

Kerio WinRoute Firewall 6

User Guide

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

This guide provides detailed description on user interfaces of *Kerio WinRoute Firewall*, version 6.7.0. The *Kerio VPN Client* application is described in a stand-alone document *Kerio VPN Client — User's Guide*. All additional modifications and updates reserved.

For current version of the product, go to <http://www.kerio.com/firewall/download>. For other documents addressing the product, see <http://www.kerio.com/firewall/manual>.

Information regarding registered trademarks and trademarks are provided in appendix [A](#).

Contents

- 1 Introduction 4**
- 2 Web user interface 5**
 - 2.1 Accessing the web interface and user authentication 5
 - 2.2 Status information and user statistics 8
 - 2.3 User preferences 10
 - 2.4 Dial-up 13
- 3 Kerio StaR — statistics and reporting 14**
 - 3.1 Connection to StaR and viewing statistics 14
 - 3.2 Accounting period 16
 - 3.3 Overall View 18
 - 3.4 User statistics 21
 - 3.5 Users' Activity 22
 - 3.6 Users by Traffic 28
 - 3.7 Top Visited Websites 29
 - 3.8 Top Requested Web Categories 31
- 4 Kerio Clientless SSL-VPN 33**
 - 4.1 Usage of the SSL-VPN interface 33
- A Legal Notices 39**
- Glossary of terms 40**
- Index 43**

Chapter 1

Introduction

Kerio WinRoute Firewall (further referred to as “*WinRoute*” or simply “firewall”) is a complex toolbox for connection of the LAN to the Internet, securing and monitoring of the network, as well as for control of users’ access to the Internet and monitoring of their browsing behaviour. *WinRoute* also provides various tools for non-administrators:

- Web user interface — used for user authentication at the firewall, viewing of status information and setting of user preferences. For details, see chapter [2](#).
- *Kerio StaR* — this component provides detailed information on user browsing activities, visited web pages, volume of transferred data, etc. For details, see chapter [3](#).
- *Kerio SSL-VPN* — allows remote access from the Internet to files stored in shared folders on LAN computers. For details, see chapter [4](#).

All the items described above are so called web interfaces. This means that they are accessed (and controlled) from a web browser, simply by using a specific address (URL). For full and correct functionality, any of the supported web browsers is required:

- *Internet Explorer 6 and higher*
- *Firefox 1.5 and higher*
- *Safari*

This user guide addresses features of individual interfaces as well as options of their use. It touches on configuration options of the very firewall. Generally, it is recommended to contact your firewall administrator, should any issues arise.

Chapter 2

Web user interface

The most basic and bare function of the *WinRoute's* web interface is user login to the firewall (authentication at a session initiation). 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 user attempts 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 user's 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),
- Set preferred language for the web interface and notifications and alerts sent by email (e.g. alerts on a virus detected or on reaching and exceeding the transferred data volume quota),
- Change password (in specific cases only).

Users with corresponding privileges can also:

- View Internet usage statistics (see chapter [3](#)),
- Dial and hang up dialed Internet lines.

2.1 Accessing the web interface and user authentication

The *WinRoute's* web interface is available in two versions: SSL-secured or unsecured (both versions include identical pages).

Use the following address (server refers to the name or IP of the *WinRoute* host, 4080 represents a standard HTTP interface port) to open the unsecured version of the web interface.

`https://server:4080/`

To use the encrypted version specify the HTTPS protocol and number of the port of the encrypted Web interface (default is 4081):

`https://server:4081/`

Users logged in

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

If the particular host belongs to the *Windows* domain, user can set to be authenticated automatically at their entrance to the web interface. If not, the firewall's authentication page is opened first waiting for a valid login username and password. The login information usually match the authentication details used for login to the user's operating system.

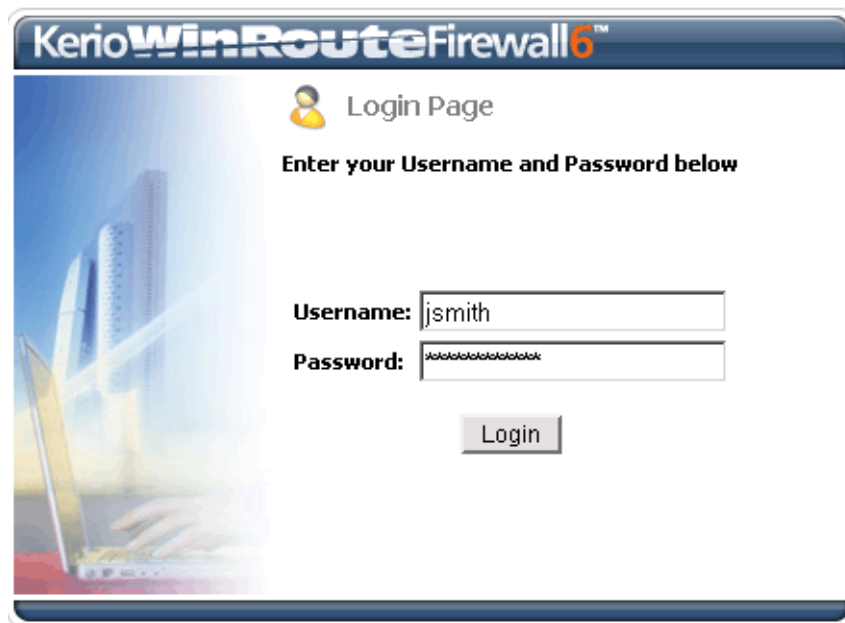


Figure 2.1 Login page of the firewall's Web interface

Warning

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

If the user is re-directed to the page automatically (after inserting the URL of a page for which the firewall authentication is required), he/she will be re-directed to the formerly requested website after successful login attempt. Otherwise, the web interface's welcome page is displayed.

The welcome page of the web interface differs according the current user's access rights:

- If the user is allowed to view statistics, the web interface will switch to the *Kerio StaR* mode and it will start with the page of overall statistics (the *overall* tab — for details, see chapter 3). The *My Account* option available at the upper-right corner can be used to switch to the user settings. It is possible to return to the statistics page by the *Statistics* link.
- If the user is not allowed to view statistics, user status info page is displayed instead (see chapter 2.2).

Log out

Once finished with activities where authentication is required, it is recommended to log out of the firewall by using the *Logout* button. It is important to log out especially when multiple users work at the same host. If a user doesn't log out of the firewall, their identity might be misused easily.

User can be logged on the firewall even if they have not used the web interface — e.g. if the firewall required user authentication during access to a website. To make user avoid opening the web interface when finishing their work and clicking on *Logout*, *WinRoute* includes a direct link for user logout:

`http://server:4080/logout`

or

`https://server:4081/logout`

This URL performs immediate logout of the user without the need of opening of the web interface's welcome page.

Hint

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

Note: *WinRoute* also allows automatic logout if idle — if the user currently logged in a session uses no Internet service for a defined time period (usually 2 hours), they are logged out of the firewall automatically. This handles situations when a user forgets to log out.

User password authentication

If an access to the web interface is attempted when an authentication from the particular host is still valid (the user has not logged out and the timeout for idleness has not expired) but the particular session¹ has already expired, *WinRoute* requires user authentication by password. This precaution helps avoid misuse of the user identity by another user.

Under such conditions, a special version of the login page is opened.



Figure 2.2 User authentication by password

Authenticated user connecting to the web interface can continue their work in the interface after entering their password. If a new user attempts to connect to the web interface, the connected user must log out first and then the new user is asked to authenticate by username and password.

2.2 Status information and user statistics

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.

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).

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.

Hint

Week and month starting days can be changed by setting of so called accounting period in the *WinRoute* configuration.

