Kerio Control

User Guide

Kerio Technologies

© 2016 Kerio Technologies s.r.o.

Contents

Viewing activity reports in Kerio Control Statistics 5
- Overview 5
- Accessing the web interface 5
- Switching between Kerio Control Statistics and account settings 6
- Displaying Kerio Control Statistics 7
  - Selecting the period to view 7
  - Printing 7
  - Overall tab 7
  - Reading the User's activity tab 10

Reading managerial statistics and reports in Kerio Control 11
- Overview 11
- Reading the summary report 13
  - Overall tab 13
  - Users by Traffic tab 16
  - Visited Sites tab 18
  - Web Categories tab 18
- Reading individual statistiscs 19

Managing your Kerio Control Statistics account 21
- Overview 21
- Accessing the web interface 21
- Switching between Kerio Control Statistics and account settings 22
- Reading statistics and reports 23
- Setting up 2-step verification 23
- Checking your quota 23
- Dialing and hanging up lines in Kerio Control Statistics 23
- Changing your password 24
- Setting a language for Kerio Control Statistics and email reports 25

Authenticating to the firewall with 2-step verification 26
- Overview 26
- Enabling the 2-step verification 26
- Disabling the 2-step verification 28
- Enabling the 2-step verification when you use Kerio Control VPN Client 29
- Enabling the 2-step verification when you use IPsec VPN client 29

Installing and configuring Kerio Control VPN Client for users 31
Overview 31
System requirements 31
Prerequisites 31
Kerio Control VPN Client for Windows 31
Removing connections 33
Changing a language 33
Enabling/disabling balloon messages 33
Verification of the VPN server's SSL certificate on Windows 34
Kerio Control VPN Client for OS X 35
Removing connections 36
Verification of the VPN server's SSL Certificate on OS X 36
Kerio Control VPN Client for Linux 38
Troubleshooting 38

Configuring IPsec VPN client on Apple OS X with machine authentication by SSL certificate 39
Summary 39
Configuring Kerio Control 39
Importing the certificate 40
Creating VPN client on Apple OS X computer 41

Legal Notices 45
Trademarks and registered trademarks 45

Viewing activity reports in Kerio Control Statistics

Overview

Kerio Control Statistics is a web interface where you can view your own browsing statistics.

If you have sufficient access rights, you can also see other users' statistics (see Reading managerial statistics and reports in Kerio Control).

The statistics show traffic between the local network and the Internet. They do not include volumes of data transferred between local hosts and web pages on local servers.

Statistics are primarily used to create reports for a specified period. Gathering and evaluating statistics requires processing large volumes of data. To reduce the load on the firewall, the data is updated hourly, so, you cannot use Kerio Control Statistics for real-time monitoring of user activity.

If you need more information about account settings, see Managing your Kerio Control Statistics account.

Accessing the web interface

To open Kerio Control Statistics:

1. Launch your web browser and type your Kerio Control address.

   The address has this pattern: `https://server:4081/`

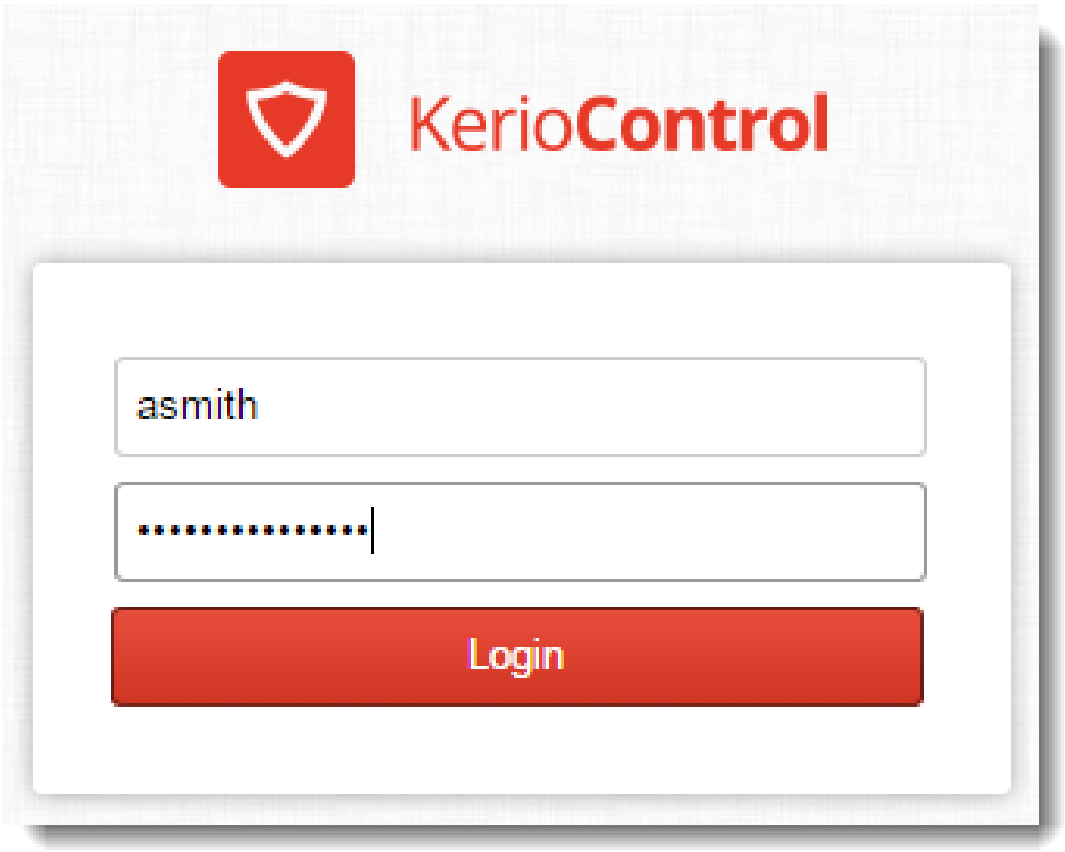
   where `server` refers to the name or IP address of Kerio Control, and `4081` represents a web interface port.

   If your browser displays a warning about a certificate invalidity, continue.

   For more information, contact your Kerio Control administrator.

2. On the Kerio Control Statistics login page, type your Kerio Control username and password.

   If you do not know your credentials, contact your administrator.



3. Click **Login**.

Switching between Kerio Control Statistics and account settings

Kerio Control Statistics has two parts:

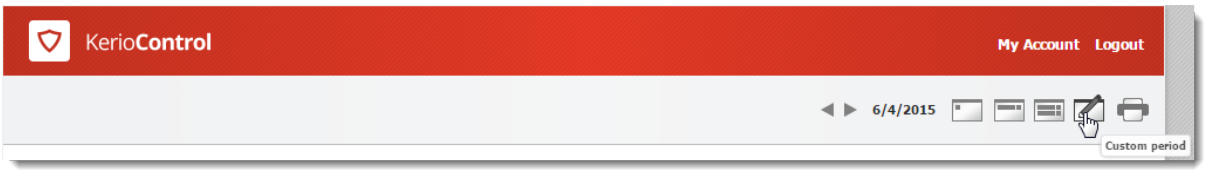
- **Statistics** displays statistics and your Internet activities.
- **My Account** lets you change your password, set 2-step verification, and check your browsing quota.

Use the option in the upper right corner to switch to the other part of the interface.

Displaying Kerio Control Statistics

Selecting the period to view

By default, Kerio Control Statistics displays the current day. To change the time period, use the toolbar at the upper right of the page.

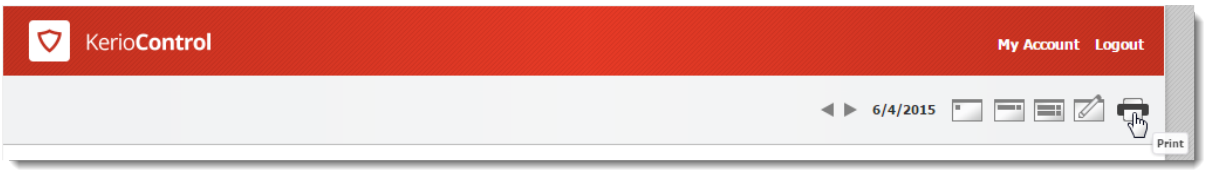


The toolbar includes buttons for switching between the daily, weekly, monthly views. The previous and next arrows to the left of those buttons allow you to jump quickly from one view to the next.

The starting day of the week and month can be changed. Contact your administrator for details.

Printing

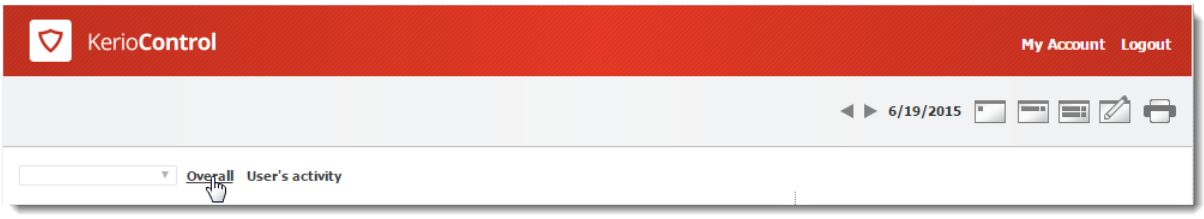
To print any page of the statistics, click the **Print** button.



Clicking **Print** displays the current page on a new tab in a printable format.

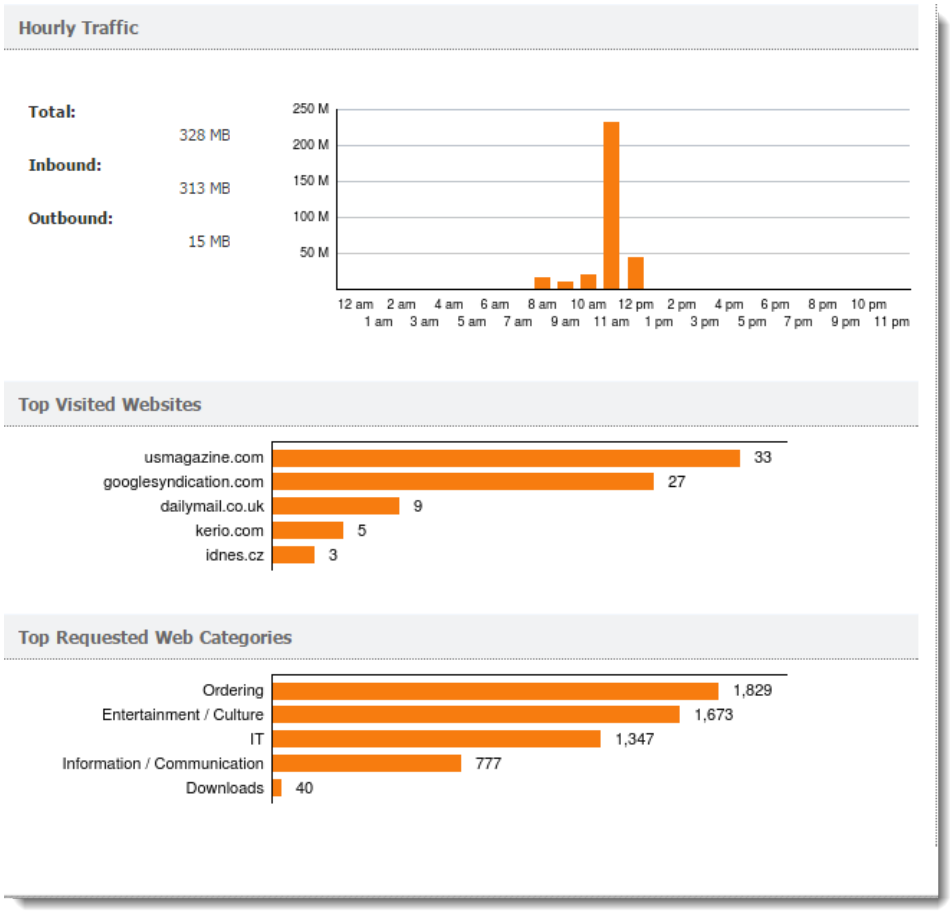
Overall tab

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 — for example, the selected user account does not exist in the particular time period, the user have not logged in to the firewall within the period, and so on.

