Kerio VPNClient

User Guide

Kerio Technologies

This guide provides detailed description on *Kerio VPN Client*, version *6.5.0*. All additional modifications and updates reserved.

This product includes software developed by the *OpenSSL Project* for use in the *OpenSSL Toolkit* (http://www.openssl.org/). *OpenSSL Toolkit* is a toolkit implementing the *Secure Sockets Layer* (SSL v2/v3) and *Transport Layer Security* (TLS v1) open-source protocols.

Contents

Chapter 1

Introduction

Kerio VPN Client is an application which enables connection from individual hosts (clients) to a remote private network via the Internet using an encrypted channel. These clients can access the private networks as if they were connected to them physically.

Kerio VPN Client is connected to the VPN server in *Kerio WinRoute Firewall* (*WinRoute*). *WinRoute* user accounts are used for authentication of clients.

Kerio VPN Client supports persistent connections. The connection is recovered automatically.

Usage of *Kerio VPN Client* is extremely easy. Only a DNS name or IP address of the server to which the connection is directed, as well as a password and username are required. Other settings will be performed automatically by *Kerio VPN Client*.

Kerio VPN Client supports user profiles. Each user of a host where *Kerio VPN Client* is installed can use a personal VPN connection.

1.1 Installation

Hardware requirements

Kerio VPN Client does not require any special hardware configuration. Configuration of the computer should meet requirements for the corresponding operating system.

Supported operating systems

Kerio VPN Client is distributed in two versions: a version for 32-bit platforms and a version for 64-bit platforms.

The 32-bit edition (the "*win32*" installation package) supports the following operating systems:

- Windows 2000
- Windows XP (32 bit)
- Windows Server 2003 (32 bit)
- Windows Vista (32 bit)
- Windows Server 2008 (32 bit)

Older versions of Windows operating systems are not supported.

The 64-bit edition (the "*win64*" installation package) supports the following operating systems:

- Windows XP (64 bit)
- Windows Server 2003 (64 bit)
- Windows Vista (64 bit)
- Windows Server 2008 (32 bit)

Conflicting software

Kerio VPN Client cannot be run on hosts where *Kerio WinRoute Firewall* is installed, otherwise *Kerio VPN Client* conflicts with *WinRoute* and *Kerio VPN Client* is not started.

Setup

To start the installation, run the installation archive for the corresponding platform (e.g. `kerio-kvc-1.2.0-511-win32.exe`). You can select a target path.

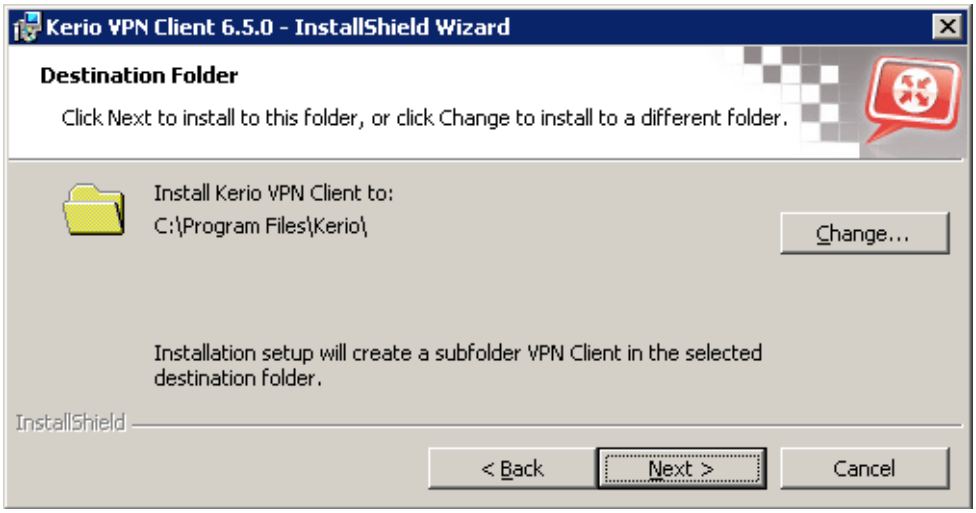

Figure 1.1 The destination directory for the installation can be selected.

