



STONEGATE IPSEC VPN 5.3

VPN CLIENT USER'S GUIDE

VIRTUAL PRIVATE NETWORKS

STONESOFT

Secure Information Flow

Legal Information

End-User License Agreement

The use of the products described in these materials is subject to the then current end-user license agreement, which can be found at the Stonesoft website:

www.stonesoft.com/en/support/eula.html

Third Party Licenses

The StoneGate software includes several open source or third-party software packages. The appropriate software licensing information for those products at the Stonesoft website:

www.stonesoft.com/en/support/third_party_licenses.html

U.S. Government Acquisitions

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

Product Export Restrictions

The products described in this document are subject to export control under the laws of Finland and the European Council Regulation (EC) N:o 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology (as amended). Thus, the export of this Stonesoft software in any manner is restricted and requires a license by the relevant authorities.

General Terms and Conditions of Support and Maintenance Services

The support and maintenance services for the products described in these materials are provided pursuant to the general terms for support and maintenance services and the related service description, which can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/terms/

Replacement Service

The instructions for replacement service can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/return_material_authorization/

Hardware Warranty

The appliances described in these materials have a limited hardware warranty. The terms of the hardware warranty can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/warranty_service/

Trademarks and Patents

The products described in these materials are protected by one or more of the following European and US patents: European Patent Nos. 1065844, 1189410, 1231538, 1259028, 1271283, 1289183, 1289202, 1304849, 1313290, 1326393, 1379046, 1330095, 131711, 1317937 and 1443729 and US Patent Nos. 6,650,621; 6,856,621; 6,885,633; 6,912,200; 6,996,573; 7,099,284; 7,127,739; 7,130,266; 7,130,305; 7,146,421; 7,162,737; 7,234,166; 7,260,843; 7,280,540; 7,302,480; 7,386,525; 7,406,534; 7,461,401; 7,721,084; and 7,739,727 and may be protected by other EU, US, or other patents, or pending applications. Stonesoft, the Stonesoft logo and StoneGate, are all trademarks or registered trademarks of Stonesoft Corporation. All other trademarks or registered trademarks are property of their respective owners.

Disclaimer

Although every precaution has been taken to prepare these materials, THESE MATERIALS ARE PROVIDED "AS-IS" and Stonesoft makes no warranty to the correctness of information and assumes no responsibility for errors, omissions, or resulting damages from the use of the information contained herein. All IP addresses in these materials were chosen at random and are used for illustrative purposes only.

Copyright © 2011 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

TABLE OF CONTENTS

CHAPTER 1		
Introduction	5	Viewing a Configuration Downloaded From a Gateway 32
How to Use This Guide	6	
Typographical Conventions	6	CHAPTER 6
Contact Information	6	Managing Certificates 33
Technical Support	6	Overview to Managing Certificates 34
Your Comments and Queries	6	Using Internal Certificates 34
		Creating a Basic Certificate Request 34
CHAPTER 2		Importing a Signed Certificate 38
Installing and Upgrading the VPN Client	7	Using External Certificates 40
Installing the VPN Client	8	Importing a PKCS # 12 File 40
Upgrading the VPN Client	9	Importing Separate Certificate and Private Key Files 42
CHAPTER 3		Changing the Certificate Passphrase 44
Connecting to a New Gateway for the First Time 11		Viewing Details of Imported Certificates 45
Getting Started With Connecting to Gateways	12	Changing User ID Type of an Imported Certificate 46
Viewing a List of Configured Gateways	12	Deleting Imported Certificates 46
Connecting to a New Pre-Configured Gateway	13	
Adding New Gateways Manually	14	CHAPTER 7
Checking the Gateway's Certificate Fingerprint	16	Troubleshooting VPN Connections 47
CHAPTER 4		Solving Connectivity Problems 48
Using the VPN Client 17		Try Different Settings Automatically 48
Overview to the VPN Client	18	Enable Random Local VPN Ports 48
Connecting to Resources	19	If the Connectivity Problems Dialog Is Displayed 48
Connecting to a Gateway at Windows Logon	19	Changing the VPN Client's MTU 49
Connecting to a Gateway Manually	20	Changing the VPN Client's MAC Address 50
Switching to an Alternative End-Point	21	Collecting Diagnostics Information 51
Authenticating Yourself	21	Capturing Network Traffic 52
Selecting the Authentication Method	21	
Authenticating with a User Name and Password	22	
Authenticating with a Certificate	22	
Authenticating with a Smartcard	23	
Closing the VPN Connection	23	
Turning the VPN Client off	24	
Activating/Deactivating User Name Memory	25	
Activating/Deactivating Domain Logon	26	
Activating/Deactivating Random Local VPN Ports	27	
Activating/Deactivating Retry With Different Settings	28	
CHAPTER 5		
Monitoring VPN Connections 29		
Viewing the VPN Connection Status	30	
Viewing Details of an Active VPN Connection	31	

CHAPTER 1

INTRODUCTION

Welcome to the StoneGate IPsec VPN client. This chapter describes how to use this Guide and provides contact details for Stonesoft.

The following sections are included:

- ▶ [How to Use This Guide](#) (page 6)
- ▶ [Contact Information](#) (page 6)

How to Use This Guide

This *StoneGate IPsec VPN Client User's Guide* describes step-by-step the use of the StoneGate IPsec VPN client for the end-users. If you are a StoneGate administrator, see the *Online Help* of the Management Client and the *StoneGate IPsec VPN Client Administrator's Guide* for information on setting up access for VPN clients and configuring the VPN client.

Typographical Conventions

The following ways to highlight special text are used throughout the guide:

Table 1.1 Typographical Conventions

Formatting	Informative Uses
VPN client text	Interface elements (such as menu options) and any other interaction with the user interface are in bold-face .
<i>References, terms</i>	Cross-references and first use of acronyms and terms are in <i>italics</i> .
Command line	File names, directories, and text displayed on the screen are monospaced.
User input	Text you need to type is monospaced bold-face .



Note – Notes provide important information that may help you complete a task.

Contact Information

For street addresses, phone numbers, and general information about StoneGate and Stonesoft Corporation, visit our Web site at <http://www.stonesoft.com/>.

Technical Support

If you experience technical problems with the VPN client, contact the network administrator responsible for the StoneGate system. Stonesoft technical support is available for StoneGate administrators based on a valid support contract.

Your Comments and Queries

We want to make our products suit your needs as well as possible. We are always pleased to receive any suggestions you may have for improvements.

- To comment on software and hardware products, e-mail feedback@stonesoft.com.
- To comment on the documentation, e-mail documentation@stonesoft.com.
- For queries and comments regarding other matters, e-mail info@stonesoft.com.

CHAPTER 2

INSTALLING AND UPGRADING THE VPN CLIENT

This section explains how to install the StoneGate IPsec VPN client as a fresh installation or as an upgrade. If your StoneGate VPN client version is older than 4.2, you must uninstall the previous version before installing the new version.

The following sections are included:

- ▶ [Installing the VPN Client](#) (page 8)
- ▶ [Upgrading the VPN Client](#) (page 9)

Installing the VPN Client

This section explains how to install using the standard installer. However, you may not need to use this standard installer, because the administrator may have preconfigured the installation so that it does not require any input from you.

▼ To install the VPN client using the standard installer

1. Double-click the executable file your network administrator has supplied. The Installation Wizard starts and the Welcome page opens.



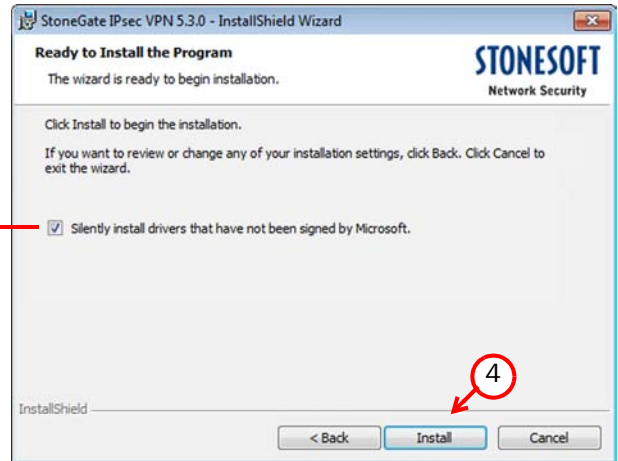
You can click **Cancel** at any time to stop the installation.

2. Click **Next** to continue.



3. Indicate that you accept the License Agreement and click **Next** to continue.

(In Windows XP) Leave **Silently install drivers that have not been signed by Microsoft** selected to avoid having to manually confirm the installation of the required drivers.



4. Click **Install** to start the installation.



Note – You may see one or more confirmation messages from Windows during the installation. You must allow the installation of all drivers and components for the VPN client to work correctly.

5. When the installation is finished, click **Finish** to close the wizard.

The installation is now complete. To complete the steps required to start using the VPN client, continue by [Connecting to a New Gateway for the First Time](#) (page 11).

Upgrading the VPN Client



Note – If the installed version of the StoneGate VPN client is earlier than 4.2, you must uninstall the previous version and perform a fresh installation of the new client.

