Kerio VPN Client

User Guide

Kerio Technologies

This guide provides detailed description on *Kerio VPN Client*, version *7.3* for *Mac OS X*. 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.

Kerio VPN Client is connected to the VPN server in *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*.

Configuration is saved in the home folder of the user currently using the *Kerio VPN Client*. 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

Supported hardware and operating systems

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

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

Conflicting software

The *Kerio VPN Client* does not collide with other applications.

1.2 Installation

To install the *Kerio VPN Client*, use a corresponding package with the `.dmg` extension (e.g. `kerio-control-vpnclient-1.2.3-4567-mac.dmg`). The package will be mounted as a disk. From the mounted drive, run the *Kerio VPN Client Installer*. Standard wizard is used for the installation.

The *Kerio VPN Client* is installed as a *System Preferences* panel. In the system, the installation creates the *kvnet0* virtual network adapter and the *Kerio VPN Client Service* system service

(*kvpncsvc*) which is run upon completion of the installation and is then initialized upon each startup of the operating system.

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 the *kvnet0* virtual network interface). 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.

The VPN server also assigns the client an address for the primary, and optionally also secondary DNS server and DNS domain extension. This allows to specify remote hosts with their names.

The change of DNS configuration has such effect that all DNS queries from the client host are sent to a DNS server in a remote private network. Users usually do not even notice any change. Upon closing of the VPN connection, the original DNS configuration will be recovered.

On *Mac OS X 10.5 Leopard*, the VPN server can assign the client also an address for the primary, and optionally also for secondary WINS server. The WINS service enables browsing in the *Microsoft Windows* network neighbourhood. Like in case of DNS, the original WINS configuration is recovered upon closing the VPN connection.

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* system preferences panel, the user can connect by entering their login information. 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 System preferences panel — definition of VPN connection

The *Kerio VPN Client* panel can be found under *System Preferences* in the *Others* section. This panel can be also opened by clicking on the status icon in the right part of the main menu bar (see chapter 2.2).

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). Only the computer administrator is allowed to open/close connections. To establish a persistent connection, it is first necessary to “unlock” the system preferences panel. If the persistent connection has just been established, an administrator username and password are required for opening of the system preferences panel.

The *Kerio VPN Client* remembers the defined VPN server, username and setting of the persistent connection option. Users can choose whether the password would be also saved.