The `C:\Program Files\Kerio` directory is set by default (if any Kerio Technologies product is already installed at the host, its directory is automatically detected and selected as the installation directory).

The *Kerio VPN* low-level driver (`kvpndrv.sys`) will be deployed and a special network interface *Kerio VPN* will be created during the installation.

Under usual circumstances, a reboot of the computer is not required after the installation (a restart may be required if the installation program rewrites shared files which are currently in use).

Files location

Executable files of the application are installed into the directory selected during the installation. Shared files and the low-level driver are installed into the corresponding system directories (`C:\WINNT\system32` and `C:\WINNT\system32\drivers`, or `C:\WINDOWS\system32` and `C:\WINDOWS\system32\drivers` by default).

The data file (i.e. the file which contains information about defined connections and other configuration data) is saved into the `Application Data\Kerio\VPNClient` subdirectory of the user account under which *Kerio VPN Client* is running.

1.2 Licensing Policy

Kerio VPN Client is provided as an accessory to *Kerio WinRoute Firewall*. *Kerio VPN Client* does not require any special license.

However, connected VPN clients are included in the total count of users (computers) during license checks in *Kerio WinRoute Firewall*. This implies that the minimal number of licensed *Kerio WinRoute Firewall* users needed for the particular server is the sum of hosts in LAN and number of VPN clients connected to the server at a moment.

Note: For detailed information on *Kerio WinRoute Firewall* licensing policy, refer to the corresponding sections of the *Kerio WinRoute Firewall — Administrator's Guide* document.

1.3 How Kerio VPN Client works

Kerio VPN Client enables connection from a client's host to a remote private network via an encrypted communication channel (in the operating system, this channel is represented by a virtual network interface — *Kerio VPN Adapter*).

The client's operating system must be aware of routes to individual subnets of a corresponding remote private network. For this purpose, *Kerio VPN Client* performs automatic update of the client's routing table (it adds new routes directed to remote subnets). These automatic updates are performed:

- after each change in network configuration at the server,
- every 1 minute.

During these updates, routes to all remote subnets (or a route to other networks defined in the VPN server configuration) are added except those IP addresses of which collide with IP addresses of the local network to which the client is connected. *Kerio VPN Client* never changes the default route (i.e. configuration of the default gateway). The encrypted traffic channel is used only for connection to a remote private network. For connection to the Internet, clients use their current Internet connections.

Chapter 2

Deployment and usage of Kerio VPN Client

Run *Kerio VPN Client* from the *Start* → *Program* → *Kerio* → *VPN Client* menu. Two modes of *Kerio VPN Client* are available:

Simple mode

This mode is recommended if *Kerio VPN Client* is used to connect only to one VPN server (i.e. if only one remote network requires access remotely) and if we are not interested in detailed information about the connection process.

Advanced mode

In advanced mode, login data for multiple servers can be stored and later used for their connection (*Kerio VPN Client* can be connected to multiple VPN servers at a moment). This mode is recommended if you intend to connect remotely to multiple private networks.
A detailed log of *Kerio VPN Client* activities is also available in this mode.

The simple mode is used by default after the first startup of *Kerio VPN Client*. Upon a startup, *Kerio VPN Client* is started in the mode used recently.

2.1 Taskbar icon

If *Kerio VPN Client* is running, an icon displaying its current status is available in the notification area of the Windows taskbar.

