

PROXIFIER USER GUIDE

Proxifier is a program that allows network applications that do not support working through proxy servers operate through a HTTP or SOCKS proxy server or a chain of proxy servers.

With Proxifier you can easily tunnel all connections on the system or separate applications.

Proxifier allows you to:

- Run any network applications through proxy server; no special configuration is required for the software.
- Access the Internet from restricted local area network through a proxy server gateway.
- Bypass firewall restrictions (connect to restricted ports).
- Use three types of proxy servers: SOCKS v4, SOCKS v5, and HTTPS.
- "Tunnel" the entire system (force all network connections in the system work through a proxy server).
- Resolve DNS names through a proxy server.
- Use flexible Proxification Rules.
- Secure privacy by hiding your IP address.
- Work through a chain of proxy servers using different protocols.
- Use NTLM authentication on HTTPS proxy
- View information on current connections (addresses, rate, data transfer, connection time, etc.) in real-time.
- View information on bandwidth usage as a colored diagram in real-time.
- Maintain log files.
- Log incoming and outgoing traffic.
- Get detailed reports on network errors.
- ... and much more.

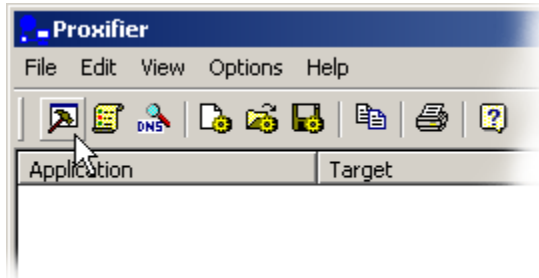
Quick Start

Install and launch Proxifier. The Proxifier icon showing traffic (information flow) will appear on the taskbar. Double click the icon to open the main window of the program.



By default, Proxifier is configured to process all network connections (TCP/IP) on the system. Thus Proxifier will manage all internet applications and allow them to directly connect to the internet. So if you gain access outside your network without a proxy you can still utilize the features of Proxifier (bandwidth, individual application control, etc).

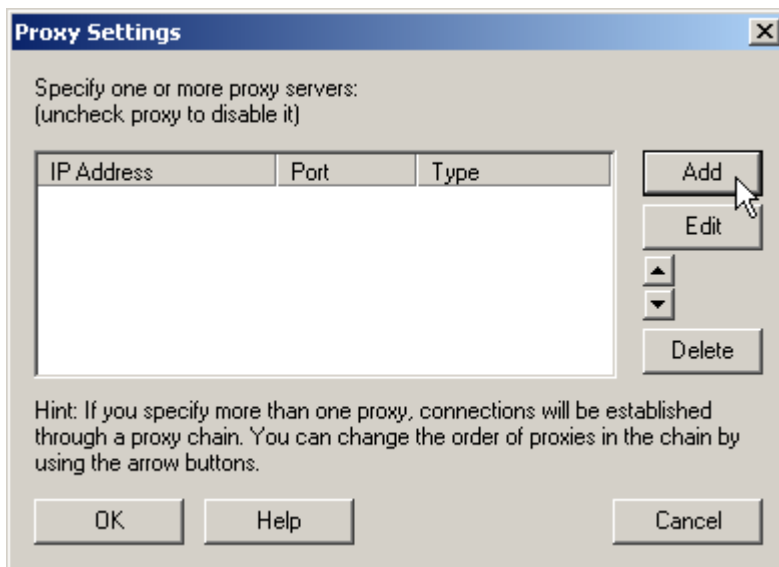
To make the connections work through a proxy server or a chain of proxy servers, you must first specify their IP address and port. Click **Proxy Settings** in the **Options** menu or click on the icon located on the toolbar:



