



STONEGATE IPSEC VPN 5.3

VPN CLIENT ADMINISTRATOR'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	Certificate Expiration 25
How to Use This Guide	6	
Typographical Conventions	6	CHAPTER 6
Documentation Available	6	Logs and Diagnostics 27
Product Documentation.	6	Overview to Logs and Diagnostics 28
Support Documentation	7	Reading Logs. 29
System Requirements.	7	Capturing Network Traffic 30
Supported Features	7	Collecting a Diagnostics File 31
Contact Information	8	
Licensing Issues	8	
Technical Support.	8	
Your Comments	8	
Other Queries.	8	
CHAPTER 2		
What's New in Release 5.3?	9	
IKEv2 Support for VPNs	10	
Support for ECDSA Certificates	10	
CHAPTER 3		
Getting Started with the VPN Client	11	
Overview to StoneGate IPsec VPN Client.	12	
Installation Options.	13	
Installation Files.	13	
Installing With the Standard Installation Package.	13	
User Authentication	14	
IP Addressing.	14	
Automatic Retry With Different Settings	15	
CHAPTER 4		
Customizing VPN Client Installations	17	
Configuration Overview	18	
Saving Gateway Contact Information to a File	18	
Exporting Gateway Contact Information	18	
Copying Gateway Contact Information Files Manually	19	
Customizing Installation Packages	19	
Creating a Transform File	19	
Installing with a Transform File	19	
CHAPTER 5		
Using Certificates with the VPN Client	21	
Overview to VPN Client Certificates	22	
Using Internal Certificates.	23	
Using External Certificates	25	

CHAPTER 1

INTRODUCTION

Welcome to StoneGate™ IPsec VPN client by Stonesoft Corporation. This chapter describes how to use the *StoneGate IPsec VPN Client Administrator's Guide* and lists other available documentation. It also provides directions for obtaining technical support and giving feedback.

The following sections are included:

- ▶ [How to Use This Guide](#) (page 6)
- ▶ [Documentation Available](#) (page 6)
- ▶ [Contact Information](#) (page 8)

How to Use This Guide

This *StoneGate IPsec VPN Client Administrator's Guide* is intended for the administrators of the StoneGate IPsec VPN client. This guide concentrates on the deployment and advanced configuration of the VPN clients. The VPN client is covered in the following guidebooks:

- Configuring VPN access for the VPN client users is described in the *Administrator's Guide* and the *Online Help* of the Management Client.
- The instructions for using the VPN clients can be found in the *VPN Client User's Guide*.

For other available documentation, see [Documentation Available](#) (page 6).

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 (e.g., 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.

Documentation Available

Product Documentation

The table below lists the available product documentation. PDF guides are available on the Management Center CD-ROM and at <http://www.stonesoft.com/support/>.

Table 1.2 Product Documentation

Guide	Description
Reference Guide	Explains the operation and features of StoneGate comprehensively. Demonstrates the general workflow and provides example scenarios for each feature area. Available for StoneGate Management Center, Firewall/VPN, and StoneGate IPS.

Table 1.2 Product Documentation (Continued)

Guide	Description
Installation Guide	Instructions for planning, installing, and upgrading a StoneGate system. Available for StoneGate Management Center, Firewall/VPN, and IPS.
Online Help	Describes how to configure and manage the system step-by-step. Accessible through the Help menu and by using the Help button or the F1 key in any window or dialog. Available in the StoneGate Management Client and the StoneGate Web Portal. An HTML-based system is available in the StoneGate SSL VPN Administrator through help links and icons.
Administrator's Guide	Describes how to configure and manage the system step-by-step. Available as a combined guide for both StoneGate Firewall/VPN and StoneGate IPS, and as separate guides for StoneGate SSL VPN and StoneGate IPsec VPN Client.
User's Guide	Instructions for end-users. Available for the StoneGate IPsec VPN Client and the StoneGate Web Portal.
Appliance Installation Guide	Instructions for physically installing and maintaining StoneGate appliances (rack mounting, cabling, etc.). Available for all StoneGate hardware appliances.

Support Documentation

The StoneGate support documentation provides additional and late-breaking technical information. These technical documents support the StoneGate Guide books, for example, by giving further examples on specific configuration scenarios.