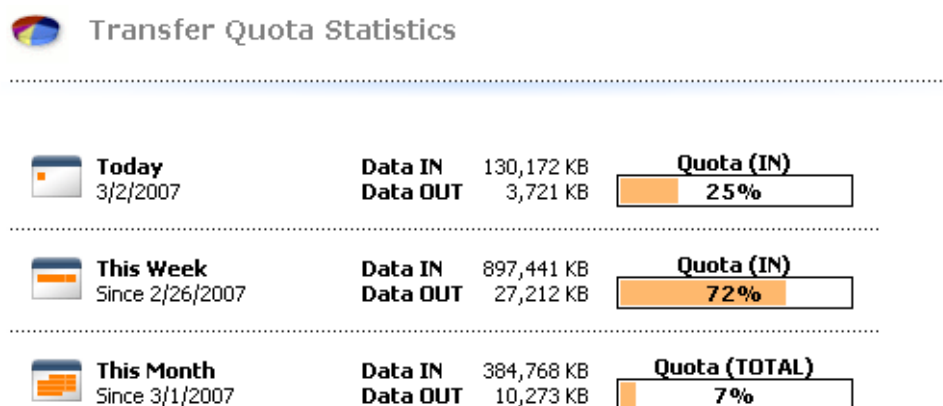


Figure 2.3 Transfer Quota Statistics

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

 Web Site Restrictions




URL	Allowed	Content Type	Time Interval
.kerio.com	 Yes	Any	Any
.ads. */ad/* *adframe* */ad-handler/* */ads/* */banner/* */please/showit* */popup/* */popups/* *.gator.com* *adserv* ad.* ad?.* ad??.* ad???.* ads???.*	 No	Any	Any
.windowsupdate.com/ *update.microsoft.com/*	 Yes	Any	Any

Figure 2.4 Current web restrictions and rules

2.3 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 *WinRoute* 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)

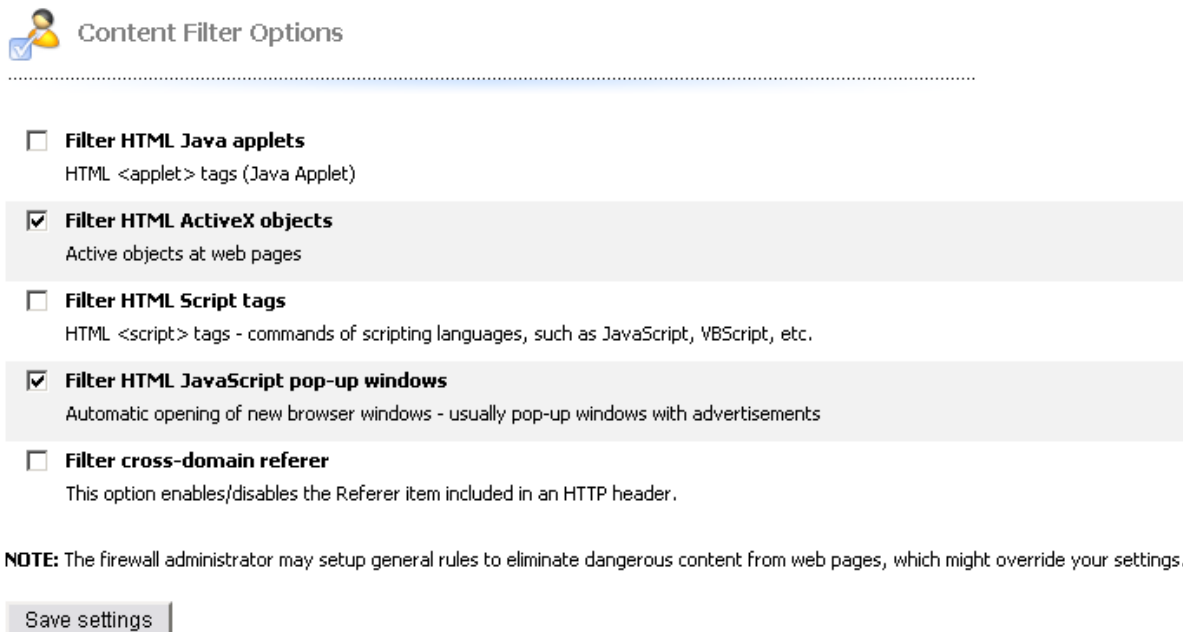


Figure 2.5 Customized Web objects filtering

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).

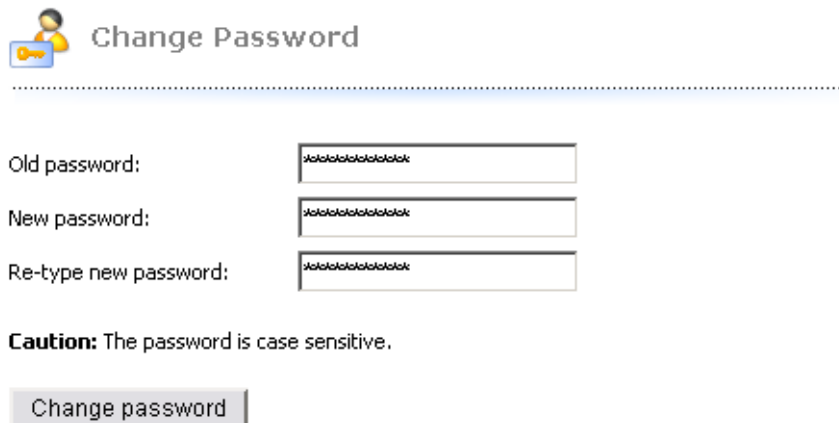
Save settings


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 cannot be changed if the user is authenticated with a *Windows* domain account (in such case, the *Change password* section is not displayed).

To change a password, enter the current user password, new password, and the new password confirmation into the appropriate text fields. Save the new password with the *Change password* button.



 **Change Password**

Old password:

New password:

Re-type new password:

Caution: The password is case sensitive.

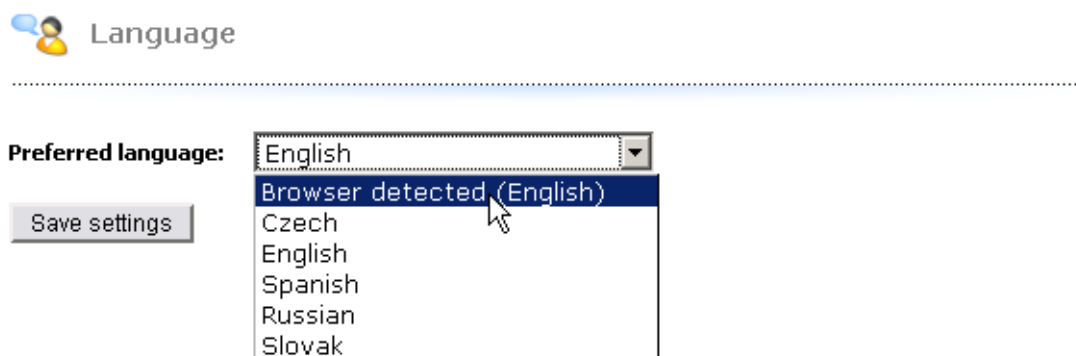
Figure 2.6 Editing user password


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,
- *Kerio StaR*,
- Cautions and further information sent to users by email (e.g. warning of a virus or notification of exceeding of the transfer quota).

Language preferences are not applied to the *Kerio Clientless SSL-VPN* interface where the language is inherited from the web browser configuration.



 **Language**

Preferred language:

- Browser detected (English)
- Czech
- English
- Spanish
- Russian
- Slovak


Figure 2.7 Setting language preferences of the web interface

In the current version of *WinRoute*, 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.

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

2.4 Dial-up

Users with rights for controlling dial-ups in *WinRoute* can dial and hang up individual RAS lines and view their status on the *Dial-up lines* tab. This tab lists all dial-up lines defined in *WinRoute*.



RAS Interfaces

RAS Interface	Current state	Action	Connection time	Incoming	Outgoing
Dial-up connection	Disconnected	Click to Dial			

This page is refreshed automatically.

Figure 2.8 Web interface — dial-ups control

The following information items are provided for each line:

- Name of the line in *WinRoute*.
- Current state — *Disconnected*, *Connecting*, *Connected*, *Disconnecting*.
- 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).

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

Chapter 3

Kerio StaR — statistics and reporting

The *WinRoute's* web interface provides detailed statistics on users, 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 *WinRoute* 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.

Note:

1. Users should be informed that their browsing activities are monitored by the firewall.
2. Statistics and reports in *WinRoute* 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.

3.1 Connection to StaR and viewing statistics

To view statistics, user must authenticate at the *WinRoute's* web interface first. User (or the group the user belongs to) needs rights for statistics viewing. For details on authentication at the *WinRoute's* web interface, see chapter [2.1](#).

Access to statistics

From any host from which access to the *WinRoute's* web interface is allowed, *Kerio StaR* can be opened by any of the methods described below:

- At `https://server:4081/star` or `http://server:4080/star` This URL works for the *StaR* only. If the user has not appropriate rights to view statistics, an error is reported.
- At `https://server:4081/` or `http://server:4080/`. This is the primary URL of the *WinRoute's* web interface. If the user possesses appropriate rights for stats viewing, the *StaR* welcome page providing overall statistics (see below) is displayed. Otherwise, the *My Account* page is opened (this page is available to any user).

Warning

For access from the Internet (i.e. from a host outside the local network), only the secured web interface will probably be available. The other option (connection via the non-secured web interface) would be too risky.

