilities. Customer shall provide its full cooperation and assistance with such audit and provide access to the applicable records and computers. Without limiting the generality of the foregoing, as part of the audit, Provider may request, and Customer agrees to provide, a written report, signed by an authorized representative, listing Customer's then current deployment of the Software and/or the number of individuals that have accessed and used SaaS Software. If Customer's deployment of the Software or, if applicable, use of the SaaS Software is found to be greater than its purchased entitlement to such Software, Customer will be invoiced for the over-deployed quantities at Provider's then current list price plus the applicable Maintenance Services and applicable over-deployment fees. All such amounts shall be payable in accordance with this Agreement. Additionally, if the unpaid fees exceed five percent (5%) of the fees paid for the applicable Software, then Customer shall also pay Provider's reasonable costs of conducting the audit. The requirements of this Section shall survive for two (2) years following the termination of the last License governed by this Agreement.

17. **SaaS Provisions.**

(a) **Data.** Customer may store data on the systems to which it is provided access in connection with its use of the SaaS Software (the "***SaaS Environment***"). Provider may periodically make back-up copies of Customer data, however, such back-ups are not intended to replace Customer's obligation to maintain regular data backups or redundant data archives. Customer is solely responsible for collecting, inputting and updating all Customer data stored in the SaaS Environment, and for ensuring that it does not (i) knowingly create and store data that actually or potentially infringes or misappropriates the copyright, trade secret, trademark or other intellectual property right of any third party, or (ii) use the SaaS Environment for purposes that would reasonably be seen as obscene, defamatory, harassing, offensive or malicious. Provider shall have the right to delete all Customer data stored in connection with the use of the SaaS Software thirty (30) days following any termination of this Agreement or any License to SaaS Software granted hereunder.

Customer represents and warrants that it has obtained all rights, permissions and consents necessary to use and transfer all Customer and/or third party data within and outside of the country in which Customer or the applicable Customer Affiliate is located (including providing adequate disclosures and obtaining legally sufficient consents from Customer's employees, customers, agents, and contractors). If Customer transmits data to a third-party website or other provider that is linked to or made accessible by the SaaS Software, Customer will be deemed to have given its consent to Provider enabling such transmission and Provider shall have no liability to Customer in connection with any claims by a third party in connection with such transmission.

(b) **Conduct.** In connection with the use of SaaS Software, Customer may not (i) attempt to use or gain unauthorized access to Provider's or to any third-party's networks or equipment; (ii) permit other individuals or entities to copy the SaaS Software; (iii) provide unauthorized access to or use of any SaaS Software or the associated access credentials; (iv) attempt to probe, scan or test the vulnerability of the SaaS Software, the SaaS Environment, or a system, account or network of Provider or any of Provider's customers or suppliers; (v) interfere or attempt to interfere with service to any user, host or network; (vi) engage in fraudulent, offensive or illegal activity of any nature or intentionally engage in any activity that infringes the intellectual property rights or privacy rights of any individual or third party; (vii) transmit unsolicited bulk or commercial messages; (viii) intentionally distribute worms, Trojan horses, viruses, corrupted files or any similar items; (ix) restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the SaaS Software (except for tools with safety and security functions); or (x) restrict, inhibit, interfere with or otherwise disrupt or cause a performance degradation to any Provider (or Provider supplier) facilities used to provide the SaaS Environment. Customer shall cooperate with Provider's reasonable investigation of SaaS Environment outages, security issues, and any suspected breach of this Section, and shall, at its expense, defend Provider and its Affiliates from any claim, suit, or action by a third party (a "***Third Party Claim***") alleging harm to such third party caused by Customer's breach of any of the provisions of this Section. Additionally, Customer shall pay any judgments or settlements reached in connection with the Third Party Claim as well as Provider's costs of responding to the Third Party Claim.

(c) **Suspension.** Provider may suspend Customer's use of SaaS Software (a) if so required by law enforcement or legal process, (b) in the event of an imminent security risk to Provider or its customers, or (c) if continued use would subject Provider to material liability. Provider shall make commercially reasonable efforts under the circumstances to provide prior notice to Customer of any such suspension.

18. **General.**

(a) **Governing Law and Venue.** This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the Santa Clara County, California. Each party hereby agrees to submit to the jurisdiction of such courts. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated.

(b) **Assignment.** Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement, the Licenses granted under this Agreement or any other rights, interest or obligations hereunder, whether voluntarily, by contract, by operation of law or by merger (whether that party is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of Provider. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void.

(c) **Severability.** If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible by law to effect the intent of the parties and the remaining provisions of this Agreement will remain in full force and effect. Notwithstanding the foregoing, the terms of this Agreement that limit, disclaim, or exclude warranties, remedies or damages are intended by the parties to be independent and remain in effect despite the failure or unenforceability of an agreed remedy. The parties have relied on the limitations and exclusions set forth in this Agreement in determining whether to enter into it.

(d) **Use by U.S. Government.** The Software is a "commercial item" under FAR 12.201. Consistent with FAR section 12.212 and DFARS section 227.7202, any use, modification, reproduction, release, performance, display, disclosure or distribution of the Software or Documentation by the U.S. government is prohibited except as expressly permitted by the terms of this Agreement. In addition, when Customer is a U.S. government entity, the language in Subsection (ii) of the *Infringement Indemnity* Section of this Agreement and the *Injunctive Relief* Section of this Agreement shall not be applicable.

(e) **Notices.** All notices provided hereunder shall be in writing and may be delivered by email, in the case of Provider to *legal@sonicwall.com* and in the case of Customer to the email address Provider has on file for Customer. All notices, requests, demands or communications shall be deemed effective upon delivery in accordance with this paragraph.

(f) **Disclosure of Customer Status.** Provider may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of Provider in its marketing communications.

(g) **Waiver.** Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

(h) **Injunctive Relief.** Each party acknowledges and agrees that in the event of a material breach of this Agreement, including but not limited to a breach of the *Software License*, *Restrictions* or *Confidential Information* Sections of this Agreement, the non-breaching party shall be entitled to seek immediate injunctive relief, without limiting its other rights and remedies.

(i**)** **Force Majeure.** Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures. For added certainty, this Section shall not operate to change, delete, or modify any of the parties' obligations under this Agreement (e.g., payment), but rather only to excuse a delay in the performance of such obligations.

(j) **Equal Opportunity.** Provider is a federal contractor and Affirmative Action employer (M/F/D/V) as required by the Equal Opportunity clause C.F.R. § 60-741.5(a).

(k) **Headings**. Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term "including" is used in this Agreement it will be construed in each case to mean "including, but not limited to."

(l) **Legal Fees.** If any legal action is brought to enforce any rights or obligations under this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fees, court costs and other collection expenses, in addition to any other relief it may be awarded.

(m) **Entire Agreement.** This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter thereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any proceeding that may involve the Agreement. Each party acknowledges that in entering into the Agreement it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in the Agreement. In those jurisdictions where an original (non-faxed, non-electronic, or non-scanned) copy of an agreement or an original (non-electronic) signature on agreements such as this Agreement is required by law or regulation, the parties hereby agree that, notwithstanding any such law or regulation, a faxed, electronic, or scanned copy of and a certified electronic signature on this Agreement shall be sufficient to create an enforceable and valid agreement. This Agreement, may only be modified or amended t by a writing executed by a duly authorized representative of each party. No other act, document, usage or custom shall be deemed to amend or modify this Agreement.

E

SonicWall Support

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

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

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

The Support Portal enables you to:

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

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

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

Index