The latest StoneGate technical documentation is available on the Stonesoft website at <http://www.stonesoft.com/support/>.

System Requirements

The system requirements for running StoneGate, including the approved network interfaces, supported operating systems, and other such hardware and software requirements for StoneGate engines and the Management Center can be found at http://www.stonesoft.com/en/products/fw/Software_Solutions/.

The hardware and software requirements for the version of StoneGate you are running can also be found in the *Release Notes* on the software download page at the Stonesoft website.

Supported Features

Not all StoneGate features are supported on all platforms. See the [Appliance Software Support Table](#) at the Stonesoft Support Documentation pages for more information.

Contact Information

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

Licensing Issues

You can view your current licenses at the License Center section of the Stonesoft website at <https://my.stonesoft.com/managelicense.do>.

For license-related queries, e-mail order@stonesoft.com.

Technical Support

Stonesoft offers global technical support services for Stonesoft's product families. For more information on technical support, visit the Support section at the Stonesoft website at <http://www.stonesoft.com/support/>.

Your Comments

We want to make our products suit your needs as best 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.

Other Queries

For queries regarding other matters, e-mail info@stonesoft.com.

CHAPTER 2

WHAT'S NEW IN RELEASE 5.3?

This section lists major changes since the previous release. For a full list of changes and version compatibility information, consult the *Release Notes* for the VPN client.

The following sections are included:

- ▶ [IKEv2 Support for VPNs](#) (page 10)
- ▶ [Support for ECDSA Certificates](#) (page 10)

IKEv2 Support for VPNs

In addition to IKEv1, also IKEv2 is now supported in VPNs. IKEv2 provides support for IKEv2 Mobility and Multihoming Protocol (MOBIKE) protocol. MOBIKE enables transparent recovery for VPN clients if the IP address of the VPN client or the IP address of the gateway to which the VPN client is connected changes in the middle of an open VPN connection.

Support for ECDSA Certificates

Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are now supported in user authentication.

CHAPTER 3

GETTING STARTED WITH THE VPN CLIENT

This chapter explains the basic concepts of the StoneGate IPsec VPN client.

The following sections are included:

- ▶ [Overview to StoneGate IPsec VPN Client](#) (page 12)
- ▶ [Installation Options](#) (page 13)
- ▶ [User Authentication](#) (page 14)
- ▶ [IP Addressing](#) (page 14)
- ▶ [Automatic Retry With Different Settings](#) (page 15)

Overview to StoneGate IPsec VPN Client

The *StoneGate IPsec VPN client* provides a secure VPN (virtual private network) connection to a StoneGate Firewall/VPN gateway for individual end-user computers running on modern Microsoft Windows platforms (see the *Release Notes* of the VPN client for the exact system requirements). The VPN client protects private information while it is transferred over the Internet and allows verification of the user's identity. StoneGate IPsec VPN client mainly runs in the background, automatically prompting the user to authenticate when a VPN is required.

VPN Client Configuration

The VPN client settings are mostly configured centrally through the Management Center. The VPN clients download a configuration file from the firewall/VPN gateways to set the correct options for establishing a client-to-gateway VPN with that gateway (for encryption, authentication, end-points to contact, and the IP addresses that are accessible through the VPN). When changes are made on the gateway, each VPN client updates its configuration the next time the VPN client starts a new VPN connection. Due to the centralized configuration method, the StoneGate IPsec VPN client can connect to StoneGate Firewall/VPN gateways only.

Deployment Overview

1. Configure the VPN-related elements and settings in the Management Client:
 - Create a new VPN or add the **IPsec Client** Gateway element to an existing VPN and configure the VPN client settings in the internal Gateway and VPN Profile elements.
 - Create the user accounts or integrate an existing LDAP database and/or an external authentication service with StoneGate.
 - Modify the Firewall Policy so that the policy allows incoming connections from the VPN clients.
2. Install the VPN clients on the end-users' computers as explained in [Installation Options](#) (page 13).
3. Provide the end-users with the necessary information so that they know how to proceed with the installation, depending on how the VPN clients are installed:
 - How end-users should install the VPN client if manual installation is required.
 - The authentication method and credentials that end-users must use in authentication.
 - The contact details of the gateway(s) if not provided in a customized installation package.