StaR page in the web interface

The page is divided into the following tabs:

- *Overall* — overall statistics including traffic of all local users (volumes of transferred data, top users, top web pages, etc.). This section is opened as a welcome page immediately upon a successful logon.
- *Individual* — statistics of individual users (volumes of transferred data, top web pages visited by the user, etc.).
- *Users' Activity* — detailed information about activity of individual users (visited websites, files transferred via FTP, remote access to other hosts, etc.).
- *Users by Traffic* — table and chart for volumes of data transferred by individual users.
- *Visited Sites* — overview of the ten most frequently visited web domains. A chart and table of top users having visited the greatest number of web pages of the domain is provided.
- *Web Categories* — the top ten most frequently visited web categories (in accordance with the *Kerio Web Filter's* categorization). A chart referring to each web category is provided, along with table of users with the highest number of requests for sites belonging to the particular category..

Detailed descriptions of individual sections are provided in the following chapters.

Updating data in StaR

First of all, the *StaR* interface is used for gathering of statistics and creating of reviews for certain periods. To *WinRoute*, gathering and evaluation of information for *StaR* means processing of large data volumes. To reduce load on the firewall (and slowdown of Internet connection), data for *StaR* is updated approximately once an hour. The top right corner of each *StaR* page displays information about when the last update of the data was performed.

For the reasons mentioned above, the *StaR* interface is not useful for real-time monitoring of user activity.

Print formatting

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

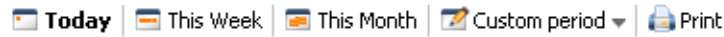


Figure 3.1 Kerio StaR — toolbar

Clicking on *Print* displays the current *StaR* 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*.

Warning

For technical reasons, pages of *StaR* 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.

3.2 Accounting period

Most frequently, statistic information needed refer to a certain time period (today, last week, etc.). This period is called *accounting period*.

Accounting period can be set in the toolbar at the top of the *Kerio StaR* page.



Figure 3.2 Kerio StaR — toolbar and accounting periods

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 *WinRoute* 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.

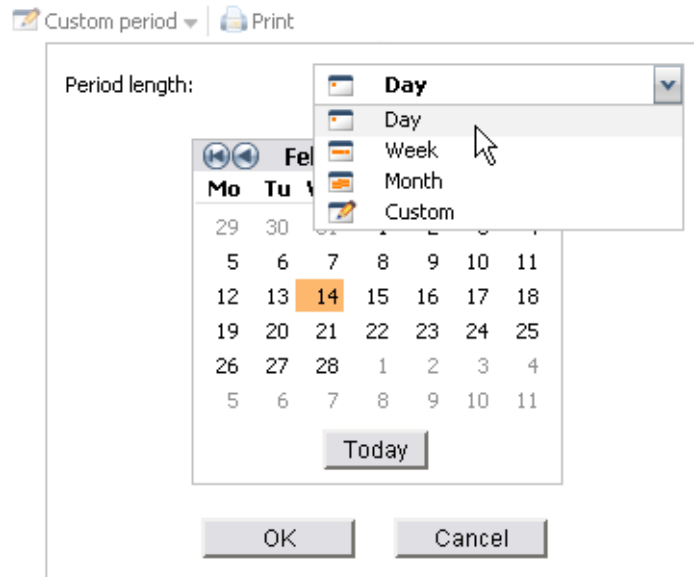


Figure 3.3 Selection of accounting period

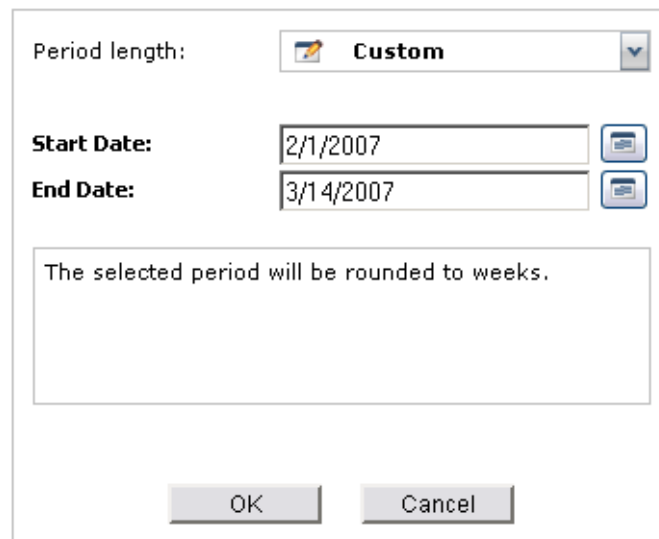


Figure 3.4 Custom accounting period

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 textfield.

The selected period applies to all tabs until a next selection (or until closing of the *Kerio StaR* interface). The “today” period is set as default and used upon each startup of the *Kerio StaR* interface.

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.

3.3 Overall View

The *Overall* tab provides overall statistics for all users within the local network (including anonymous, i.e. unauthenticated users) for the selected accounting period.

Traffic by periods

The first chart provides information on the volume of data transferred in individual sub-periods of 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 only² (for details, see chapter 3.2).

● Daily Traffic

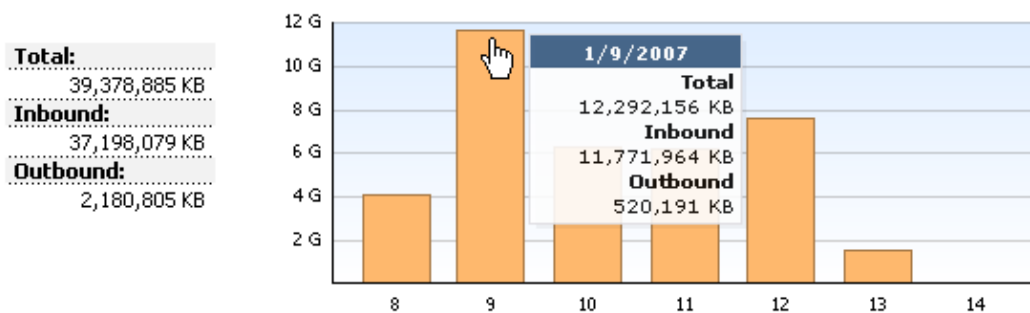


Figure 3.5 Daily Traffic

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.

Note: WinRoute “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.

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.

• Top Visited Websites

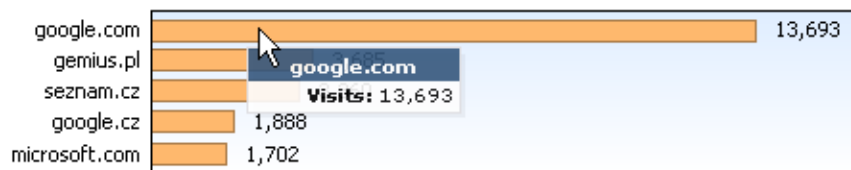


Figure 3.6 Chart of top visited web domains

Top Requested Web Categories

This chart shows top five web categories requested in the selected period sorted by the *Kerio 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 Requested Web Categories

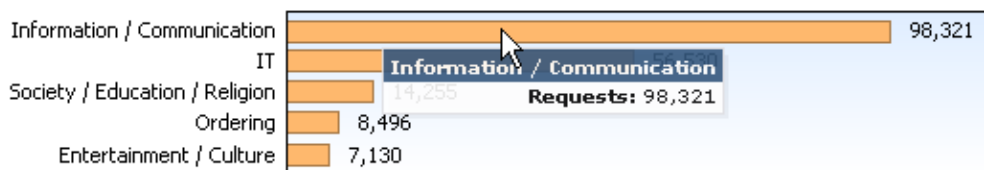


Figure 3.7 The chart of top requested web categories

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 (see chapter 3.4) 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, this information is not very useful and, therefore, it is recommended to set firewall to always require authentication.
3. Method of username displaying in the table can be set in the *WinRoute* configuration.

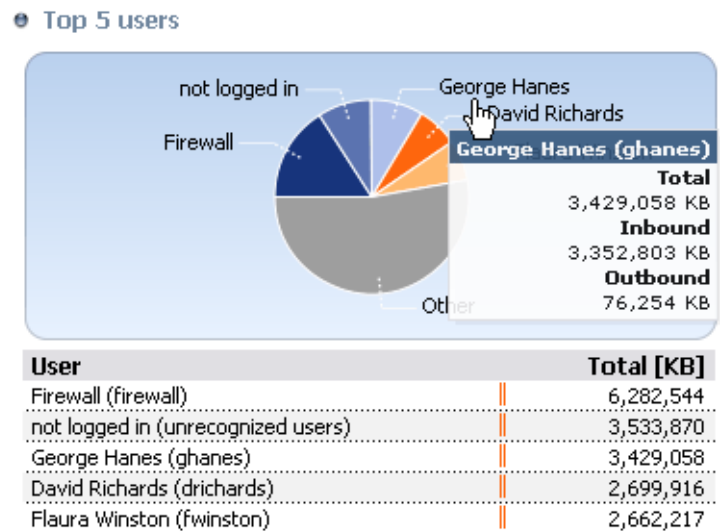


Figure 3.8 Top 5 users statistics

Only full names are shown in charts (or usernames if the full name is not defined in the account of the particular user).