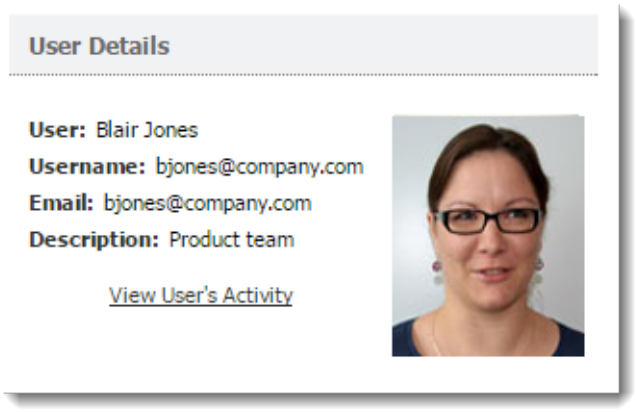


The **Overall** tab includes information about:

- **Hourly/Weekly/Monthly Traffic** — You can change the time period in the tool bar.
- **Top Visited Web Sites** — The five sites that got the most traffic during the selected period.
- **Top Requested Web Categories** — The five categories that were most often viewed during the selected period.

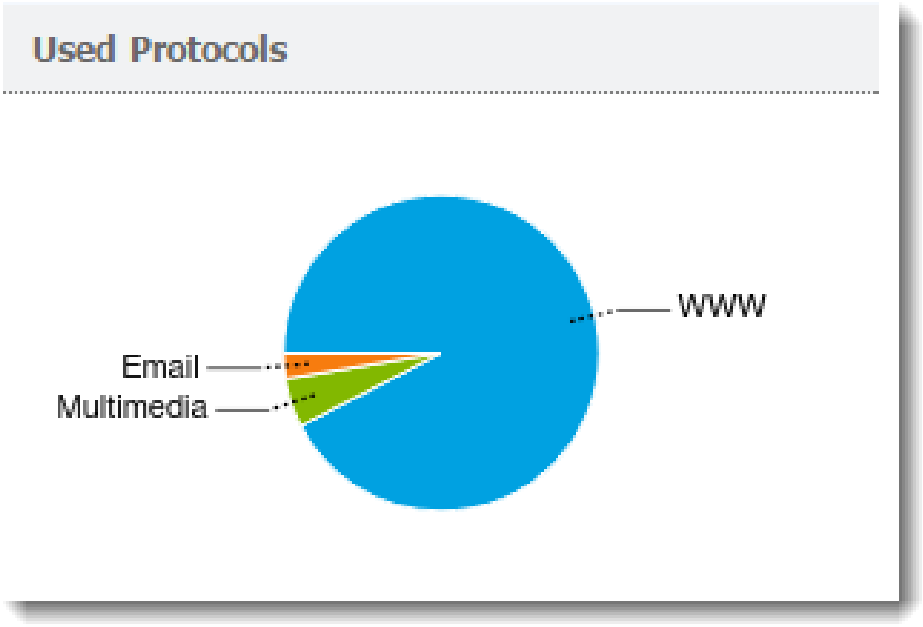


- **User Details** — Your user information stored in Kerio Control.



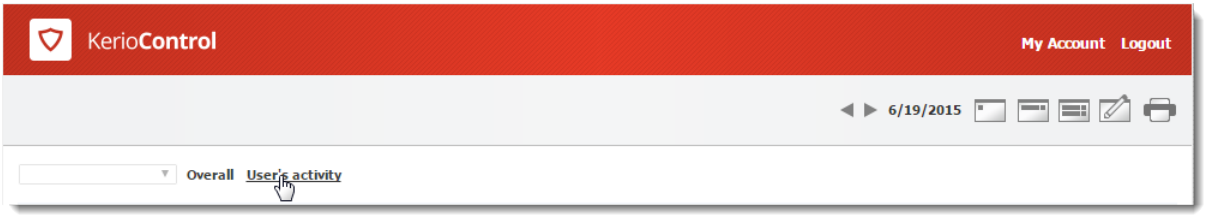
The **User's Activity** link is visible only if Kerio Control gathers users' activity records.

- **Used Protocols** — The **Used Protocols** pie chart is shown if you uses web, multimedia, VoIP, email, and so on.



Reading the User's activity tab

- The User's Activity tab is visible only if Kerio Control gathers users' activity records.
- 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 — for example, the selected user account does not exist in the particular time period, the user have not logged in to the firewall within the period, and so on.



The **User's activity** tab shows detailed information about your browsing activities. You can see:

- What you were doing on the Internet during the selected period
- How much time you spent browsing web pages

Gathering and evaluating statistics requires processing large volumes of data. To reduce the load on the firewall, the data is updated hourly, so, you cannot use Kerio Control Statistics for real-time monitoring of activity.

Activity Categories

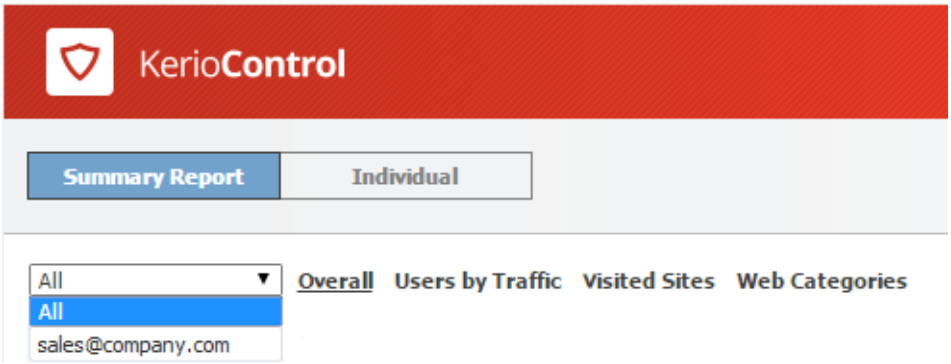
Activity categories are ranked in the order shown here. If there was no activity in a category in the selected period, that category is omitted.

- Web pages
- Messaging, which includes email communication (SMTP, IMAP, and POP3 protocols) and instant messaging
- Large file transfers, for example, archives, installation media, and so on
- Multimedia, such as video sharing sites, online radio and television channels (streaming)
- VoIP — SIP (Internet telephony)
- Remote access, such as VPN.

Reading managerial statistics and reports in Kerio Control

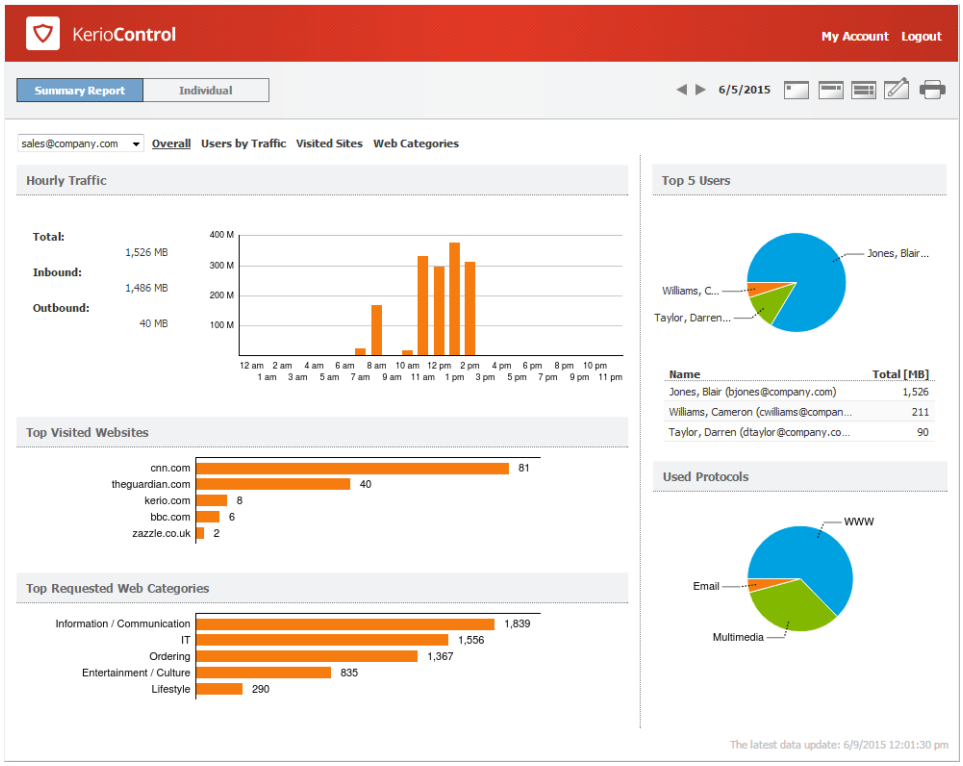
Overview

Kerio Control can gather and display Internet statistics all data (all Kerio Control users + all non-authenticated users + all guest users), for various user groups, and for all individual users in these groups. These statistics let you keep an eye on your subordinates' browsing activities. Ask your administrator for a configuration and permissions.

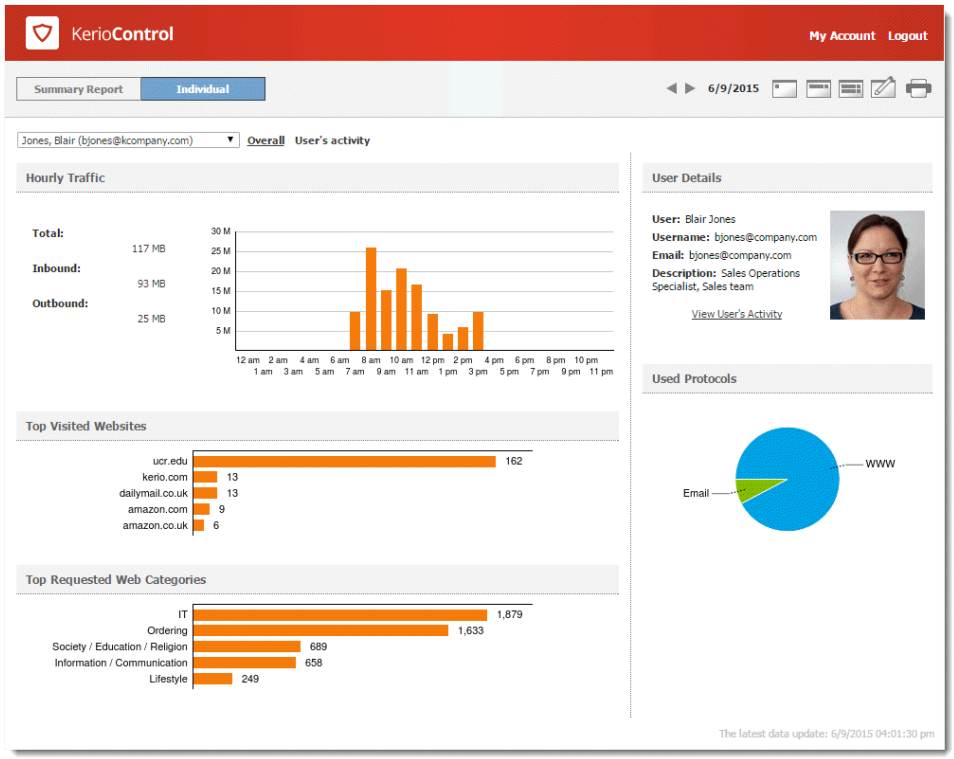


Once you have the permissions, you can see two tabs in Kerio Control Statistics:

- **Summary Report**, which lets you view statistics by user group.