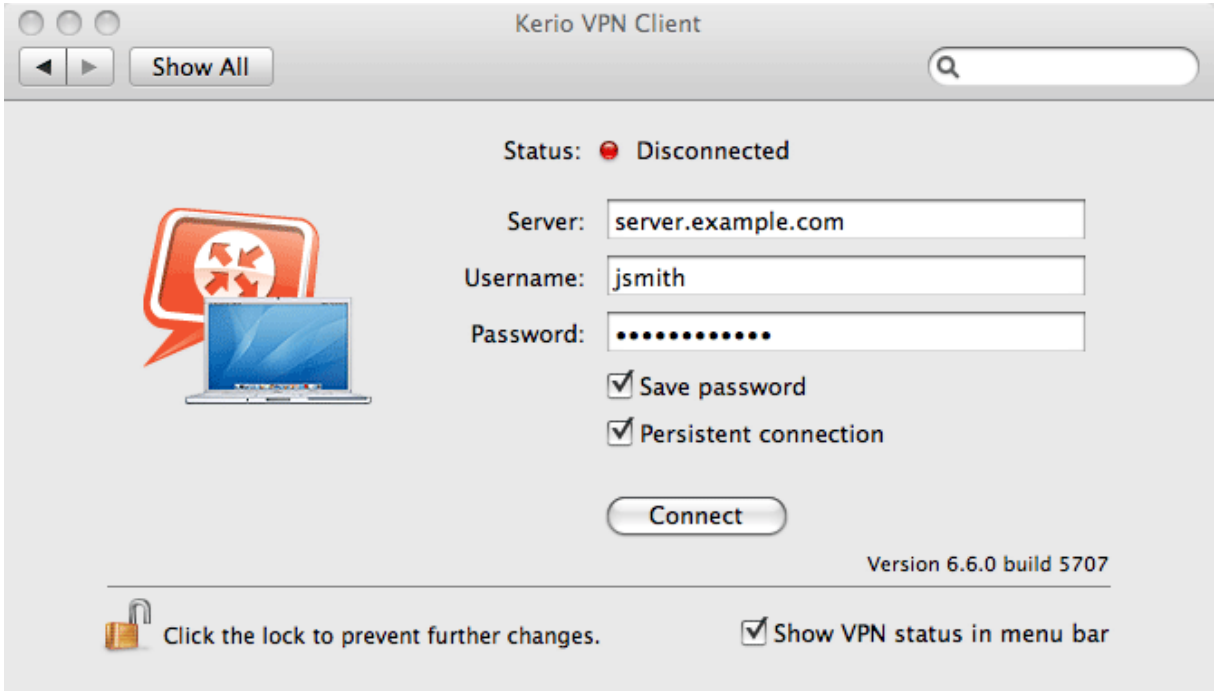

Figure 2.1 Kerio VPN Client's main window

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 panel includes either current status information (connected/disconnected, connecting/disconnecting, etc.) or an error report (connection failed, user authentication error, etc).

Basic information of the VPN connection status (disconnected, connecting, disconnected) is also shown by the *Kerio VPN Client* icon on the right side of the main menu bar. This icon can be enabled/disabled by using the *Show VPN status on menu bar* option. For details, see chapter 2.2.

2.2 Status icon on the main menu bar

The *Kerio VPN Client* includes a status icon displayed on the right side of the main menu bar. Clicking on this icon shows a context menu with the status information and other options.

Note: Displaying of the icon can be disabled in the *Kerio VPN Client* system preferences panel (see chapter 2.1).

- Idleness (VPN connection not established) is represented by an empty bubble icon — the *Kerio Technologies* product logo.

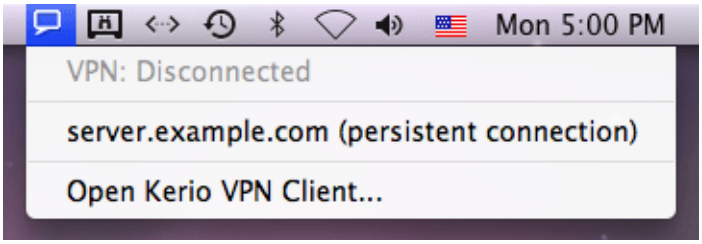

Figure 2.2 The Kerio VPN Client icon for the off status

The server name in the menu links to saved login information for the particular VPN server. Upon, clicking on this name, the *Kerio VPN Client* initiates the defined VPN connection. If this connection is defined as persistent, it is first necessary to enter a username and password of a user with administrator rights for the client host.

- When the VPN connection is in progress, an arrow is displayed in the icon.

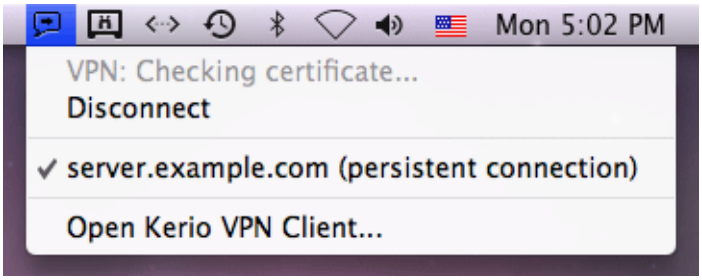

Figure 2.3 The Kerio VPN Client icon for the process of connection initiation

To interrupt establishing of the connection, you can use the *Disconnect* option.

- Active VPN connection is represented by an icon with the *Kerio Control* logo.

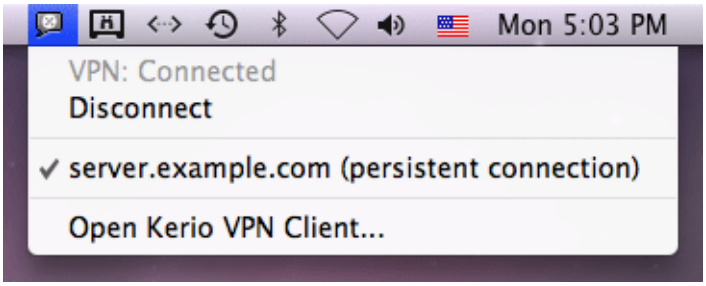

Figure 2.4 The Kerio VPN Client icon for the on status

The *Disconnect* option closes the current session. If this a persistent connection, it is first necessary to enter a username and password of a user with administrator rights for the client host.

In this particular case, the server name is only informative.

2.3 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.