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. 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.).

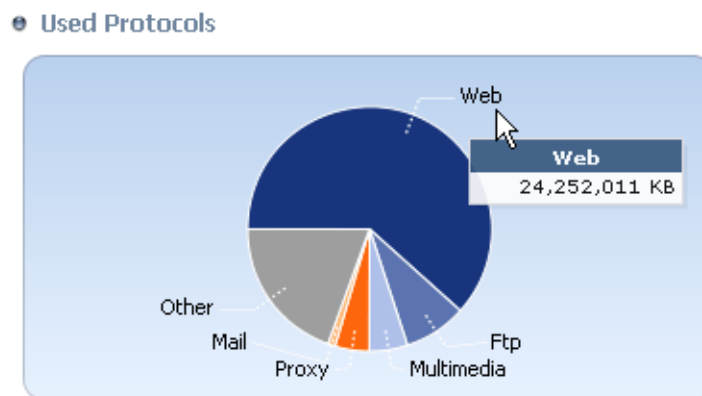


Figure 3.9 Parts of individual protocols in the total volume of transferred data

For better reference, *WinRoute* 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*),
- *P2P* — file-sharing protocols (*peer-to-peer* — e.g. *DirectConnect*, *BitTorrent*, *eDonkey*, etc.). The traffic is accounted only if *WinRoute* 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*, *MSN Messenger*, *Yahoo! Messenger*, etc.
 - *Other* — any traffic which does not belong to any of the previously described categories.

Note:

1. The *No data available* alert informs that no data is available in *WinRoute*'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. *WinRoute* 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, *WinRoute* offers another period where data for the requested statistics might be found.

● Top Visited Websites

The requested data is not available for selected time period.
Please select different time period which (partially) covers the requested period:


-  1/1/2007 - 1/31/2007
-  1/1/2007 - 1/7/2007
-  1/8/2007 - 1/14/2007
-  1/15/2007 - 1/21/2007
-  1/22/2007 - 1/28/2007

Figure 3.10 Selection of a new time period for website statistics

3.4 User statistics

The *Individual* tab allows showing of statistics for a 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.



Figure 3.11 Selection of a user

Hint

Method of username displaying can be set in the *WinRoute* configuration.

When a user is selected, full name, username and email address are displayed (if defined in the user account). The *View User's Activity* link switches *StaR* to the *Users' Activity* page providing detailed information on traffic of the particular user in the selected time period (for details, see chapter [3.5](#)).

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

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

For detail information on individual statistic sections, see chapter [3.3](#).

3.5 Users' Activity

The *Users' Activity* tab allows showing of detailed information on “browsing activities” of individual users. This section answers questions like *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.)

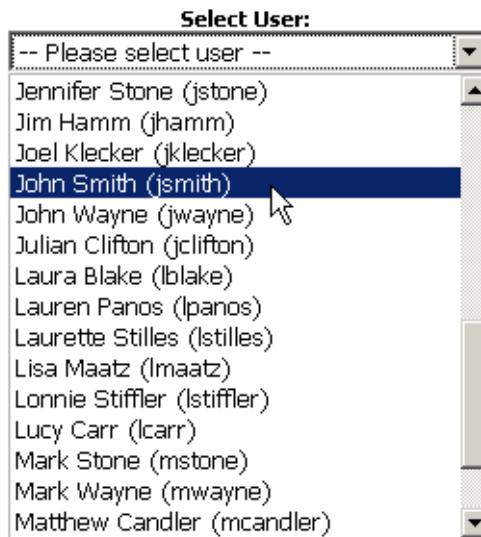


Figure 3.12 Selection of a user



User's Activity - John Smith

Username: jsmith
 E-mail: jsmith@company.com
 Description: Technician

Figure 3.13 User's Activity — user info

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 it 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:
 - *Updating data in StaR* — to *WinRoute*, gathering and evaluation of information for *StaR* means processing of large data volumes. To reduce load on the firewall, data for *StaR* is updated approximately once an hour (see information about the last 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.



Start	Duration	Details
09:06 am	0:20	google.com Visits: 2 Google
09:06 am	0:59	google.cz: kerio vpn client kerio.com Visits: 4 Kerio Technologies Inc. Kerio WinRoute Firewall VPN support
09:07 am	2:47	di.fm Visits: 4 Categories: Entertainment / Culture, IT Digitally Imported Radio - Free Internet Radio Station DI.fm
09:08 am	1:41	wcmcs.net Visits: 3 Untitled Page
09:10 am	0:47	www.cnn.com Visits: 5 Categories: Entertainment / Culture, Information / Communication CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News
09:14 am	4:55	youtube.com Visits: 11 Categories: Entertainment / Culture YouTube - Broadcast Yourself.
09:59 am	0:16	google.com Visits: 2 Categories: Information / Communication Google
09:59 am	0:01	emule.com: emule emule-project.net Visits: 1 Categories: IT eMule-Project.net - Official eMule Homepage, Downloads, Help, Docu, News...
09:59 am	0:15	emule.com Visits: 2 Categories: IT eMule - eMule Plus - download eMule

Figure 3.14 User's Activity — access to web pages

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

Each record of connection to a web page includes:

- Start time and duration (see above).
- Domain to which the page belongs (statistics in *StaR* are created by domains — see e.g. chapter 3.7).
- Number of visits — the number says how many times the page was visited within this activity.
- Page category — site classification by the *Kerio Web Filter* module. If *Kerio Web Filter* 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:

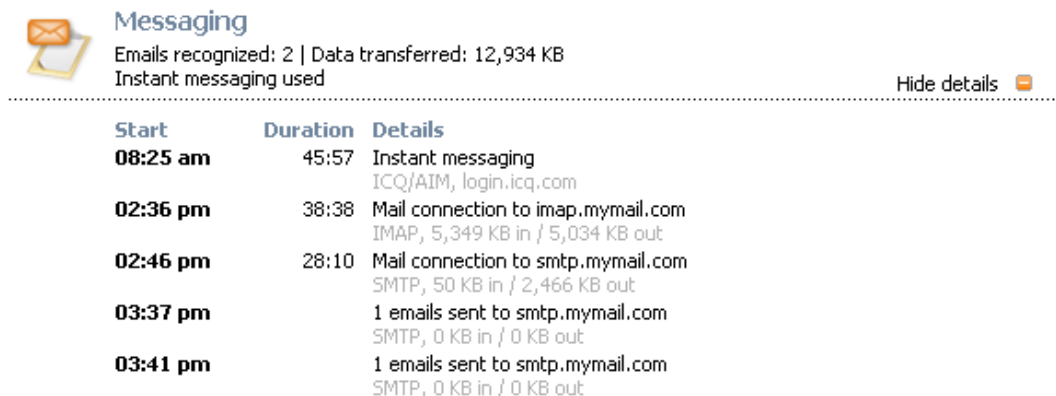
- Name (or IP address) of the server.
- Protocol (*HTTPS*).
- Volume of data transferred in each direction.

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 screenshot shows a 'Messaging' section with a sub-header 'Emails recognized: 2 | Data transferred: 12,934 KB Instant messaging used' and a 'Hide details' button. Below is a table with columns 'Start', 'Duration', and 'Details'.

Start	Duration	Details
08:25 am	45:57	Instant messaging ICQ/AIM, login.icq.com
02:36 pm	38:38	Mail connection to imap.mymail.com IMAP, 5,349 KB in / 5,034 KB out
02:46 pm	28:10	Mail connection to smtp.mymail.com SMTP, 50 KB in / 2,466 KB out
03:37 pm		1 emails sent to smtp.mymail.com SMTP, 0 KB in / 0 KB out
03:41 pm		1 emails sent to smtp.mymail.com SMTP, 0 KB in / 0 KB out

Figure 3.15 User's Activity — email and Instant Messaging

The header informs about number of detected email messages and total volume of data transferred by email protocols. *WinRoute* 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 connection), 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).