▼ To upgrade StoneGate IPsec VPN client

1. Double-click the executable file your network administrator has supplied. A confirmation dialog opens.



2. Click **Yes**. The Welcome screen for the InstallShield Wizard opens.



3. Click **Next** to start the upgrade.

4. When the upgrade is finished, click **Finish** to close the wizard.

CHAPTER 3

CONNECTING TO A NEW GATEWAY FOR THE FIRST TIME

Connecting to a gateway for the first time is a different process than connecting to the same gateway in subsequent daily use. If the gateway requires certificate authentication, you cannot connect to the gateway until you have a valid certificate. Your administrator should inform you if you need to take action to obtain a certificate. Instructions for certificate-related tasks can be found in [Managing Certificates](#) (page 33).

The following sections are included:

- ▶ [Getting Started With Connecting to Gateways](#) (page 12)
- ▶ [Viewing a List of Configured Gateways](#) (page 12)
- ▶ [Connecting to a New Pre-Configured Gateway](#) (page 13)
- ▶ [Adding New Gateways Manually](#) (page 14)
- ▶ [Checking the Gateway's Certificate Fingerprint](#) (page 16)

Getting Started With Connecting to Gateways

After the installation, you cannot connect to gateways and end-points until they are configured in the VPN client. Also, if the VPN client is configured to allow domain logon (through the Windows logon screen), only gateways you have connected to at least once are available on the logon screen. The administrator may have preconfigured the gateways for you so that you can connect to them just by selecting them on a list. Alternatively, the administrator may provide you with contact information for each gateway either in a file or just as an address that you can contact.

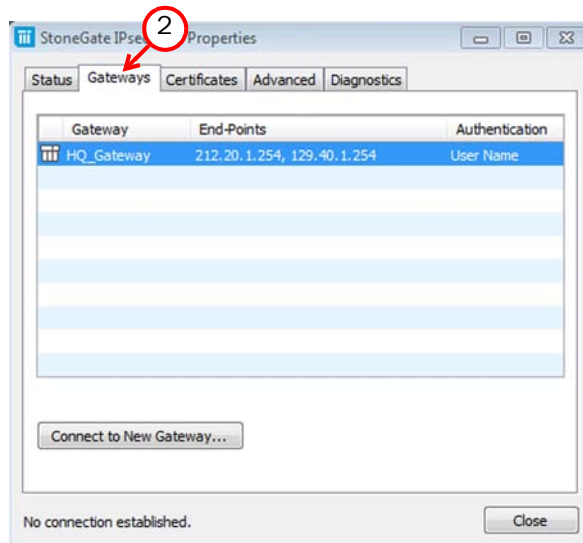
What's Next?

- ▶ If you are unsure if the gateway that you want to connect to is configured, see [Viewing a List of Configured Gateways](#) (page 12).
- ▶ If you know the gateway that you want to connect to is configured, see [Connecting to a New Pre-Configured Gateway](#) (page 13).
- ▶ If you know the gateway information is not present, add the information as explained in [Adding New Gateways Manually](#) (page 14).

Viewing a List of Configured Gateways

▼ To check which gateways are configured

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.
2. Switch to the **Gateways** tab. All configured gateways are listed in the table.

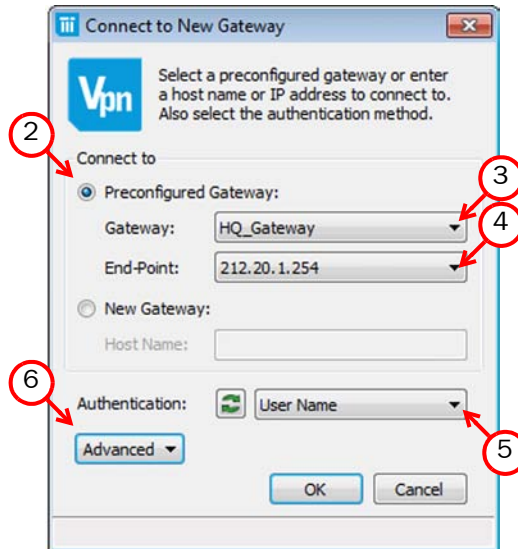


Connecting to a New Pre-Configured Gateway

If the gateway requires certificate authentication, you need a valid certificate to connect. The administrator should inform you if you need to obtain a certificate (see [Managing Certificates](#) (page 33)).

▼ To connect to a new preconfigured Gateway

1. Right-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar, and select one of the following from the menu:
 - If there are no fully configured gateways yet, select **Connect to New Gateway** directly at the main level.
 - Otherwise, select **Select Gateway**→**Connect to New Gateway**.



2. Make sure **Preconfigured Gateway** is selected. If the setting is disabled, add any new gateways manually as explained in [Adding New Gateways Manually](#) (page 14).
3. Select the preconfigured **Gateway**.
4. (Optional) Select the **End-Point** to connect to. End-points usually correspond to different Internet connections at the office.
5. (Optional) If you are allowed to authenticate using different methods, select the authentication method you want to use from the **Authentication** list.
6. (Optional) Select **Advanced** to define the Advanced settings.



Note – Do not modify the Advanced settings unless your network administrator specifically instructs you to do so.

7. (Optional) If TCP tunneling is enabled for the selected end-point and the initial connection to the gateway should be made through a TCP tunnel, select **Use TCP Tunneling to Port** and enter the number of the port defined for TCP tunneling on the end-point.

8. (Optional) If your organization prohibits the use of strong cryptographic methods, select **Use Limited Cryptography**.



Caution – Select this option only if you are required to use limited cryptographic methods.

9. (Optional; only if the Authentication Method is User Name) Under **Gateway Authentication**, select the signature type that matches the gateway's certificate.

10. Click **OK**. The User Authentication dialog opens.

What's Next?

- Log in as explained in [Authenticating Yourself](#) (page 21).

Adding New Gateways Manually

If the gateway requires certificate authentication, you need a valid certificate to connect. The administrator should inform you if you need to obtain a certificate (see [Managing Certificates](#) (page 33)).

To manually connect to a gateway that is not preconfigured in your installation, you need the following information from your network administrator:

- One address for each gateway you need to connect to.
- Information on which credentials to use for authentication.
- The gateway's certificate fingerprint that allows you to verify the gateway's identity.

▼ To add a gateway by typing the address manually

1. Right-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar, and select one of the following from the menu:
 - If there are no fully configured gateways yet, select **Connect to New Gateway** directly at the main level.
 - Otherwise, select **Select Gateway**→**Connect to New Gateway**.



2. Select **New Gateway**. If there are no preconfigured gateways that have not been contacted, the setting is selected by default.

3. Enter the gateway's address in the **Host Name** field.
4. (Optional) If you are allowed to authenticate using different methods, select the authentication method you want to use from the **Authentication** list.
5. (Optional) Select **Advanced** to define the Advanced settings.



Note – Do not modify the Advanced settings unless your network administrator specifically instructs you to do so.

6. (Optional) If TCP tunneling is enabled for the selected end-point and the initial connection to the gateway should be made through a TCP tunnel, select **Use TCP Tunneling to Port** and enter the number of the port defined for TCP tunneling on the end-point.
7. (Optional) If your organization prohibits the use of strong cryptographic methods, select **Use Limited Cryptography**.



Caution – Select this option only if you are required to use limited cryptographic methods.

8. (Optional; only if the Authentication Method is User Name) Under **Gateway Authentication**, select the signature type that matches the gateway's certificate.
9. Click **OK**.
10. If you authenticate with a certificate, enter the **Passphrase** defined for this certificate. The New Gateway dialog opens prompting you to verify the identity of the gateway by checking its certificate fingerprint.

What's Next?

- ▶ Continue by [Checking the Gateway's Certificate Fingerprint](#) (page 16).

Checking the Gateway's Certificate Fingerprint

When you connect to a new gateway for the first time, you must verify its identity.



Note – The Certificate Fingerprint is an important security feature that protects the confidentiality of your communications. An incorrect fingerprint may indicate a malicious attempt to spy on your communications.

▼ To check the Gateways Certificate Fingerprint

1. Compare the **Subject Name** and the **Certificate Fingerprint** to the information the administrator has provided.



2. Proceed according to the result of the comparison:
 - If there is a difference in the values, click **Cancel** and contact the administrator.
 - If the values match, click **OK**.



Note – If the gateway's certificate changes, you may have to check the Certificate Fingerprint again at a later date. The administrator informs you if this is necessary and provides you with the information for checking the new Certificate Fingerprint.

What's Next?

- ▶ If your authentication method is user name and password, you must now enter this information. See [Authenticating Yourself](#) (page 21).
- ▶ See the next chapter for more information on how to use the VPN client.

CHAPTER 4

USING THE VPN CLIENT

This chapter explains concepts and tasks related to the daily use of the StoneGate IPsec VPN client.

