# Kerio VPN Client

## User Guide

Kerio Technologies

© 2004 Kerio Technologies. All Rights Reserved.

Printing Date: June 1, 2004

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

### *System requirements*

Minimum hardware configuration for *Kerio VPN Client* installation:

- CPU Intel Pentium II or compatible; 300 MHz
- 128 MB RAM
- 3 MB free disc space (for the installation)

The following operating systems are supported:

- Windows 2000
- Windows XP
- Windows Server 2003

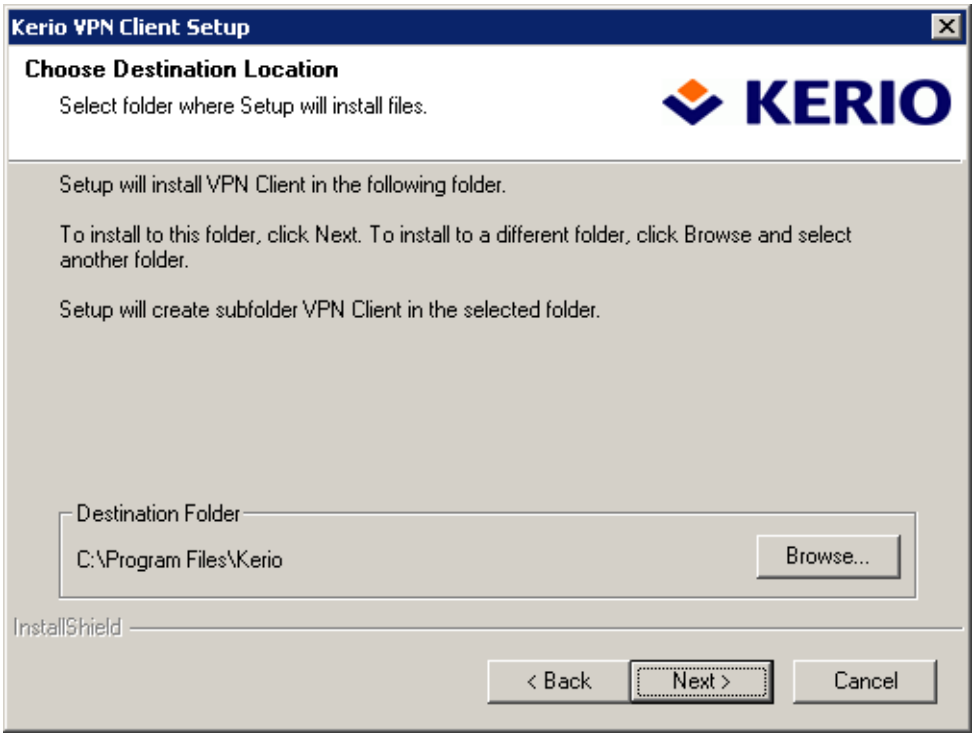
Earlier versions of Windows operating systems are not supported.

### *Conflicting software*

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

### *Setup*

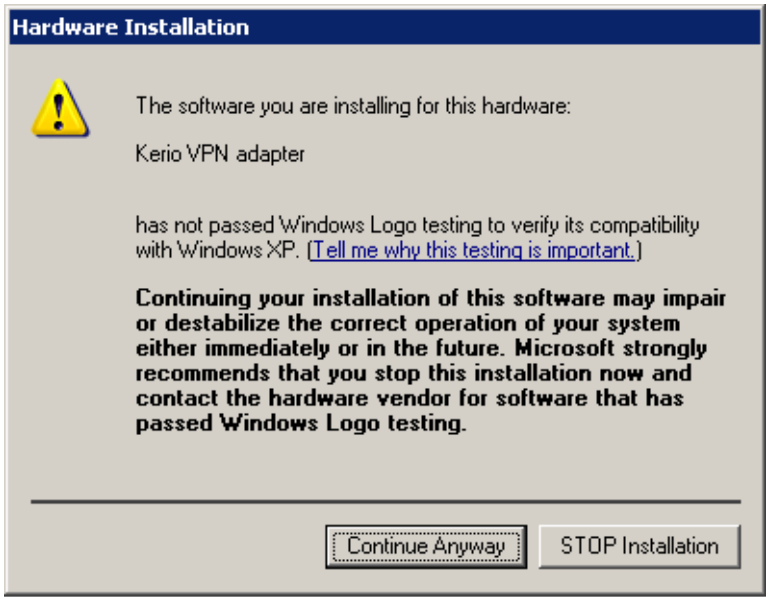
To run the installation, execute the corresponding installation archive (e.g. `kerio-vpnclient-1.0.0.exe`). The destination directory for the installation can be selected.




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.

*Note:* During the installation process of the *Kerio VPN* low-level driver, the operating system may display a warning message informing that compatibility of the driver with the Windows operating system cannot be verified (this depends on configuration of the operating system).




However, the driver provided within the *Kerio VPN* installation package has been tested on all supported Windows operating systems. Therefore, these operating systems may be considered as compatible.

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*.

*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*).

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,
- each 1 minute.

During these updates, routes to all remote subnets 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 conenction (*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*.

## 2.1 Systray icon

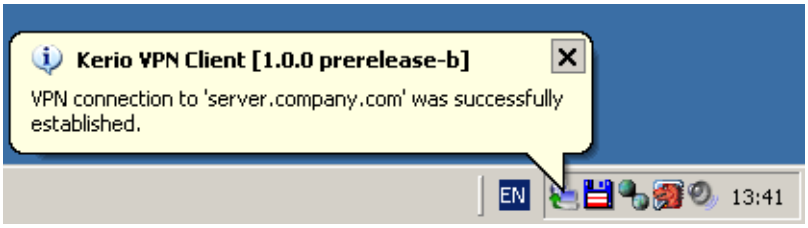
If *Kerio VPN Client* is running, an icon displaying its current status is available in the Systray.