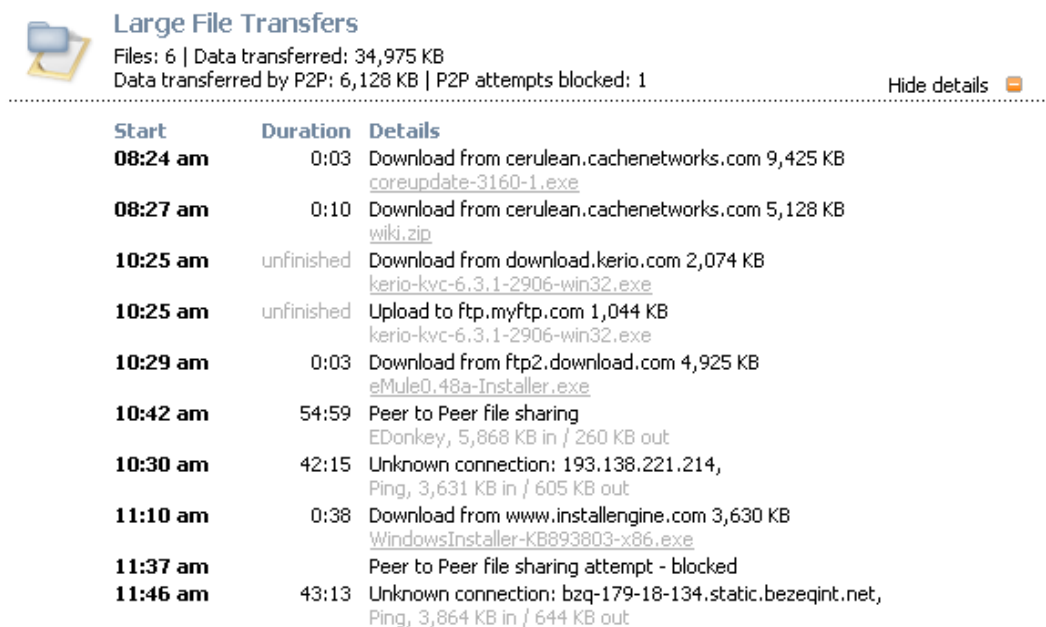


Figure 3.16 User’s Activity — large file transfers and usage of P2P networks

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).

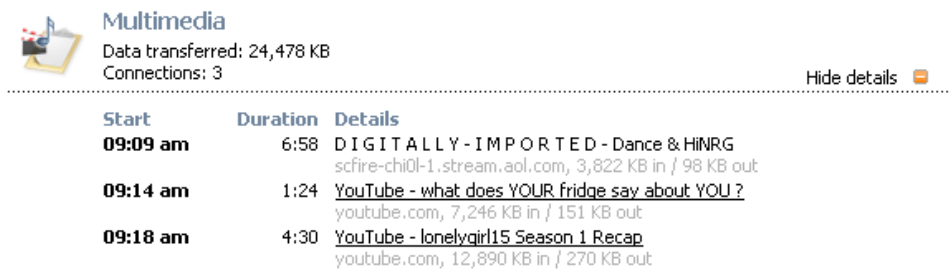


Figure 3.17 User's Activity — multimedia

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.

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.

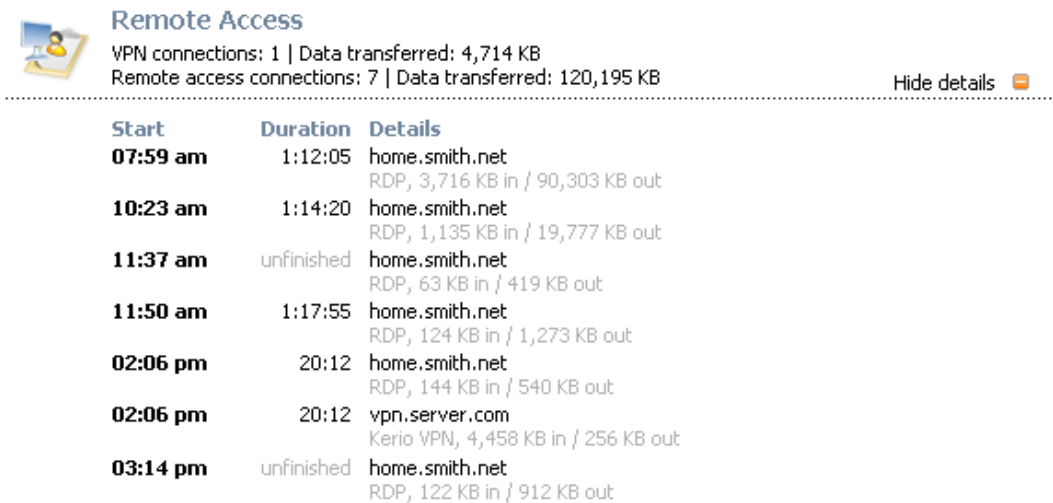


Figure 3.18 User's Activity — remote and VPN access

3.6 Users by Traffic

The *Users by Traffic* section shows table of all users sorted by volume of transferred data. 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. streams from online radio channels).

Note: For detailed description of protocol classes distinguished in *Kerio StaR*, see chapter 3.3.

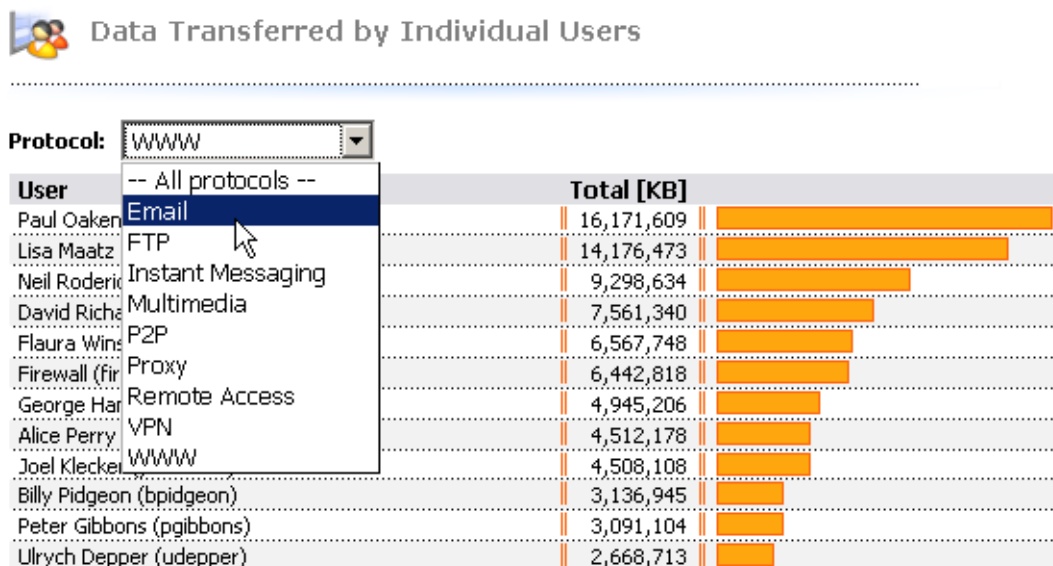


Figure 3.19 The Users by Traffic table

Each row of the table provides name of the user along with information of data transferred by the user: incoming data (download), outgoing data (upload) and the total volume of transferred data. If a particular protocol is selected, only total volume of transferred data is displayed.

Click on the name of a user to switch to the *Individual* tab and see detailed statistics of the particular user (see chapter 3.4).

Hint

Method of username displaying in the table can be set in the *WinRoute* configuration.

3.7 Top Visited Websites

The *Visited Sites* tab includes statistics for the top ten most frequently visited web domains. These statistics provide for example the following information:

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

The chart at the top of the tab shows top ten 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.

Note: *WinRoute* “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.

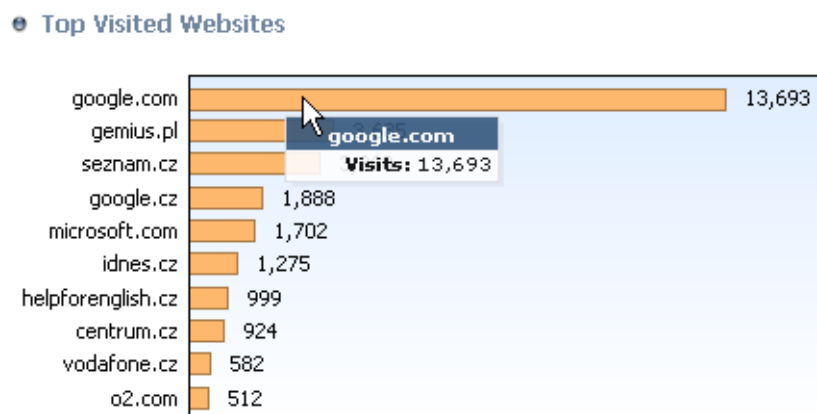


Figure 3.20 Top visited web domains

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.

