Kerio Control

User Guide

Kerio Technologies

Contents

Kerio Control client interface

What is Kerio Control client interface

The firewall is usually configured to allow access to internet services (web pages, multimedia, FTP servers, etc.) only to authenticated users. The firewall allows viewing browsing statistics of individual users (visited web pages, data volume transferred, etc.) and applies possible restrictions. To keep the manipulation as simple as possible, automatic redirection to the web interface's authentication page is usually set for cases when you attempt to access a web page without having been authenticated at the firewall. Upon a successful login, the browser redirects to the requested web page. This procedure usually takes part at the opening of the home page upon startup of user's web browser. This makes your authentication at the firewall almost transparent.

All users, regardless their user rights, can use the web interface to:

- View their daily, weekly and monthly transferred data volume quotas and their current status,
- View web access restriction rules,
- Set filtering of specific web items (e.g. blocking of pop-ups),
- Setting language preferences of the web interface, reports and email alerts,
- Change password (in specific cases only).

Users with appropriate access rights can also:

- View their own Internet usage statistics,
- View Internet usage statistics of other users,
- Dial and hang up dialed Internet lines.

Accessing the web interface

To access the Kerio Control web interface, use a URL in your browser following this pattern:

`https://server:4081/`

`server` refers to the name or IP of the Kerio Control host, `4081` represents a web interface port.

The browser may show warning regarding certificate invalidity. You can ignore this warning and continue connecting. If you are not sure what to do, contact your Kerio Control administrator.

User login

User authentication is required for access to the Kerio Control's web interface. Any user with their own account in Kerio Control can access the web interface (regardless their access rights).

In some cases you may get logged in the web interface automatically. If not, the firewall's login page is opened first waiting for a valid username and password. The login information usually match the authentication details used for login to your operating system.

 In network with multiple domains (typically in huge branched organizations), username with domain can be required (e.g. `wsmith@us-office.company.com`). To get this information, contact your network administrator.

The welcome page of the web interface differs according to your access rights:

- If you are not allowed to view statistics, status info and preferences are displayed instead (**My Account**).
- If you are allowed to view statistics, the web interface will switch to the statistics mode and it will start with the page of overall statistics. The link in the upper right corner of the page allows to switch between statistics and user preferences.
- If your rights are set to the level for viewing only your own statistics, the page with your statistics is opened.

Logging out from the web interface

Once finished with activities where authentication is required, it is recommended to log out of the Kerio Control web interface by using the **Logout** link. It is important to log out especially if multiple users share the same computer. If you don't log out, your authenticated session can be hijacked by another user who may work in the web interface using your identity.

Bear in mind that you can be logged on the firewall even if you have not been using the very web interface — e.g. if the firewall required user authentication at your access to a website. To avoid opening the web interface to log out when finishing your work, Kerio Control includes a direct link for user logout:

`https://server:4081/logout`

Clicking on this link performs immediate logout of the user from Kerio Control without the need of opening the web interface's welcome page.

Hint
URL for user logout from Kerio Control can be added to the web browser's toolbar as a link. User can use this "button" for quick logout.

Kerio Control automatically logs out users from idle sessions, i.e. sessions where the web interface and any other Internet service is not used for a defined time period (usually 2 hours). This handles situations when a user forgets to terminate the session (logout).

User password authentication

If an access to the web interface is attempted when an authentication from the particular host is still valid (you have not logged out and the timeout for idleness has not expired) but the particular session[1] has already expired, Kerio Control requires user authentication by password. This precaution helps avoid misuse of the user identity by another user.

Under the conditions described above, the welcome page displays a warning message informing that another user is already logged on the firewall from the particular host.

If the user is you, you can enter your password for authentication and continue working in the web interface. If another user is currently authenticated at the web interface, log the user out and authenticate by your username and password.

Status Information (quota and web site restrictions)

On the **Status** tab, the following information is provided:

User and firewall information
: The page header provides user's name or their username as well as the firewall's DNS name or IP address.

Transfer Quota Statistics
: The upper section of the **Status** page provides information on the data volume having been transferred by the moment in both directions (download, upload) for the particular day (today), week and month. In case that any quota is set, current usage of individual quotas (percentage) is displayed.
Week and month starting days depends on setting of so called accounting period in Kerio Control. If you wish to change this setting, contact your firewall administrator.

Web Site Restrictions
: The lower part of the **Status** tab provides an overview of current URL rules applied to the particular user (i.e. rules applied to all users, rules applied to the particular user and rules applied to the group the user belongs to). This makes it simple to find out which

[1] *Session* is every single period during which a browser is running. For example, in case of *Internet Explorer*, *Firefox* and *Opera*, a session is terminated whenever all windows and tabs of the browser are closed, while in case of *SeaMonkey*, a session is not closed unless the *Quick Launch* program is stopped (an icon is displayed in the toolbar's notification area when the program is running).

web pages and objects are allowed or restricted for the particular user. Time intervals within which the rules are valid are provided as well.

User preferences

The **Preferences** tab allows setting of custom web content filtering and preferred language for the web interface. Users not using an account belonging to the *Windows* domain can also change their password in preferences.

Content filtering options

The upper section of the page enables to permit or deny particular items of web pages.

Content filter options

Checking of the field gets the corresponding item filtered by the firewall.
If a particular item is blocked by the Kerio Control administrator, the corresponding field on this page is inactive — user cannot change the settings. Users are only allowed to make the settings more restrictive. In other words, users cannot enable an HTML item denied by the administrators for themselves.

- **Java applets** — `<applet>` HTML tag blocking
- **ActiveX** — *Microsoft ActiveX* features (this technology enables, for example, execution of applications at client hosts)
  This option blocks `<object>` and `<embed>` HTML tags.
- **Scripts** — `<script>` HTML tag blocking (commands of JavaScript, VBScript, etc.)
- **Pop-up windows** — automatic opening of new windows in the browser (usually advertisements)
  This option will block the `window.open()` method in *JavaScript*.
- **Cross-domain referer** — blocking of the `Referer` items in HTTP headers.
  This item includes pages that have been viewed prior to the current page. The **Cross-domain referer** option blocks the `Referer` item in case this item does not match the required server name.
  Cross-domain referer blocking protects users' privacy (the `Referer` item can be monitored to determine which pages are opened by a user).

Save settings

To save and activate settings, click on this button.

Editing user password

The middle section of the **Preferences** page allows setting of user password. Password can be changed only if you have an account created in Kerio Control.

For details contact your local administrator.

Preferred Language

At the bottom of the **Preferences** tab it is possible to set language preferences. This language will be used for

- the firewall's web interface,
- Reports, alerts other information sent to users by email (e.g. warning of a virus or notification of exceeding of the transfer quota).

In the current version of Kerio Control, you can choose from 16 languages. The language can be either selected from a menu or it can be set automatically according to the web browser's settings (default option). This option exists in all supported web browsers. English will be used if no language set as preferred in the browser is available.

Language settings affect also the format of displaying date and numbers.

Dial-up

If you have rights for controlling dial-ups in Kerio Control, you can dial and hang up lines and view their status on the **Dial-up lines** tab. This tab lists all dial-up lines defined in Kerio Control.

Dial-up details:

- Name of the line in Kerio Control.
- Current status — **Disconnected**, **Connecting** (the line is being dialed), **Connected**, **Disconnecting** (the line is being disconnected).
- Action — hypertext link that dials or hangs up the line when clicked (depending on its current state).
- Connection time.
- Volume of data transferred in either direction (**Incoming** = from the Internet to the LAN, **Outgoing** = from the LAN to the Internet).

The **Dial-up** page is automatically refreshed in regular time intervals.

Kerio Control client statistics

About Kerio Control statistics

The Kerio Control client interface provides detailed statistics on users and groups, volume of transferred data, visited websites and web categories. This information may help figure out browsing activities and habits of individual users.

The statistics monitor the traffic between the local network and the Internet. Volumes of data transferred between local hosts and visited web pages located on local servers are not included in the statistics (also for technical reasons).

One of the benefits of web statistics and reports is their high availability. The user (usually an office manager) does not need the **Administration Console** and they even do not need Kerio Control administrator rights (special rights are used for statistics). Statistics viewed in web browsers can also be easily printed or saved on the disk as web pages.

- Users should be informed that their browsing activities are monitored by the firewall.
- Statistics and reports in Kerio Control should be used for reference only. It is highly unrecommended to use them for example to figure out exact numbers of Internet connection costs per user.

Logging in Kerio Control client interface and viewing statistics

To view statistics, user must authenticate at the Kerio Control client interface first. User (or the group the user belongs to) needs rights for statistics viewing.