- The following icon represents a disconnected *Kerio VPN Client*:

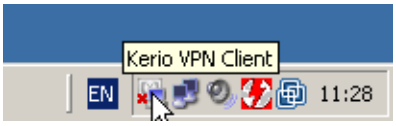

Figure 2.1 The Kerio VPN Client icon for the off status

- The following icon represents a connected *Kerio VPN Client*:

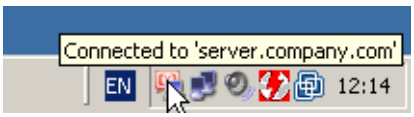

Figure 2.2 The Kerio VPN Client icon for the on status

If a single connection is active, name of the corresponding server is displayed in the hint box (upon hovering the icon by the mouse pointer). If two or more connections are active (in advanced mode — see chapter 2.3), only their number is displayed.

Information about connection/disconnection

Immediately after a successful connection, information about a server to which *Kerio VPN Client* is connected is displayed over the notification area.

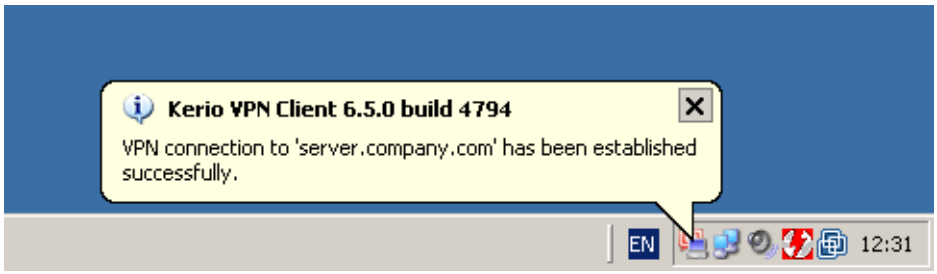

Figure 2.3 A bubble informing that the connection has been established

Information about a disconnection is displayed immediately after a disconnection from a corresponding server.

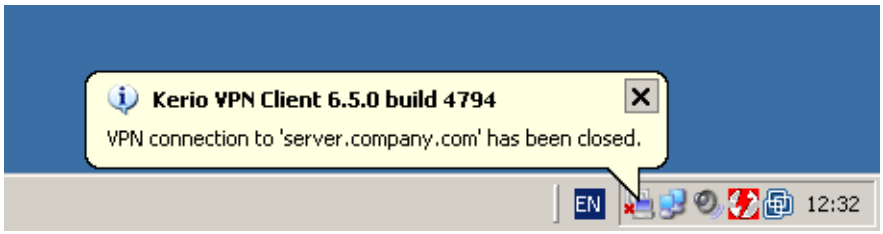

Figure 2.4 A bubble informing that the connection was closed

Functions available through the taskbar icon

Right-click the icon to open a context menu providing the following options:

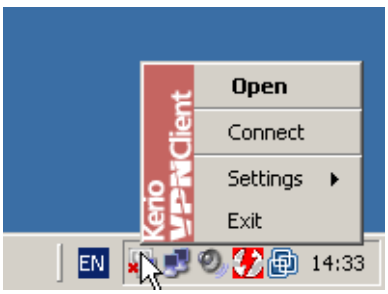

Figure 2.5 Context menu (simple mode)

- *Open* — this option opens the main dialog box of *Kerio VPN Client* (according to the mode used for the last connection). If the main window is already open, the option is not available.

- *Disconnect* — this option closes the current connection to a VPN server.

  In the advanced mode (see chapter 2.3), *Kerio VPN Client* can be connected to multiple servers at one moment. In such cases, options for disconnection of individual servers are provided in the context menu available through the taskbar icon.