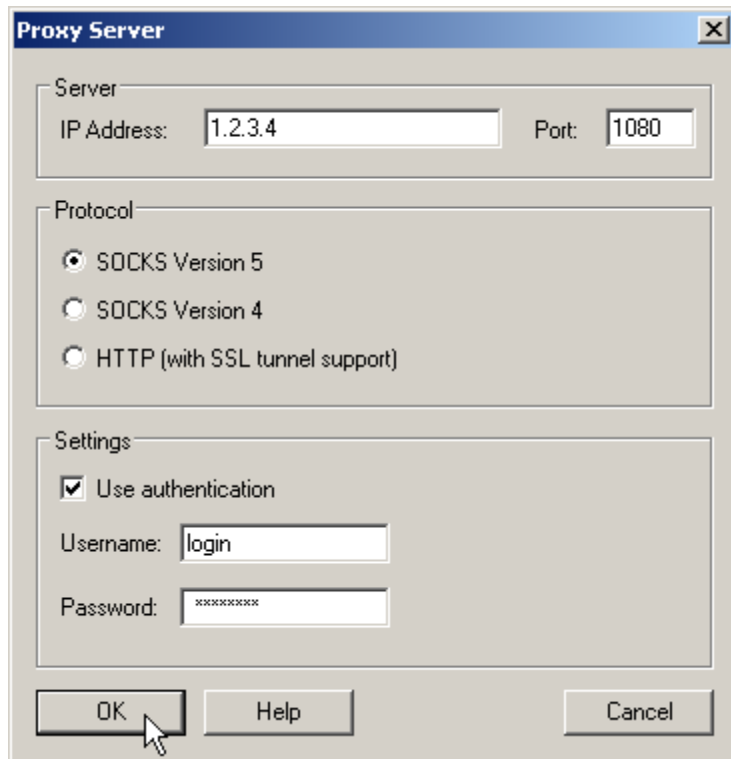
WARNING:

If you were using proxies before you installed the Proxifier, then you should disable any old proxy settings. This means that your applications should be configured to connect "directly" to the Internet (rather than through proxies).

Click the **Add** button in the new dialog window:

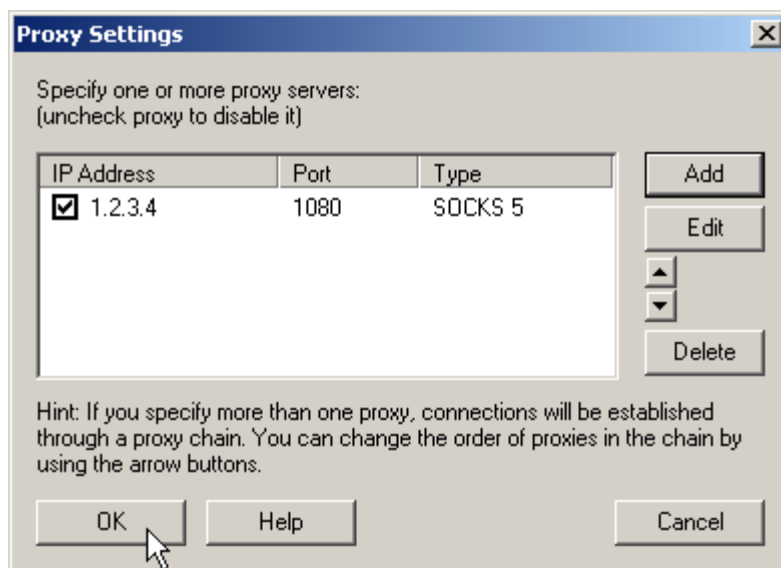


Fill in the form specifying the parameters of the proxy server (type, address, port) that you want to add and click **OK**:



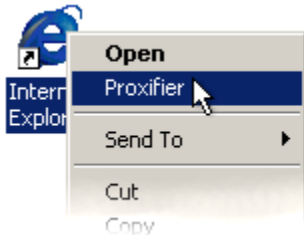
(this is not a real proxy, only a sample)

Your proxy server will appear in the list, click **OK** to confirm the use of this server:



From now on all new network connections will be established through the specified proxy server.

If you do NOT want to "tunnel" all connections, but only separate programs, click the **Process Only the following + Manually proxified applications** item in the **Options -> Proxification Rules** dialog window. Then, to "tunnel" any application, right-click on its icon shortcut and click Proxifier in the context menu.



The application will be started and all its connections will work through the specified proxy server.

Another way to tunnel only selected connections is **Proxification Rules**.

Proxification modes

(Proxifier Standard Edition only)

To be able to work successfully with Proxifier, you should understand the term 'proxification'. Proxification means processing a network connection in such a way that it works through one or more proxy servers. For client applications the process of proxification is absolutely transparent, it means that the application does not know that its connections work through a proxy server.

Note: only TCP/IP connections are supported.

Proxifier can work in two modes:

1. Tunneling connections automatically.
2. Tunneling applications that was running manually by "Proxifier" command (see the screenshot below).

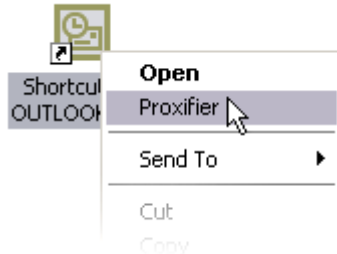
By default, Proxifier will tunnel all connections automatically after the installation. (Except loopback connections).