Access to statistics

From any host from which access to the Kerio Control client interface is allowed, statistics can be opened by any of the methods described below:

- At `https://server:4081/star`. This URL can only be used for access to statistics. If you lack the rights to view the statistics, an error is reported.
- At `https://server:4081/`. This is the primary URL of the Kerio Control client interface. If you possess appropriate rights for stats viewing, the welcome page providing overall or your own statistics (see below) is displayed. Otherwise, the **My Account** page is opened (this page is available to any user).

Updating data for statistics

Statistics are primarily used for creating reports for certain periods. Gathering and evaluation of information for statistics means processing large data volumes. To reduce load on the firewall (and slowdown of Internet connection), data for the statistics is updated approximately once an hour.

For these reasons, the Kerio Control statistics are not useful for real-time monitoring of user activity.

Statistics in Kerio Control client interface

Statistic types

Two basic statistic types are available in Kerio Control:

Overall statistics
: Overall statistics covering either all users or a selected user group. These statistics show total volume of transferred data, frequently used network protocols and top visited web sites and web categories.

User Statistics
: Detailed statistics for a selected user. These statistics provide an overview of transferred data, used protocols and visited web sites and web categories. If Kerio Control also monitors user activity, a detailed list of browsing activities of the selected user is also ïncluded.
It is possible to use a special access right to allow users to view their own statistics (including the detailed list of their browsing activities).

Selecting period of statistics

Most frequently, statistical information needed refer to a certain time period (today, last week, etc.). The period can be set in the toolbar at the top of the page.

The toolbar includes buttons for fast switching between accounting periods (daily, weekly, monthly). Arrows (previous/next) next to the date (current period) allow fast browsing through the selected period. This browsing is not available for custom accounting periods.

The **Custom period** option at the top of the statistics page can be used for definition of custom period.

Select an item in the **Period length** combo box (day, week, month). Further options are displayed depending on which option has been selected.

Note: Weeks and months might not correspond with weeks and months of the civil calendar. In Kerio Control statistics settings, so called accounting periods can be set — the first day of each month and week (any change takes effect only for new data, i.e. the information already saved in the database are kept unchanged).

It is also possible to set a custom accounting period, defined by starting and ending days.

The starting and ending day can be defined manually or selected from the thumbnail calendar available upon clicking on the icon next to the corresponding text field.

The selected period applies to all tabs until a next selection (or unless the window is closed). The "today" period is set as default and used upon each login.

Note: Under certain circumstances, an information may be reported that this period will be rounded to whole weeks or months. In such a case, the real (rounded) period for the statistics will be set and shown above the **Change Period** button.

Print formatting

Any page of the statistics can be converted to a printable version. For this purpose, use the **Print** option in the upper toolbar.

Clicking on **Print** displays the current page in a new window (or on a new tab) of the browser in a printable format and the browser's print dialog is opened. Size and paging are optimized for the two top-used paper formats, — *A4* and *Letter*.

 For technical reasons, pages of statistics cannot be printed by the classic **File** → **Print** method (or by pressing *Ctrl+P*). This method would print out the original (uncustomized for printing) page.

Displaying overall statistics in Kerio Control client

About overall statistics

For general info on statistics, read article Kerio Control client statistics.

Section **Overall** provides overall statistics for all users within the local network or a selected group for the selected accounting period.

In the drop-down menu, you can select option *All* overall statistics for all users within the local network (including anonymous, i.e. unauthenticated users) or a user group for which statistical data is gathered.

Gathering of statistics for groups need to be explicitly set by the firewall administrator.

Overall statistics

Overall View

Page **Total** brings a quick overview of the network traffic of the selected user group.

Traffic by periods

The first chart provides information on the volume of data transferred within the selected period. The table next to the chart informs on data volumes transferred in the entire selected period (total and for both directions as well). Simply hover a column in the chart with the mouse pointer to view volume of data transferred in the corresponding subperiod. Click on a column in the chart to switch to the information on the particular subperiod only.[2]

The subperiod length depends on the current period:

- *day* — the chart shows traffic by hours,
- *week* or *month*— the chart shows traffic by days.

For custom periods:

- *up to 2 days* — the chart shows traffic by hours,
- *up to 5 weeks* — the chart shows traffic by days,
- *up to 6 months* — the chart shows traffic by weeks,
- *more than 6 months* — the chart shows traffic by months,

Top Visited Websites

The chart of the most frequented websites shows top five domains (second level) by their visit rate. The number in the chart refers to number of visits of all web pages of the particular domain in the selected accounting period.

[2] It is not possible to switch to a selected subperiod if the traffic is displayed by hours. The shortest accounting period to be selected is one day.

Note: Kerio Control "can see" only separate HTTP requests. The information, therefore, cannot be precise, though the approximation is very good.

Top Requested Web Categories

This chart shows top five web categories requested in the selected period sorted by the Kerio Control Web Filter module. The number in the chart refers to total number of HTTP requests included in the particular category. For technical reasons, it is not possible to recognize whether the number includes requests to a single page or to multiple pages. Therefore, number of requests is usually much higher than number of visited websites in the previous chart.

Top 5 users

Top five users, i.e. users with the greatest volume of data transferred in the selected accounting period.

The chart includes individual users and total volume of transferred data.

The chart shows part of the most active users in the total volume of transferred data in the selected period. Hover a user's name in the chart by the mouse pointer to see volume of data transferred by the user, both in total numbers and both directions (download, upload).

Click on a user's name in the chart or in the table to switch to the **Individual** tab where statistics for the particular user are shown.

These charts and tables provide useful information on which users use the Internet connection the most and make it possible to set necessary limits and quotas.

Note:

1. Total volume of data transferred by a particular user is a summary of data transferred by the user from all hosts from which they have connected to the firewall in the selected period.
2. Data transferred by unauthenticated users is summed and accounted as the **not logged in** user. However, the value of this information is not very high. The administrator should set the firewall so that it avoids anonymous Internet browsing by always requiring user authentication.

Used Protocol

The chart of used protocols shows part of individual protocols (i.e. their classes) in the total volume of data transferred in the selected accounting period. Hover a protocol name with the mouse pointer to see volume of data transferred by the particular protocol. For better reference, Kerio Control sorts protocols to predefined classes — see below.

Such information might, for example, help recognize type of traffic between the local network and the Internet. If the internet line is overloaded, it is possible to use the information to set necessary limits and restrictions (traffic rules, URL rules, etc.).

Note:

1. The **No data available** alert informs that no data is available in Kerio Control's database for the selected statistics and accounting period. This status can be caused by various

different reasons — e.g. that the selected user account did not exist in the particular time period, the user did not login to the firewall within the period, etc.

2. Kerio Control tries to optimize size of the statistic database and volume of processed data. The greatest volume of data is generated by statistics of visited websites. For this reason, daily statistics of visited websites are kept only for the last 40 days. Weekly and monthly statistics are available for the entire data storage period as set in the configuration (2 years by default).

   If a period is selected for which no data is available, Kerio Control offers another period where data for the requested statistics might be found.

Users by Traffic

Page *Users by Traffic* shows volume of data transferred by individual users of the selected group in both directions (download, upload). It is possible to show either all network traffic or filter traffic statistics by network protocol.

The table provides an information of part of the user in the total volume of the transferred data. It is possible to use the table to view all transferred data or only data transferred by a selected protocol (or protocol class). This allows to get information about which users have transferred the most data by a service (e.g. web browsing).

For better reference, Kerio Control sorts protocols to predefined classes:

- **Web** — *HTTP* and *HTTPS* protocols and any other traffic served by the *HTTP* protocol inspector.
- **E-mail** — *SMTP*, *IMAP*, *POP3* protocols (and their secured versions).
- **FTP** — *FTP* protocol (including traffic over proxy server).
- **Multimedia** — protocols enabling real-time transmission of sound and video files (e.g. *RTSP*, *MMS*, *RealAudio*).
- *VoIP - SIP* — Voice over telephony via *SIP* protocol.
- **P2P** — file-sharing protocols (*peer-to-peer* — e.g. *DirectConnect*, *BitTorrent*, *eDonkey*, etc.). The traffic is accounted only if Kerio Control detects that it is traffic within a *P2P* network.
- **VPN** — connection to remote private networks (e.g. *Kerio VPN*, *Microsoft PPTP*, etc.).
- **Remote Access** — "terminal" access to remote hosts (e.g. *Remote desktop*, *VNC*, *Telnet* or *SSH*).
- *Instant Messaging* — online communication via services such as *ICQ*, *Jabber*, etc.

Web Pages

Overview of visited web pages (second-level domains). The number refers to number of visits of all web pages of the particular domain in the selected accounting period.