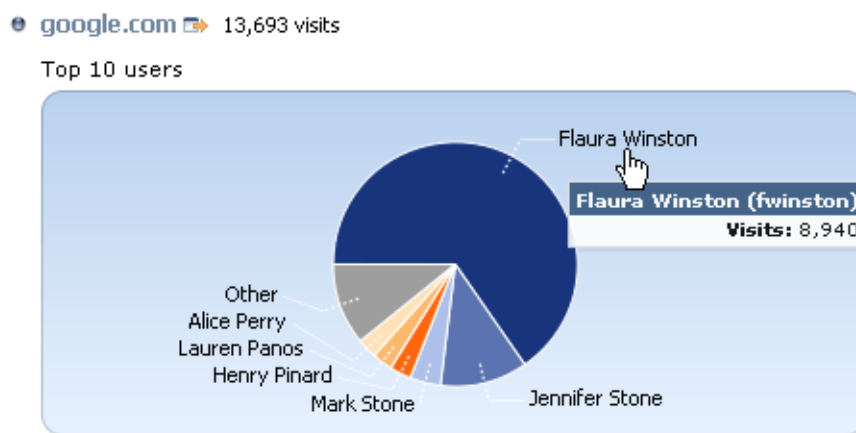


Figure 3.21 Chart of top active users for the particular domain

- The table next to the chart shows the most active users sorted by number of visits at websites within the particular domain (up to ten users).

User	Visits
Flora Winston (fwinston)	8,940
Jennifer Stone (jstone)	1,588
Mark Stone (mstone)	560
Henry Pinard (hpinard)	391
Lauren Panos (lpanos)	375
Alice Perry (aperry)	357
Norman Flanders (nflanders)	294
Lisa Maatz (lmaatzt)	222
Paul Oakenfold (poakenfold)	144
Ulrych Depper (udepper)	98

Figure 3.22 Table of top active users for the particular domain

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 (see chapter 3.4).

Hint

Method of username displaying in the table can be set in the *WinRoute* configuration. Only full names are shown in charts (or usernames if the full name is not defined in the account of the particular user).

3.8 Top Requested Web Categories

The *Web Categories* section includes statistics of the top ten visited web pages categorized by the *Kerio Web Filter*. Statistics of categories provide more general information of visited websites. For example, the information help figure out how much users browse websites not related to their work issues.

The chart on the left shows the top ten 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 (see chapter 3.7).

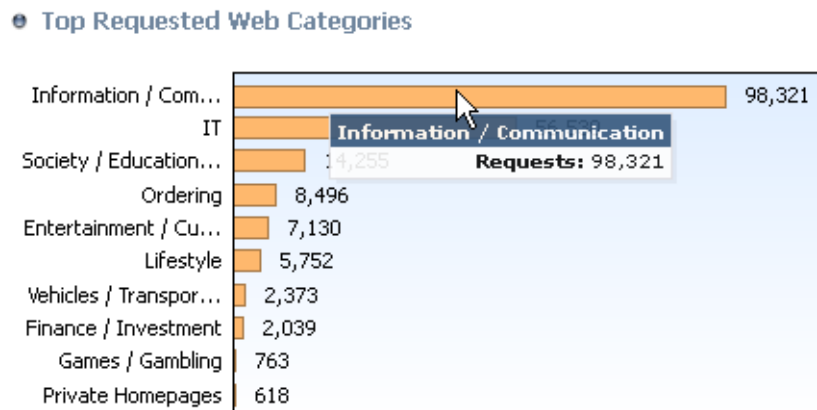


Figure 3.23 Top visited websites sorted by categories

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 (up to ten users).

Information / Communication 98,321 requests

Top 10 users

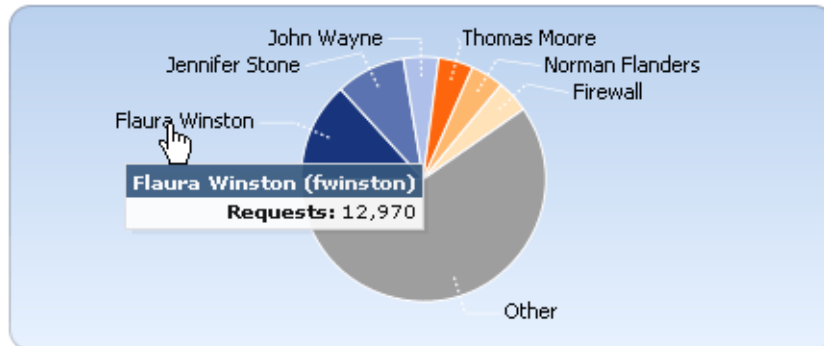


Figure 3.24 Chart of top users for a selected web category

User	Requests
Flaura Winston (fwinston)	12,970
Jennifer Stone (jstone)	9,064
John Wayne (jwayne)	4,572
Thomas Moore (tmoore)	4,537
Norman Flanders (nflanders)	4,310
Firewall (firewall)	4,240
Alice Perry (aperry)	4,025
George Hanes (ghanes)	3,715
Andrew McKay (amckay)	3,440
Laurette Stilles (lstilles)	2,939

Figure 3.25 Table of top users for a selected 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 (see chapter [3.4](#)).

Hint

Method of username displaying in the table can be set in the *WinRoute* configuration. Only full names are shown in charts (or usernames if the full name is not defined in the account of the particular user).

Note: 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.

Chapter 4

Kerio Clientless SSL-VPN

Kerio Clientless SSL-VPN (thereinafter “*SSL-VPN*”) is a special interface used for secured remote access to shared items (files and folders) in the network protected by *WinRoute* via a web browser.

To a certain extent, the *SSL-VPN* interface is an alternative to *Kerio VPN Client*. Its main benefit is that it enables an immediate access to a remote network from any location without any special application having been installed and any configuration having been performed (that’s the reason for calling it *clientless*). The main disadvantage of this alternative is that network connections are not transparent. *SSL-VPN* is, in a manner, an alternative to the *My Network Places* system tool) — it does not enable access to web servers or other services in a—remote network.

SSL-VPN is suitable for an immediate access to shared files in remote networks in such environments where it is not possible or useful to use *Kerio VPN Client*.

4.1 Usage of the SSL-VPN interface

The interface can be accessed from most of common web browsers (see chapter [1](#)). Specify URL in the browser in the

`https://server/`

format, where `server` represents the name or IP address of the *WinRoute* host. If *SSL-VPN* uses another port than the default port for *HTTPS* (443), it is necessary to specify the used port in the URL, e.g.

`https://server:12345/`

Upon a connection to the server, the *SSL-VPN* interface’s welcome page is displayed localized to the language set in the browser. If the language defined as preferred is not available, the English version will be used.

For access to the network by *SSL-VPN*, authentication to the particular domain at the login page by username and password is required. The login information usually match the authentication details used for login to the user’s operating system. Any operations with shared files and folders are performed under the identity of the user currently logged in.



Figure 4.1 Clientless SSL-VPN — login dialog

Handling files and folders

The way the *SSL-VPN* interface is handled is similar to how the *My Network Places* system window is used.