The following sections are included:

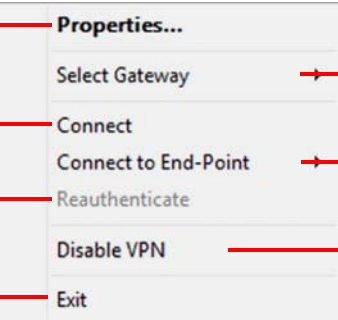
- ▶ [Overview to the VPN Client](#) (page 18)
- ▶ [Connecting to Resources](#) (page 19)
- ▶ [Authenticating Yourself](#) (page 21)
- ▶ [Closing the VPN Connection](#) (page 23)
- ▶ [Turning the VPN Client off](#) (page 24)
- ▶ [Activating/Deactivating User Name Memory](#) (page 25)
- ▶ [Activating/Deactivating Domain Logon](#) (page 26)
- ▶ [Activating/Deactivating Random Local VPN Ports](#) (page 27)
- ▶ [Activating/Deactivating Retry With Different Settings](#) (page 28)

Overview to the VPN Client

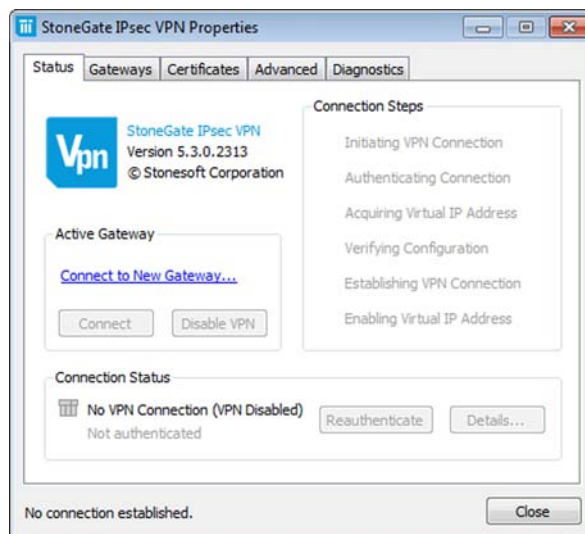
The StoneGate IPsec VPN client lets you access your organization's internal resources securely through the Internet. The VPN client establishes an encrypted connection to the StoneGate gateways that control access to your organization's internal resources, hiding the information you transfer from anyone who might intercept it in transit.

The VPN client adds an icon to the Notification area in the Windows Taskbar. The color of the VPN client icon changes according to the status of the VPN client (see [Monitoring VPN Connections](#) (page 29) for more information). You can view the status as text when you hold the mouse pointer over the VPN client icon.

Frequently needed commands are available in the menu that opens when you right-click the VPN client icon. The items change with the status of the VPN connection.

More actions and status information.			
Use Connect/Disconnect to open and close a VPN.		Select Gateway	Select where you want to connect.
Reauthenticate when convenient (instead of waiting for the timeout).		Connect	
Shut down the VPN client.		Connect to End-Point	Select end-point if the gateway has several.
		Reauthenticate	
		Disable VPN	Disconnect the VPN and turn off automatic authentication prompts.
	Exit		

More information and commands are available in the **Properties** dialog that opens through the command in the right-click menu or by double-clicking the VPN client icon.



Connecting to Resources

You must authenticate yourself each time you connect with either user name and password, a certificate passphrase, or your smartcard. Usually, the administrator selects a single method that you can use, but in some cases you can select from alternative methods (see [Selecting the Authentication Method](#) (page 21)). As a further security measure, your authentication is valid for a specific period of time after which you need to reauthenticate. Reauthentication may also be required if the VPN connection is cut due to networking problems.

There are three ways to establish a VPN:

- You may be able to log on to the VPN on the Windows logon screen. This way, the computer can connect all internal network resources (such as network drives) immediately when it starts up. See [Connecting to a Gateway at Windows Logon](#) below.
- You can manually connect your VPN client to a gateway and end-point of your choice. See [Connecting to a Gateway Manually](#) (page 20).
- When you are outside the office, the VPN client automatically prompts you to authenticate when you access a service or application that requires a VPN. See [Authenticating Yourself](#) (page 21).

Connecting to a Gateway at Windows Logon

Depending on the VPN client's settings, you may be able to open the VPN connection at the Windows logon screen before you log in to Windows. This way, network drives and other resources can be connected when you log in to Windows, avoiding error messages and delays that may sometimes occur if resources are not available.



Note – This feature is not available in Windows XP.

The integrated logon feature (domain logon) can be disabled and enabled in the properties dialog of the VPN client (Advanced tab), see [Activating/Deactivating Domain Logon](#) (page 26).



Note – Only gateways that you have already previously contacted can be accessed through the logon screen as explained below. See [Connecting to a New Gateway for the First Time](#) (page 11).

▼ To open the VPN connection through the Windows Logon screen

1. In the Windows logon screen, select **Switch User**. Windows displays icons for all configured user accounts and previously contacted VPN Gateways.



2. Select the gateway that you want to connect to. The logon screen for that gateway is displayed.
 - If you do not see any VPN gateways even though you have successfully connected to a gateway previously, this feature is most likely turned off in your installation, see [Activating/Deactivating Domain Logon](#) (page 26).
 - If a VPN connection is already active, you can disconnect it here.



3. If the authentication method calls for user name and password, make a selection for the **Use same credentials to log on to** setting:
 - If the same user name and password are valid for both the VPN access and the Windows account, select the option so that you are also logged in to Windows without having to provide the details again.
 - If the Windows logon information is different from your VPN client credentials, make sure the option is deselected to avoid a Windows logon failure.
4. Enter your credentials for the VPN connection. The VPN is established. Depending on the authentication method and the options selected, you will either need to log in to Windows or you are automatically logged in.

After logging in to Windows, the VPN connection is active and you can use resources through the VPN as soon as the Windows desktop is loaded.

Related Tasks

- ▶ [Authenticating Yourself](#) (page 21)
- ▶ [Closing the VPN Connection](#) (page 23)
- ▶ [Monitoring VPN Connections](#) (page 29)

Connecting to a Gateway Manually

If you want to connect to a gateway that is not yet listed, you must add the gateway as described in [Connecting to a New Gateway for the First Time](#) (page 11).

▼ To connect again to the previously contacted gateway

1. Right-click the IPsec VPN icon and select **Connect**.
2. Enter your credentials for the VPN connection (see [Authenticating Yourself](#) (page 21)). The VPN is established.

▼ To connect to a different gateway than you previously contacted

1. Right-click the IPsec VPN icon and select the gateway from the **Select Gateway** sub-menu.

2. Enter your credentials for the VPN connection (see [Authenticating Yourself](#) (page 21)). The VPN is established and the Gateway you selected is stored as your default connection.

Switching to an Alternative End-Point

Some gateways may be reached through several end-points. These usually correspond to different Internet connections at the office to which you are connecting. Selecting a different end-point may be useful when one of the Internet connections at the office you are connecting to is experiencing technical difficulties.

▼ To select an end-point

1. Right-click the IPsec VPN icon and select the correct end-point from the **Connect to End-Point** sub-menu.
2. Enter your credentials for the VPN connection (see [Authenticating Yourself](#) (page 21)). The VPN is established and the end-point you selected is stored as your default connection.

Authenticating Yourself

You must authenticate yourself whenever you connect to a gateway with the VPN client. The authentication method depends on the gateway to which you connect.

If you authenticate yourself to a gateway with a user name and a password, the VPN client asks you to reauthenticate yourself periodically. If a certificate or a smartcard is used, reauthentication is automatic.

Related Tasks

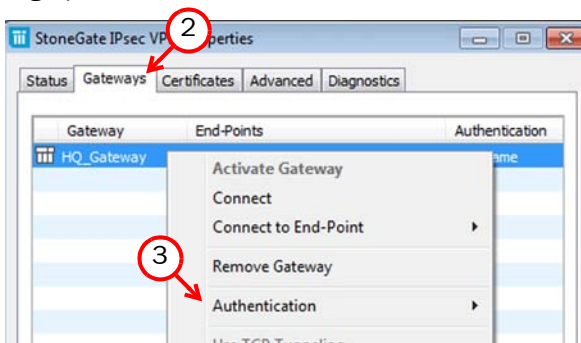
- ▶ [Selecting the Authentication Method](#) (page 21)
- ▶ [Authenticating with a User Name and Password](#) (page 22)
- ▶ [Authenticating with a Certificate](#) (page 22)
- ▶ [Authenticating with a Smartcard](#) (page 23)

Selecting the Authentication Method

A gateway may allow you to select how you want to authenticate. In that case, you can select which authentication method is used as explained below.

▼ To select the authentication method

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Gateways** tab. All configured gateways are listed in the table.
3. Right-click the gateway for which you want to select the authentication method and select **Authentication**→**Username** or **Authentication**→**Certificate**→[name used in certificate].
 - Smartcards contain certificates, so the list of available certificates also includes certificates stored on smartcards.
 - If you have certificate(s) that can be used for authentication in the Microsoft Certificates Store on your local machine, also those certificate(s) are listed here.
 - Note that all gateways may not accept all authentication methods.

The selected authentication method is used the next time you authenticate yourself.

Authenticating with a User Name and Password

The user name and password authentication dialog is displayed for any method that requires you to enter your user name manually. The password you enter can be fixed or, for example, a code generated by physical security token that you carry with you. The network administrator provides you the necessary details for logging in.



Note – You cannot change your password through the VPN client. Contact the network administrator if you need information for changing the password.

Authenticating with a Certificate

The certificate is protected with a passphrase. You have either defined the passphrase yourself or you should have received the passphrase code from the administrator.



Related Tasks

- ▶ [Managing Certificates](#) (page 33)
- ▶ [Changing the Certificate Passphrase](#) (page 44)

Authenticating with a Smartcard

If you have a smartcard, the VPN client uses the smartcard software installed on your computer to prompt you for your passphrase when authentication is needed. The dialog you see depends on the smartcard software installed on your computer. The certificates stored on smartcards are included on the list of available certificates when you select the method for authenticating to a gateway (see [Selecting the Authentication Method](#) (page 21)).