To specify the connections that should be (or should not be) proxified automatically, please create one or several **Proxification Rules**.

If you don't want to have all connections proxified automatically by default, please click **Options** -> **Proxification Rules** -> **Process Only the following**.

Note: These changes will affect only newly established connections.

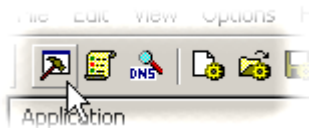
Now to process an application, right-click its icon shortcut and select the Proxifier item in the context menu:



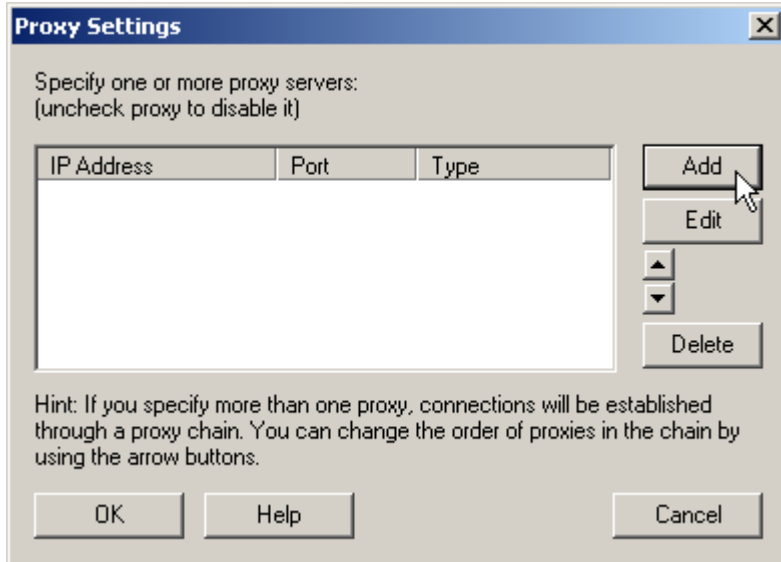
Proxification of Microsoft® Outlook® by Proxifier

Adding a proxy server

To add a proxy server, click either **Proxy Settings** in the **Options** menu or the corresponding item on the toolbar:



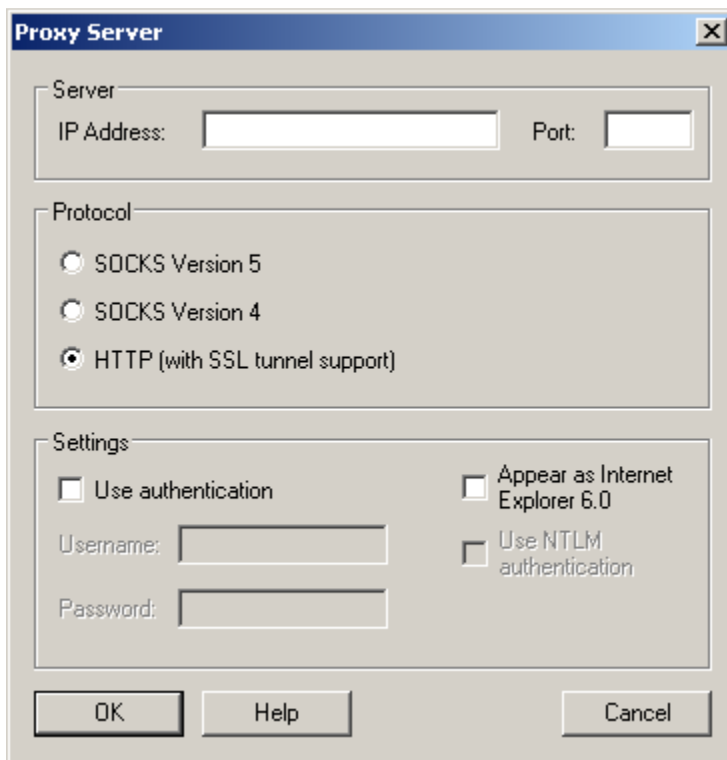
It will open a dialog window where you can add, edit or delete a proxy server used by Proxifier. If several proxy servers are specified, you can change their order in the chain.



WARNING:

If you were using proxies before you installed the Proxifier, then you should disable any old proxy settings. This means that your applications should be configured to connect "directly" to the Internet (rather than through proxies).