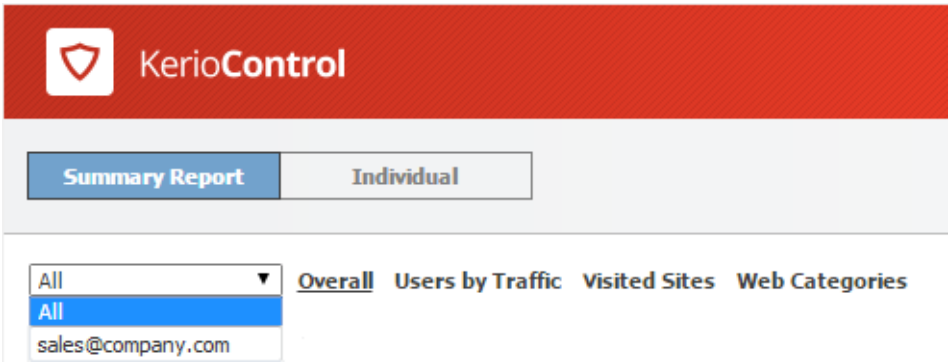
- **Individual**, which lets you select single users (or yourself) to see their statistics.



Reading the summary report

The **Summary Report** tab gives you an overview of the available user groups.

First, select a user group from the drop-down list.



Alternatively, choose **All** to see all users, including guest users and non-authenticated users. You need special permissions to see this group.

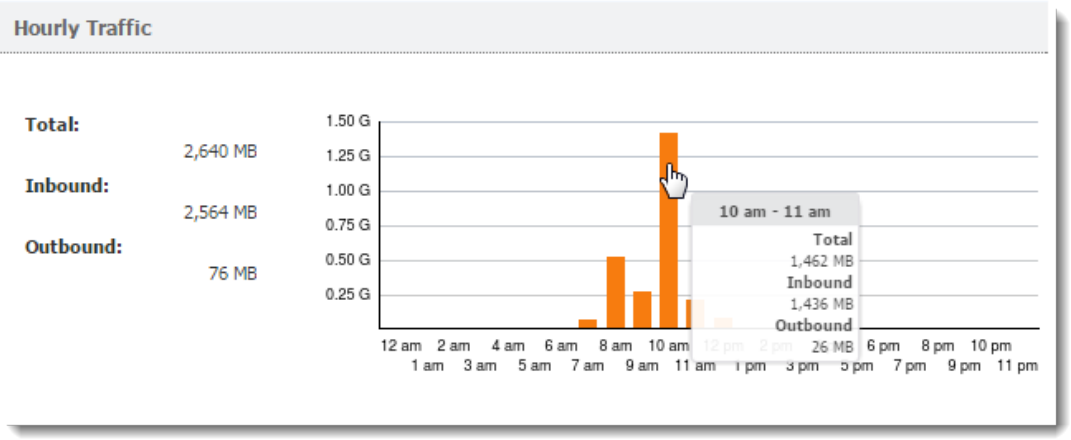
The **No data available** alert informs you that no data is available in Kerio Control's database for the selected statistics and period (for example, the selected user account does not exist, the user does not log in to get through firewall, and so on).

The **Summary Report** tab has several additional tabs, as described below:

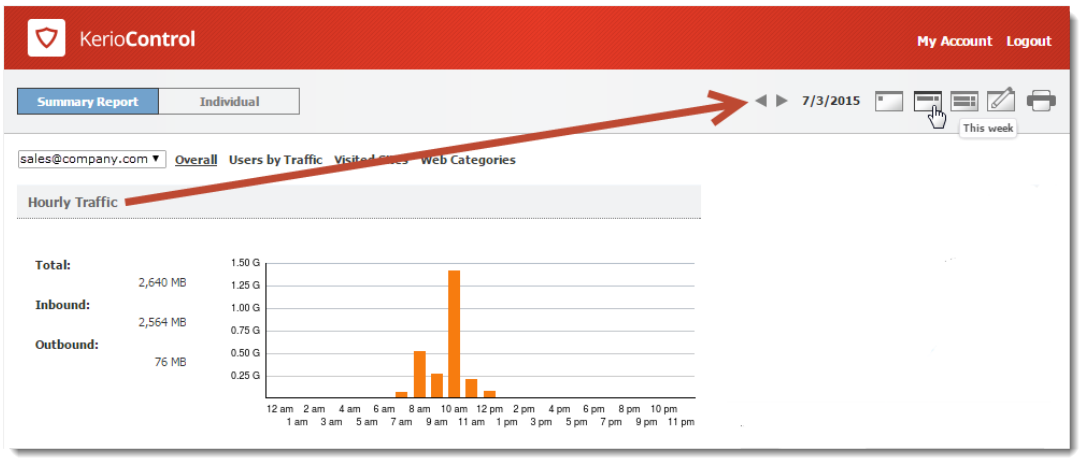
Overall tab

Hourly/Weekly/Monthly Traffic graph

The first graph on the **Overall** tab provides information on the volume of data transferred within the selected period. When you move the pointer over the chart, you see information about data volumes transferred over the entire selected period (total and in each direction).



By default, the **Hourly Traffic** chart is set to show the current day. To change to the current week or month, use the toolbar in the upper right corner.



The shortest period you can view is one day.

Top Visited Websites graph

The Top Visited Websites chart shows the five domains ranked by visits. The numbers in the chart show how many visits were made to all pages on that domain during the selected period.

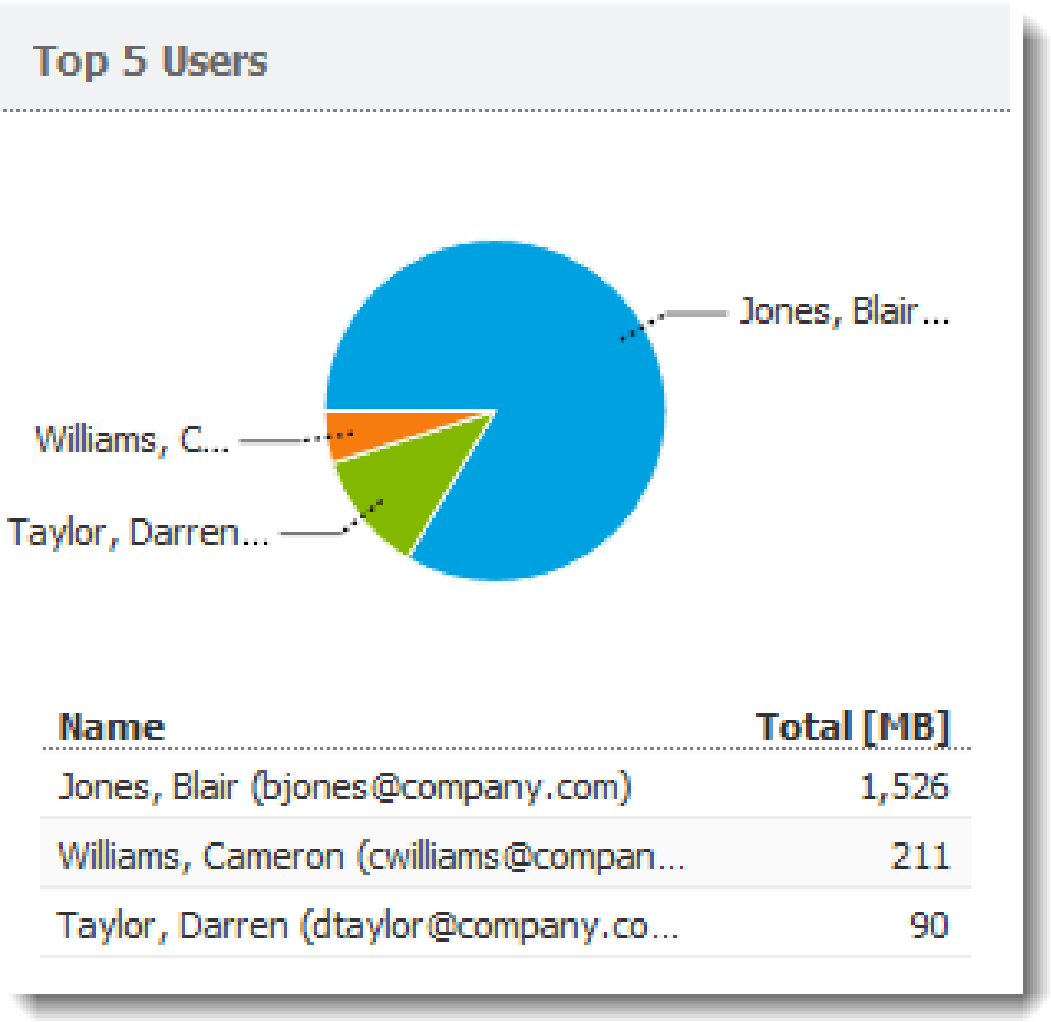
For more information, click the chart and Kerio Control Statistics takes you to the Visited Sites tab, where you can see further details.

Top Requested Web Categories graph

To see a chart of the most requested pages by category (such as IT or lifestyle), click **Web Categories**. The **Top Requested Web Categories** chart shows the top five categories requested during the selected period, as sorted by the Kerio Control Web Filter module.
The numbers in the chart reflect the total number of HTTP requests in the each category. Because the number may represent requests to multiple pages on a site. The number of requests is usually much higher than number of websites visited.
For more information, click the chart, Kerio Control Statistics takes you to the Web Categories tab, where you can see further details.

Top 5 Users graph

To see which users are using the largest amount of bandwidth, click **Users by Traffic**. The **Top 5 Users** chart shows the five users who transferred the greatest volume of data during the selected period.



The chart includes individual users and the total volume of transferred data. Hover the pointer over a user's name to see the volume of data transferred by that user, in both total volume and by direction (download, upload).

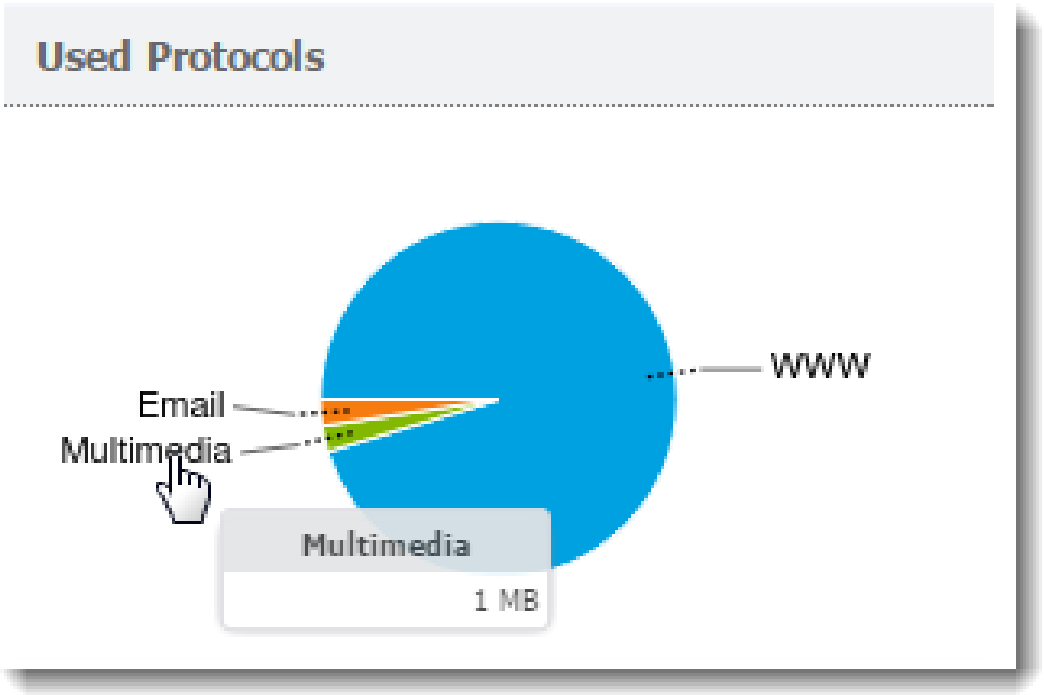
To see statistics for a particular user, click the user's name in the chart. The results are displayed on the **Individual** tab.