These statistics provide for example the following information:

- which sites (domains) are visited by the users regularly,
- which users are the most active at web browsing,

The chart at the top of the tab shows the most visited web domains. The number in the chart refers to number of visits of all web pages of the particular domain in the selected accounting period.

Under the chart, detailed statistics for each of top ten visited domains are shown:

- The header provides name of the DNS name and total number of visits at websites on servers belonging to the domain. Domain name is also a link to the "main" web site of the particular domain (the `www` prefix is attached to the domain name, i.e. for example the `www.google.com` page is opened for the `google.com` domain).
- The chart shows part of the most active users (up to six items) in the total visit rate of the particular domain. Hovering of a user's name by the mouse pointer shows total number of web pages visited by the user.
- The table next to the chart shows the most active users sorted by number of visits at websites within the particular domain.

Note: Kerio Control "can see" only separate HTTP requests. To count number of visited pages (i.e. to recognize which requests were sent within a single visit), a special heuristic algorithm is used. The information, therefore, cannot be precise, though the approximation is very good.

Website categories

Overview of the top visited web categories. Web categories provide better reference on which sorts of websites are the most visited among your users and whether their browsing activities are rather of the inside-the-business or out-of-the-business character.

The chart on the left shows the most visited web categories in the selected accounting period. The number in the chart refers to total number of HTTP requests included in the particular category. For technical reasons, it is not possible to recognize whether the number includes requests to a single page or to multiple pages. Therefore, number of requests is usually much higher than number of visits in statistics of the top visited websites.

Below the chart, detailed statistics for each of top ten visited web categories are shown:

- The header provides name of the category and total number of requests to websites belonging to the category.
- The chart shows part of the most active users (up to six items) in the total visit rate of the particular category. Hovering of a user's name by the mouse pointer shows total number of the user's requests to the particular web category.
- The table next to the chart shows the most active users sorted by number of requests to the particular web category.

Click on the name of a user in the chart or table to switch to the **Individual** tab and see detailed statistics of the particular user.

Note:

1. Web categorization is performed by Kerio Control Web Filter, an optional module of Kerio Control. If you want to use web categories in your statistics, you need a valid license for this module in Kerio Control.
2. Statistics of visited categories might be affected by wrong categorization of some web pages. Some pages might be difficult to categorize for technical reasons and, rarely, it may happen that a website is included in a wrong category.

Displaying statistics of individual users in Kerio Control client

About user statistics

For general info on statistics, read article Kerio Control client statistics.

Section **Overall** provides overall statistics for all users within the local network or a selected group for the selected accounting period.

In the drop-down menu, you can select option *All* overall statistics for all users within the local network (including anonymous, i.e. unauthenticated users) or a user group for which statistical data is gathered.

Gathering of statistics for groups need to be explicitly set by the firewall administrator.

User Statistics

Section **User** shows individual statistics for the selected user.

First, select a user in the **Select User** menu. The menu includes all users for which any statistic data is available in the database — i.e. users which were active in the selected period.

When a user is selected, full name, username and email address are displayed (if defined in the user account).

> ***Hint***
> Method of username displaying in the table can be set in the Kerio Control configuration.

The same type of statistics as total statistics in the **Summary Report** section will be shown for the selected user, as follows:

- volume of data transferred within the selected accounting period,
- top visited websites,
- top requested web categories,
- used protocols and their part in the total volume of transferred data,

Users' Activity

The **Users' Activity** tab allows showing of detailed information on "browsing activities" of the selected user. This section answers such questions as *What was this user doing in the Internet in the selected period? How much time did this user spend by browsing through web pages?*, etc.

In the top right section of the **Users' Activity** tab, select a user whose activity you wish to see.

The top left section of the page shows a header with all available information about the selected user (username, email address, etc.)

Under this header, all detected activities of this user in the selected time period are listed. If there are no records meeting the criteria, the **No data available** information is displayed. Technically, it is not possible to recognize whether there was any activity by this user in the period or not, but is has not been recorded for any reason.

Note:

1. The **Users' Activity** section provides overview of user's activity for a certain period, but it is not useful for real-time monitoring of the use activity. Detected activities are always shown with certain delay caused especially by these factors:

    - *Update of statistical data* — gathering and evaluation of information for statistics means processing large data volumes. To reduce load on the firewall, data for statistics is updated approximately once an hour (see information regarding latest data update).

    - *Delay in recording of activities* — each activity is recorded 15 minutes after it's finished. The reason for this is that similar activities in row are counted as one record (for better transparency of user's activity).

2. User's activity can be shown for up to 7 days (for better transparency). If a longer period is selected, shorter periods covering the selected period will be provided.

Activity Categories

Detected activities are sorted in a few categories. Under the title of each category, summary information (total number of connections, total volume of transferred data, etc.) is provided, followed by detailed overview of activities. Details can be optionally hidden. If a period longer than one day is selected, records are divided in sections by days. Optionally, daily records can also be hidden.

Each activity record includes this time information: start time and duration of the activity. If an activity is marked as unfinished, the particular connection has not been closed yet (it is still open).

Activity categories are ordered as listed in the following description. If there was no corresponding activity by the user in the selected period, the category will not be shown.

Web Pages

This category addresses one of the top user activities, web browsing.

The header informs about the total number of visited web pages in the selected period and the total number of web searches. Kerio Control correctly detects most of the common web browsers.

Each record of connection to a web page includes:

- Start time and duration (see above).
- Domain which the page belongs to (statistics are created from data regarding second-level domains).
- Number of visits — the number says how many times the page was visited within this activity.
- Page category — site classification by the Kerio Control Web Filter module. If this module is not running or classification failed, category will not be displayed.
- Page title. Page title is displayed as a link — it is possible to simply click on the link to open the page in a new window (or a new tab) of the browser. If the page has no title, it will not be included in the activity list.

Connections to secured pages (*HTTPS*) are encrypted; therefore, titles and URLs of these pages cannot be recognized. In these cases, the record includes only the following information:

- Name (or IP address) of the server,
- Protocol (*HTTPS*),
- Volume of data transferred in each direction.

The search record includes:

- Search engine (only domain).
- Searched string. The searched string is displayed as a link which can be clicked to perform the corresponding search in the relevant search engine and to view the search results in a new window (or a new tab) of the browser.

Messages (e-mail and instant messaging)

This category covers two types of activity: email communication (by *SMTP*, *IMAP* and *POP3* protocols) and *Instant Messaging* — services such as *ICQ, AOL Instant Messenger (AIM)*, *Yahoo! Messenger*, *MSN Messenger*, etc.

The header informs about number of detected email messages and total volume of data transferred by email protocols. Kerio Control can recognize only email communication by *SMTP* and *POP3* unless the traffic is encrypted. Otherwise (the IMAP protocol, encrypted communication, etc.), only volumes of data transferred by individual protocols are monitored.

The **Messaging** section includes the following types of records:

- Connection to server — connection of email client to *SMTP*, *IMAP* or *POP3* server. The record includes name (or IP address) of the server, used protocol and volume of data transferred in each direction.
- Sent/Received messages — number of messages (transferred within one connec-

tion), name (or IP address) of the incoming/outgoing email server, used protocol and volumes of data transferred in each direction.
Note: Volume of transferred data is rounded to kilobytes. If data volume is smaller than 0.5 KB, the value is set to *0*.

- Instant messaging — only connection to and disconnection from the server is recorded. The record includes protocol (IM service) and name (or IP address) of the login server.
  In this case, duration of the activity stands for the length of connection to the service, regardless of how many messages the user sent or received.

Large File Transfers

This category addresses user activities where large data volumes are transferred — downloads from web and FTP servers, uploads to FTP servers or sharing of files in P2P networks. "Large files" are files exceeding 1 MB (or 2 MB of data transferred by an unknown connection — see below).
The header informs about total number of recognized files, total volume of transferred data (in both directions), data transferred via P2P networks (in both directions) and number of blocked attempts for sharing of files in P2P networks (this information is displayed only if there was such attempt detected and blocked).
Types of records in the **Large File Transfers** category:

- File downloads and uploads — the record includes name (or IP address) of the server, volume of transferred data and name of the transferred file.
  If the record points at download from a web server or from an anonymous FTP server, the file name is displayed as a link. Clicking on the link downloads the file.
- Sharing (transfers) of files in P2P networks — the record includes name of detected P2P network and volume of data transferred in each direction.
- Blocked P2P file sharing attempts — information about attempts for file sharing in P2P networks that was blocked by *P2P Eliminator*.
- Unknown connection — any traffic between the local network and the Internet within which more than 2 MB of data was transferred and which cannot be sorted in another category (e.g. in *Multimedia*). The record includes name or IP address of the server, protocol/service (if recognized) and volume of data transferred in each direction.