Detailed step-by-step instructions for tasks that you need to perform in the Management Client can be found in the *Online Help* of the Management Client and the *Administrator's Guide* PDF, in the section called **Virtual Private Networks**.

Installation Options

The VPN client can be installed in interactive mode by manually launching the installer, or in automatic mode through a remote software deployment service. The installation must be executed with administrator privileges.

The VPN clients are licensed as part of the Firewall/VPN gateway, which may possibly have a licensed limit on how many users can be connected at the same time. There is no license or serial code enforcement in the VPN client; you can freely install it on any number of hosts.

Installation Files

There are two files that you can use for installing the VPN client:

- `StoneGate_IPsec_VPN_<version>.exe` (where `<version>` is the exact version number that changes each time an update is released).
- `StoneGate_IPsec_VPN.msi`.

The VPN client can be installed locally with the `.exe` installer. The `StoneGate_IPsec_VPN.msi` package allows remote installation and/or customized installations that remove the need for some end-user actions:

- With a standard installation package, the end-users type the gateway IP address manually, authenticate themselves to the gateway, and verify the certificate fingerprint of the gateway. Alternatively, you can export the contact details of the gateway to a file and instruct the end-users to copy the file to the correct location.
- If you generate a customized installation package, the gateway information can be included in the installation package, requiring no end-user intervention. For more information, see [Customizing VPN Client Installations](#) (page 17).

Installing With the Standard Installation Package

End-users either install the VPN client following the instructions in the Installation Wizard (see the *StoneGate IPsec VPN Client User's Guide* for more information) or you can provide a batch file for silent installation. Use the following commands for silent installation (replace `<version>` with the exact version number in the file you are using):

- With an `.exe` file:
`StoneGate_IPsec_VPN_<version>.exe /s /v"/qn"`
- With the `.msi` file:
`msiexec /i StoneGate_IPsec_VPN.msi /quiet.`

User Authentication

VPN client users must authenticate themselves before they can connect to a gateway. You can select different authentication method(s) for each gateway. If several authentication methods are allowed for a user, the user can select between the methods in the VPN client.

There are three basic authentication schemes: user name and password, certificate, or smartcard. Different methods may be used on the same gateway simultaneously.

The user name and password method supports integration with external RADIUS or TACACS+ authentication servers, allowing various authentication schemes such as RSA SecurID cards, Active Directory/IAS authentication, or StoneGate SSL VPN's internal authentication methods.

For a detailed overview to user authentication, see the *StoneGate Firewall/VPN Reference Guide*. For step-by-step configuration instructions, see the *Management Client Online Help* or the *StoneGate Administrator's Guide*.

Related Tasks

- ▶ [Using Certificates with the VPN Client](#) (page 21)

IP Addressing

The primary access method for production use is the Virtual Adapter feature, which allows the VPN clients to have a second, virtual IP address that is independent of the client's address in the local network. The virtual IP address is only used in communications through the VPN tunnels. The IP address and related network settings are assigned by your organization's DHCP server that the client contacts through the gateway. For one-way access without DNS resolving, the VPN gateway can alternatively be set up to apply NAT to translate the VPN clients' connections. This method is mainly meant for testing purposes.

The VPN gateway specifies the destination IP addresses for traffic that the VPN clients send into the VPN tunnel. The IP addresses are configured as Site elements for each Gateway in the Management Client. When the Sites contain specific internal networks, the VPN clients receive a configuration for so called "split tunneling"; only the specified portion of traffic uses the VPN tunnel, and other connections use the local network as usual.

By default, when the VPN client's virtual adapter requests an IP address, it uses the MAC address of the physical interface (the interface that is used in the VPN connection). The virtual adapter MAC address can be changed through the VPN client's properties dialog (Advanced tab). The VPN client's MAC address also can be changed through the command line or in a script by running the `sgvmac.exe` command with the new MAC address as a parameter.

Example To change the MAC address to 06:05:04:03:02:01, enter

```
sgvmac.exe 06:05:04:03:02:01
```

Detailed step-by-step instructions for configuring the IP address distribution on the gateway can be found in the *Online Help* of the Management Client and the *Administrator's Guide* PDF, in the section called **Virtual Private Networks**.