The total volume of data transferred by a particular user is sum of all data transferred by the user from all hosts connected to the firewall.

Used Protocols graph

The Used Protocols chart of shows the total volume of data transferred in the selected period.

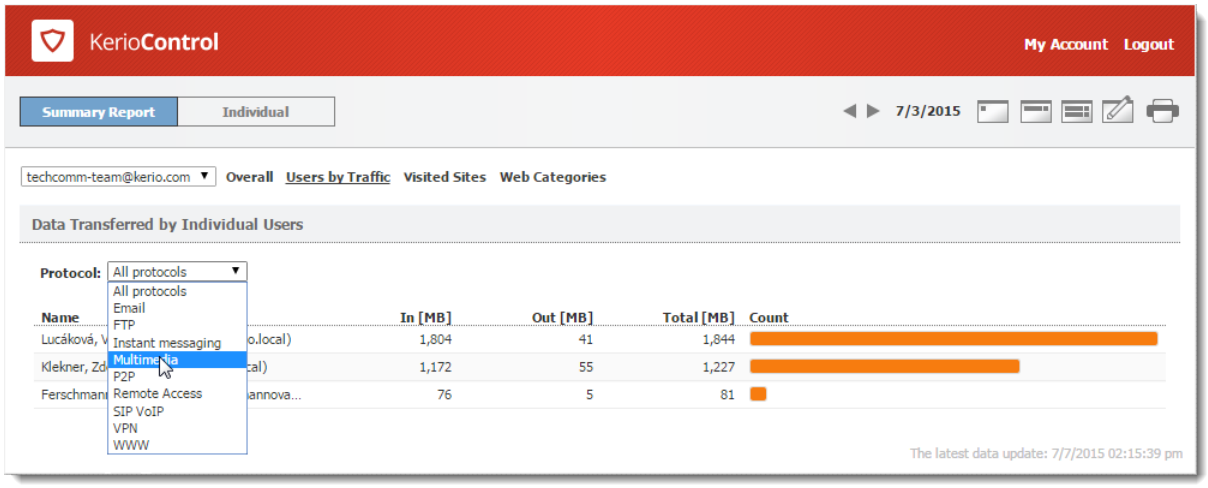
Hover the pointer over a protocol to see the volume of data transferred by that protocol (see figure below).



This chart helps you recognize the type of traffic going between the local network and the Internet. If the Internet line is overloaded, you can use this information to set necessary limits and restrictions (traffic rules, URL rules, and so on).

Users by Traffic tab

The **Users by Traffic** tab shows the volume of data transferred by individual users in the selected group in both directions (download, upload). You can choose between all network traffic and traffic statistics filtered by network protocol.



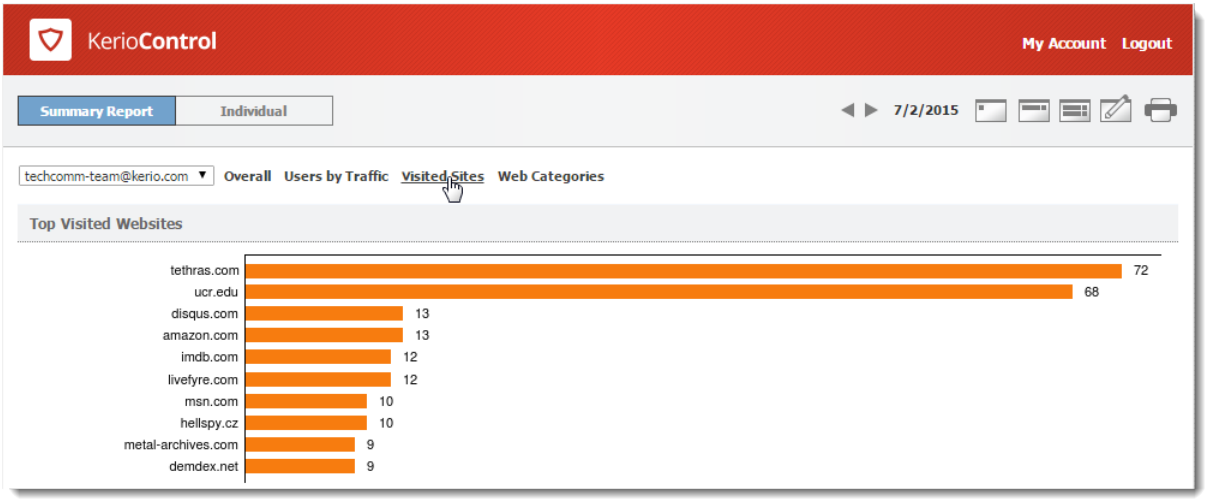
The table breaks down the total volume of transferred data by user. You can use the table to view all transferred data or only data transferred by a selected protocol (or protocol class). This allows you to get information about which users have transferred the most data via a particular service (for example, web browsing).

For better reference, Kerio Control sorts protocols by several predefined classes:

- **Email**: SMTP, IMAP, POP3 protocols and their secured versions.
- **FTP**: FTP protocol, including traffic over proxy server.
- **Instant messaging**: Online communication via services such as ICQ and Jabber.
- **Multimedia**: Protocols enabling real-time transmission of sound and video files, for example, RTSP, MMS, RealAudio.
- **P2P**: Peer-to-peer file-sharing protocols, for example, DirectConnect, BitTorrent, eDonkey, and so on. The traffic is counted only if Kerio Control detects that it is traffic within a P2P network.
- **Remote Access**: Terminal access to remote hosts such as Remote desktop, VNC, Telnet or SSH.
- **SIP-VoIP**: Voice over telephony via SIP protocol.
- **VPN**: Connection to remote private networks, for example, Kerio VPN, Microsoft PPTP, IPsec.
- **WWW**: HTTP and HTTPS protocols and any other traffic served by the HTTP protocol inspector.

Visited Sites tab

The **Visited Sites** tab gives you an overview of web pages users have visited.



These statistics tell you things such as:

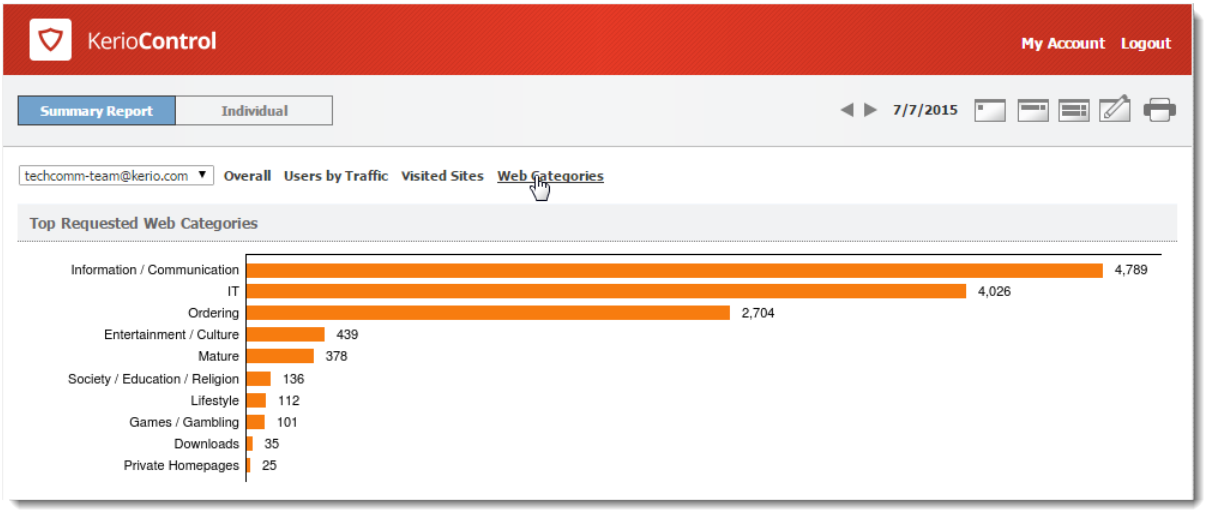
- What websites are visited by users regularly,
- Which users do the most browsing,

The chart at the top of the tab shows the most visited websites. The numbers in the chart reflect the number of visits to all pages on the site in the selected period.

Beneath the chart, you can see detailed statistics for each of the top ten websites.

Web Categories tab

The **Web Categories** tab gives an overview of popular web categories for the selected period.



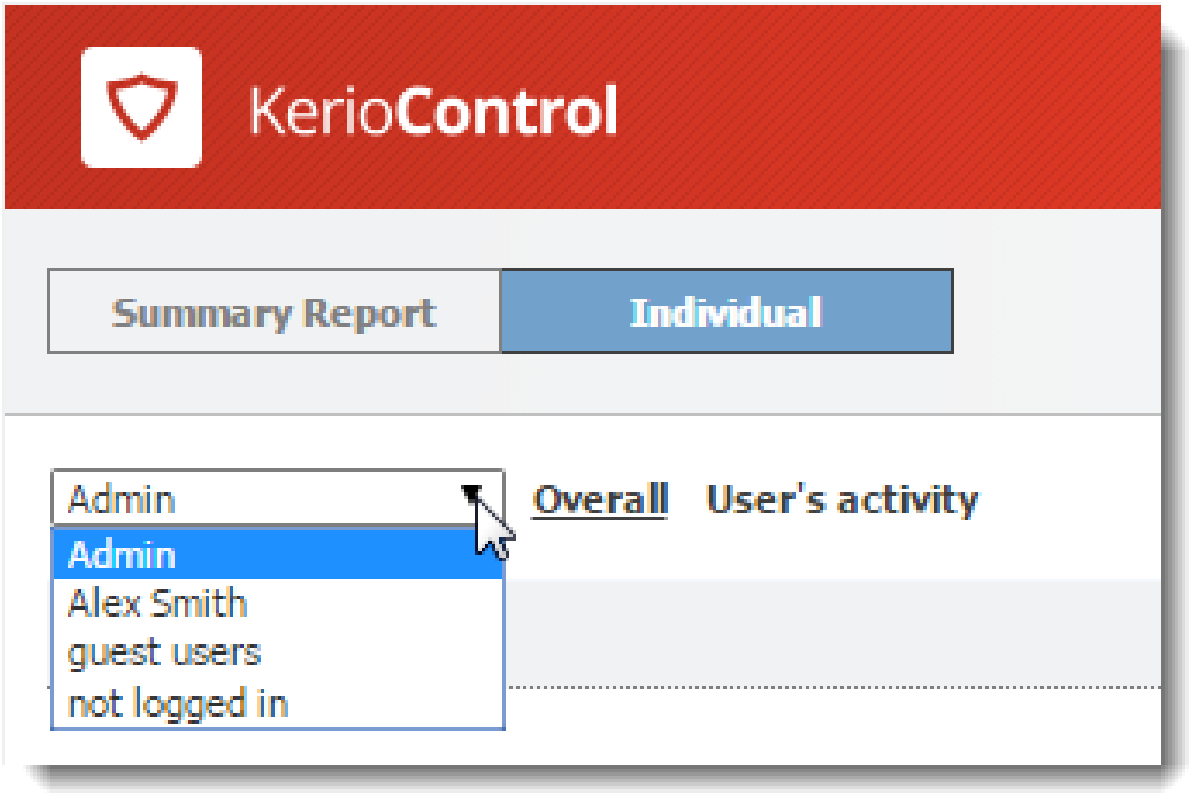
The numbers in the chart show the total number of HTTP requests in each category. Because a number may include requests to multiple pages on a site. The number of requests is usually much higher than the number of visits shown for the top visited websites.