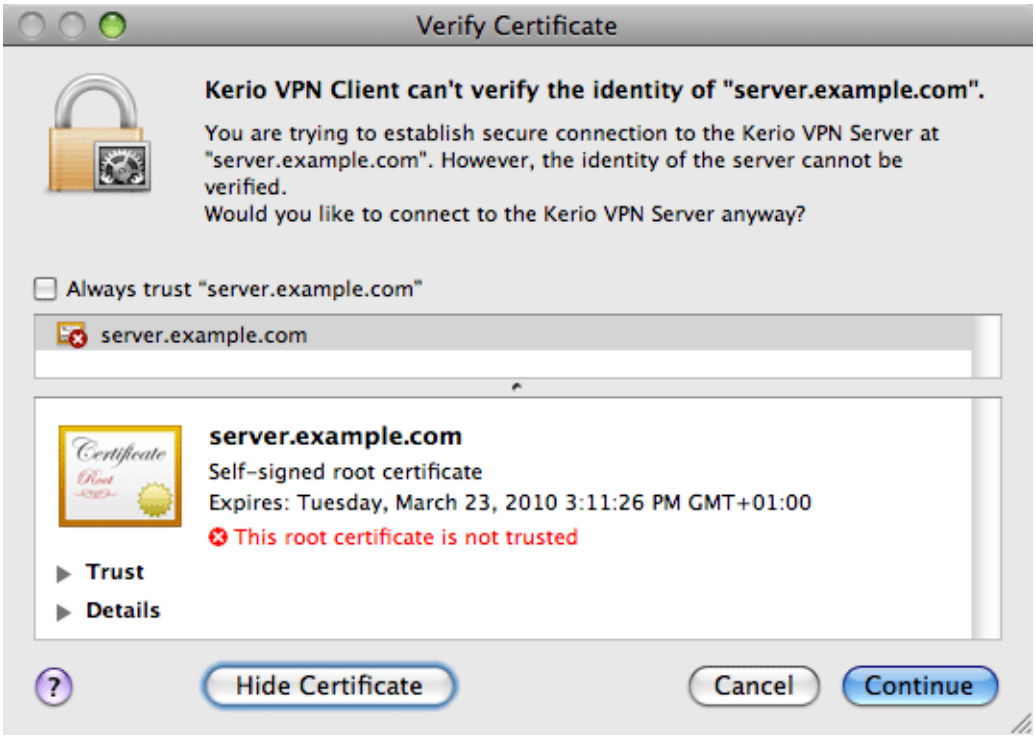

Figure 2.5 A dialog informing about detected problems with the VPN server's certificate

Click on the *Details* option to get detailed information about the VPN server's certificate (issuer, server for which it was issued, expiration date, etc.). Regarding this information, user can select one of the following options:

- Cancel — cancels the operation in case that any doubts about trustworthiness of the VPN server occur. It is also recommended to contact the server administrator and inform them about any issues under such circumstances.

- Continue — adequate for cases where the server can be trusted and certificate issues are only temporary. The *Kerio VPN Client* allows connection to the server only for this

time and next time the warning message will be displayed again (unless the certificate issue would have been solved by the time).

- Continue and always trust the certificate (the *Always trust* option). The certificate will be saved in the system *Keychain* and from now on, no warning will be displayed. This option is adequate especially if the server uses a self-signed certificate.

  Note: On *Mac OS X 10.4 Tiger*, it is not allowed to set a self-signed certificate as always trusted. To break this restriction and set the certificate as always trusted anyway, it is necessary to insert the certificate in the keychain manually — see below.

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

Setting a certificate as always trusted on Mac OS X 10.4 Tiger

On *Mac OS X 10.4 Tiger*, it is not possible to set a self-signed certificate as always trusted (only certificates issued by a trustworthy certification authority is allowed to be saved in the system keychain). To break this rule, follow this procedure:

1. In the window warning you that the certificate is not trustworthy (see figure 2.5), click on the certificate image and drag it to the desktop. This creates a file with the certificate on the desktop (e.g. `server.company.com.cer`).

2. *Important note:* The *Keychain Access* application must NOT be running at the moment. If it is running, close it.

3. Clicking on the certificate file on the desktop runs the *Keychain Access* application and displays a dialog asking for specification of the keychain to save the certificate in.