Automatic Retry With Different Settings

Due to different port filtering and NAT arrangements, the VPN clients may need to use slightly different settings at different locations. The VPN client can work within the allowed settings to automatically try to connect with TCP tunneling enabled/disabled or using different port combinations if the automatic IKE retry option is active in the VPN client installation (Advanced tab in VPN Client Properties). The VPN client tries the settings one by one in the following order until the connection succeeds or all options are exhausted:

1. Enable/disable TCP tunneling (if allowed for the end-point on the gateway).
2. Enable/disable the option to use random local source ports on the client.
3. Use only destination port UDP/4500 (NAT-T port) for the gateway (instead of both port UDP/500 and UDP/4500).
4. Use a combination of random local source port and destination port UDP/4500 for the gateway.

Additionally, the VPN client can automatically react if a connection to port UDP/500 succeeds, but port UDP/4500 (NAT-T) is unavailable. In this situation, the VPN client tries the connection with TCP tunneling enabled/disabled (if allowed for the end-point on the gateway). If changing the TCP tunneling option does not help, the VPN client defaults to using destination port UDP/500 only.

The end-user is notified if the VPN client is unable to use one of the two necessary ports.

CHAPTER 4

CUSTOMIZING VPN CLIENT INSTALLATIONS

This section explains how you can customize the StoneGate IPsec VPN client installation package. It also explains how you can help the VPN client users to add the contact information of a new security gateway by providing the information in a file.

The following sections are included:

- ▶ [Configuration Overview](#) (page 18)
- ▶ [Saving Gateway Contact Information to a File](#) (page 18)
- ▶ [Customizing Installation Packages](#) (page 19)

Configuration Overview

Customizing the installation allows you to add information into the installation package and to install and update the VPN clients remotely.

1. Save the configuration of each gateway to a file as explained in [Exporting Gateway Contact Information](#).
2. Create a customized installation package as explained in [Creating a Transform File](#) (page 19).
3. Use the custom package to install the clients locally or remotely as explained in [Installing with a Transform File](#) (page 19).

Saving Gateway Contact Information to a File

You can save the contact information for security gateways in a file, which can then be added into a customized installation package or copied to the end-user computers that already have a VPN client installed. The gateway contact information allows the end-users to connect to new gateways without the need to add the security gateway address manually and verify the gateway's certificate fingerprint.

Exporting Gateway Contact Information

You must first use the Management Client to export the contact information of each security gateway to which the VPN client users connect. The contact information is always gateway-specific.

▼ To export the gateway contact information

1. Select **Configuration**→**Configuration**→**VPN** from the menu in the Management Client. The VPN Configuration view opens.
2. Select **Gateways** in the element tree.
3. Right-click the internal Gateway element for which you want to save the configuration and select **Tools**→**Save Gateway Contact Information**. The Save Contact Information dialog opens.
4. Browse to the folder where you want to save the contact information file.
5. Enter a file name and click **Save**. The contact information of the selected security gateway is saved in an `.xml` file.

Repeat the steps as necessary to save the contact information of other security gateways and distribute the contact information file(s) to the end-users for manual copying or add the file(s) to a customized installation package.

Copying Gateway Contact Information Files Manually

To add the contact information of new gateways to an existing VPN client installation, the gateway contact information file(s) can be copied to the client machines. Provide the file(s) to the VPN client end-users and instruct them to copy the file(s) to the correct location.

▼ To copy the gateway contact information files

- ↳ Copy the security gateway's contact information .xml file to the %ALLUSERSPROFILE%\Application Data\Stonesoft\StoneGate IPsec VPN\gateway_info directory on the client machine.
 - In Windows Vista and Windows 7, the directory is
<system_drive>\ProgramData\Stonesoft\StoneGate IPsec VPN\gateway_info.
 - In Windows XP, the directory is
<system drive>\Documents and Settings\All Users\Application Data\Stonesoft\StoneGate IPsec VPN\gateway_info.



Note – Application Data is a hidden folder.

Customizing Installation Packages

The VPN client installation package can be customized by creating a MSI (Microsoft Installer) transform file from the StoneGate_IPsec_VPN.msi file. The contact information of the security gateways is added to the transform file. To customize the installation package, you must have a basic knowledge of MSI transforms and know how they can be applied to installation packages.