Closing the VPN Connection

There is usually no need to close the VPN connection when you stop using it. An unused connection automatically times out after a while.

You can still disconnect an active VPN manually at any time in the following ways:

- Select **Disconnect** from the right-click menu for the VPN client's icon in the Windows Taskbar.
- Click **Disconnect** on the Status tab in the VPN client's properties dialog.
- Right-click the active gateway on the Gateways tab in the VPN client's properties dialog and select **Disconnect** from the menu that opens.
- Click **Disconnect** in the Windows user switch screen (see [Connecting to a Gateway at Windows Logon](#) (page 19)).

When you do one of the listed actions, the status of the VPN changes to *No VPN connection*. If you or some application on your computer tries to access a resource that requires a VPN, the authentication prompt appears; to avoid this from happening, turn off the VPN client as explained in [Turning the VPN Client off](#) (page 24).

Turning the VPN Client off

If necessary, you can disable the VPN client so that it does not prompt you for authentication automatically. This can be done in the following alternative ways:

- Right-click the VPN client's icon in the Windows Taskbar and select **Disable VPN**.
- Click **Disable VPN** on the Status tab in the VPN client's properties dialog.
- When the authentication prompt is automatically displayed, click the grey icon in the authentication dialog (illustrated below) to disable the VPN.



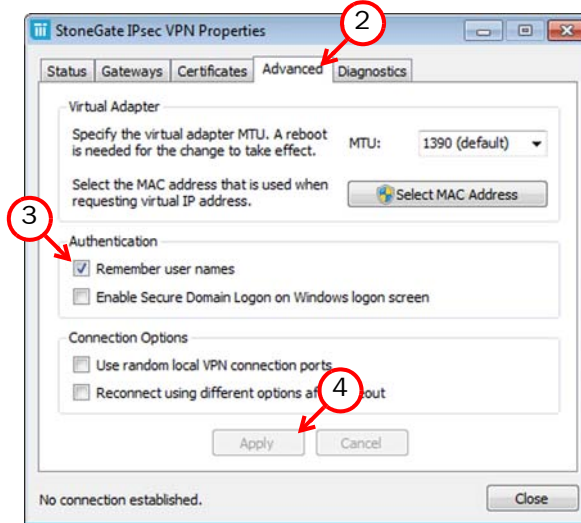
When you disable the VPN client, the status of the VPN changes to “No VPN connection (VPN Disabled)”. You can connect the VPN manually following the usual procedure without specifically re-enabling the VPN client. You are not able to use any resource through the VPN before you connect manually. See [Connecting to Resources](#) (page 19).

Activating/Deactivating User Name Memory

By default, the VPN client remembers up to five most recently used user names. This prevents the need to type frequently used user names each time you authenticate.

▼ To activate/deactivate user name memory

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Advanced** tab.
3. Deselect/select **Remember User Names**.
4. Click **Apply**.
5. Click **Close**.

Activating/Deactivating Domain Logon

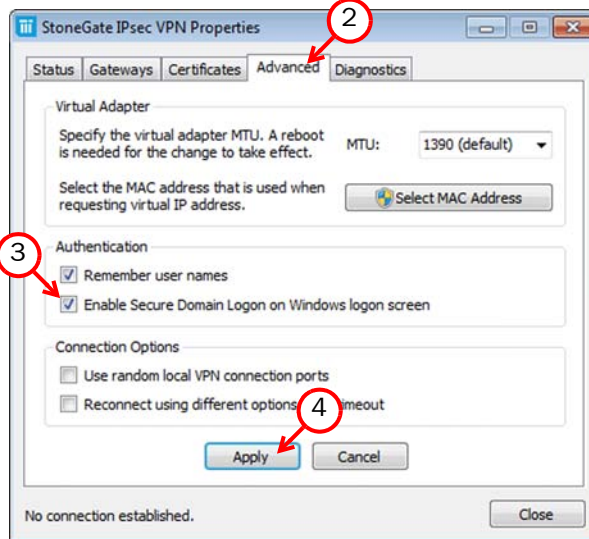
Domain logon allows you to open the VPN connection before you log in to Windows directly on the Windows logon screen. This way, network drives and other resources can be connected when you log in to Windows, avoiding error messages and delays that may sometimes occur if resources are not available.



Note – This feature is not available in Windows XP.

▼ To activate/deactivate domain logon

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Advanced** tab.
3. Select/deselect **Enable Secure Domain Logon**.
4. Click **Apply**.
5. Click **Close**.

By default, all Gateways you have contacted at least once are listed at Windows Logon when this feature is enabled. You can remove gateways from the logon screen by manually disabling the secure domain logon feature through each Gateway's right-click menu on the Gateways tab of the StoneGate IPsec VPN Properties dialog.

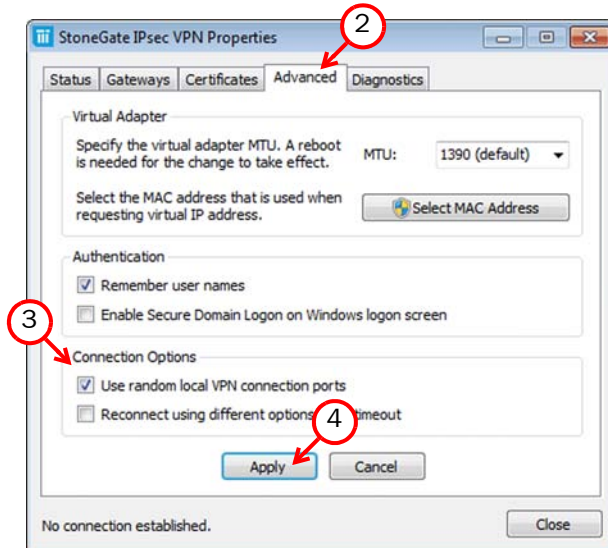
See [Connecting to a Gateway at Windows Logon](#) (page 19) for information on how to use this feature.

Activating/Deactivating Random Local VPN Ports

By default, the VPN client uses local ports 500 and 4500 for VPN connections. If these ports cannot be used for VPN connections in your environment, you can enable that the ports are randomly selected from the range of 1025 - 65535 every time a VPN connection is made.

▼ To active/deactivate random local VPN ports

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



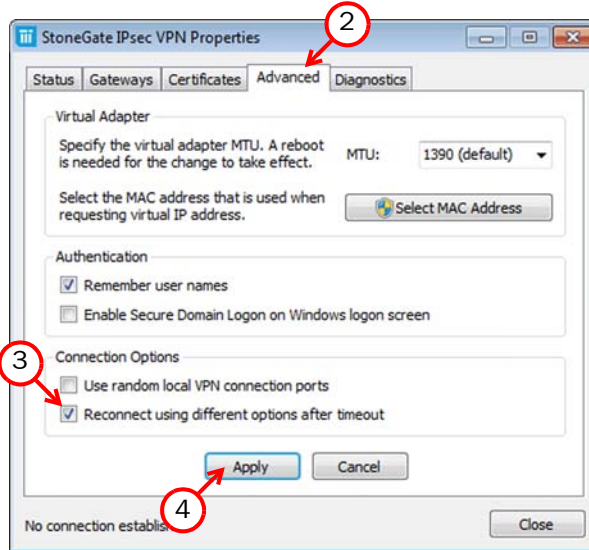
2. Switch to the **Advanced** tab.
3. Select/deselect **Use Random Local VPN Connection Ports**.
4. Click **Apply**.
5. Click **Close**.

Activating/Deactivating Retry With Different Settings

Some locations may require different connection settings than the previous locations from which you have connected. To help you with some types of connection issues, the VPN client can try different options automatically if the VPN fails to establish. The automatic retry setting is disabled by default.

▼ To activate/deactivate automatic reconnect using different options

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Advanced** tab.
3. Deselect/select **Reconnect using different options after timeout**.
4. Click **Apply**.
5. Click **Close**.

CHAPTER 5

MONITORING VPN CONNECTIONS

This chapter explains how you can manage and monitor VPN connections when they are active.