To add a proxy server, click the **Add** button. It will open the form where you can specify the parameter of the proxy server:



IP Address

The IP address of the proxy server.

Port

The port number to connect to the proxy server (usually 1080, 80, 8080, 3128, etc.)

Protocol

The protocol used by the proxy server. Proxifier supports three types of protocols:

- **SOCKS version 4** – a widely used proxy server protocol that does not support authentication. You can specify only User ID.
Technical documentation: <http://archive.socks.permeo.com/protocol/socks4.protocol>
- **SOCKS version 5** – has a lot more features than version 4 and supports authentication. You can specify a username and password.
Technical documentation: <http://www.ietf.org/rfc/rfc1928.txt> and <http://www.ietf.org/rfc/rfc1929.txt>
- **HTTP proxy** – the most commonly used type of proxy servers working with the HTTP protocol, but if the server supports the SSL tunneling technology, it can be used for tunneling of any other protocols.
Technical documentation: <http://www.ietf.org/rfc/rfc2817.txt>

HTTP proxy with SSL tunnel support is also known as:

- HTTPS proxy
- CONNECT proxy
- SSL proxy

Attention! Not every HTTP proxy server supports SSL tunneling, therefore, not every HTTP proxy server can be used.

Settings (depend on the type of the proxy server)

Additional proxy server parameters.

- **SOCKS proxy**

Username and Password for SOCKS v5, User ID for SOCK v4.

SOCKS 4A extension allows remote name resolving ("DNS through proxy" feature) for SOCKS v4 proxy.

- **HTTP proxy**

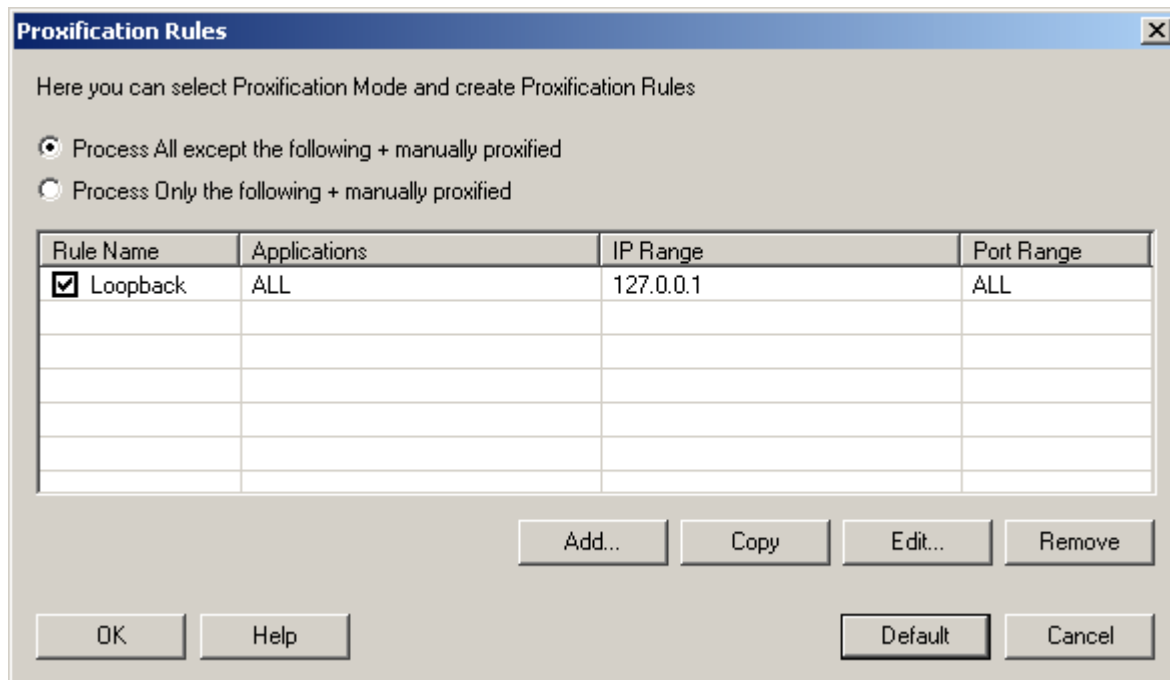
"Appear as Internet Explorer 6.0" - If checked, Proxifier emulates browser's environment and appears as Internet Explorer 6.0 (some firewalls deny all request that do not come from a browser).

"Use NTLM authentication" - NTLM is widely used authentication protocol, it uses encryption for secure transmission of passwords. Not every proxy supports this.