Beneath the chart, Kerio Control Statistics shows detailed statistics for each of the top 10 web categories.

Web categorization is performed by Kerio Control Web Filter, an optional module of Kerio Control. To use web categories in your statistics, you need a valid license.

Reading individual statistiscs

To see detailed statistics for a particular user, click the user's name in a chart or table to switch to the Individual tab. Alternatively, you can click the Individual tab on the main page and choose a user's name from the drop-down list.



The charts and tables in Kerio Control Statistics provide useful information on which users use the Internet connection the most and make it possible to set necessary limits and quotas.

For details, see Viewing activity reports in Kerio Control Statistics.

Managing your Kerio Control Statistics account

Overview

Kerio Control Statistics is a web interface where you can view your own browsing statistics. It also includes tools for:

- Enabling 2-step verification
- Changing the password used to log in to Kerio Control
- Setting language preferences for the Kerio Control Statistics interface, reports and email alerts

Accessing the web interface

To open Kerio Control Statistics:

1. Launch your web browser and type your Kerio Control address.

   The address has this pattern: `https://server:4081/`

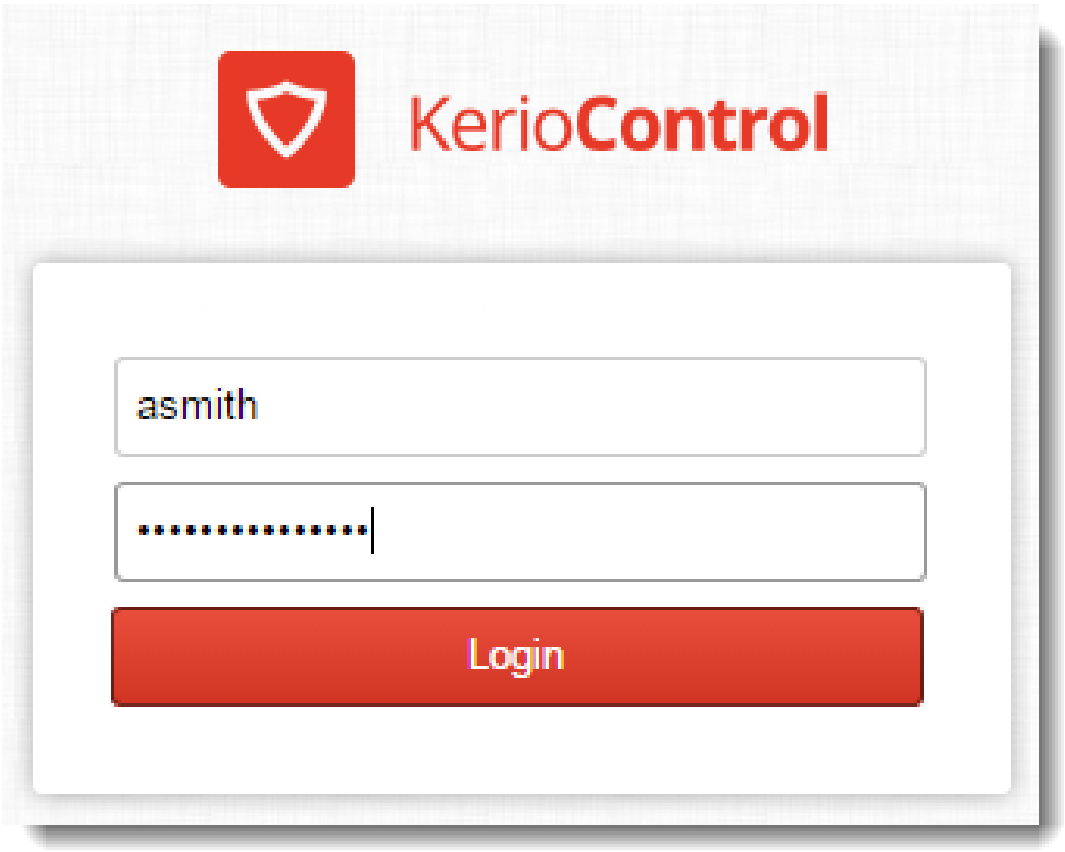
   where `server` refers to the name or IP address of Kerio Control, and `4081` represents a web interface port.

   If your browser displays a warning about a certificate invalidity, continue.

   For more information, contact your Kerio Control administrator.

2. In the Kerio Control Statistics login page, type your Kerio Control username and password.

   If you do not know your credentials, contact your administrator.



3. Click **Login**.

Switching between Kerio Control Statistics and account settings

Kerio Control Statistics has two parts:

- **Statistics** displays statistics and your Internet activities.
- **My Account** enables you to change your password, set up 2-step verification, and check your Kerio Control quota.

Use the option in the upper right corner to switch to the other part of the interface.

Reading statistics and reports

See Viewing activity reports in Kerio Control Statistics and Reading managerial statistics and reports in Kerio Control.

Setting up 2-step verification

See Authenticating to the firewall with 2-step verification.

Checking your quota

In Kerio Control Statistics, you can check the upload/download quota set for your Kerio Control account.

This section of the interface provides information on the data volume downloaded/uploaded for the current day, week, or month. If your administrator has set up quota, Kerio Control Statistics displays your current usage as a percentage of your quota.

To see your quota:

1. In the **Kerio Control Statistics** interface, go to **My Account**.
2. On the **Account** tab, see the **Transfer Quota Statistics** section.

The starting day for the week or month can be changed. Contact your administrator for details.

Dialing and hanging up lines in Kerio Control Statistics

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.

The **Dial-up Lines** section is visible only if you have rights for controlling dial-ups in Kerio Control.

To dial or hang up the line, click the link in the **Action** column.

The following dial-up details are shown:

- Name of the line in Kerio Control.
- Current state — **Disconnected**, **Connecting** (the line is being dialed), or **Connected**, **Disconnecting** (the line is being disconnected).

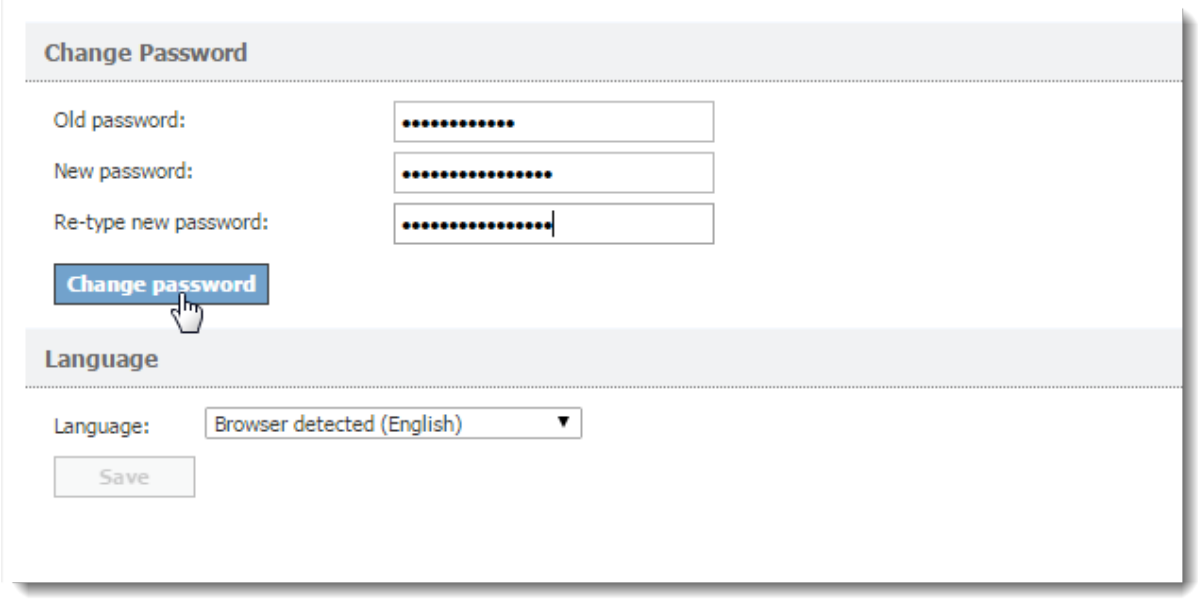
- Action — hypertext link that dials or hangs up the line when clicked (depending on its current state).
- Connection time.
- Volume of data transferred in either direction **Incoming** = from the Internet to the LAN, **Outgoing** = from the LAN to the Internet.

Changing your password

You can change your password only if your account does not belong to a directory service.

The middle section of the **Account** tab allows you to set your user password.

1. In the **Kerio Control Statistics** interface, go to **My Account**.
2. On the **Account** tab, type the old password once and the new password twice.
3. Click **Change password**.



Setting a language for Kerio Control Statistics and email reports

Kerio Control can display and send statistics, reports and email alerts in various languages. To change the language:

1. In the **Kerio Control Statistics** interface, go to **My Account**.
2. On the **Account** tab, scroll to the **Language** section at the bottom of the tab.
3. Select a language.
4. Click **Save**.

Kerio Control saves your settings and reloads the Kerio Control Statistics interface in the new language.

Language settings also affect the format of dates and numbers.

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://winauth.com/)

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**.

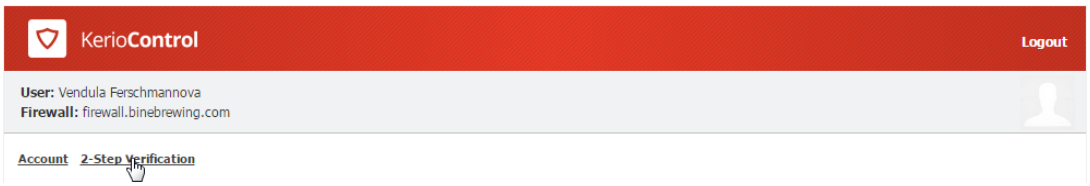


Figure 1 The 2-Step Verification tab

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**.