The following sections are included:

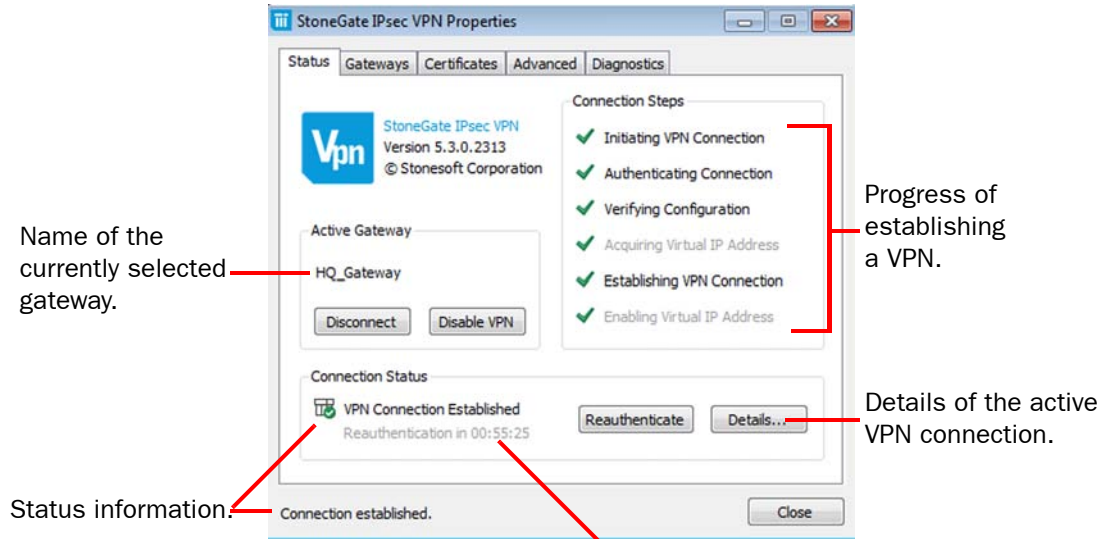
- ▶ [Viewing the VPN Connection Status](#) (page 30)
- ▶ [Viewing Details of an Active VPN Connection](#) (page 31)
- ▶ [Viewing a Configuration Downloaded From a Gateway](#) (page 32)

Viewing the VPN Connection Status

The VPN client icon in the Windows Taskbar and on the Status tab of the VPN client properties dialog shows the status of VPN connections using the following colors:

- Gray: VPN is disabled.
- Blue: No VPN connection.
- Green: VPN established.
- Alternating red and green: Connectivity problems.
- Red: Error.

You can manage and monitor the VPN connections on the Status tab in the VPN client's Properties dialog.



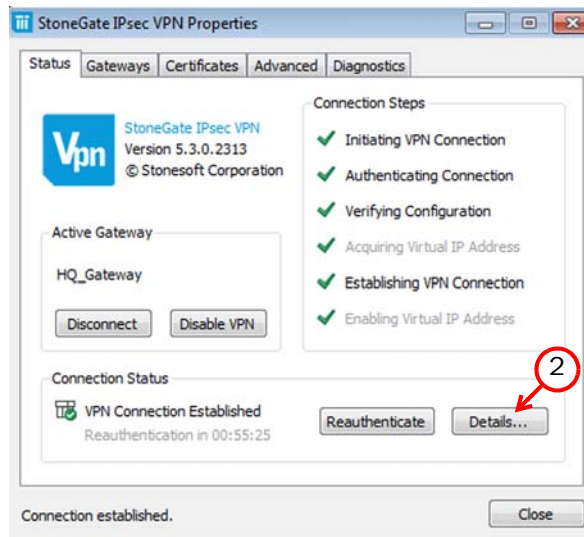
Reauthentication is required at regular intervals. The timer shows how long it takes until the authentication dialog automatically pops up again.

Viewing Details of an Active VPN Connection

Detailed information on the established VPN connection is available. This information is mainly useful for advanced users and administrators, and interpreting the details requires knowledge about IPsec standards.

▼ To view details of a VPN connection

1. Double-click the IPsec VPN icon to open the StoneGate IPsec VPN properties.



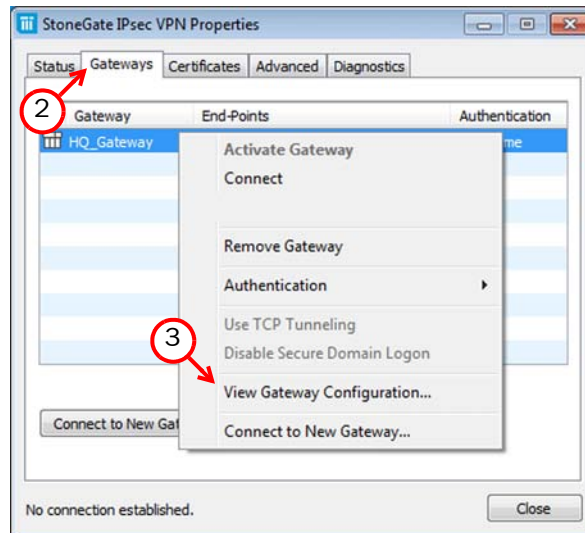
2. Click **Details**. The VPN Details dialog opens.
3. Check the settings used in the currently active VPN connection in the dialog that opens. IPsec-related terms are used as follows:
 - **IKE**: settings for negotiation phase 1.
 - **IPsec**: settings for negotiation phase 2.
4. Click **Close** when you are done.

Viewing a Configuration Downloaded From a Gateway

The VPN client receives many of its settings from the Gateway. When you connect to a gateway, the VPN client checks if there are previously downloaded settings from the gateway in question, and whether such settings are up-to-date. If necessary, a new configuration is downloaded, replacing the old configuration.

▼ To view a configuration

1. Double-click the IPsec VPN icon to open the StoneGate IPsec VPN properties.



2. Switch to the **Gateways** tab.
3. Right-click a gateway to which you have previously connected and select **View Gateway Configuration**. The settings that the client has downloaded from that gateway are displayed in a new dialog.
4. Click **Close** when you are done.

CHAPTER 6

MANAGING CERTIFICATES

This chapter explains how you can manage VPN client certificates.

The following sections are included:

- ▶ [Overview to Managing Certificates](#) (page 34)
- ▶ [Using Internal Certificates](#) (page 34)
- ▶ [Using External Certificates](#) (page 40)
- ▶ [Changing the Certificate Passphrase](#) (page 44)
- ▶ [Viewing Details of Imported Certificates](#) (page 45)
- ▶ [Changing User ID Type of an Imported Certificate](#) (page 46)
- ▶ [Deleting Imported Certificates](#) (page 46)

Overview to Managing Certificates

If you use certificates imported through the VPN client, you can manage the imported certificates directly in the VPN client. The signed certificates that you have imported are listed on the Certificates tab. You can, for example, change the certificate key's passphrase. You can also view general information on the imported certificate(s) and the Certificate Authority that signed them.

Certificates stored on smartcards or in the Microsoft Certificates Store on the local machine are not listed on the Certificates tab. They are included on the list of available certificates when you select the authentication method for connecting to a gateway (see [Selecting the Authentication Method](#) (page 21)). You cannot otherwise manage these certificates in the VPN client.

If you must create a new internal certificate request or import an internal certificate that an administrator has signed, see [Using Internal Certificates](#). If you want to import a certificate created and signed outside StoneGate, see [Using External Certificates](#) (page 40).

All certificates have a set period of use, typically of a few years. When the certificate expires, it can no longer be used, and you need to obtain a new certificate. You can view your installed certificate's expiration date in the VPN client, see [Viewing Details of Imported Certificates](#) (page 45).

Using Internal Certificates

The administrator may have defined that your VPN connections require a client certificate on your machine. Follow these instructions if the administrator informs you that you must generate a certificate request in the VPN client and send it for signing to your network administrator.

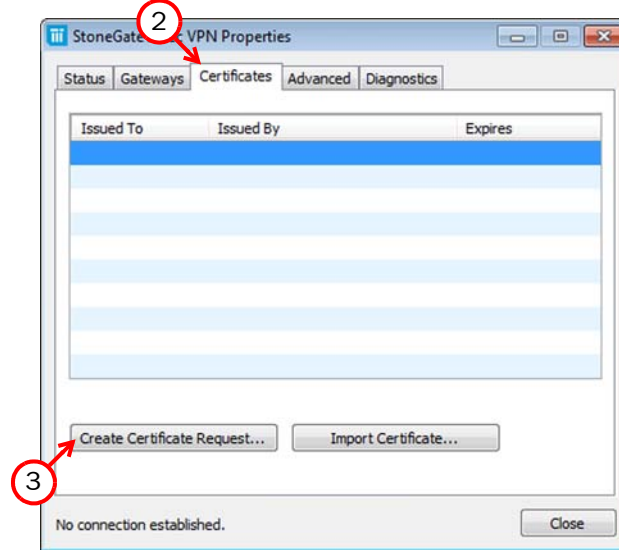
If the client certificate on your computer or the Certificate Authority that signed the client certificate has expired, repeat the same process to renew the certificate.

Creating a Basic Certificate Request

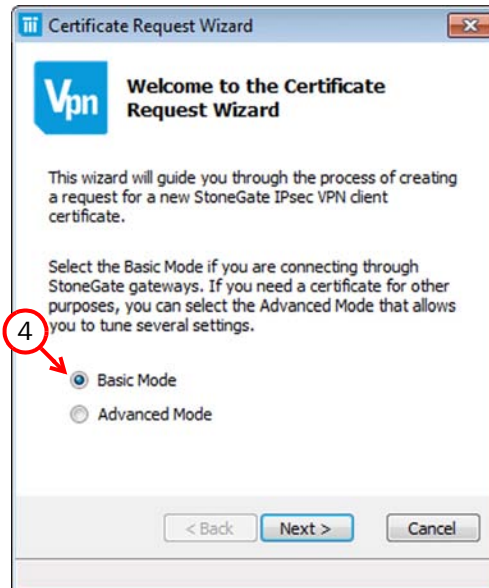
The following instructions describe how you can create a basic certificate request for an internal certificate in the VPN client. If the administrator informs you that you must create an advanced certificate request for an internal certificate, see the *IPsec VPN Client Administrator's Guide* for instructions.

▼ **To create a basic certificate request for an internal certificate**

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Certificates** tab.
3. Click **Create Certificate Request**.