Creating a Transform File

You can create a customized installation package from the StoneGate_IPsec_VPN.msi file with any Windows installation package editor (for example, with Orca). A how-to document that describes how you can customize the installation package with Orca is available at the Stonesoft website at <http://www.stonesoft.com/support/>.

Installing with a Transform File

You can use an .mst transform file that you have created together with the StoneGate_IPsec_VPN.msi file to install the IPsec VPN client either remotely or locally on the command line of the client machine. If you want the end-users to install the IPsec VPN client on the command line, provide the transform file and the gateway contact information file(s) to the end-users and instruct them how to proceed with the installation.

▼ To install IPsec VPN clients with a transform file

1. Copy the transform file to the same directory as the StoneGate_IPsec_VPN.msi file.
2. Create the path All Users\Application Data\Stonesoft\StoneGate IPsec VPN\gateway_info in the directory where you have the installation files.
3. Copy the exported gateway contact information file(s) to the gateway_info directory.

4. Start the installation:

- In a remote installation: Run the `StoneGate_IPsec_VPN.msi` file with the transform `.mst` file following the instructions of the software solution you are using.
- In a command line installation: If an earlier version of the StoneGate IPsec VPN is already installed on the machine, run the command
`msiexec /i StoneGate_IPsec_VPN.msi REINSTALLMODE=vomus REINSTALL=ALL TRANSFORMS=<transform_file>` on the command line.
Otherwise, use the command
`msiexec /i StoneGate_IPsec_VPN.msi TRANSFORMS=<transform_file>`.

CHAPTER 5

USING CERTIFICATES WITH THE VPN CLIENT

This chapter explains the use of certificates for authenticating VPN client users.

The following sections are included:

- ▶ [Overview to VPN Client Certificates](#) (page 22)
- ▶ [Using Internal Certificates](#) (page 23)
- ▶ [Using External Certificates](#) (page 25)
- ▶ [Certificate Expiration](#) (page 25)

Overview to VPN Client Certificates

StoneGate IPsec VPN client supports using certificates to authenticate VPN client users. In certificate-based authentication, a certificate request is first created. This also generates a private key for the certificate. The certificate cannot be used without the private key, which should always be protected by a passphrase to prevent unauthorized use of the certificate. The certificate request must be signed by a valid certificate authority (CA) to produce a valid certificate. For a gateway to accept the client certificate as a proof of identity, the gateway must be configured to trust the CA that has signed the certificates of the VPN clients.

Supported Certificate Authentication Schemes

There are four general options for setting up certificates required for authentication:

- You can create certificates using StoneGate's internal tools by creating a certificate request in the VPN client and signing the request through the Management Client using the Management Server's internal VPN CA.
- You can create certificates externally and import them (with their associated private key) into the VPN client.
- The certificate and its private key can be stored on a smartcard. In this case, the VPN client calls the external smartcard software on the computer and there is no need for any configuration steps on the VPN client; the smartcard is ready to use as such and is available when inserted if the smartcard reader is correctly configured in Windows.
- If there are certificates that can be used for authentication in the Microsoft Certificates Store on the local machine (in the **Certificates**→**Personal** folder), the certificates are automatically available in the VPN client.

When the certificate request is generated in the VPN client, the resulting certificate is called an *Internal Certificate* in the VPN client. When the certificate request is created using other tools, the certificate is called an *External Certificate* in the VPN client.

User Identity

Certificates are a proof of the certificate holder's identity. The exact form of the identity used can vary. There are two fields in internal certificates that can be used for authentication in client-to-gateway VPNs:

- **Subject Name** field contains a *Distinguished Name* (DN) that can consist of multiple items such as *Common Name* (CN), *Organization* (O), *Country* (C), and *E-mail Address* (E).
- **Subject Alternative Name** field usually contains the VPN Client user's e-mail address. Some client certificates do not have a Subject Alternative Name. This field is used in authentication if it is available in the client certificate.

Depending on the certificate, a VPN client user can authenticate to a gateway either with an e-mail address, a subject name, a DNS name, or an IP address. The user can change their user ID type in the VPN client (except for certificates stored on smartcards or in the Microsoft Certificates Store). The certificate information is matched against details defined in the User elements in the Management Client or in an external LDAP database. For more information, see the *IPsec VPN Client User's Guide*.