Multimedia

The **Multimedia** category includes real-time transfers of multimedia data — so called *streaming* (typically online radio and television channels).
The header informs about total volume of data transferred by multimedia protocols and total number of connections to such servers.
Records addressing individual activities include the following information:

- Stream name (or URL, if the name is not available). Under certain circumstances, name can be displayed as a link by which the stream can be opened.
- Name (or IP address) of the server.

- Volume of data transferred in each direction.

VoIP - SIP

This category covers the user's phone calls carried out via SIP.
The header shows total count of calls (both incoming and outgoing) and their duration. Call direction is seen from the point of view of the user monitored by Kerio Control.
Detailed call logs include the following information:

- Telephone number of the caller and the callee, and name if specified for the number,
- IP address of the caller and the callee,
- Volume of data transferred in each direction.

Remote access

This category addresses remote access to Internet hosts (e.g. *Microsoft Remote Desktop*, *VNC*, *Telnet* and *SSH*) as well as VPN access to remote networks. Remote access (if not used for work purposes) can be quite dangerous. User can use it to get round local firewall rules — e.g. by browsing through banned web pages on a remote host or by transferring forbidden files by VPN.
The **Remote Access** header informs about:

- number of VPN connections and total volume of data transferred via VPN,
- number of remote connections and total volume of transferred data.

Records addressing individual activities include the following information:

- name (or IP address) of the server to which the user connected,
- name of protocol/service,
- volume of data transferred by the connection in each direction.

Authenticating to the firewall with 2-step verification

Overview

New in Kerio Control 8.5!

The 2-step verification means you can protect your Kerio Control account and access to your company network by requiring two independent authentication steps. With the 2-step verification enabled, when you want to access your company network or log into Kerio Control Statistics from the Internet, you must use your credentials to authenticate, and also type a special time-limited code generated by the special mobile application such as Google Authenticator. You can try the following applications:

- Google Authenticator — Available for iOS, Android and Windows Phone
- FreeOTP Authenticator — Available for iOS and Android (https://fedorahosted.org/)
- Authenticator for iOS (http://mattrubin.me/)
- Authenticator for Windows Phone (http://www.windowsphone.com/)
- WinAuth for Windows OS (https://code.google.com/p/winauth/)

The verification code is not required if your device is connected within the Kerio Control network. Kerio Control requires the code only if you use the Internet to access your company network:

- Through Kerio Control VPN Client/IPsec VPN client
- To use Kerio Control Statistics
- To use Kerio Control Administration

Enabling the 2-step verification

You can enable the 2-step verification in your account in Kerio Control Statistics.

If you administrator sets the 2-step verification as compulsory, you must follow the steps in this section to enable the 2-step verification in Kerio Control Statistics.

To enable the 2-step verification, you must pair your device with your Kerio Control account:

1. Install the authenticator application on your mobile device.
2. Log into your account in Kerio Control Statistics.
3. Click **2-Step Verification**.

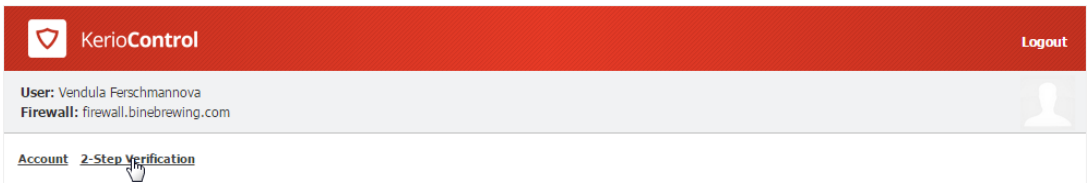


Figure 1 The 2-Step Verification tab

4. Open the authenticator application and scan a QR code or type the code shown below the QR code.

   You get a six-digit verification code that is time limited. The authenticator generates a new code every 30 seconds. All codes generated on the basis of the Kerio Control QR code are valid for Kerio Control authentication.

5. Type the verification code in Kerio Control Statistics, as shown below.
6. Click **Verify**.

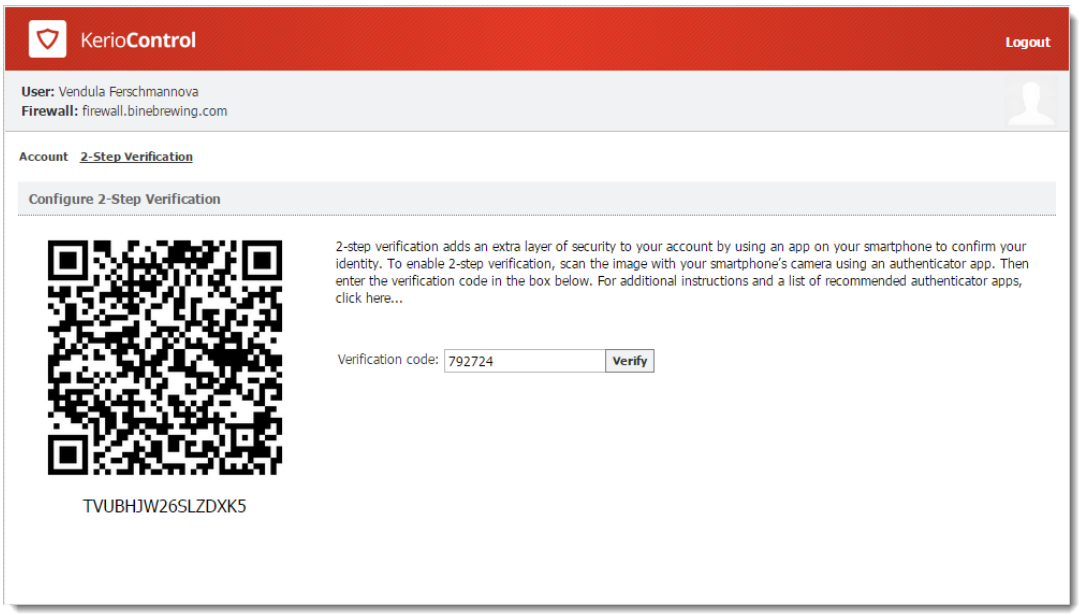


Figure 2 The 2-Step Verification tab

From now on, you authenticate with the verification code generated by the authenticator. For example, to connect to the Kerio Control Statistics page:

1. Type the Kerio Control Statistics URL in your browser.
2. On the login screen, type your username and password.
3. Click **Login**.

   The 2-step verification page appears.
4. Open the authenticator and type the Kerio Control code in the box provided.

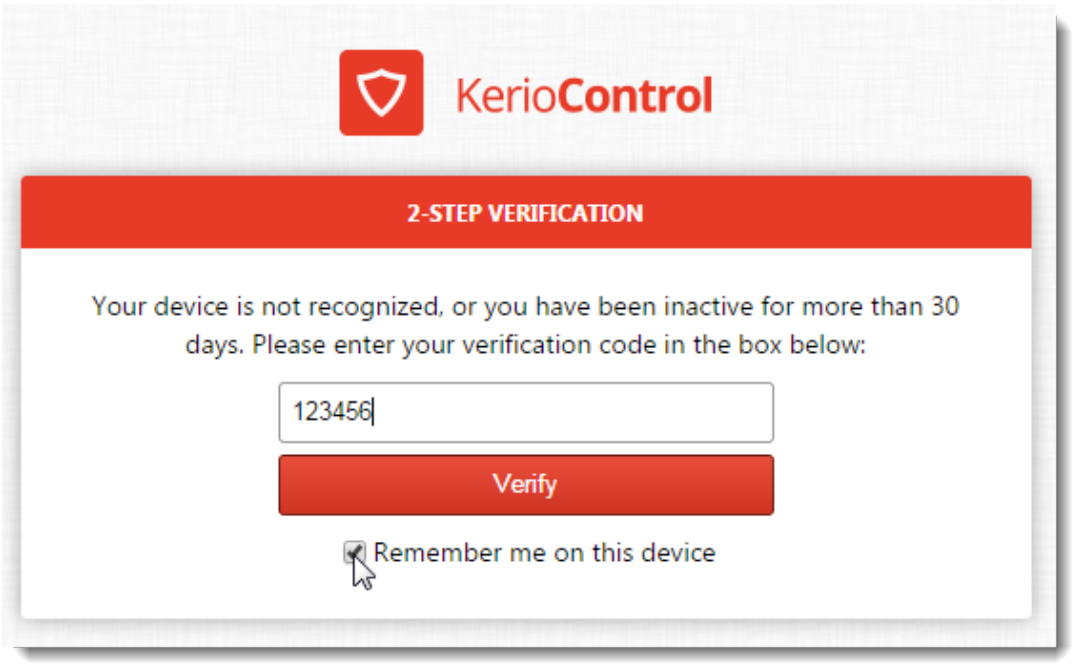


Figure 3 The 2-Step Verification tab

5. Select **Remember me on this device**. Your browser remembers the connection for the next 30 days from the last connection, so you do not have to type the code every time.
6. Click **Verify**.