4. Leave **Basic Mode** selected and click **Next**.

5. Enter the **User Name**. This must correspond to what is defined on the gateway. Contact the administrator if you are unsure of what to enter as the user name.
6. Enter and confirm a **Passphrase** to use whenever you authenticate yourself using the certificate. You can select this passphrase yourself.

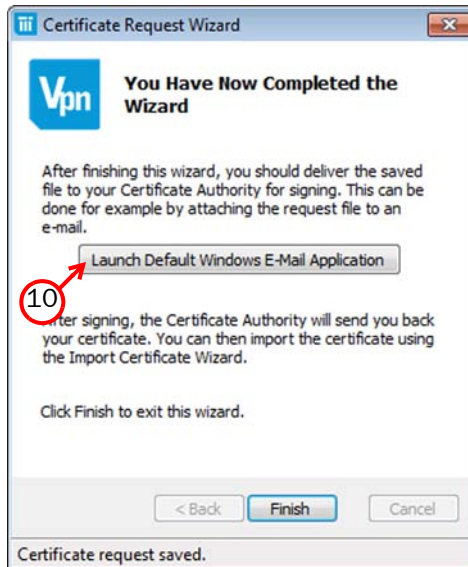


Note – Passphrases should be at least eight characters long and contain a combination of numbers, letters, and special characters. Secure passphrases are never based on personal information such as names, birthdays, ID numbers, phone numbers, registration plate numbers, or any of the above written backwards.

7. Click **Create**.

8. Click **Save**. A file save dialog opens.

9. Browse to the correct folder, enter a file name and click **Save**. Make sure that **Certificate Requests (*.csr)** is selected as the file type.



10. Click **Launch Default Windows E-Mail Application** to create a new message in your default e-mail application or click **Finish** to just close the window.
11. Send the certificate request (the `.csr` file that you just saved) to your network administrator for signing.
12. Click **Finish** to exit the Certificate Request Wizard.

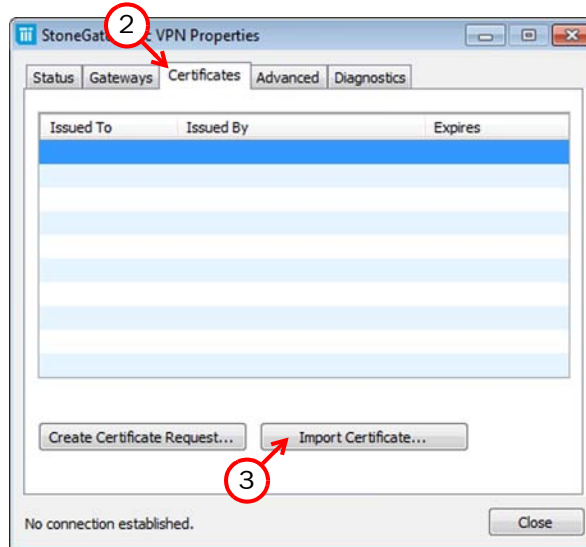
When you get the signed internal certificate back, import it as described in [Importing a Signed Certificate](#) (page 38) below.

Importing a Signed Certificate

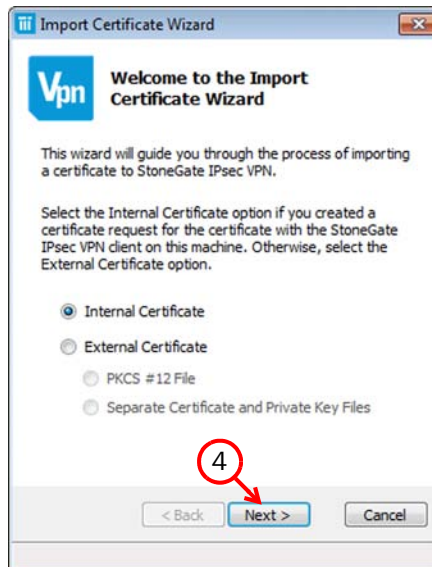
Once the administrator has signed your certificate request for an internal certificate and sent it back to you, import the signed certificate in your VPN client.

▼ To import an internal certificate

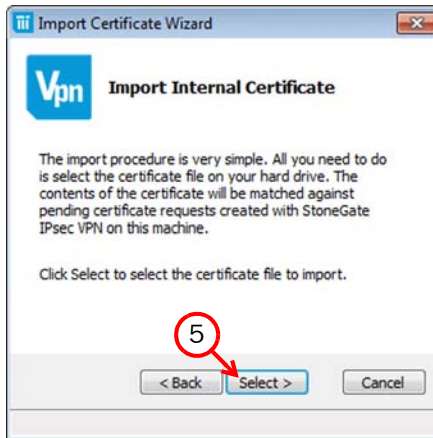
1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Certificates** tab.
3. Click **Import Certificate**. The Import Certificate Wizard opens.



4. Leave **Internal Certificate** selected and click **Next**.



5. Click **Select**. A Windows file browser opens.
6. Browse to the correct folder, select the signed certificate and click **Open**.
7. Click **Finish** to close the wizard. The signed internal certificate is now listed on the Certificates tab with information about the certificate, such as its expiration date.

Related Tasks

- ▶ [Managing Certificates](#) (page 33)

Using External Certificates

There are three ways of using previously generated external certificates with the VPN client. You can use an external certificate stored on a smartcard, a certificate stored in the Microsoft Certificates Store on your local machine, or you can import the certificate in the VPN client.

There are two types of external certificates that you can import: you can either import the certificate and its private key as a single PKCS # 12 file or as two separate files. Follow the instructions below if the administrator informs you that you must import an external certificate in the VPN client.

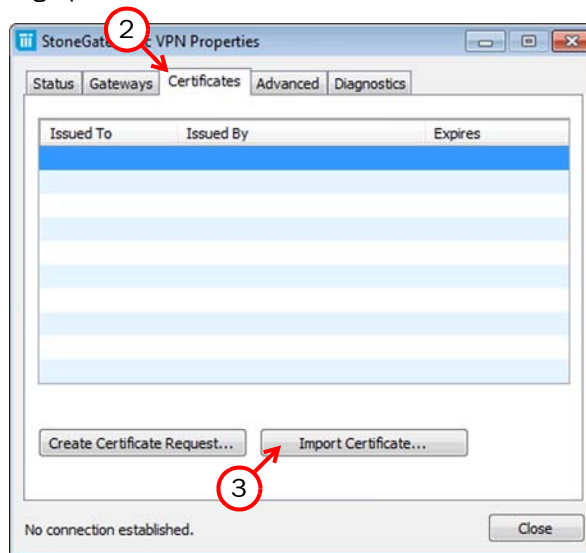
What's Next?

- ▶ [Importing a PKCS # 12 File](#) (page 40).
- ▶ [Importing Separate Certificate and Private Key Files](#) (page 42).

Importing a PKCS # 12 File

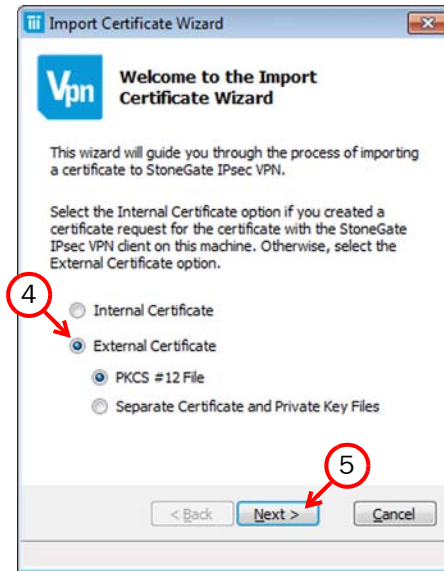
▼ To import a PKCS # 12 file

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.

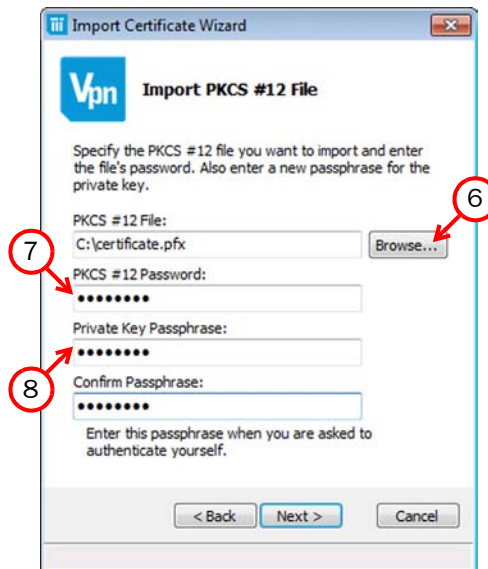


2. Switch to the **Certificates** tab.

3. Click **Import Certificate**. The Import Certificate Wizard opens.



4. Select **External Certificate**.
5. Leave **PKCS # 12 File** selected and click **Next**.



6. Click **Browse** and select the PKCS #12 File to import.
7. Enter the **PKCS #12 Password** for the certificate file.

8. Enter and confirm a **Passphrase** to use whenever you authenticate yourself using the certificate. You can select this passphrase yourself.



Note – Passphrases should be at least eight characters long and contain a combination of numbers, letters, and special characters. Secure passphrases are never based on personal information such as names, birthdays, ID numbers, phone numbers, registration plate numbers, or any of the above written backwards.