Using Internal Certificates

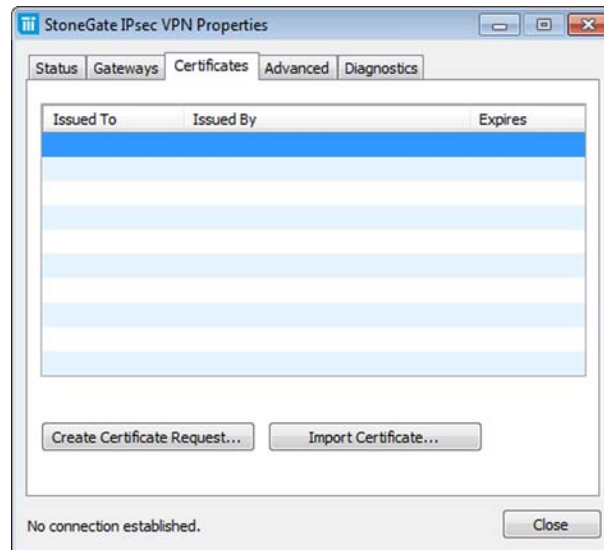
The VPN client has tools for creating a certificate request (and the associated private key). When the certificate request is ready, the end-user must deliver the certificate request to a trusted CA for signing. The request can be signed using StoneGate Management Server's internal VPN CA or some other certificate authority. The signed certificate is sent back to the end-user, who must import it in the VPN client. To use the certificate for authentication, the end-user must enter the passphrase that protects the private key (selected by the end-user when creating a certificate request or when they decide to change the key) each time.

This section provides an overview to the topic. For detailed step-by-step instructions for these tasks, see the *VPN Client User's Guide*.

Creating Certificate Requests

The certificate-related actions are available on the **Certificates** tab of the StoneGate IPsec VPN Properties dialog. To open the dialog, double-click the IPsec VPN client icon in the Windows Task Bar.

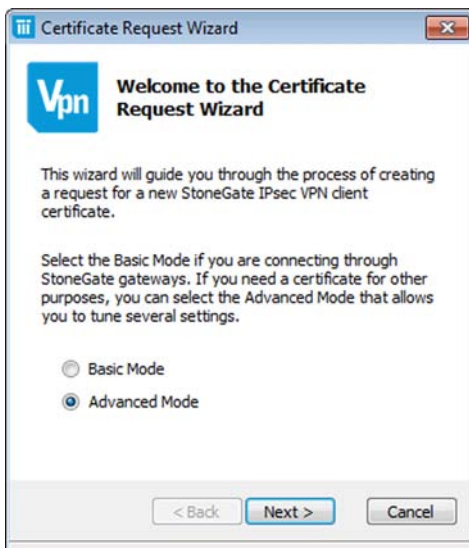
Illustration 5.1 StoneGate IPsec VPN Client Properties Dialog - Certificates Tab



There are two kinds of certificate requests in the VPN client:

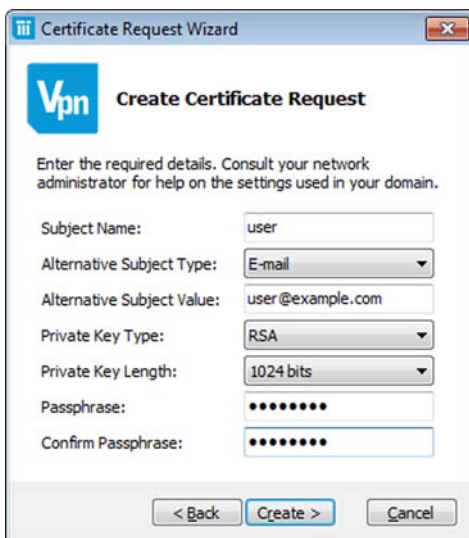
- A basic certificate request contains the information required for certificate requests that are signed using the Management Server's internal VPN CA. For information on creating basic certificate requests, see the *IPsec VPN Client User's Guide*.
- An advanced certificate request offers more options than a basic certificate request for defining the properties of the certificate request and the private key. The exact options to use depend on the capabilities of the CA and the requirements and preferences of your organization.