Proxification Rules

This feature allows you to specify the connections that should be proxified. The rules can be based on target IP addresses, port numbers and application names.

To access this feature please click **Proxification Rules** in the **Options** menu. The following dialog window will appear:



As you can see there is a predefined rule – "Loopback". When this rule is enabled – Proxifier doesn't tunnel connections to the loopback interface (IP address 127.0.0.1).

First of all you should choose one of the following modes:

Process All except the following + manually proxified:

Proxifier will Process **ALL** connections **EXCEPT** the ones that match the rules **AND** all [manually proxified applications](#) will be proxified.

The mode is useful when you plan to use Proxifier in almost all of your network activities. For the connections that should not go through proxy server – please create corresponding rules.

Process Only the following + manually proxified:

Proxifier will tunnel **ONLY** the connections that match the rules **AND** all **manually proxified applications** will be proxified.

The mode is useful when the most of your connections should be established directly; however some connections should go through a proxy server. All you need is to create the rules for these connections.

You can **Add** a rule, **Copy**, **Edit (double-click)** or **Remove (Delete button)** a selected rule. **Default** button will reset the rules and the options to default values.

The following form is used to **Add** (create) or **Edit** a rule:

The image shows a dialog box titled "Edit Proxification Rule". It has a close button in the top right corner. The "Rule Name" field contains "New Rule". There are three sections for configuration: "Applications", "IP Ranges", and "Port Range". Each section has a list box containing "ALL" and three buttons: "Add...", "Remove", and "Remove All". At the bottom are "OK" and "Cancel" buttons.

Here you can specify **Applications**, **IP Ranges** and **Port Range**. Please note that you can specify several items in each group.

Note:

The rules have no effect on **manually proxified applications** ('Proxifier' command in the context menu of executable files). In other words, applications started by the 'Proxifier' command will always be redirected through a proxy server.

Warning:

Proxification rules based on IP addresses and Port numbers cannot be used when the **DNS through Proxy** feature is enabled. Only applications names and target ports can be used.

Saving settings

Proxifier automatically saves current settings (proxy list and proxification rules) on exit (without prompting) into a special file. However, you can save settings into another file by clicking **File - > Save Settings As...** menu item.

The file with the settings stores all the necessary information about the proxy server(s) and proxification rules.

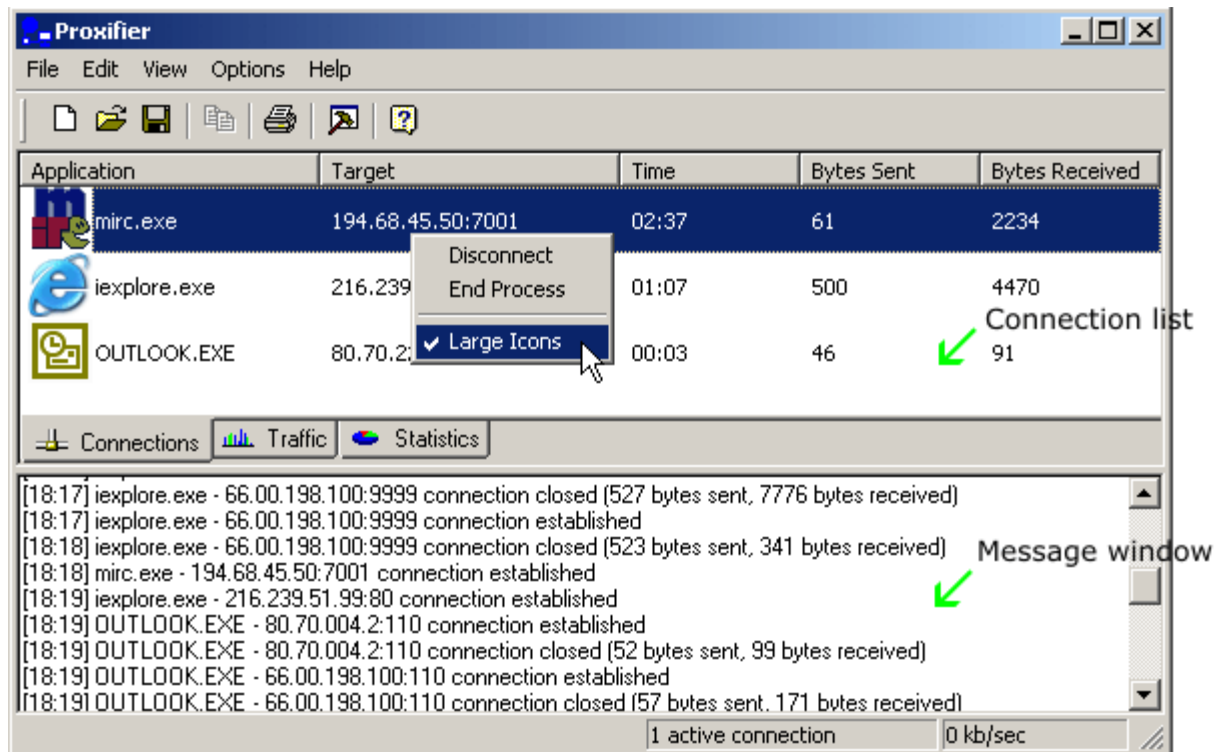
You can create as many files with Proxifier settings as you like and easily load them by clicking **Load Settings** either in the **File** menu or on the toolbar icon. Please keep in mind that the loaded settings do not affect those connections that are already active.