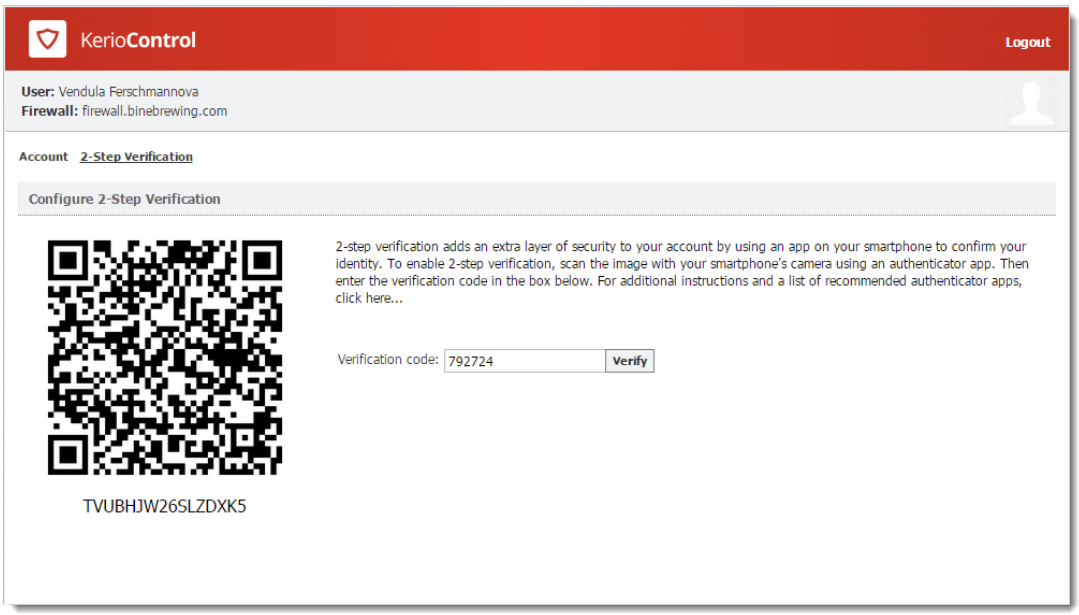


Figure 2 The 2-Step Verification tab

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.

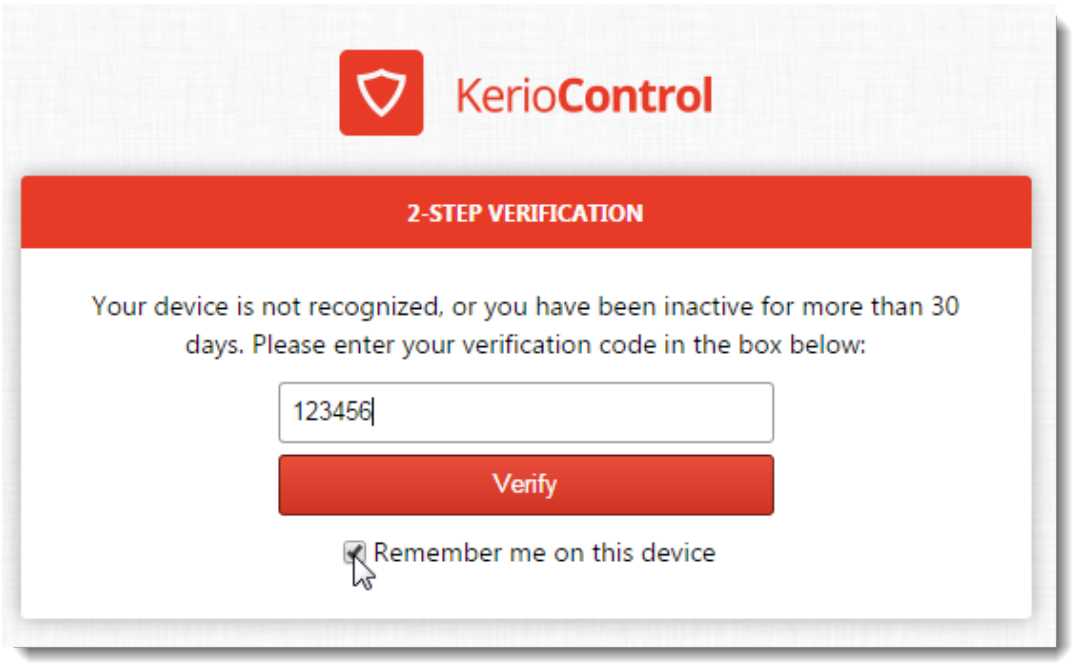


Figure 3 The 2-Step Verification tab

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**.

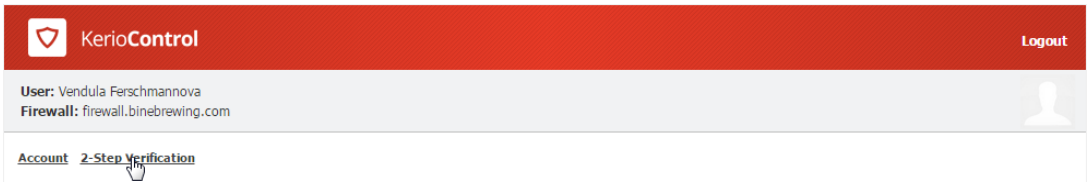


Figure 4 The 2-Step Verification tab

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.

Installing and configuring Kerio Control VPN Client for users

Overview

Kerio Control VPN Client enables encrypted connection from individual hosts (clients) to a remote private network via the Internet. 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

If you have administration rights to your computer, you can establish a persistent connection. Persistent connections are reestablished any time you restart your machine.

System requirements

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

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

Prerequisites

To connect to Kerio Control network, you must know:

- Your Kerio Control username and password
- Name of Kerio Control or its IP address

Kerio Control VPN Client for Windows

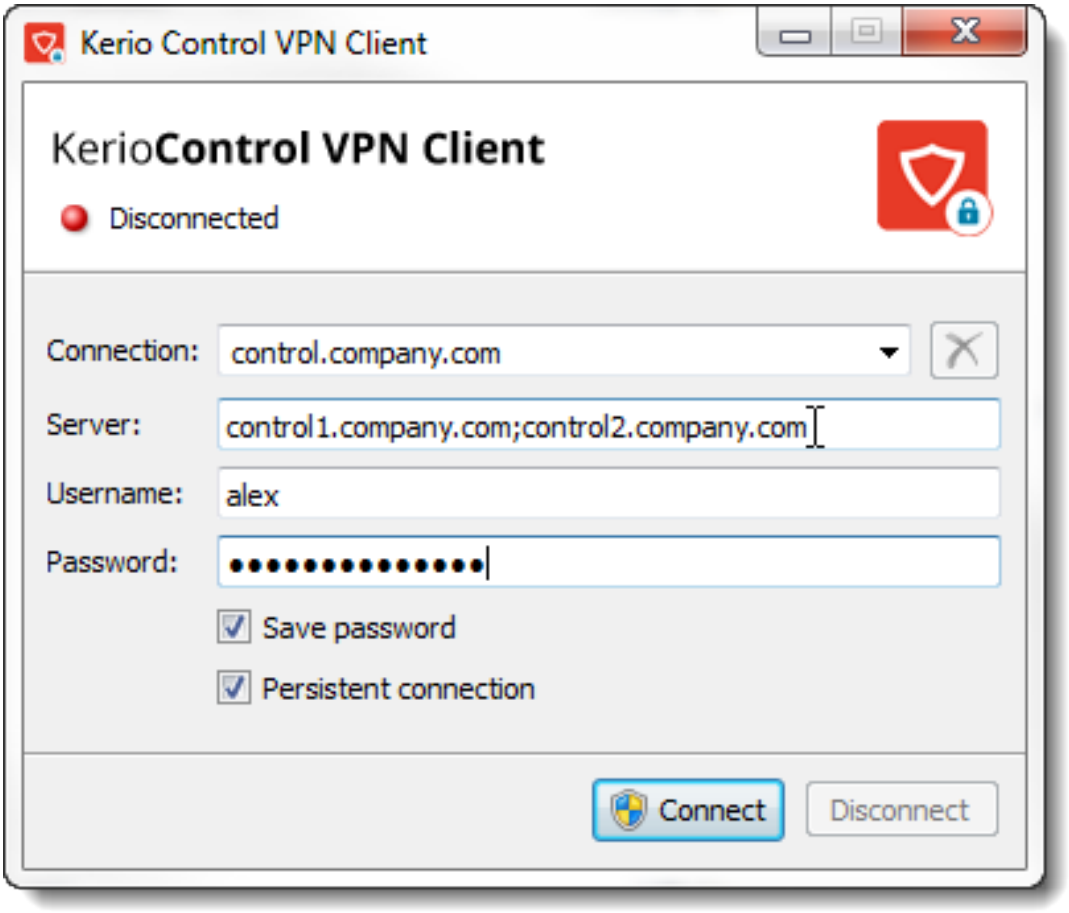
1. Download and install Kerio Control VPN Client.

   Kerio Control VPN Client starts automatically after installation and you can see the Kerio Control VPN Client window.

2. In the **Connection** field, type a name for the new connection.

3. In the **Server** field, type the Kerio Control server name or IP address.

   If your administrator gives you more server names or IP addresses, separate them by semicolons.



4. In the **Username** and **Password** fields, type your Kerio Control credentials.
5. (Optional) Select **Save password** to save your password in Kerio Control VPN Client.
6. (Optional) Select **Persistent connection** if you have administration rights to your computer.

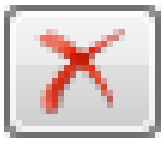
   Persistent connections are reestablished any time you restart your machine.
7. Click **Connect**.

If Kerio Control VPN Client is running, Windows taskbar displays the icon.

Kerio Control can require a 2-step verification. For more details, read Authenticating to the firewall with 2-step verification

Removing connections

To remove old or broken connections:

1. Open Kerio Control VPN Client.
2. In the **Connection** menu, select the connection.
3. Click the  icon.

   Kerio Control VPN Client asks you if you want to remove selected connection.
4. Click **Yes**.

Kerio Control VPN Client removes your connection.

Changing a language

To change a language of the Kerio Control VPN Client interface:

1. Right-click the icon in the notification area of the Windows taskbar (Systray).

2. In the context menu, click **Settings**.
3. In the **Kerio Control VPN Client Settings** dialog box, select your preferred language.
4. Click **OK**.

Kerio Control VPN Client switches to the language version immediately.

Enabling/disabling balloon messages

Balloon messages in Kerio Control VPN Client are all pop-up messages appearing in the Windows taskbar at the Kerio Control VPN Client icon. To enable or disable the balloon messages:

1. Right-click the icon in the notification area of the Windows taskbar.
2. In the context menu, click **Settings**.

3. In the **Kerio Control VPN Client Settings** dialog box, select **Enable balloon messages**.

4. Click **OK**.

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. If you consider the server trustworthy, click **Yes**. Kerio Control VPN Client saves the certificate and stops displaying the warning.

Troubleshooting

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 you accept 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).

Kerio Control VPN Client for OS X

1. Download and install Kerio Control VPN Client.

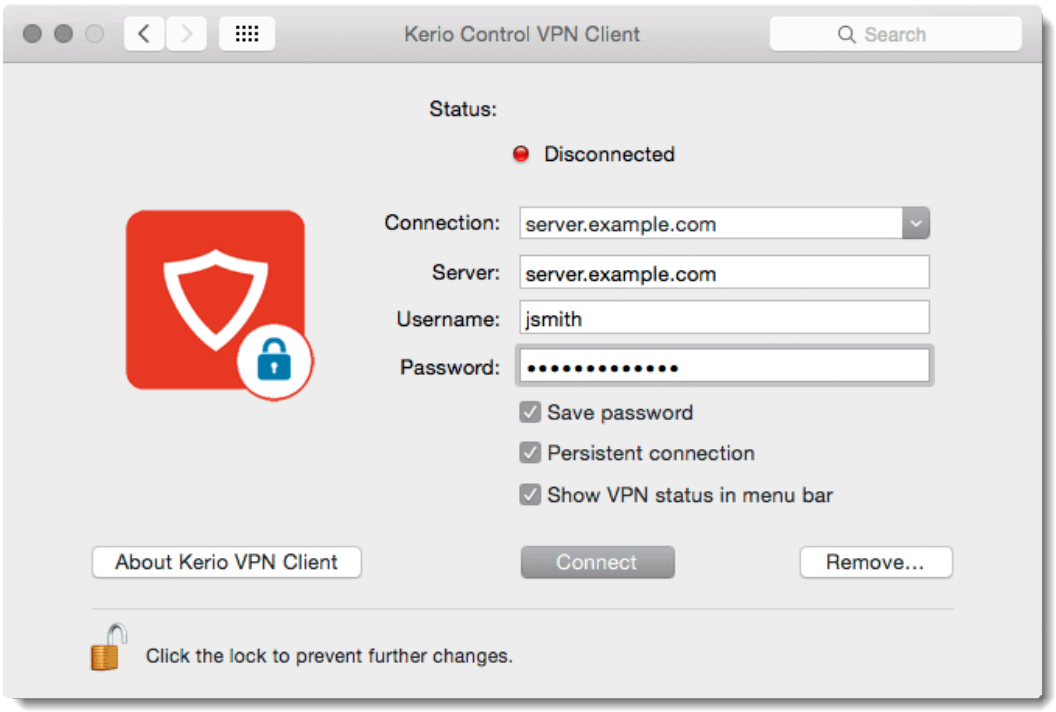
   Kerio Control VPN Client starts automatically upon the logon and you can see the Kerio Control VPN Client window.