Kerio Control redirects you to Kerio Control Statistics.

Disabling the 2-step verification

1. Type the Kerio Control Statistics URL in your browser.
2. On the login screen, type your username and password and then the verification code.
3. On the Kerio Control Statistics page, click **2-Step Verification**.

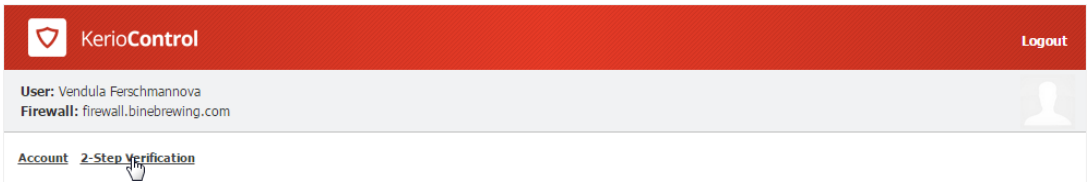


Figure 4 The 2-Step Verification tab

4. Generate a new code in your authenticator.
5. Type the code in the **Verification code** field.
6. Click **Disable**.

Kerio Control disables the 2-step verification for your account.

From now on, the 2-step verification is in the initial state and you can enable it again.

If you lose your mobile device, ask your system administrator to disable the 2-step verification for you.
If your administrator sets the 2-step verification as compulsory, you must enable it in Kerio Control Statistics again before accessing your company network from the Internet.

Enabling the 2-step verification when you use Kerio Control VPN Client

1. Install Kerio Control VPN Client 8.5 or later.
2. Connect to Kerio Control VPN Client as usual.
3. Kerio Control VPN Client automatically opens the 2-step verification page in your browser:
   - If you have a device paired with your account, type the new code from your authenticator.
   - If you don't have a device paired with your account, click **Continue** and follow the steps in Enabling the 2-step verification above.

Enabling the 2-step verification when you use IPsec VPN client

1. Connect to IPsec VPN client as usual.
2. Go to your browser and open any page.

   Kerio Control opens the 2-step verification dialog box:

- If you have a device paired with your account, type the new code from your authenticator.
- If you don't have a device paired with your account, click **Continue** and follow the steps in Enabling the 2-step verification above.

Configuring Kerio Control VPN Client

Kerio Control VPN Client overview

Kerio Control 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 Control VPN Client exists in three variants:

- Kerio Control VPN Client for Windows
- Kerio Control VPN Client for Mac
- Kerio Control VPN Client for Linux (read more in the readme file)

Kerio Control VPN Client is connected to the VPN server in Kerio Control. Kerio Control user accounts are used for authentication of clients.

Configuration is saved in the home folder of the user currently using the Kerio Control VPN Client. Each user of a host where Kerio Control 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.

System requirements

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

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

Licensing Policy

The Kerio Control 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.

Connecting to Kerio VPN Server

1. Firstly you have to configure Kerio VPN server in Kerio Control.

2. Install Kerio Control VPN Client to users' computers.

   For Kerio Control 8.5.0 and higher: Kerio Control VPN Client for Mac uses a PackageMaker installer and you can deploy it to users' computers silently through Apple Remote Desktop or similar application.

   Kerio Control VPN Client is started automatically upon user logon.

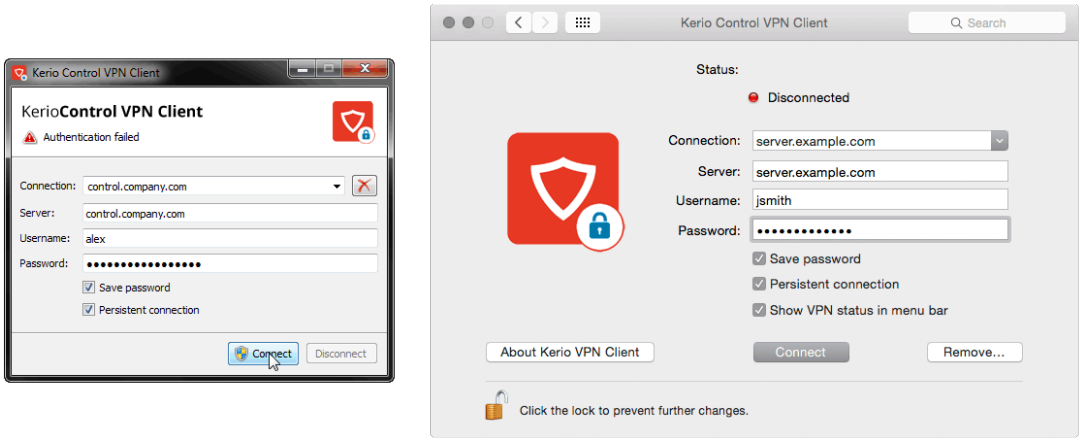


Figure 1 Kerio Control VPN Client

3. Tell your users the login details:

   - username and password for login to Kerio Control
   - Kerio Control hostname (or IP address)

4. Check **Persistent connection**, if your users have administrator rights for the client host.

   In persistent mode, once a user establishes a VPN connection, this connection is kept persistently. Thanks to this feature, e.g. connection of the user to a remote private network domain is enabled.

Windows: If Kerio Control VPN Client is running, an icon displaying its current status is available in the notification area of the Windows taskbar (Systray).

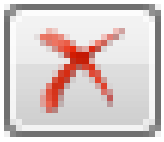
Mac: If Kerio Control VPN Client is running, a status icon displayed on the right side of the main menu bar.

Multiple endpoints can be defined to configure VPN failover in case the Kerio Control VPN server is load balancing with multiple Internet links. To separate entries, use a semicolon (for example, `primary.example.com;secondary.example.com`)

Removing connections

If you want to remove old or broken connections:

1. Open Kerio Control VPN Client.
2. In the **Connection** menu, select the connection.
3. Click the **Remove** button on Mac.

   Click the  icon on Windows.
4. Kerio Control VPN Client asks you if you want to remove selected connection.
5. Click **Yes**.

Kerio Control VPN Client removes your connection.

Configuring Kerio Control VPN Client (for Windows only)

You can configure:

- localization (language) of Kerio Control VPN Client
- balloon messages settings

1. In the notification area of the Windows taskbar (Systray), go to Kerio Control VPN Client context menu.
2. Click **Settings**.

When a language is changed, the user interface is switched to the language version immediately.

Enable balloon messages enables/disables informative balloon messages at the Kerio Control VPN Client icon located in the system notification area. These messages are optional and depend on user preferences.

Verification of the VPN server's SSL Certificate on Windows

Whenever a connection is being established, Kerio Control VPN Client performs verification of the VPN server's SSL certificate. 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.

If **Yes** is clicked, Kerio Control VPN Client considers the VPN server as trustworthy. The certificate is saved and no warning is displayed upon subsequent 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 Control 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 Control 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 Control VPN Client saves the certificate of the server as trustworthy. For any later connections, Kerio Control 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).

Verification of the VPN server's SSL Certificate on Mac

Whenever a connection is being established, Kerio Control VPN Client performs verification of the VPN server's SSL certificate. 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.