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


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


### *Information about connection/disconnection*

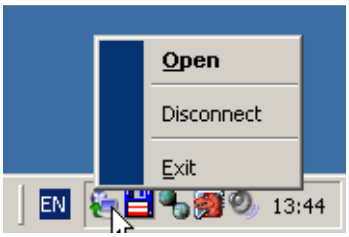
Immediately after a successful connection, information about a server to which *Kerio VPN Client* is connected is displayed over the Systray area.




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

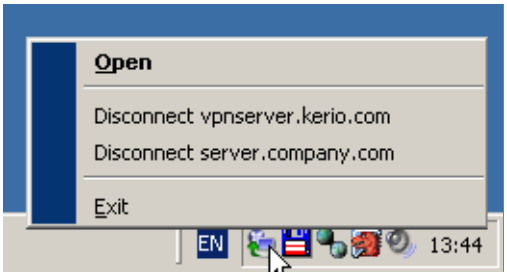

### *Functions available through Systray icon*

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




- *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. If *Kerio VPN Client* is currently not connected to any server, the option is not available.

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




## 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.


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 unex-

pected disconnection (e.g. Internet connection dropout), after a new login (after a user logout or operating system reboot). For automatic reconnections, *Kerio VPN Client* needs to know a corresponding user password —this implies that the option is available only if the password is saved (the *Save password* option must be 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). The dialog box will be hidden immediately after the connection is established successfully. Connection status information will be provided through the Systray icon (see chapter 2.1).

Use the *Disconnect* button to close connection to the VPN server. After disconnenction, 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 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 Systray icon (see chapter 2.1).

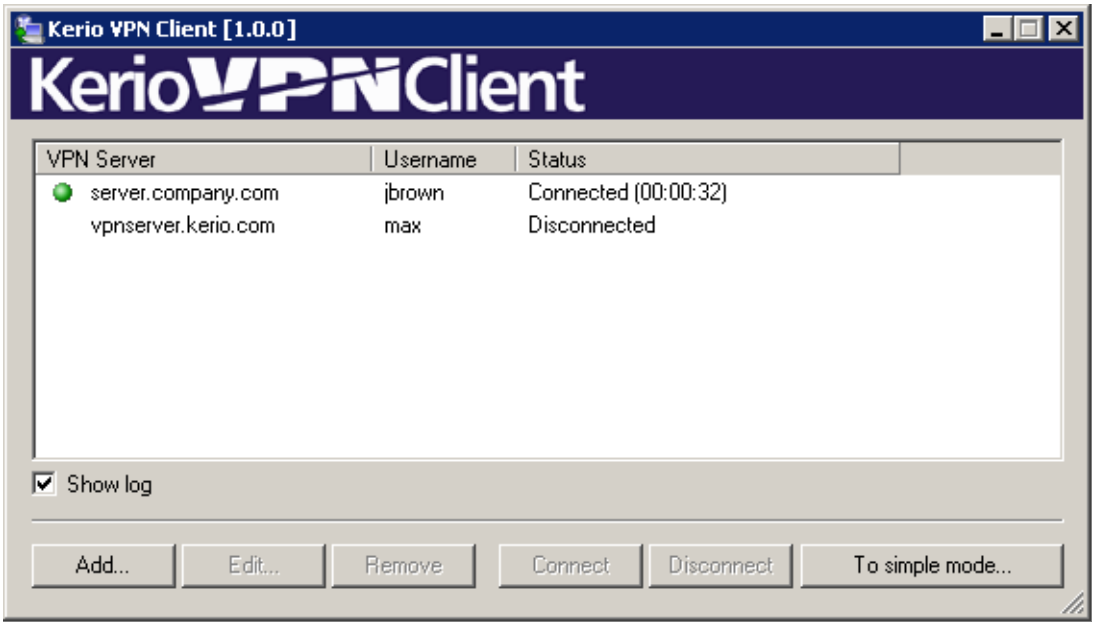
## 2.3 Kerio VPN Client in the advanced mode

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.

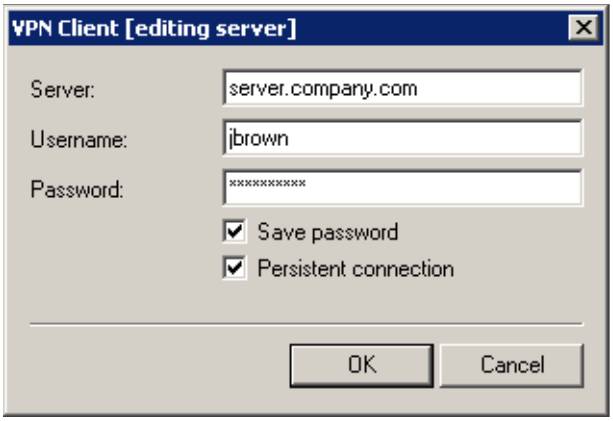
The top part of the window provides information about defined connections — the *VPN server* (name or IP address of the server), *Username* and *Status* (information about the current connection status) columns.

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* — error detected during the connection.




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




- *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 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).

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 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 Systray 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.

All significant events are logged, such as client initialization, connection establishment, authentication, exchange of routing information, detected errors, etc. Each line provides information on 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.

Log information can be used during testing and debugging as well as for better reference during troubleshooting with Kerio Technologies technical support.

## 2.4 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* otpion is 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 persistent connection is enabled (see chapter 2.3).

If no 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.