2. In the **Connection** field, type a name for the new connection.

3. In the **Server** field, type the Kerio Control server name or IP address.

   If your administrator gives you more server names or IP addresses, separate them by semicolons.

4. In the **Username** and **Password** fields, type your Kerio Control credentials.



5. (Optional) Select **Save password** to save your password in Kerio Control VPN Client.

6. (Optional) Select **Persistent connection** if you have administration rights to your computer.

   Persistent connections are reestablished any time you restart your computer.

7. (Optional) Select **Show VPN status in menu bar** to display a status icon on the right side of the main menu bar when Kerio Control VPN Client is running.

Removing connections

To remove old or broken connections:

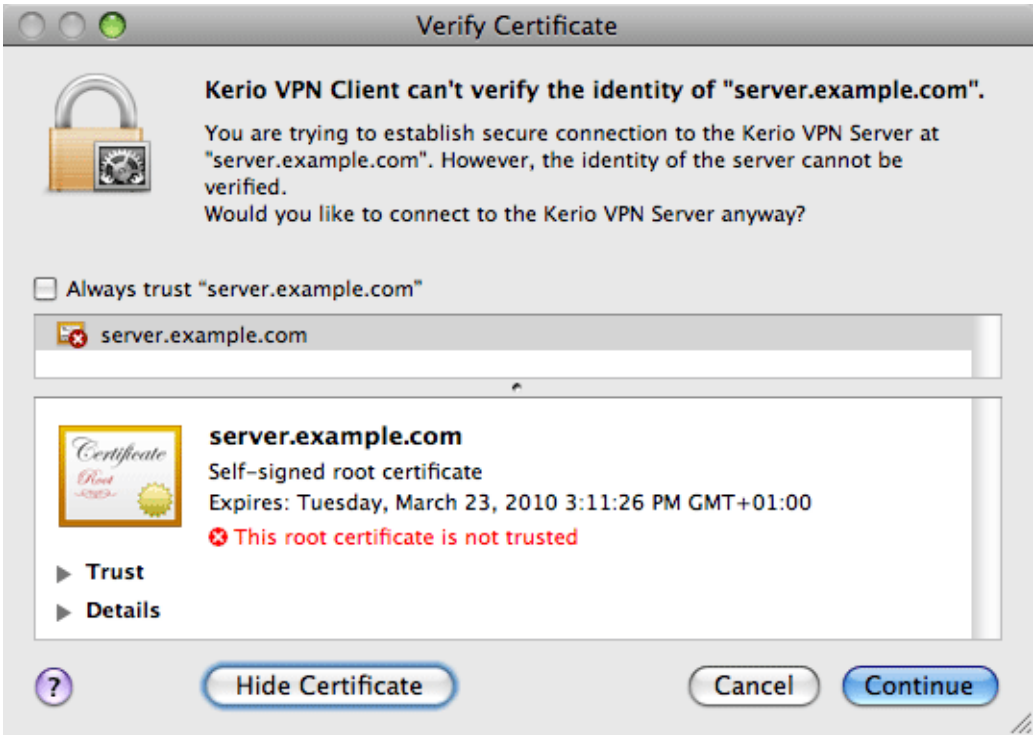
1. Open Kerio Control VPN Client.
2. In the **Connection** menu, select the connection.
3. Click the **Remove** button.

   Kerio Control VPN Client asks you if you want to remove selected connection.
4. Click **Yes**.

Kerio Control VPN Client removes your connection.

Verification of the VPN server's SSL Certificate on OS X

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.



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.

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.

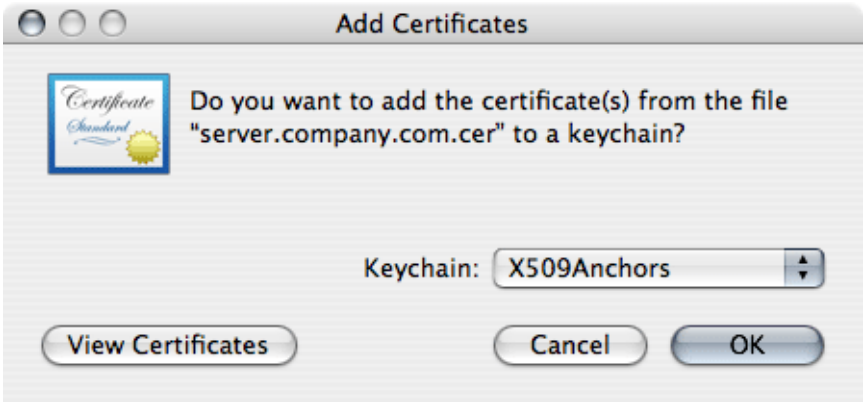
Setting a certificate as always trusted

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, 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.

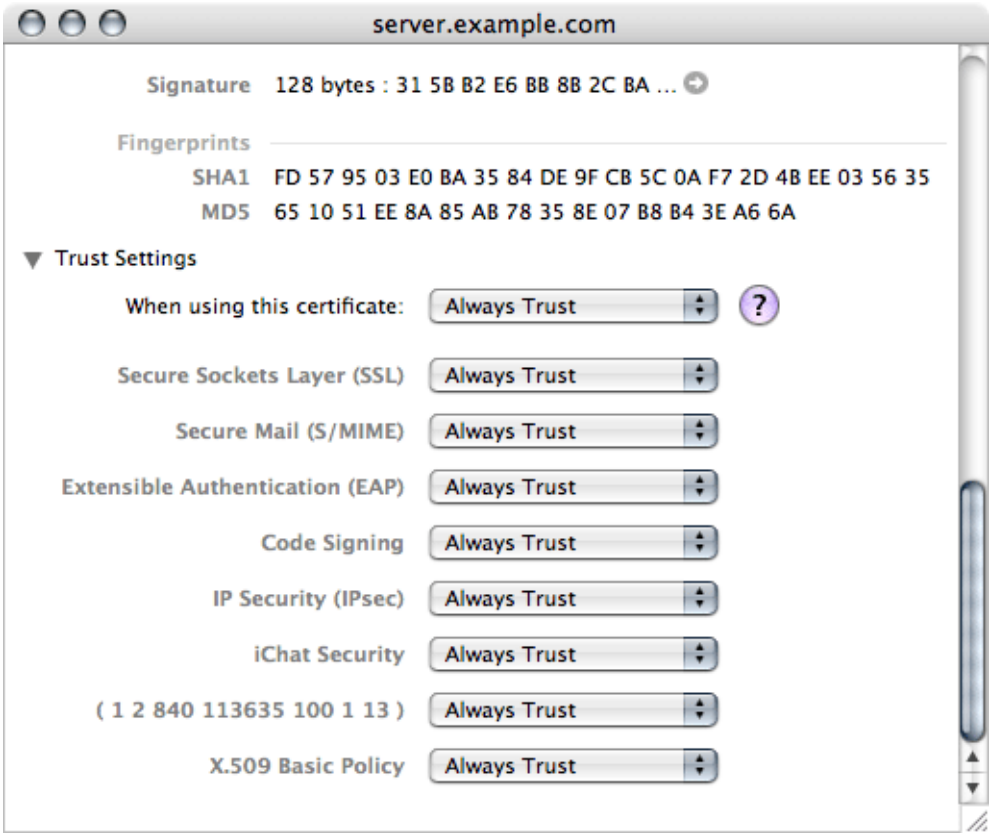


3. Select the **X509Anchors** keychain. This keychain contains certificates that are allowed to sign other certificates (these are typically certificates of certification authorities).

   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 (for example 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.



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.

Kerio Control VPN Client for Linux

Detailed information about Kerio Control VPN Client for Linux are included in the read-me file attached to the installation package.

Troubleshooting

The Kerio Control VPN Client generates logs including information about its own activity and detected errors. For details, read Installing and configuring Kerio Control VPN Client for administrators.

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.

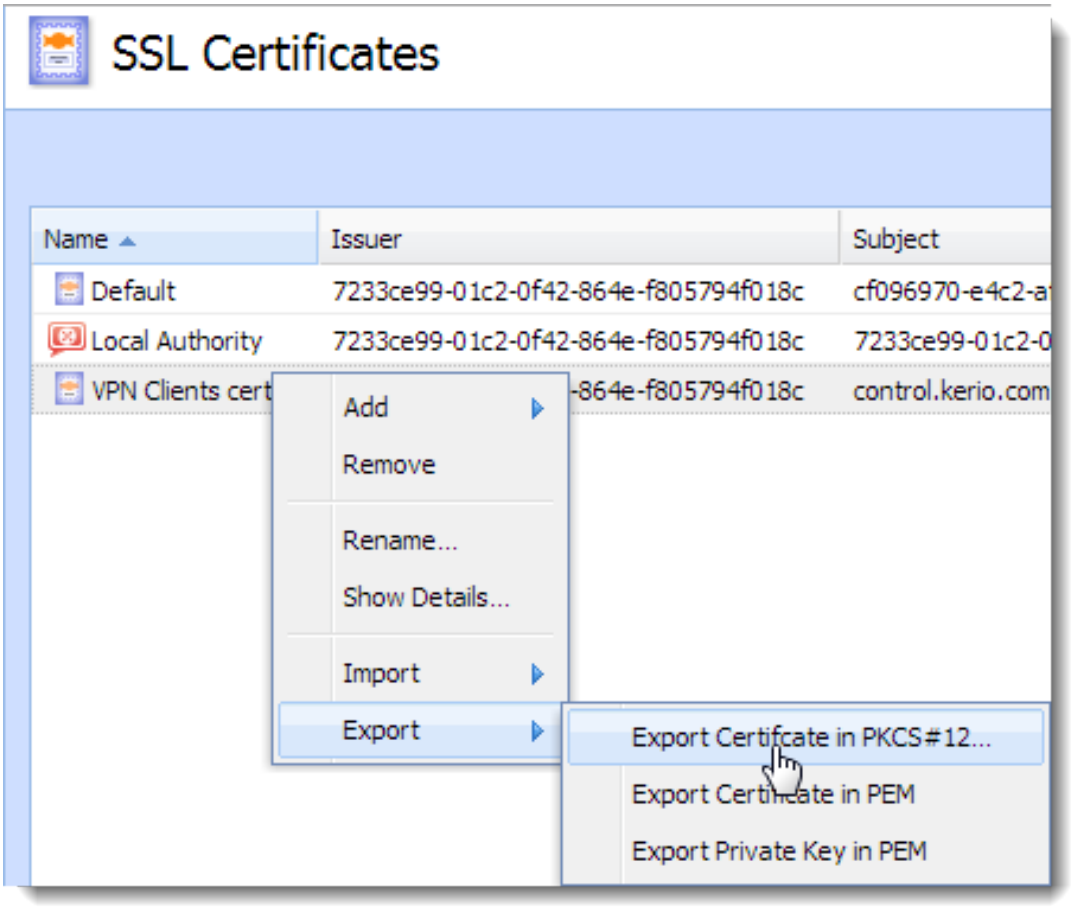


Figure 1 Export Certificate in PKCS#12

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:

