Kerio VPN Client

User Guide

Kerio Technologies

© 2012 Kerio Technologies s.r.o. All rights reserved.

This guide provides detailed description on *Kerio VPN Client*, version *7.2* for *Windows*. All additional modifications and updates reserved.

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.

Connection of the *Kerio VPN Client* to the VPN server is established via *Kerio Control*. *Kerio Control* user accounts are used for authentication of clients.

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

Users with administrator rights can also established so called persistent connections. Such connections are also automatically recovered upon each workstation reboot.

1.1 System requirements

Hardware requirements and supported operating systems

For up-to-date system requirements, please refer to:

http://www.kerio.com/control/technical-specifications

Conflicting software

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

1.2 Installation

To start the installation, run the installation archive for the corresponding platform (e.g. `kerio-control-vpnclient-7.2.0-2345-win32.exe`). You can select a target folder (installation path).

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

Installation creates the *Kerio Virtual Network Adapter* and a special network interface called *Kerio Virtual Network* in the *Windows* operating system. In addition to that, the *Kerio VPN Client Service* is installed and started immediately (it will be started automatically upon every startup of the operating system).

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

1.3 Licensing Policy

The *Kerio VPN Client* is provided as an accessory to *Kerio Control*. The *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 Control*. This implies that the minimal number of licensed *Kerio Control* 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 Control* licensing policy, refer to the corresponding sections of the *Kerio Control — Administrator's Guide* document.

1.4 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 Virtual Network*). The *Kerio Control* VPN server assigns to this interface an IP address belonging to the particular private network.

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

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.

VPN server also assigns the client an address of a primary and optionally also a secondary WINS server. These services enable to specify hosts in remote networks by their names and browse in *Microsoft Windows* network neighbourhood.

Note: The *Kerio VPN Client* does not allow opening of more than one concurrent VPN connections. However, it is possible to connect to any number of servers, one by one.

Chapter 2

Deployment and usage of Kerio VPN Client

Two modes of *Kerio VPN Client* are available:

User mode

In this mode, it is the user currently working on the host who initiates and closes VPN connection. In the *Kerio VPN Client* window, the user enters their login information or simply selects one of the preconfigured connection profiles and attempts to connect. The session is closed by the user or automatically upon closing the *Kerio VPN Client*, user logout or computer shutdown/reboot.

For initiation of a VPN session in this mode, no special user rights for the client host are required — i.e. any user of the particular host can use the *Kerio VPN Client* there.

Persistent connection mode

In this mode, once a user establishes a VPN connection, this connection is kept persistently. The *Kerio VPN Client Service* system service forces the connection to be kept even after closing the *Kerio VPN Client* and/or user logout, and it will be recovered automatically after the computer shutdown/reboot. Upon the computer startup, the VPN connection is recovered immediately, even before the user authenticates. Thanks to this feature, e.g. connection of the user to a remote private network domain is enabled.

For successful initiation and closing of persistent VPN connections, the user needs administrator rights for the client host (an account of the *administrator* type). Non-administrators can access only the remote private network if the VPN connection has already been established.

2.1 Application Startup

Kerio VPN Client is started automatically upon user logon and it is shown as an icon in the system's notification area (see chapter 2.2).

If the icon is not displayed (usually when the application is closed manually), the application can be started again by using the option *Start* → *Programs* → *Kerio* → *VPN Client* → *Kerio VPN Client*. Upon startup from the *Start* menu, a VPN connection definition dialog box is displayed (see chapter 2.3).

2.2 Taskbar icon

If *Kerio VPN Client* is running, an icon displaying its current status is available in the notification area of the Windows taskbar. Hovering the icon with the mouse pointer displays more details (brief help text).

- Idleness (VPN connection is not established) is represented by a red cross with the greyed logo of *Kerio Control*.

- Active VPN connection is represented by the full-colored icon.

Figure 2.1 The Kerio VPN Client icon for the off status

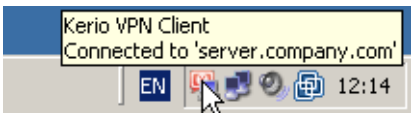

Figure 2.2 The Kerio VPN Client icon for the on status

- Persistent connection can be recognized by a text tag.

Figure 2.3 The Kerio VPN Client icon for the on status

Functions available through the taskbar icon

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

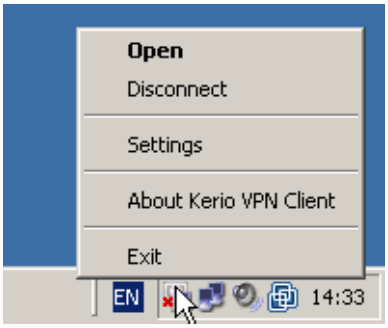

Figure 2.4 Context menu of the toolbar icon

- *Open* — use this option to open the main window of the *Kerio VPN Client*.
- *Disconnect* — option for closing of the current VPN connection.
- *Settings* — configuration of some *Kerio VPN Client's* parameters (see chapter 2.4).
- *About* — information about versions of individual *Kerio VPN Client* components (the program core, system service and low-level driver).
- *Exit* — use this option to close *Kerio VPN Client*. This option also disconnects temporarily established active VPN connections (see chapter 2.3).

The *Exit* option does not stop the system service *Kerio VPN Client Service* nor it disconnects persistent VPN connections.

2.3 Main window — VPN connection definition

The *Kerio VPN Client* main window is used for definition and specification of the VPN connection. To open this window, double-click on the application's icon displayed in the notification area and click on the *Open* option in the notification area context menu (see chapter 2.2) or go to the *Start* menu and use option *Start* → *Programs* → *Kerio* → *VPN Client* → *Kerio VPN Client*.