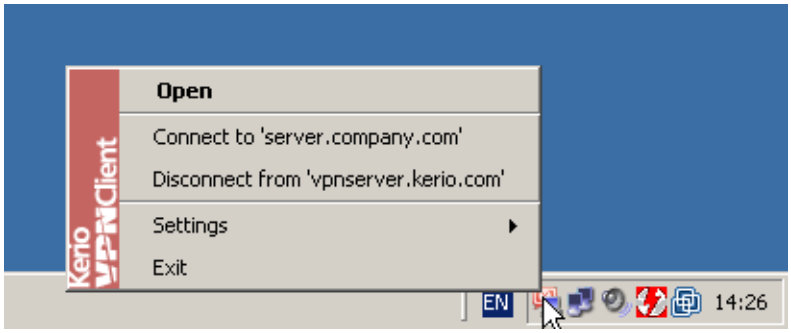

Figure 2.6 Context menu (advanced mode)

- *Settings* — configuration of some *Kerio VPN Client's* parameters (see below).

- *Exit* — use this option to close *Kerio VPN Client*.

Settings

Select *Settings* in the context menu to open a menu where localization (language) of *Kerio VPN Client* user interface can be selected and bubble messages settings can be changed.

The menu provides all localizations available at the moment. The latest version of the *Kerio VPN Client* is available in English, Spanish, Czech, Slovak and Russian.

When a language is changed, the user interface is switched to the language version immediately. The *Automatically* option is set as default and it corresponds with the national environment settings set in the operating system (*Control panel / Regional and Language Options*).

English is used as the basic (built-in) language. Correspondent definition files (files with the `.qm` extension in the `Translations` subdirectory in the *Kerio VPN Client's* installation directory) are required for other localizations.

Use the *Enable bubble messages* option to enable/disable pop-up bubble messages when VPN connection is established/closed. These messages are optional (the information can be easily found out in the *Kerio VPN Client's* main window).

2.2 Kerio VPN Client in the simple mode

In the simple mode, the main dialog box of the *Kerio VPN Client* provides only the dialog for connection to a server.

Figure 2.7 The main window in the simple mode

Specify the *Server*, *Username* and *Password* entries with the server name (or IP address), username and password.

Check the *Save password* option to make *Kerio VPN Client* remember the password. For following connections, this parameter will not be required (the password is saved into the profile of the user under whose account *Kerio VPN Client* is currently running). It is not recommended to save the password unless you are sure that no undesirable user can misuse these settings.

The *Persistent connection* option enables/disables persistent connection mode. Under the persistent connection mode, connection is recovered automatically after an unexpected disconnection (e.g. Internet connection dropout). If the *Auto connect* option is enabled as well, the persistent connection will be re-established upon a new user login/logout (or upon a system restart).

For automatic connection recovery, *Kerio VPN Client* needs to know the corresponding user password — therefore, the option is available only if the *Save password* is enabled.

Click *Connect* to establish specified connection — i.e. to create an encrypted traffic channel between the client and the remote private network (the button is available only if the connection has not been established yet). During the connection establishment, *Kerio VPN Client*

performs check of the SSL certificate of the corresponding WWW server (for details, refer to chapter 2.4).

The dialog box will be hidden immediately after the connection is established successfully. Connection status information will be provided through the taskbar icon (see chapter 2.1).

Use the *Disconnect* button to close connection to the VPN server. After disconnection, the default connection dialog will be available again.

Use the *To advanced mode* button to switch *Kerio VPN Client* to the advanced mode. The modes can be switched only if *Kerio VPN Client* is disconnected. For details on the advanced mode, refer to chapter 2.3.

Notes:

1. No login data is remembered for the new mode.

2. Closing this main window does not close *Kerio VPN Client*! *Kerio VPN Client* can be exited by using the *Exit* option in the context menu available through the taskbar icon (see chapter 2.1).

2.3 Kerio VPN Client in the advanced mode

In the advanced mode, the top division of the main dialog window of *Kerio VPN Client* provides a list of saved connections (items including login data for individual servers). Optionally, the bottom part of the main window provides log information about the program events.