9. Click **Next**.
10. Click **Finish**.

The signed certificate is now listed on the Certificates tab. The Certificates tab displays, among other information, the expiration date of the certificate.

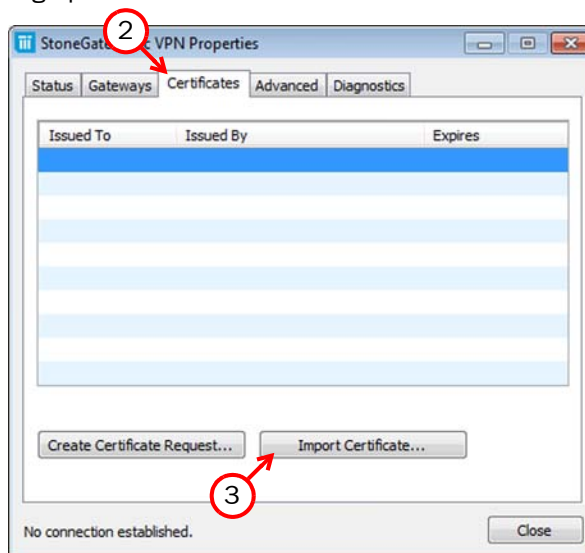
Related Tasks

- ▶ [Managing Certificates](#) (page 33)

Importing Separate Certificate and Private Key Files

▼ To import separate certificate and private key files

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.

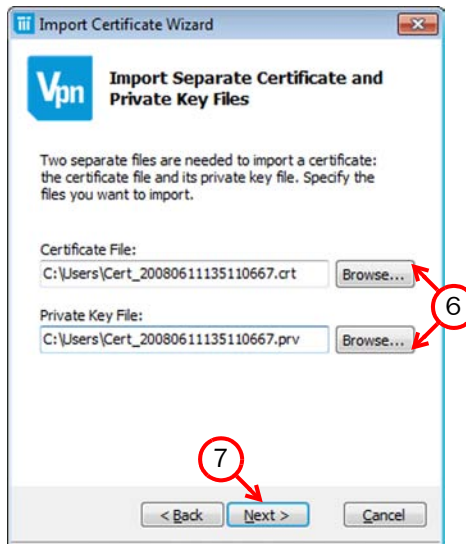


2. Switch to the **Certificates** tab.

3. Click **Import Certificate**. The Import Certificate Wizard opens.



4. Select **External Certificate**.
5. Select **Separate Certificate and Private Key Files** and click **Next**.



6. Click **Browse** to select the certificate file and private key file to import.
7. Click **Next**.
8. Click **Finish**.

The certificate is now listed on the Certificates tab. The Certificates tab displays, among other information, the expiration date of the certificate.

Related Tasks

- [Managing Certificates](#) (page 33)

Changing the Certificate Passphrase

You must enter a passphrase every time the VPN client asks you to authenticate yourself using this certificate. You can change the passphrase of a certificate that you have imported through the VPN client.



Note – Passphrases should be at least eight characters long and contain a combination of numbers, letters, and special characters. Secure passphrases are never based on personal information such as names, birthdays, ID numbers, phone numbers, registration plate numbers, or any of the above written backwards.

▼ To change the key passphrase

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.
2. Switch to the **Certificates** tab.
3. Right-click the certificate and select **Change Key Passphrase** from the menu. The Change Key Passphrase dialog opens.

Change Key Passphrase

Enter the old and new passphrase. If you leave the new passphrase field empty, the private key will not be encrypted.

Old Passphrase:

New Passphrase:

Confirm Passphrase:

OK Cancel

4. Enter the current passphrase and the new passphrase in both fields provided, and click **OK**.



Note – If you leave the new passphrase fields empty, the private key of the certificate will not be encrypted. For security reasons, it is highly recommended that you enter a passphrase.

Viewing Details of Imported Certificates

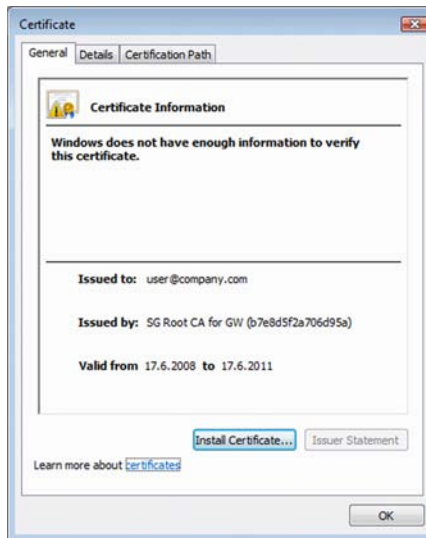
Although this dialog provides tools for installing the user certificate in the Microsoft Certificates Store on your computer and the issuer certificate in the Trusted Root Certification Store, such tasks are not necessary for the operation of the VPN client.



Note – This dialog is a standard operating system dialog, not part of the StoneGate VPN client. If you would like more instructions for using this dialog, press F1 to view the context-specific Windows help on this dialog (or a short description of the selected control in Windows XP).

▼ To view details of a user certificate

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.
2. Switch to the **Certificates** tab.
3. Right-click the certificate and select **Details of User Certificate** or **Details of Issuer Certificate**. The Windows Certificate dialog opens.



The **General**, **Details**, and **Certification Path** tabs provide detailed information about the certificate.

Changing User ID Type of an Imported Certificate

Several user IDs may be available for each imported certificate. The administrator may ask you to change the user ID type for the imported certificate.



Note – The network administrator has defined your user ID and its type. Do not change the user ID type unless the network administrator specifically instructs you to do so.

▼ To change an imported certificate's user ID type

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.
2. Switch to the **Certificates** tab.
3. Right-click the certificate for which you want to change the user ID type and select one of the following from the menu:
 - **Certificate ID to Use**→**E-mail**
 - **Certificate ID to Use**→**Subject Name**
 - **Certificate ID to Use**→**DNS Name**
 - **Certificate ID to Use**→**IP Address**.

The options available depend on which types of information are included in the certificate.

Deleting Imported Certificates

Sometimes, an imported certificate may become unnecessary. In such cases, you can delete the obsolete certificate through the VPN client.

▼ To delete a certificate

1. Double-click the StoneGate IPsec VPN icon in the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.
2. Switch to the **Certificates** tab.
3. Right-click the certificate and select **Delete Certificate**. A confirmation dialog is shown.
4. Click **Yes** to permanently delete the certificate.

CHAPTER 7

TROUBLESHOOTING VPN CONNECTIONS

This chapter explains what you can do if you have problems with your VPN connections.

The following sections are included:

- ▶ [Solving Connectivity Problems](#) (page 48)
- ▶ [Collecting Diagnostics Information](#) (page 51)
- ▶ [Capturing Network Traffic](#) (page 52)

Solving Connectivity Problems

Try Different Settings Automatically

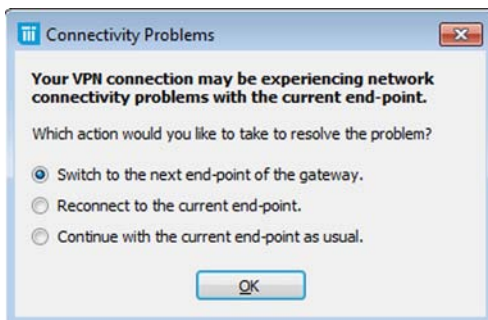
Some connectivity problems can be solved by changing the VPN clients' settings slightly. You can make the VPN client automatically try different combinations of settings. See [Activating/Deactivating Retry With Different Settings](#) (page 28). The automatic retry setting is particularly useful in dealing with network connections that severely restrict the allowed communications. In such situations, you are generally able to browse the Internet outside the VPN connection, but the VPN client is unable to connect to the gateway.

Enable Random Local VPN Ports

VPN connections may sometimes fail because the default local ports that the VPN client uses for VPN connections (ports 500 and 4500) cannot be used in your environment. You can enable that the local VPN ports are randomly selected when the VPN client opens a VPN connection. See [Activating/Deactivating Random Local VPN Ports](#) (page 27) for more information.

If the Connectivity Problems Dialog Is Displayed

If network connectivity problems occur when the VPN client has already established a VPN to a gateway, the Connectivity Problems dialog may be displayed.



▼ To troubleshoot network connectivity problems

1. Select one of the available options:

Option	Description
Switch to the next end-point of the gateway	If the gateway has several end-points, the VPN client tries to establish a VPN by switching to the next end-point. This action helps if there are several Internet connections at the office you are connecting to and the link you were using is down.
Reconnect to the end-point	The VPN client tries to establish a new connection to the currently selected end-point. This action helps if your connection to the gateway was cut because of a temporary problem at any point along the communications path.

Option	Description
Continue with the current end-point as usual	The VPN client waits for the already established connection to the current end-point to become available. This action helps particularly with network problems related to your local environment, for example, if the network cable is removed and re-inserted.

2. Click **OK**.

If the VPN client fails to establish a connection according to the selected option, wait until network connections become available again and then try to connect to the gateway manually as described in [Connecting to Resources](#) (page 19).