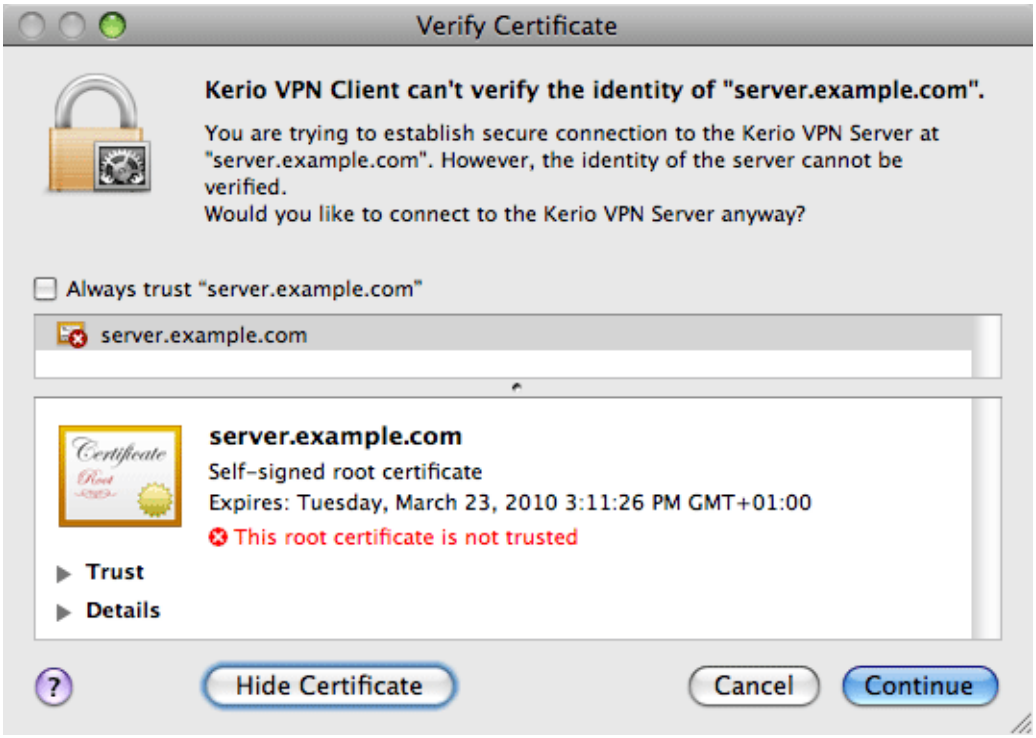


Figure 2 A dialog informing about detected problems with the VPN server's certificate

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.). If it is a certificate for Kerio Control, check **Always trust** and click **Continue**. The certificate will be saved in the system *Keychain* and from now on, no warning will be displayed.

Note: On *Mac OS X 10.5 Leopard* and higher, 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.

Setting a certificate as always trusted

It is not possible to set a self-signed certificate as always trusted:

1. In the window warning you that the certificate is not trustworthy (see figure 2), click on the certificate image and drag it to the desktop. This creates a file with the certificate on the desktop (e.g. `server.example.com.cer`).

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

2. 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.

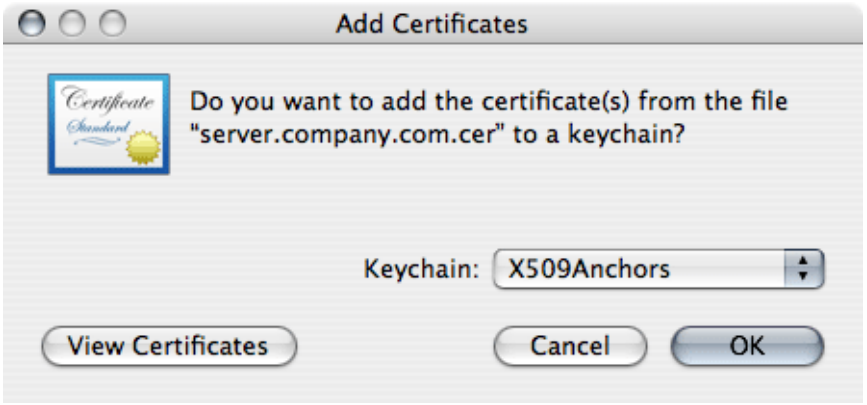


Figure 3 Saving certificates in keychain

3. 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.

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

5. 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.

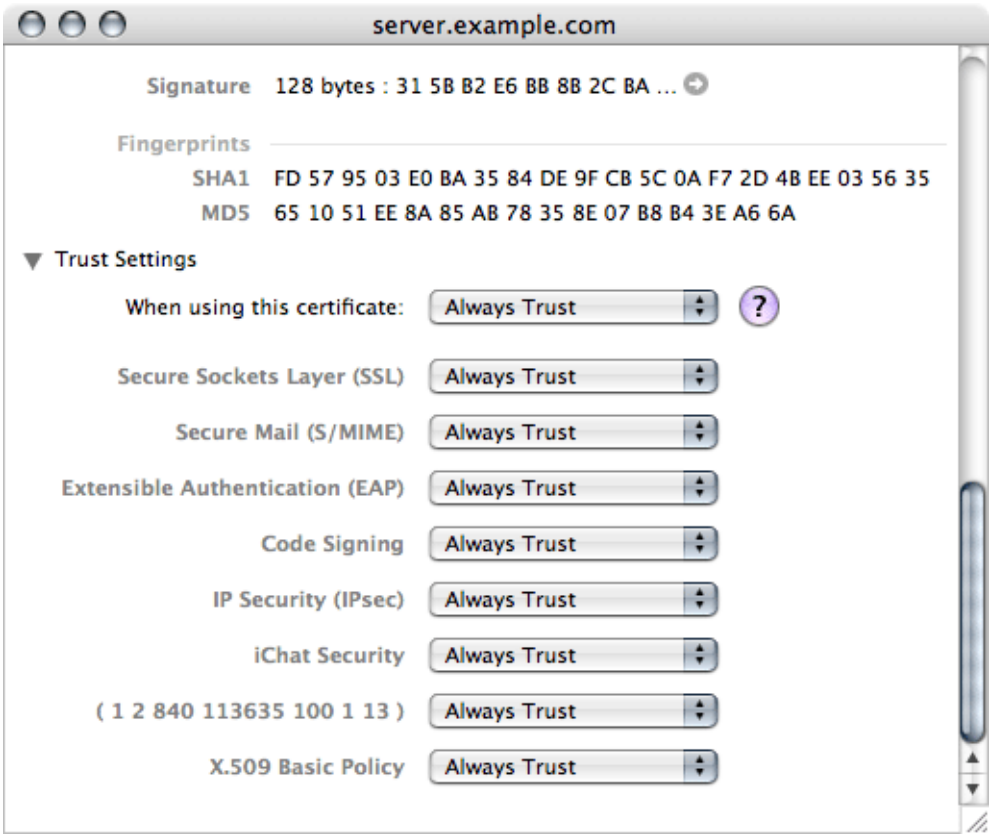


Figure 4 Certificate properties — setting a certificate as trusted

6. Close all running applications and log out of the system.
7. Reboot the system and try to establish a VPN connection to the particular server. From now on, no untrustworthy certificate warning should display.

Troubleshooting

The Kerio Control 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 Control VPN Client is installed, the following path is used by default:

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

Mac: `/usr/local/kerio/vpnclient/logs`

Linux: `/var/lib/kerio-control-vpn/logs`

Two log files are available here:

- `error.log` — critical errors, such as information that the Kerio VPN Client Service failed to start, 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 on Windows are stored in the corresponding folder of the user account of the user working with Kerio Control VPN Client. By default, the following path is used:

`Application Data\Kerio\VPNClient\logs`

Logs of the user interface on Mac are stored in the corresponding hidden subfolder of the home folder of the user working with the Kerio Control 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 Kerio VPN Client Service.
- `debug.log` — detailed information on activities of the application and detected errors.

Configuring IPsec VPN client on Apple OS X with machine authentication by SSL certificate

Summary

When you want to connect an Apple OS X computer to your company network through IPsec VPN and authenticate with an SSL certificate, you must configure the IPsec VPN server in Kerio Control, create an SSL certificate and import the certificate to Keychain Access. Then you must configure the VPN client as L2TP over IPsec.

Configuring Kerio Control

You must:

1. configure an IPsec VPN server
2. generate and export a new SSL certificate in the PKCS#12 format for VPN clients

To do this follow these steps:

1. Setup IPsec VPN server to use certificates issued by a Local Certification Authority (see details in the Configuring IPsec VPN article).
2. Go to **Definitions** → **SSL Certificates**.
3. Click **Add** → **New Certificate** and create a new certificate for VPN clients.

   Tzpe the hostname, not the IP address.

4. Click **Apply** in the **SSL Certificates** section.
5. Export this certificate in the PKCS#12 format (see figure 1).
6. In the **Export Certificate in PKCS#12 Format** dialog, use a password without national characters.
7. Check the **Include all certificates in the certification path if possible** box.

   Kerio Control exports all higher certificates including the certification autohority (it is the default Kerio Control Local Authority in figure 1).
8. Click **OK**.

Kerio Control creates and exports the certificate to your computer.