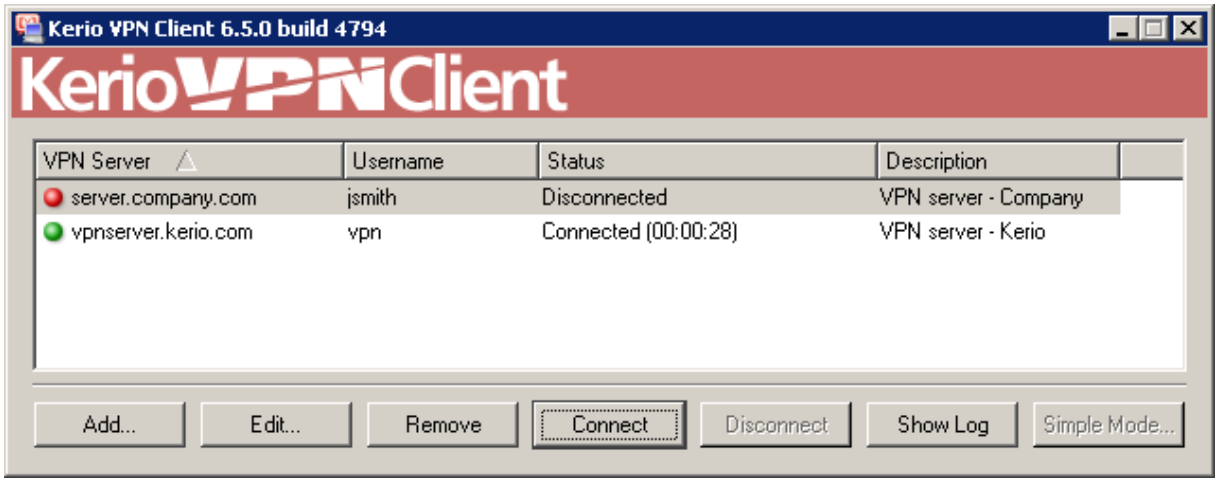

Figure 2.8 The main window in the advanced mode

The following status types can be reported in the *Status* column:

- *Disconnected* — the server is disconnected,
- *Connecting...* — connection is just being established,

- *Connected (hh:mm:ss)* — the server is connected (information about the time when the connection was initiated is provided in parenthesis),
- *Error (nnn): Text* — error detected when establishing the connection (information about the error number is provided in parenthesis followed by a description of the error)

The *Add...* button can be used to create a new VPN connection.

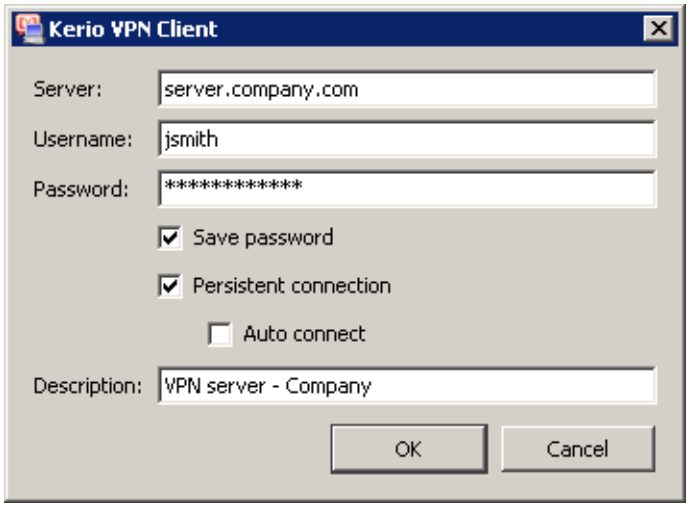

Figure 2.9 Advanced mode — connection parameters

- *Server* — DNS name or IP address of the server to which *Kerio VPN Client* is connecting.
- *Username* — username used for authentication at the VPN server.
- *Password* — password used for authentication at the VPN server.
- *Save password* — if this option is enabled, the password for the user profile will be saved.