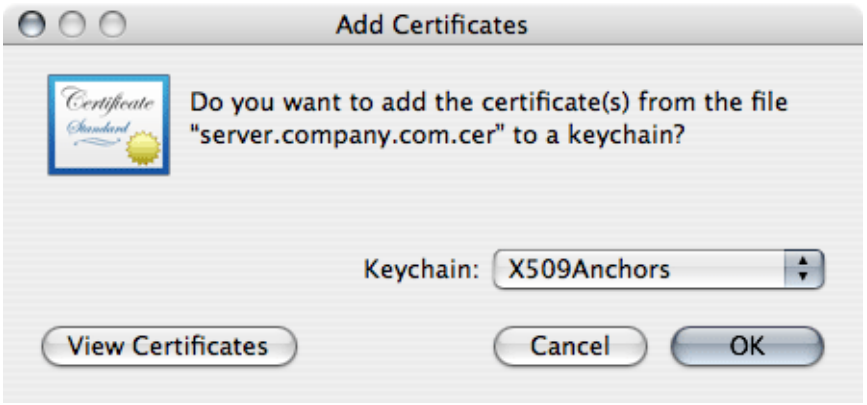

Figure 2.6 Saving certificates in keychain

4. Select the *X509Anchors* keychain. This keychain contains certificates that are allowed to sign other certificates (these are typically certificates of certification authorities).

   To add a certificate successfully, authentication with an administrator account is required.

5. In the *Keychain Access* application, select the *X509Anchors* keychain, look up the new certificate (e.g. *server.company.com*) and click on it to open it.

6. In the certificate window, scroll to the bottom, open the *Trust Settings* section and set the *Always Trust* option for the *When using this certificate* entry.

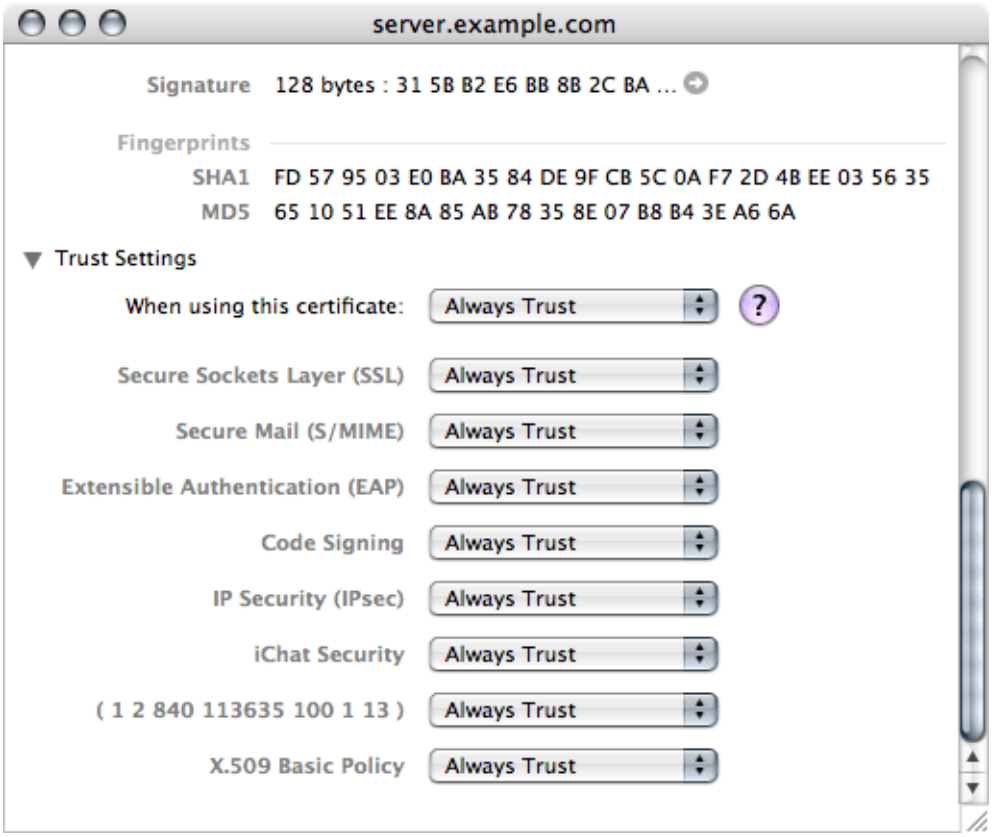

Figure 2.7 Certificate properties — setting a certificate as trusted

7. Close all running applications and log out of the system.

8. Reboot the system and try to establish a VPN connection to the particular server. From now on, no untrustworthy certificate warning should display.

2.4 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, i.e. `/usr/local/kerio/vpnclient`.

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 hidden subfolder of the home folder of the user working with the *Kerio VPN Client*, namely:

`~/.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

Mac OS® and *Safari*™ are registered trademarks or trademarks of *Apple Inc.*

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