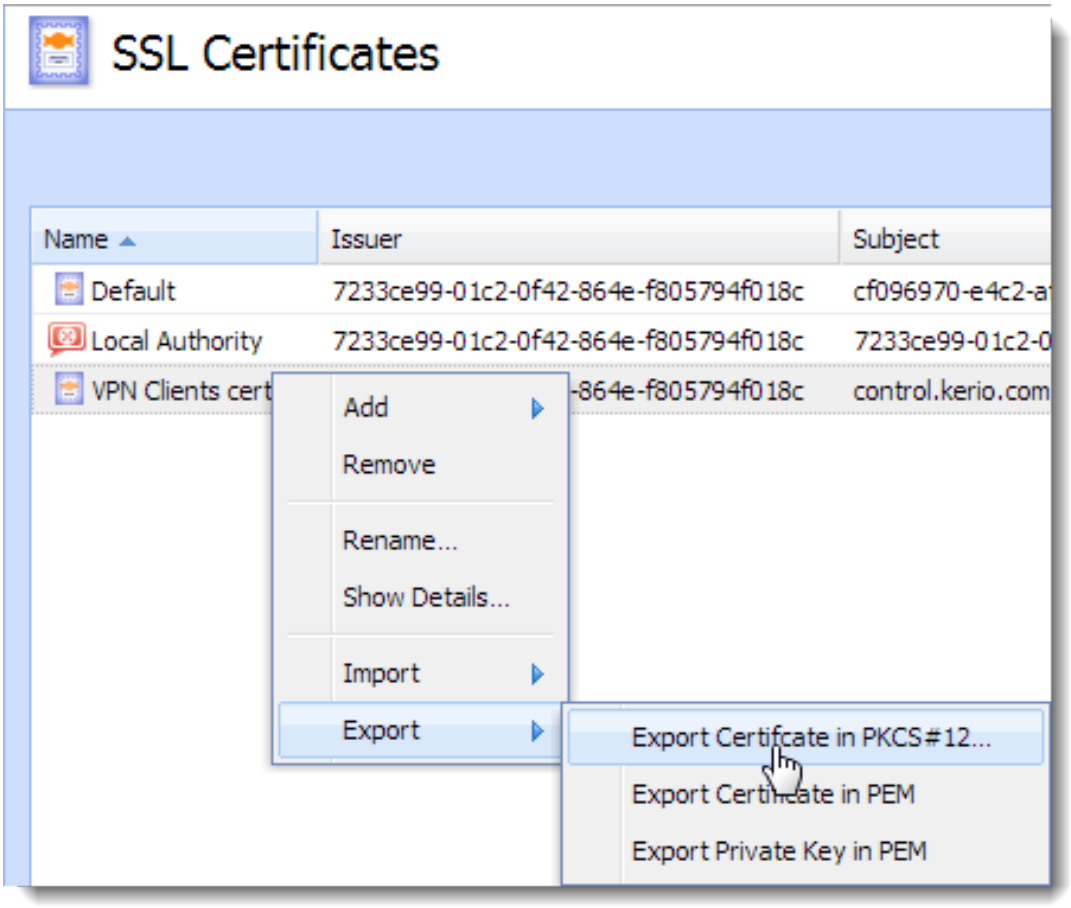


Figure 1 Export Certificate in PKCS#12

Importing the certificate

Import the SSL certificate to the Keychain Access utility in your Apple OS X:

1. Go to **Applications** → **Utilities** → **Keychain Access**.
2. Switch view to **System** keychain and unlock the keychain.

   Do not confuse keychains, default **Login** keychain is unwanted in this case.

3. Drag the PKCS#12 file, drop it to the **System** keychain.

   There are at least two Kerio Control certificates — one or more certificates (blue certificate icon) and Certification Authority (gold certificate icon) in the Keychain Access.

4. Locate the imported Certification Authority (CA) in the **System** keychain.

5. Set the CA trust properties to **Always trusted**.
6. Locate the imported certificate and ensure the certificate is trusted.

   Since Mac OS X 7:

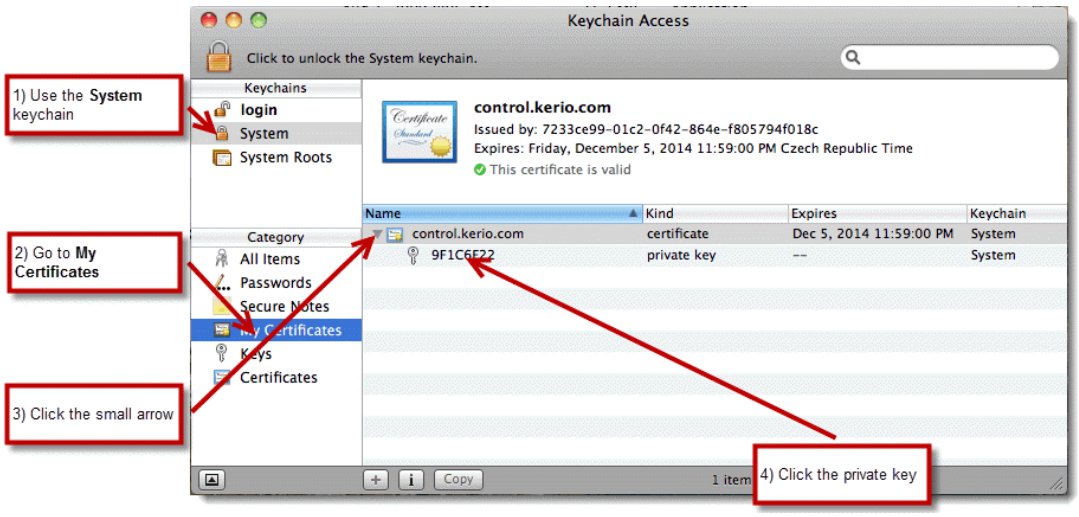


Figure 2 Mac OS 7 and higher settings

   a. In the **System** keychain, go to **My Certificates** (see figure 2).

   b. Find your certificate and click the small arrow.

      A private key appears.

   c. Double-click the private key and go to the **Access Control** tab.

   d. Click the + icon and add the following executable to the list: `/usr/sbin/racoon`

      If you don't see the `/usr` folder when browsing for the executable, use the **Show hidden files**.
      The shortcut is `cmd-shift-.` (cmd-shift-dot).

   e. Click **Open**.

Keychain Access uses your SSL certificate.

Creating VPN client on Apple OS X computer

You must create a VPN connection based on L2TP over IPsec:

1. Go to **System Preferences** → **Network**.
2. In the **Network** dialog, click the + icon and add **VPN**.
3. Select the **L2TP over IPsec** mode.

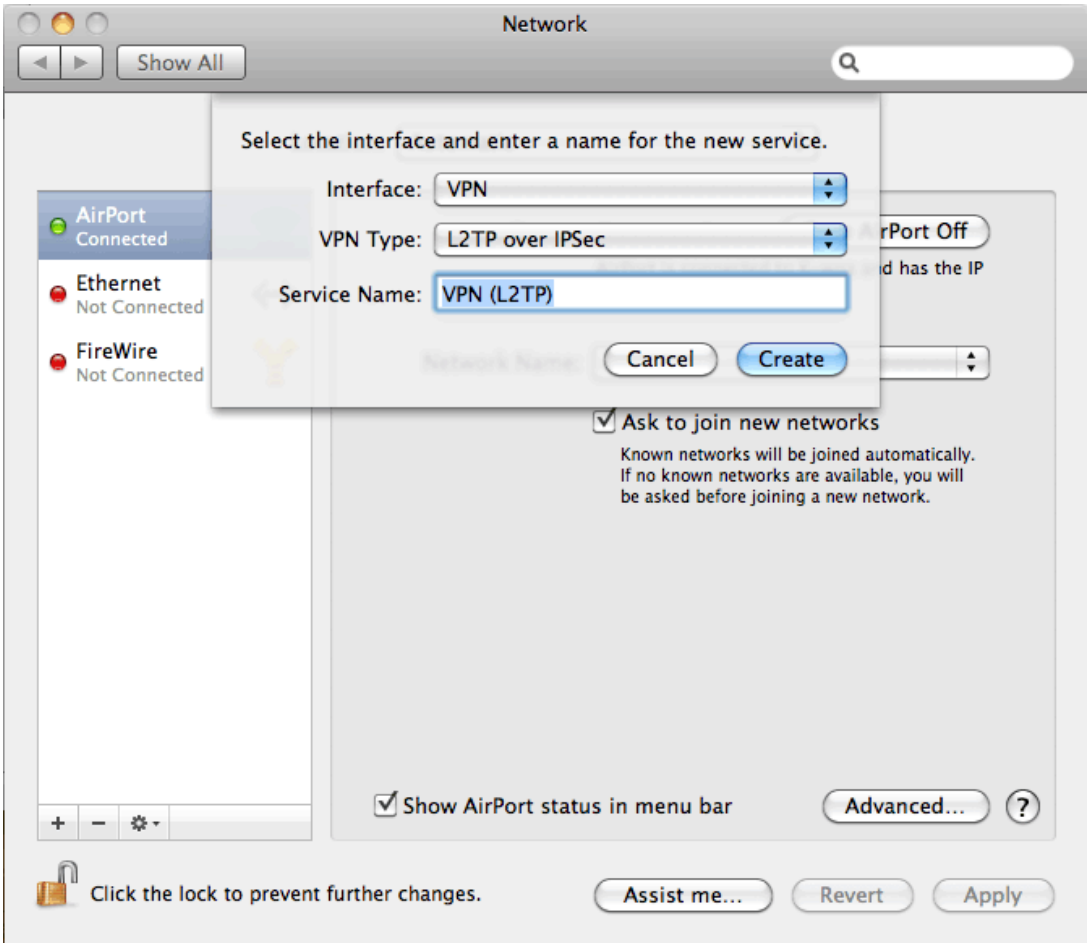


Figure 3 The Network dialog

4. Type a hostname of Kerio Control to **Server Address** and your Control's username to **Account Name**.

   Do not use IP address instead of the Kerio Control hostname.