Figure 2.5 Kerio VPN Client's main window

In the *Server* field, enter the name or public IP address of the host where *Kerio Control* installed and which is used as Internet gateway of the particular network. Then, enter username and password for user authentication. Depending on the firewall configuration, in same cases username including domain is required to be specified (e.g. `wsmith@company.local`). If you are not sure about this point, contact the firewall administrator.

Connection can be established wither in temporary or persistent mode (see chapter 2). For successful initiation or closing of persistent connections, the user needs administration rights (*administrator*) for the client host. On *Windows Vista* and *Windows Server 2008*, the *User Account Control* feature may be enabled (*UAC*). In such cases, the operation of connection/disconnection requires confirmation, sometimes also authentication with administrator username and password.

Kerio VPN Client remembers defined VPN servers, usernames and setting of the persistent connection option. Users can choose whether the password would be also saved.

To define a new VPN connection, simply rename the server and use appropriate login information. Next time you access the page, simply choose a desired VPN server (and enter a valid password, if not saved).

Warning:
For security reasons, do not save password for VPN connections unless you are the only person using the particular user account on the host. Otherwise, you risk misuse of fragile access information and jeopardy of the remote private network.

Status information and error reports

The top part of the window includes either current status information (connected/disconnected, connecting/disconnecting, etc.) or an error report (connection failed, user authentication error, etc).

If the feature is enabled, status information and error reports are also displayed in so called ball messages at the *Kerio VPN Client* icon located on the toolbar (see chapter 2.4).

2.4 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 current version of the *Kerio VPN Client* is localized in 16 languages.

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*).

The *Enable balloon messages* option enables/disables informative balloon messages at the *Kerio VPN Client* icon located in the system notification area. These messages are optional and depend on user preferences (the connection status information can be easily found in the main window anytime).

2.5 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.

Click *View Certificate* to get 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 2.6 A dialog informing about detected problems with the VPN server's certificate

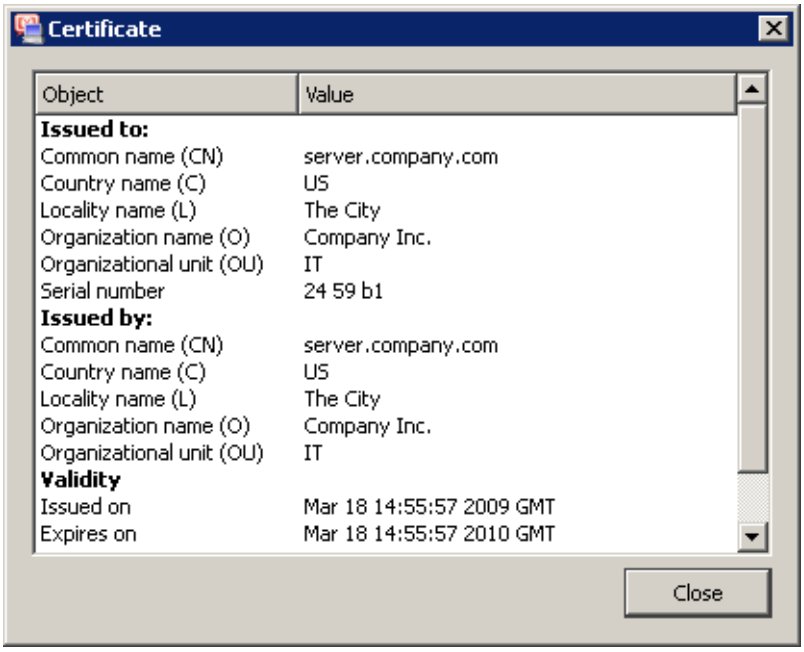

Figure 2.7 Viewing details of VPN server's certificate

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.

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).

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).
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).

Warning:
Should any obscurity occur or identity of the VPN server be doubted, contact the firewall administrator immediately.

2.6 Logs

The *Kerio VPN Client* generates logs including information about its own activity and detected errors. The system service and the application's user interface work separately. Therefore, separate logs are generated for each of these components. Log files can be used for troubleshooting while communicating with the *Kerio Technologies* technical support department (especially the system service logs are critical and can be extremely helpful).

The system service logs

Logs of the *Kerio VPN Client Service* can be found in the `logs` subfolder of the folder where the *Kerio VPN Client* is installed, the following path is used by default:

```
C:\Program Files\Kerio\VPN Client\logs
```

Two log files are available here:

- `error.log` — critical errors, such as information that start of the *Kerio VPN Client Service* failed, that the VPN server is not available, that user authentication failed, etc.
- `debug.log` — detailed information on activities of the system service and detected errors.

The user interface logs

Logs of the user interface are stored in the corresponding folder of the user account of the user working with the *Kerio VPN Client*. By default, the following path is used:

```
Application Data\Kerio\VPNClient\logs
```

or

```
Application Data\Kerio\VPNClient\logs
```

Like in case of the system service, two log files are available:

- `error.log` — critical errors, such as information that it is not possible to establish connection to the *Kerio VPN Client Service*.
- `debug.log` — detailed information on activities of the application and detected errors.

Appendix A

Legal Notices

Microsoft®, *Windows*® and *Windows Vista*™ are registered trademarks or trademarks of *Microsoft Corporation*.

Other names of real companies and products mentioned in this document may be registered trademarks or trademarks of their owners.