  It is not recommended to save the password unless you are sure that no undesirable user can misuse these settings to connect to the remote private network.
- *Persistent connection* — this option enables/disables persistent connection. Under the persistent connection mode, connection is recovered automatically after an unexpected disconnection (e.g. Internet connection dropout), after a new login (after a user logout or operating system reboot).
- *Auto connect* — persistent connection will be recovered automatically upon any connection of the user (after disconnection, restart or computer shut-down).

Use the *Edit...* button to open the dialog where parameters of a selected connection can be edited (this dialog is identical with the dialog used for creation of a new connection). The

Remove button can be used to remove a selected connection. Both buttons are available only if a selected connection is currently *Disconnected*.

Click the *Connect/Disconnect* buttons to connect to or disconnect from the selected server (only one of these buttons is available — this depends on the status of a selected connection).

Clicking the *To simple mode* button switches *Kerio VPN Client* to the simple mode (refer to chapter 2.2). All connections must be currently disconnected, otherwise switching to the other mode is not possible and an error is reported.

Notes:

1. No login data is remembered for the new mode.

2. Closing this main window does not close *Kerio VPN Client*! *Kerio VPN Client* can be exited by using the *Exit* option in the context menu available through the taskbar icon (see chapter 2.1).

Kerio VPN Client event log

The *Show log* option displays the bottom part of the log window providing detailed information about *Kerio VPN Client* events.

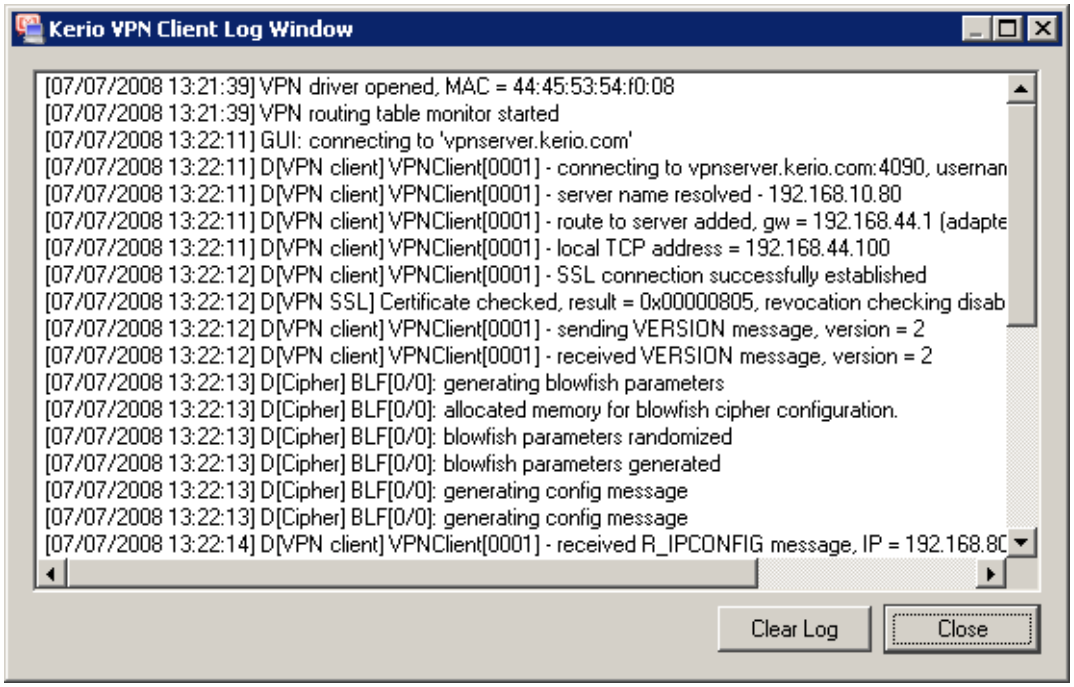

Figure 2.10 Kerio VPN Client's log

All significant events are logged, such as *Kerio VPN Client* initialization, connection establishment, authentication, exchange of routing information, detected errors, etc. Each line includes information associated with one event. Each line is started with a time stamp (date and time when the event was initialized). Time stamps are followed by corresponding descriptions.