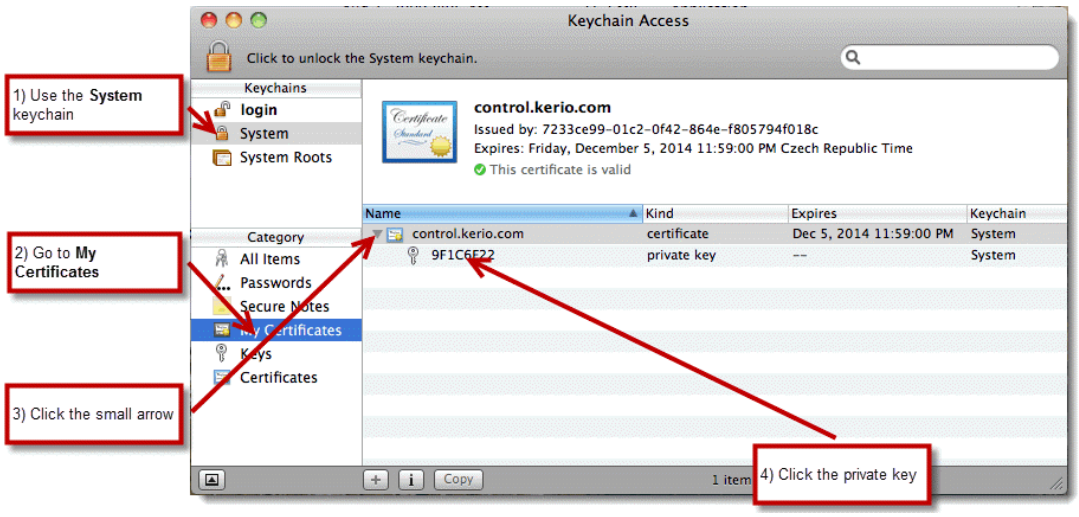


Figure 2 Mac OS 7 and higher settings

   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.

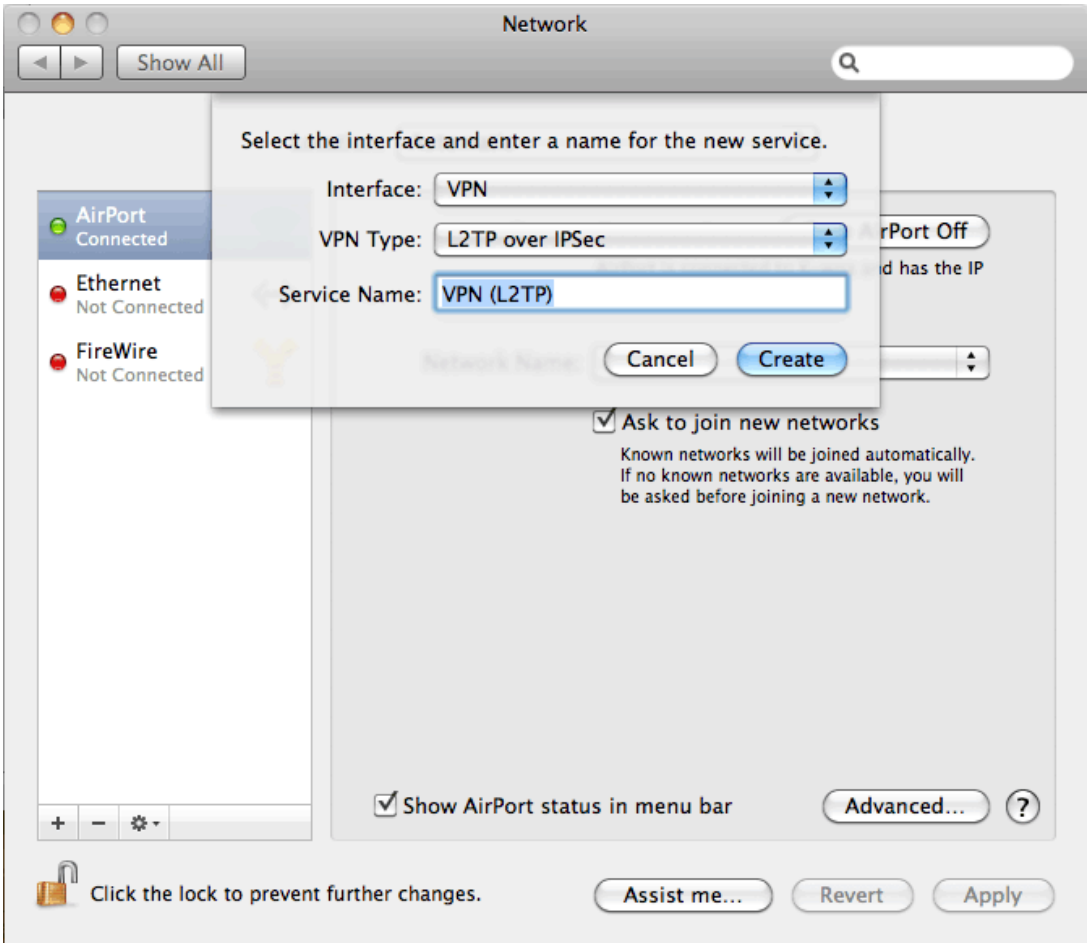


Figure 3 The Network dialog

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.

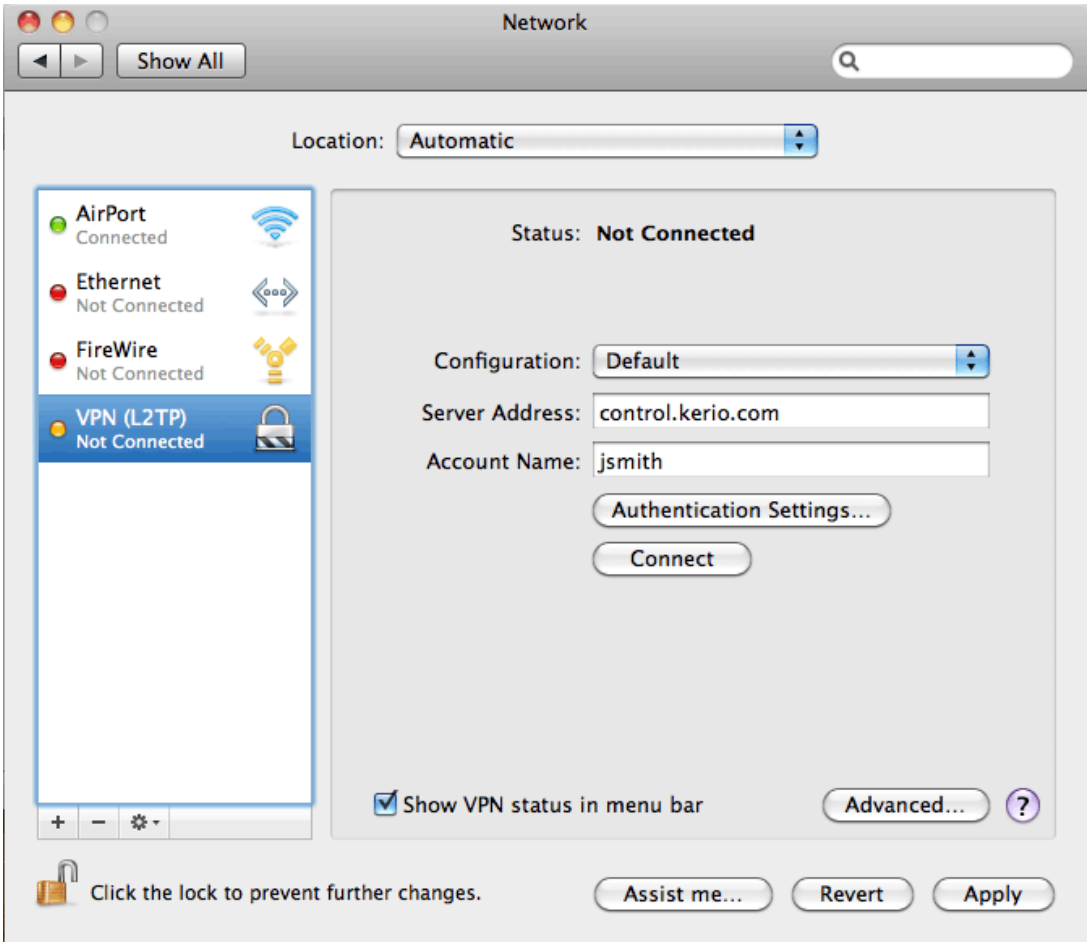


Figure 4 Type a hostname of Kerio Control and your user name

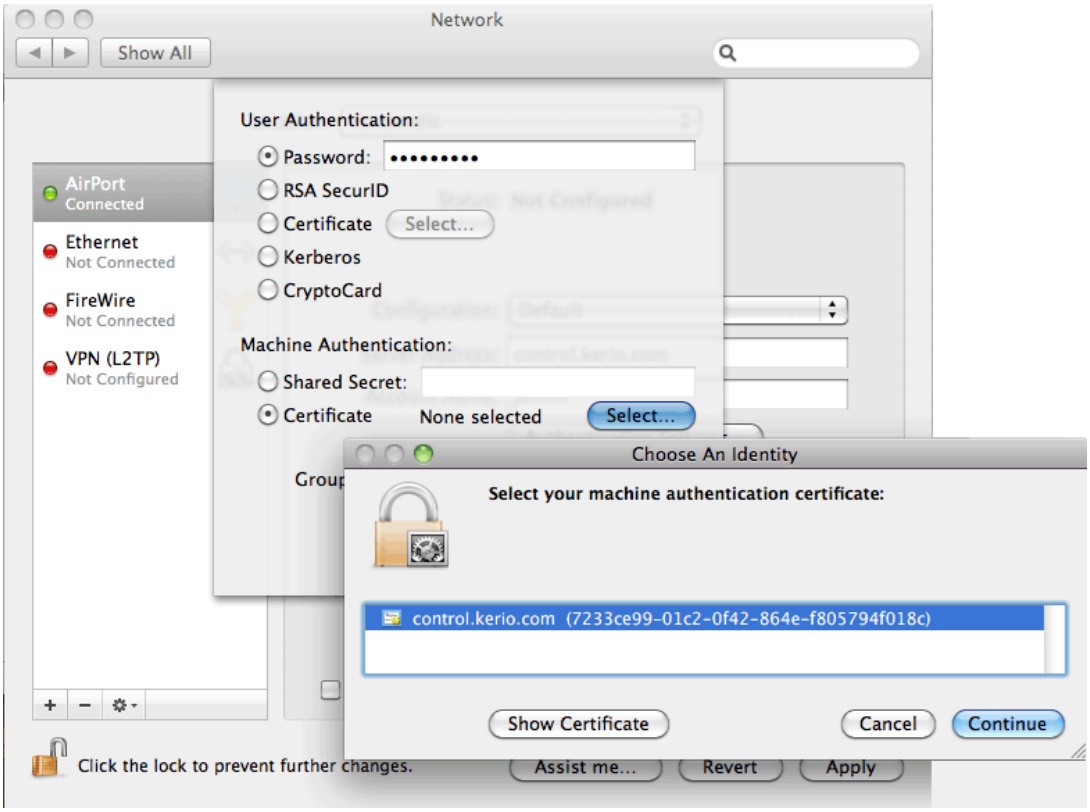


Figure 5 Set Machine Authentication by a certificate

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.