5. Click **Authentication Settings**.

6. Set user authentication by password and type your Kerio Control's password.

   MS-CHAPv2 might be needed.

7. Set **Machine Authentication** by a certificate, click **Select** and select the certificate from step 6.

Apple OS X can connect to Kerio Control through IPsec VPN.

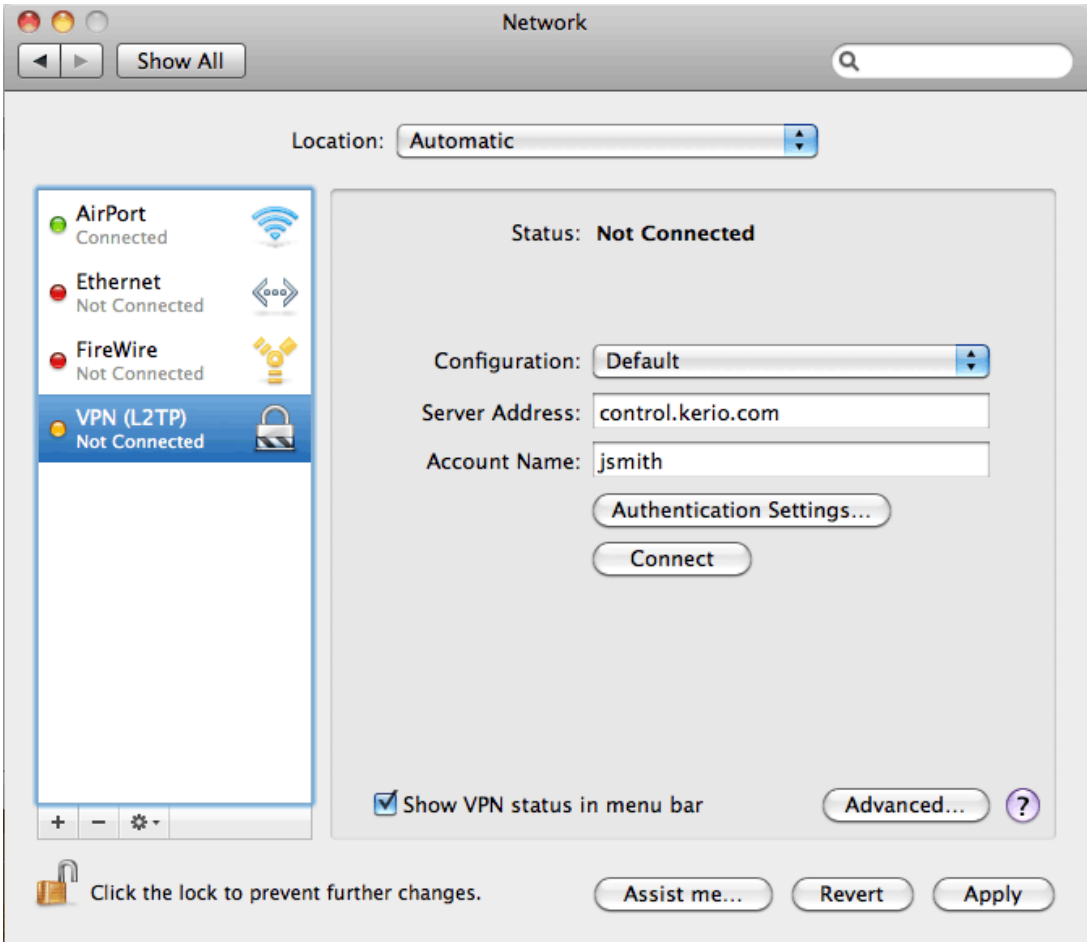


Figure 4 Type a hostname of Kerio Control and your user name

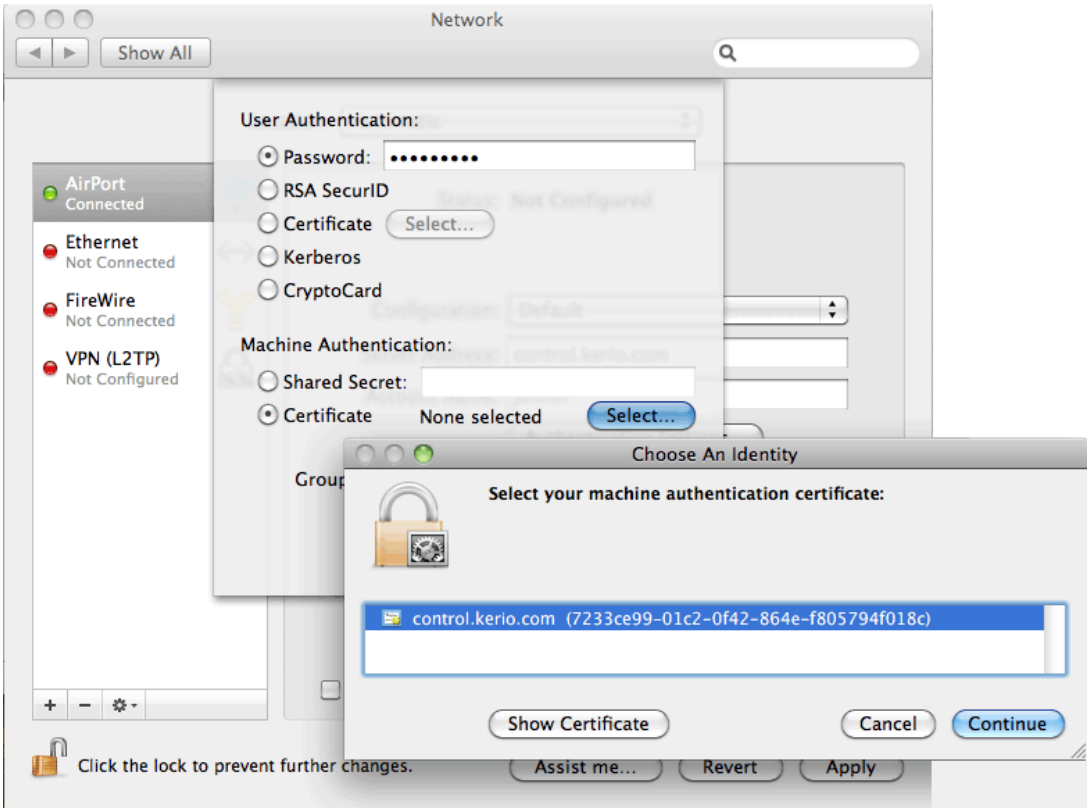


Figure 5 Set Machine Authentication by a certificate

Legal Notices

Trademarks and registered trademarks

Microsoft®, Windows®, Windows NT®, Windows Vista™, Internet Explorer®, ActiveX®, and Active Directory® are registered trademarks or trademarks of Microsoft Corporation.

Mac OS®, OS X®, iPad®, Safari™ and Multi-Touch™ are registered trademarks or trademarks of Apple Inc.

IOS® is registered trademark of Cisco Systems, Inc.

Linux® is registered trademark kept by Linus Torvalds.

VMware® is registered trademark of VMware, Inc.

Mozilla® and Firefox® are registered trademarks of Mozilla Foundation.

Chrome™ is trademark of Google Inc.

Kerberos™ is trademark of Massachusetts Institute of Technology (MIT).

Snort® is registered trademark of Sourcefire, Inc.

Sophos® is registered trademark of Sophos Plc.

avast!® is registered trademark of AVAST Software.

ClamAV™ is trademark held by Tomasz Kojm.

ESET® and NOD32® are registered trademarks of ESET, LLC.

AVG® is registered trademark of AVG Technologies.

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