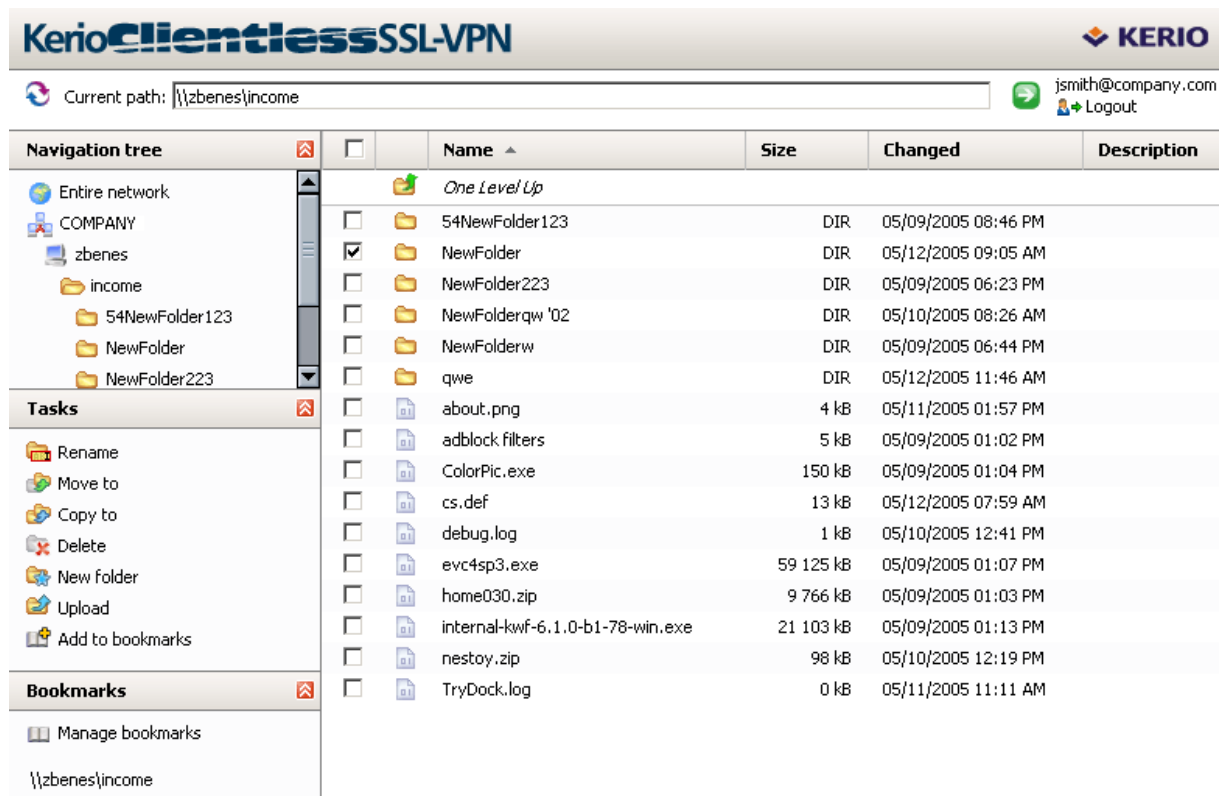


Figure 4.2 Clientless SSL-VPN — main page

At the top of the page, an entry is available, where location of the demanded shared item (so called *UNC path*) can be specified — for example:

```
\\server\folder\subfolder
```

The path may be specified regularly even if folder or/and file names include blank spaces — for example:

```
\\server\my folder\my file.doc
```

All shared items in the domain can be browsed using a so called navigation tree on the left. The navigation tree is linked to the entry (this means that in the entry, the path associated with the selected item in the tree is displayed, and vice versa — if a path is entered in the line, a corresponding item is selected in the tree).

Right under the navigation tree, actions available for the specified location (i.e. for the selected item or folder) is provided. The basic functions provided by the *SSL-VPN* interface are download of a selected file to the local host (the host where the user's browser is running) and uploading a file from the local host to a selected location in the remote domain (the user must have write rights for the destination). Downloading or uploading of more than one file or of entire folders is not possible.

For files and folders, any standard functions, such as copying, renaming, moving and removals, are still available. Files and folders can be copied or moved within the frame of shared files in the particular domain. In the current path, new folders can be created and empty folders can be removed.

Antivirus control

WinRoute administrator can set antivirus control for files transferred via the *SSL-VPN* interface (only saved files are scanned for viruses by default). The *SSL-VPN* interface thus guarantees security of files transferred between the client host and a remote local network. If a virus is detected in either downloaded or saved file, the operation is interrupted and a warning is displayed.

Bookmarks

For quick access to frequently used network items, so called bookmarks can be created. Bookmarks work on principles similar to the *Favorites* tool in *Windows* operating systems.

The *Add to bookmarks* option creates a new bookmark for the current path (the path displayed in the URL entry). It is recommended to label by a short unique name — this will help you with the bookmarks maintenance, especially if more bookmarks are used. If the name is not specified, the bookmark will be listed in the list of bookmarks under the UNC path.

The *Folder administration* option allows editing or removing of created bookmarks as well as creating of a new bookmark for any path (folder). The destination path can be specified manually or it can be browsed in the folder tree and it is also possible to use an existing bookmark as a starting point.

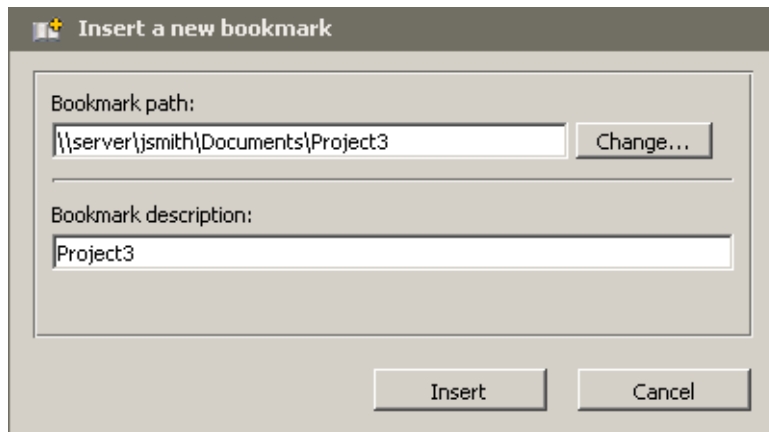


Figure 4.3 Clientless SSL-VPN — new bookmark

Examples of operations with files and folders

In this section, several examples of manipulation with files and folders via the *SSL-VPN* interface.

Creating folders

The dialog allows creating of a new folder in the specified location. By default, the current path specified in the URL line is indicated. However, it is possible to enter a new path.

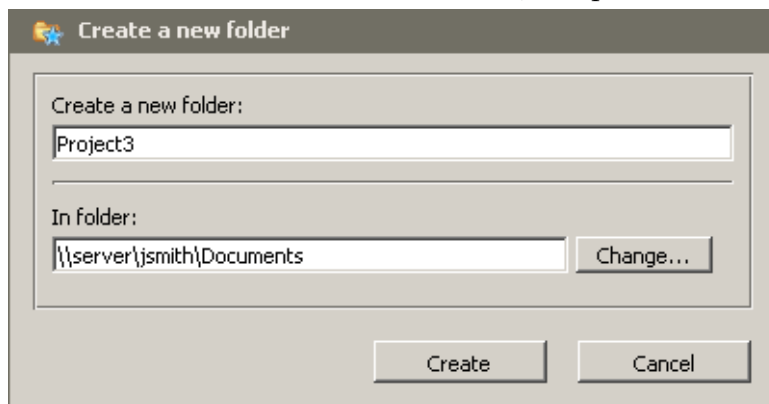


Figure 4.4 Clientless SSL-VPN — new folder

Use the *Edit* button to select a new path (folder) where the new folder will be created:

- use a bookmark,
- select it in the folder tree.

Renaming a file or a folder

Renaming is very simple — use the dialog to specify a new name for the selected folder or file.

Copying or moving files/folders

The *SSL-VPN* interface allows copying or moving of any number of files or/and folders at a time. First, select files and folders by checking the fields next to their names (checking of the field in the header selects all files and folders in the current location).