The log is kept in the buffer only, it is not saved in any file. This means that any information is cleared and cannot be recovered when the *Clear Log* button is clicked or when *Kerio VPN Client* is closed.

Information provided in the log can be used for testing and debugging as well as for troubleshooting with the Kerio Technologies technical support.

HINT: It is possible to select a part of the log text with the mouse pointer and use the context menu (by clicking the right mouse button) to copy the selection to the clipboard. Using the context menu, whole log can be selected as well by choosing the appropriate option. And, of course, standard *Ctrl-C* and *Ctrl-A* hot keys can be used for copying the text in the clipboard.

2.4 Verification of the VPN server's SSL Certificate

Whenever a connection is being established, *Kerio VPN Client* performs verification of the VPN server's SSL certificate (the same verification is performed by web browsers when attempting to use the *HTTPS* protocol). If any certificate-related problems are detected, a warning appears inquiring whether the user finds the VPN server trustworthy and whether the connection to the server should be allowed.

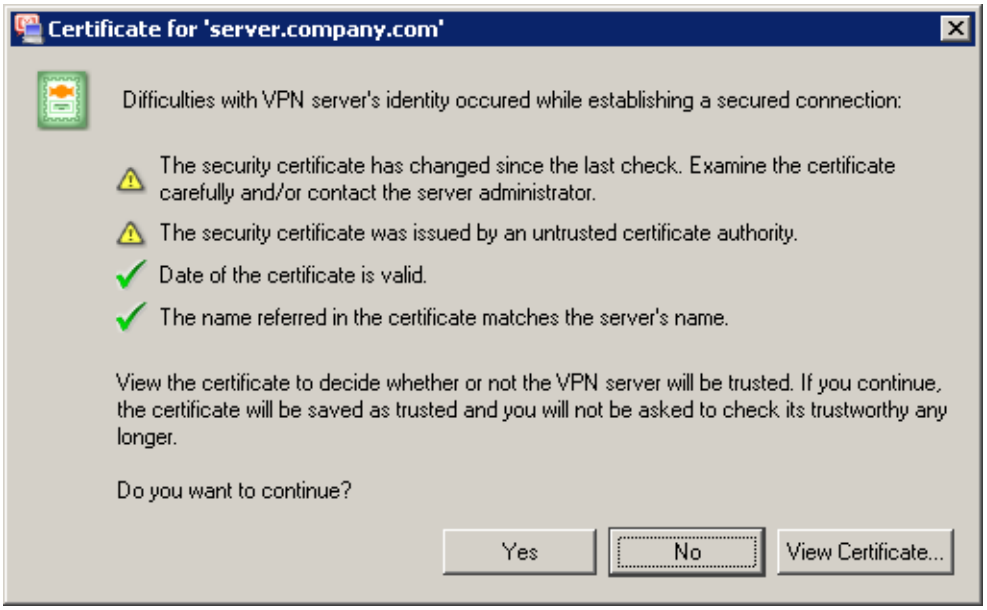

Figure 2.11 A dialog informing about detected problems with the VPN server's certificate

Click *View Certificate* to view detailed information about the VPN server's certificate (issuer, server for which it was issued, expiration date, etc.). According to the information provided, the user can decide whether to handle the server as trustworthy and allow the connection or to forbid it.