Illustration 5.2 Selecting Between Basic and Advanced Mode



If you configured internal certificates as a gateway's authentication method, inform the end-users that they must create a certificate request in the VPN client. You must also provide them with the information they must enter and inform them which options they must select when they create the certificate request (especially if generating advanced certificate requests). The certificate request is saved as a `.csr` file.

Illustration 5.3 Options for Advanced Certificate Requests



Signing Certificate Requests

Certificate requests generated in the VPN client are signed either by the Management Server's internal VPN CA or by a third party CA. The CA that signs the VPN client certificate must be defined as a trusted VPN certificate authority in the system. To sign a certificate request internally, use the certificate signing tool in the VPN Configuration view (see the section called **Virtual Private Networks** in the *Administrator's Guide* or the *Online Help* of the Management Client for more information).

Using External Certificates

You may prefer to use external tools to create the certificate request instead of having it created in the VPN client (especially if the end-users already have suitable signed certificates and private keys that can be utilized).

If end-users have certificates that can be used for authentication in the Microsoft Certificates Store on their local machines, the certificates are automatically available to the end-users in the VPN client. In all other cases, the end-users must import both the certificate and the private key in the VPN client. The certificates and the private keys can be imported either as a single PKCS # 12 file or as two separate files. You must inform the end-users which options they must select when importing the external certificates. See the *IPsec VPN Client User's Guide* for more information.

Only certificates signed by the Management Server's internal VPN Certificate Authority are trusted by default. Other certificate signers must be specifically configured as trusted on the gateway to allow the end-users to authenticate (see the section called **Virtual Private Networks** in the *Administrator's Guide* or the *Online Help* of the Management Client for more information).

Certificate Expiration

For added security, certificates have an expiration date. Certificates signed by the Management Server's internal VPN CA are valid for three years from their creation. It is not possible to extend the validity of the certificates. To continue using certificate authentication for more than three years on the same installation, you must create a new certificate.

The CA also has an expiration date. The Management Server's internal VPN CA is valid for ten years. A new CA is automatically created six months before the expiration, and you must create new certificates for the clients with the new CA.

CHAPTER 6

LOGS AND DIAGNOSTICS

This section explains how you can use logs and diagnostics in the VPN client to analyze VPN connections.

The following sections are included:

- ▶ [Overview to Logs and Diagnostics](#) (page 28)
- ▶ [Collecting a Diagnostics File](#) (page 31)
- ▶ [Capturing Network Traffic](#) (page 30)
- ▶ [Reading Logs](#) (page 29)

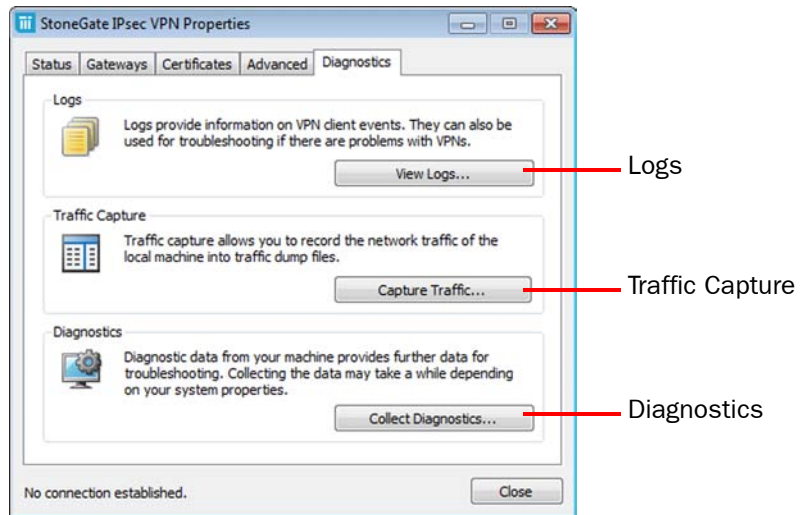
Overview to Logs and Diagnostics

Logs and diagnostics are a useful resource for administrators and Stonesoft's technical support personnel when troubleshooting VPNs. The most convenient way to gather information from end-user computers is to instruct them to collect a diagnostics file (which also includes the logs). You can also view the logs separately when you are troubleshooting a VPN client locally.