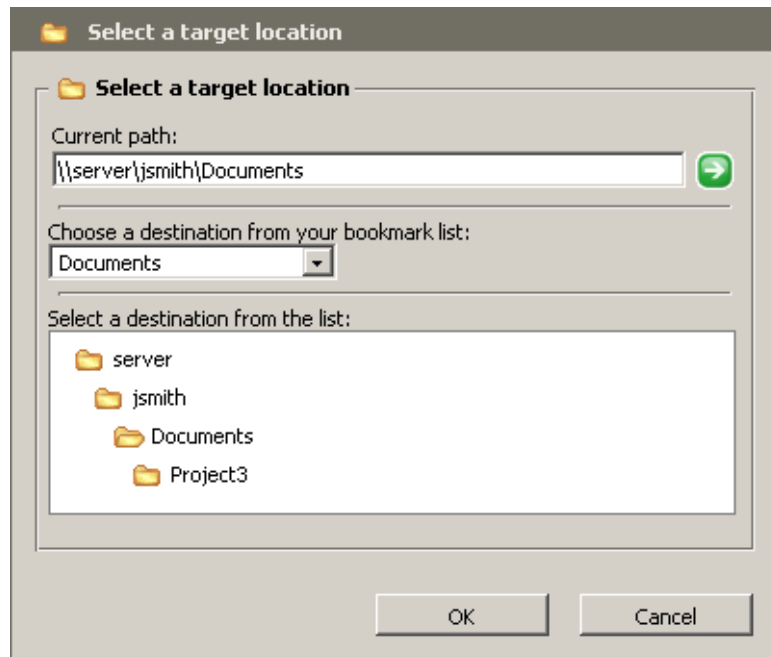


Figure 4.5 Clientless SSL-VPN — destination path (folder) selection

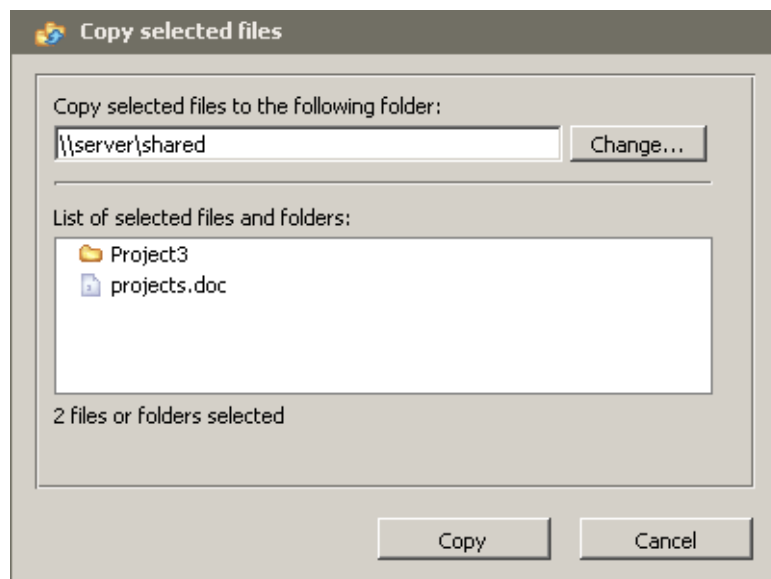


Figure 4.6 Clientless SSL-VPN — copying or moving of files/folders

In the copy/move dialog, specify the destination path (folder) or select it in the tree or it is also possible to use a bookmark (see above).

Moving of files / folders

It is also possible to remove any number of folders or/and files as well as all files and folders in the current path.

Downloading files

Downloading of files from remote shared folders to the local host is performed in the same way as usual downloading of files from web pages. Simply click on a file to open

a standard download dialog.

It is not possible to download whole folders or multiple files at a time.

Uploading files

The upload dialog allows selection of a destination folder (by default, the folder which is currently opened in the *SSL-VPN* interface is set). Destination folder can be specified manually, selected in the folder tree or loaded from a bookmark (see above).

Use the *File* entry to specify full path to a local file. Files can be also selected by using the *Browse...* button (click this link to open the standard system dialog for opening of a file).

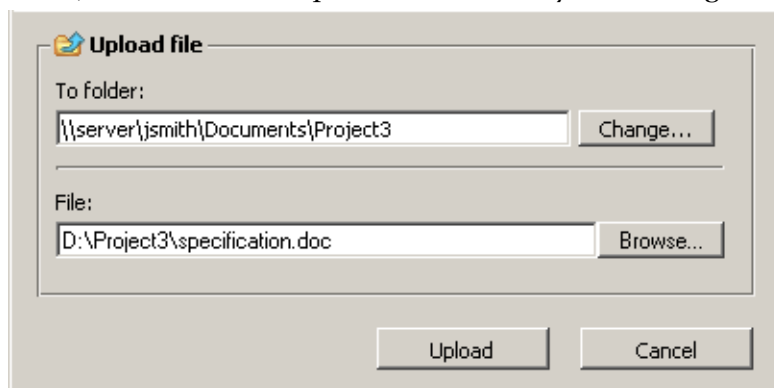


Figure 4.7 Clientless SSL-VPN — uploading files to shared folders

It is not possible to upload whole folders or multiple files at a time.

Appendix A

Legal Notices

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

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

Linux® is registered trademark kept by Linus Torvalds.

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

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

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

Glossary of terms

ActiveX

This *Microsoft's* proprietary technology is used for creation of dynamic objects for web pages. This technology provides many features, such as writing to disk or execution of commands at the client (i.e. on the host where the Web page is opened). This technology provides a wide range of features, such as saving to disk and running commands at the client (i.e. at the computer where the Web page is opened). Using *ActiveX*, virus and worms can for example modify telephone number of the dial-up.

ActiveX is supported only by *Internet Explorer* in *Microsoft Windows* operating systems.

Connections

A virtual bidirectional communication channel between two hosts.

[See also TCP](#)

Firewall

Software or hardware device that protects a computer or computer network against attacks from external sources (typically from the Internet).

In this guide, the word *firewall* represents the *WinRoute* host.

FTP

File Transfer Protocol.

IMAP

Internet Message Access Protocol (IMAP) enables clients to manage messages stored on a mail server without downloading them to a local computer. This architecture allows the user to access his/her mail from multiple locations (messages downloaded to a local host disk would not be available from other locations).

IP address

IP address is a unique 32-bit number used to identify the host in the Internet. It is specified by numbers of the decimal system (0–255) separated by dots (e.g. 195.129.33.1).

P2P network

Peer-to-Peer (P2P) networks are world-wide distributed systems, where each node can represent both a client and a server. These networks are used for sharing of big volumes of data (this sharing is mostly illegal). *DirectConnect* and *Kazaa* are the most popular ones.

POP3

Post Office Protocol is an email accessing protocol that allows users to download messages from a server to a local disk. It is suitable for clients who don't have a permanent connection to the Internet.

Port

16-bit number (1–65535) used by TCP and UDP for application (services) identification on a given computer. More than one application can be run at a host simultaneously (e.g. WWW server, mail client, FTP client, etc.). Each application is identified by a port number. Ports 1–1023 are reserved and used by well known services (e.g. 80 = WWW). Ports above 1023 can be freely used by any application.

PPTP

Microsoft's proprietary protocol used for design of virtual private networks.

[See chapters and sections concerning VPN.](#)

Proxy server

Older, but still wide-spread method of Internet connection sharing. Proxy servers connect clients and destination servers.

A proxy server works as an application and it is adapted for several particular application protocols (i.e. HTTP, FTP, Gopher, etc.). It requires also support in the corresponding client application (e.g. web browser). Compared to NAT, the range of featured offered is not so wide.

Script

A code that is run on the Web page by a client (Web browser). Scripts are used for generating of dynamic elements on Web pages. However, they can be misused for ads, exploiting of user information, etc. Modern Web browsers usually support several script languages, such as *JavaScript* and *Visual Basic Script (VBScript)*.

SMTP

Simple Mail Transfer Protocol is used for sending email between mail servers. The SMTP envelope identifies the sender/recipient of an email.

SSL

SSL is a protocol used to secure and encrypt network communication. SSL was originally designed in order to guarantee secure transfer of Web pages over HTTP protocol. Nowadays, it is used by almost all standard Internet protocols (SMTP, POP3, IMAP, LDAP, etc.).

At the beginning of communication, an encryption key is requested and transferred using asymmetrical encryption. This key is then used to encrypt (symmetrically) the data.

TCP

Transmission Control Protocol is a transmission protocol which ensures reliable and sequential data delivery. It is used by most of applications protocols which require reliable transmission of all data, such as *HTTP, FTP, SMTP, IMAP*, etc.

TCP/IP

Name used for all traffic protocols used in the Internet (i.e. for IP, ICMP, TCP, UDP, etc.). *TCP/IP* does not stand for any particular protocol!

Glossary of terms

UDP

User Datagram Protocol is a transmission protocol which transfers data through individual messages (so called datagrams). It does not establish new connections nor it provides reliable and sequential data delivery, nor it enables error correction or data stream control. It is used for transfer of small-sized data (i.e. DNS queries) or for transmissions where speed is preferred from reliability (i.e. realtime audio and video files transmission).

VPN

Virtual Private Network, *VPN* represents secure interconnection of private networks (i.e. of individual offices of an organization) via the Internet. Traffic between both networks (so called tunnel) is encrypted. This protects networks from tapping. *VPN* incorporates special tunneling protocols, such as *PPTP (Point-to-Point Tunnelling Protocol)* and *Microsoft's IPsec*.

WinRoute contains a proprietary *VPN* implementation called *Kerio VPN*.

Index

C

Clientless SSL-VPN [33](#)
 antivirus check [35](#)
 bookmarks [35](#)
 deployment [33](#)

P

preferred language [12](#)

S

SSL-VPN [33](#)
 antivirus check [35](#)
 bookmarks [35](#)
 deployment [33](#)
StaR [14](#)
 accounting period [16](#)
 overall view [18, 21](#)
 overview [14](#)
 top requested web categories [31](#)
 top visited websites [29](#)
 users' activity [22](#)
 volume of transferred data [28](#)

statistics

 accounting period [16](#)
 in the Web interface [14](#)
 Kerio StaR [14](#)
 overall view [18, 21](#)
 overview [14](#)
 top requested web categories [31](#)
 top visited websites [29](#)
 users' activity [22](#)
 volume of transferred data [28](#)

V

VPN
 Kerio Clientless SSL-VPN [33](#)

W

Web Interface [5](#)
 dial-ups [13](#)
 login page [5](#)
 preferred language [12](#)
 user preferences [10](#)
 user statistics [8](#)