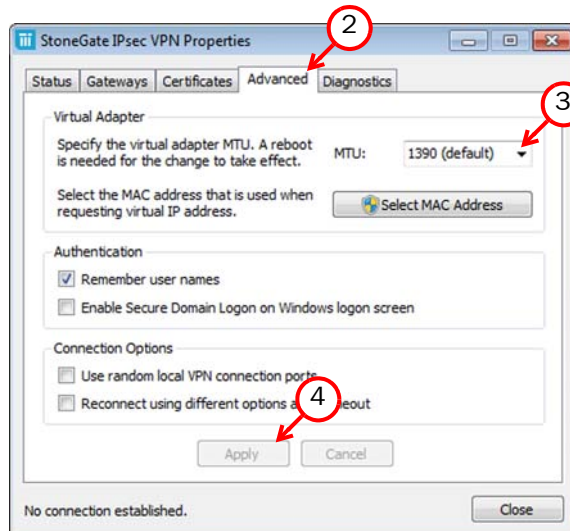
Changing the VPN Client's MTU

Large chunks of data you send over networks are broken down into several smaller units (packets) for transfer. The MTU (maximum transmission unit) defines how large the packets can be. A larger MTU is more efficient, but the packet size may have to be reduced if the packets are sent through a network or device that can not handle large packets.

If you experience network problems, your administrator may request that you adjust the MTU size for your VPN client installation.

▼ To change the MTU

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Advanced** tab.
3. Select the correct **MTU** from the list or type in the correct value according to the information you have received from the administrator.
4. Click **Apply**.
5. Click **Close**.
6. Restart the computer.

Changing the VPN Client's MAC Address

If you experience networking problems, your administrator may request you to adjust the MAC address of your VPN client installation.

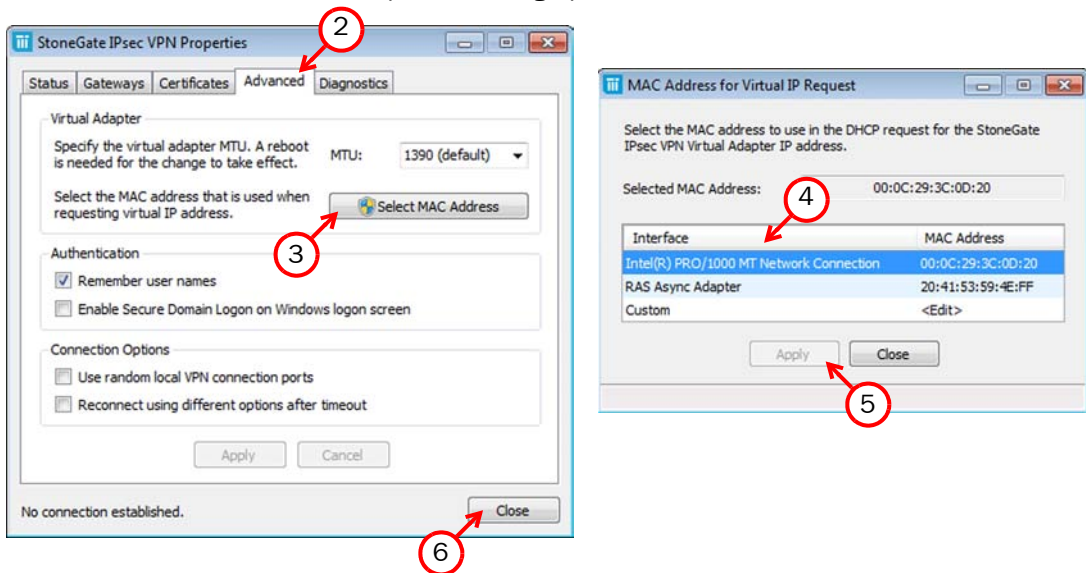
Changing the MAC address requires Windows administrator privileges.

Background:

- The MAC (media access control) address is a fixed identifier of a network device.
- The VPN client borrows the MAC address of a network card on your computer when it sends information.
- In some configurations, the MAC address picked up like this may not be unique between different users, causing intermittent connection problems when the same address is used for two different VPN connections at the same time.

▼ To change the MAC address

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



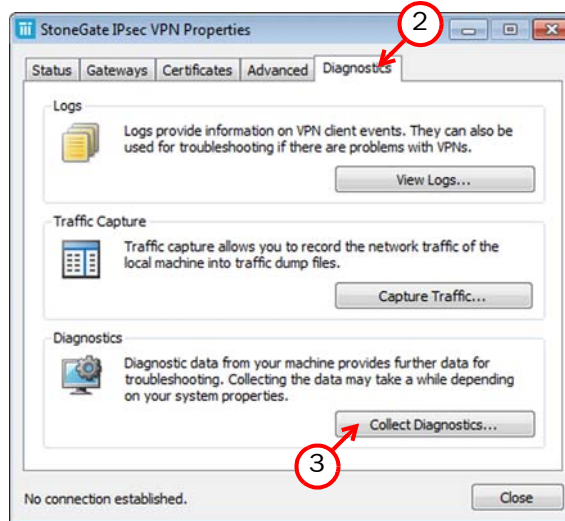
2. Switch to the **Advanced** tab.
3. Click **Select MAC Address**. The MAC Address for Virtual IP Address dialog opens (Windows may display a security dialog before the dialog opens).
4. Select the correct value according to the information from the administrator.
5. Click **Apply**.
6. Click **Close**.

Collecting Diagnostics Information

Diagnostics information is meant for administrators. If you are experiencing connection problems with the VPN client, the administrator may ask you to collect and send in a file containing diagnostics information about your installation.

▼ To collect diagnostics

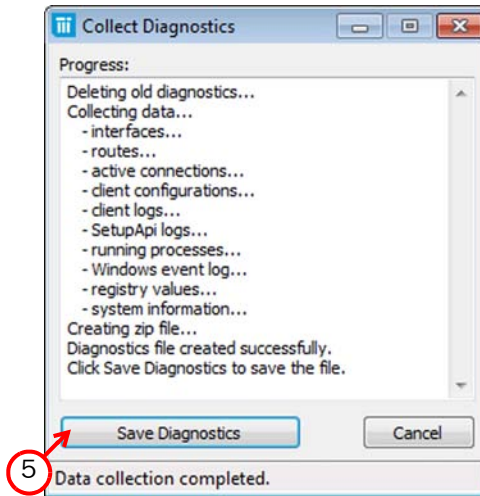
1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Diagnostics** tab.
3. Click **Collect Diagnostics**. The Collect Diagnostics dialog opens and displays the progress of the data collection.
4. Wait while the information is gathered. You may see an additional dialog open when system information is gathered.



Note - Collecting the diagnostic data will take some time.



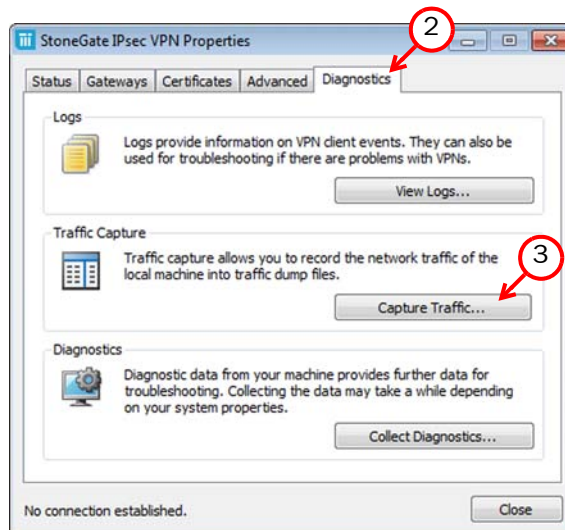
5. When the data collection finishes, click **Save Diagnostics**. A Windows file dialog opens.
6. Browse to the location where you want to save the file, enter a file name and click **Save**.

Capturing Network Traffic

The administrator may ask you to record the network traffic of the local machine during a problem situation to assist in troubleshooting. Alternatively, the administrator may capture local network traffic through your VPN client. The traffic recordings are saved on the local machine in the traffic dump files `adapter.pcap` and `protocol.pcap` in the specified folder.

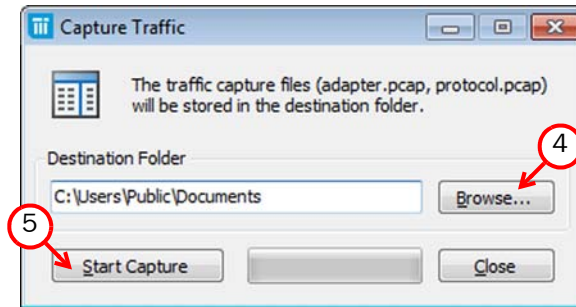
▼ To capture network traffic

1. Double-click the StoneGate IPsec VPN icon in the Notification area of the Windows Taskbar. The StoneGate IPsec VPN Properties dialog opens.



2. Switch to the **Diagnostics** tab.

3. Click **Capture Traffic**. The Capture Traffic dialog opens.



4. (Optional) Click **Browse** and browse to the folder where you want to save the traffic capture files.
5. Click **Start Capture**. The traffic capture begins.
6. Click **Stop Capture** when all traffic related to the problem has been recorded.
7. Click **Close** to close the Capture Traffic dialog.

StoneGate Guides

Administrator's Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.

User's Guides - step-by-step instructions for end-users.

For more documentation, visit
www.stonesoft.com/support/

Stonesoft Corporation

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1349

STONESOFT

Secure Information Flow

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

Tel. +1 770 668 1125
Fax +1 770 668 1131