▼ To access logs and diagnostics

1. Double-click the IPsec VPN client icon in the Windows Task Bar.
2. Switch to the **Diagnostics** tab.

Illustration 6.1 StoneGate IPsec VPN Properties - Diagnostics Tab



Reading Logs

The VPN client maintains its own log of events related to its operation. You can view this log directly in the VPN client. This log is also included in the diagnostics file. Depending on the issue you are troubleshooting, there may be additional relevant logs in the Windows logs.

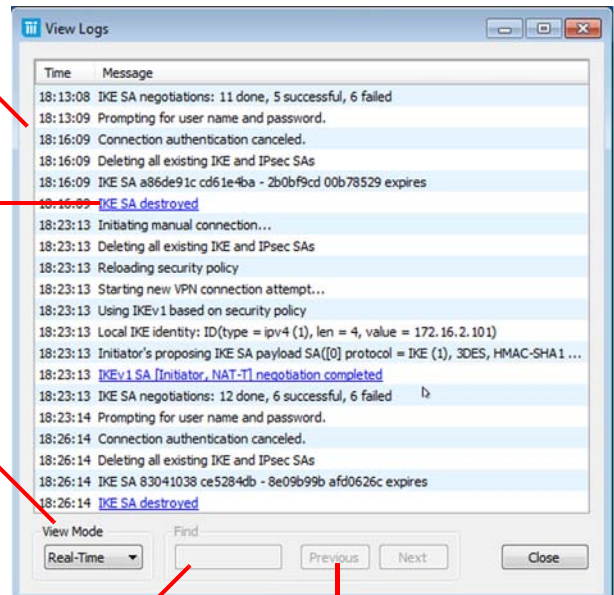
Illustration 6.2 View Logs Dialog

You can select all entries or copy information to the clipboard in the right-click menu.

Click links in the log entries to view more detailed information.

Different **View Modes** allow you to view logs in real-time, from a certain time period, all stored logs, or the most recent logs with detailed information.

To look for specific log entries, enter a keyword in the **Find** field (not available in all view modes).



Click **Previous** or **Next** to find more occurrences of the keyword.

Capturing Network Traffic

Traffic captures record the network traffic of the local machine to assist in troubleshooting when network problems are suspected. The recorded traffic is saved on the local machine in the traffic dump files `adapter.pcap` and `protocol.pcap`. These files can be opened with any program that can display `.pcap` files.

You can customize how traffic is captured by modifying values for the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\sgravn\Parameters` on the local machine.

Table 6.1 Registry Values for Customizing Traffic Captures

Name	Type	Description
CaptureMaxSize	REG_DWORD	The maximum traffic capture file size in megabytes. If not defined, the maximum size is 10 MB.
CaptureDirectory	REG_SZ	The default directory in which traffic capture files are stored.
CaptureSnapLength	REG_DWORD	The number of bytes captured from each network packet. If not defined, the whole packet is captured.
CaptureSystemStartup	REG_DWORD	If set to '1', the traffic capture is started immediately when the operating system starts.

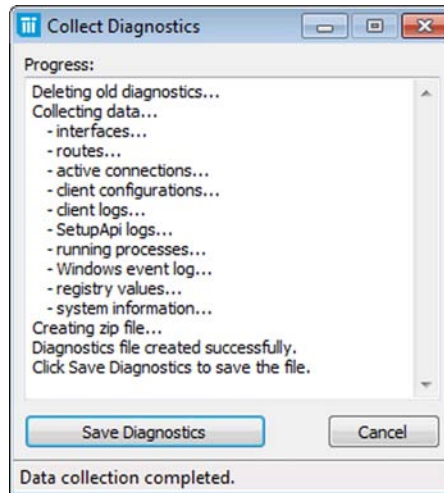
Collecting a Diagnostics File

Diagnostics collect together all relevant information on how the VPN client operates, including logs, network interface status, routes, and active connections. If you need logs from end-users for troubleshooting purposes, instruct the users to collect the diagnostics. The *VPN Client User's Guide* contains detailed step-by-step instructions for collecting diagnostics.



Note – Collecting diagnostic data will take some time.

Illustration 6.3 Collect Diagnostics Dialog



The diagnostics are collected in a single archive for easy transfer. The file does not contain secret information such as passwords, but it does contain information related to the VPN configuration such as internal IP addresses. Depending on your operating environment, the file may need to be handled securely.

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