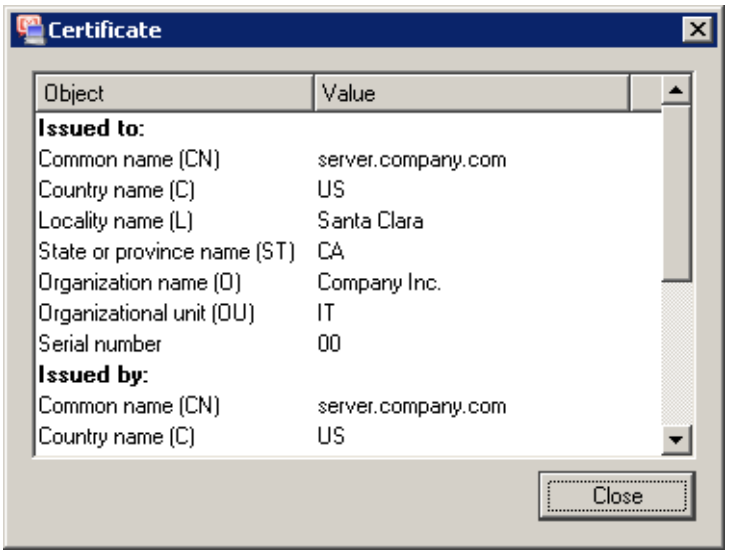

Figure 2.12 Viewing details of VPN server's certificate

If *Yes* is clicked, *Kerio VPN Client* considers the VPN server as trustworthy. The certificate is saved and no warning is displayed upon next connections to the server.

Note: For more information on VPN servers' certificates, see the *Kerio WinRoute Firewall — Administrator's Guide*.

Common certificate-related problems and their solutions

Certificate-related problems are often caused by one of the following issues:

The certificate was issued by an untrustworthy authority

Kerio VPN Client verifies whether a certificate was issued by an authority included in the list of trustworthy certificate publishers stored in the operating system (the *Certificates* section of the *Content* tab under *Control Panel / Internet Options*). Since a certificate is imported, any certificates issued by the same authority will be accepted automatically (unless any problem is detected).

Note: When the *Generate Certificate* option is used, a *self-signed* certificate is created — the publisher of the certificate is identical with its subject. This type of certificate does not guarantee the highest security and it cannot be accepted automatically at the client's side. To provide full security, it is necessary to use a certificate issued by a trustworthy certification authority. For details, refer to the *Kerio WinRoute Firewall* manual.

The name referred in the certificate does not match with the server's name

Name of the server specified in the certificate does not correspond with the server name which *Kerio VPN Client* is connecting to. This problem might occur when the server uses an invalid certificate or when the server name has changed. However, it may also point at an intrusion attempt (a false DNS record with an invalid IP address is used). It is recommended to discuss this issue with the administrator of the corresponding VPN server.

Note: Certificates can be issued only for servers' DNS names, not for IP addresses.

Date of the certificate is not valid

For security reasons, validity of SSL certificates is limited by time. If an invalid date is reported, it means that the certificate's validity has already expired and it is necessary to update it. Contact the VPN server's administrator.

The security certificate has changed since the last check

When a user accepts connection to a VPN server, *Kerio VPN Client* saves the certificate of the server as trustworthy. For any later connections, *Kerio VPN Client* checks certificates with the saved one. If these certificates do not correspond, it might be caused by the fact that the certificate has been changed at the server (e.g. for expiration of the original certificate). However, this might also point at an intrusion attempt (another server using a different certificate). Contact the VPN server's administrator.

2.5 Mode selection and persistent connection

Upon each Windows startup, *Kerio VPN Client* attempts to recover persistent connections. The following rules are applied:

- If *Kerio VPN Client* was closed in the simple mode, it will attempt to open the connection defined in the simple mode dialog window (if the *Persistent connection* and *Connect automatically* options are enabled — see chapter 2.2).
- If *Kerio VPN Client* was exited in the advanced mode, it will attempt to recover all VPN connections defined in the advanced mode dialog box for which the automatic persistent connection is enabled (see chapter 2.3).

If no automatic persistent connection is defined in a current mode, *Kerio VPN Client* will be closed (users can start it by hand).

This implies that it is quite important under which mode *Kerio VPN Client* is closed. Therefore, it is recommended to use only one mode.