Note:

Proxifier Settings are individual for each user on the System.

Users interface

The main Proxifier window looks like this:



It consists of the following main parts:

Message window

In this window Proxifier displays the information about connections, errors, warnings, etc. in the form of text messages. You can specify the types of messages you would like to get in the **View->Output Level** menu.

To work with the text, right-click the message window and use the context menu.

Connection list

The information about active connections is displayed on this tab. The information about each connection includes the program name the remote address, time, and the number of received and sent bytes. You can sort the list by any of these parameters by just click the corresponding column header.

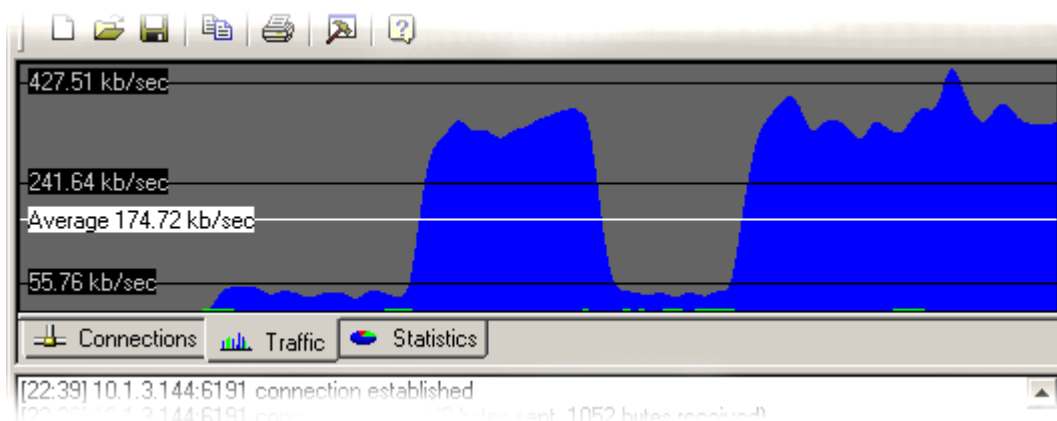
If you right click on a connection, the context menu will be shown. It contains the following items:

Disconnect - closes selected connections.

End Process - ends process which creates selected connection

Large Icons - check to display large icons, uncheck to display small ones.

Traffic



The Traffic tab allows you to view the graphic presentation of the data on the amount of information being transferred. The blue color presents the incoming traffic, while the green one is the outgoing traffic. The horizontal black lines indicate the levels of data transfer rate (kilobytes per second). The white line indicated the average transfer rate for the displayed period

of time.

Right-clicking the Traffic tab will open a context menu. Using it, you can copy or clear the graph and also specify the type of the graph.

Statistics

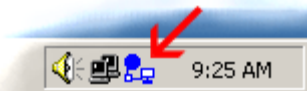
This tab shows various statistics on the work of Proxifier: the total number of connections processed by the program, the number of active connections, the amount of sent and received bytes, the time Proxifier has been working.

System Tray Icon

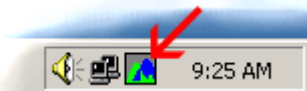
To see the Proxifier icon on the taskbar, check the **Icon in The System Tray** item in the **Options** menu. After that the System Tray will have the Proxifier icon in it and the main window of the program will be hidden when minimized. To maximize the main window of the program, double-click its icon with the left mouse button or select the Open Proxifier item from the context menu.

There are two ways for the Proxifier icon to be presented in the system tray:

- a usual static icon:



- a small graph displaying the process of data transfer, which is in fact a small copy of the graph on the Traffic tab:



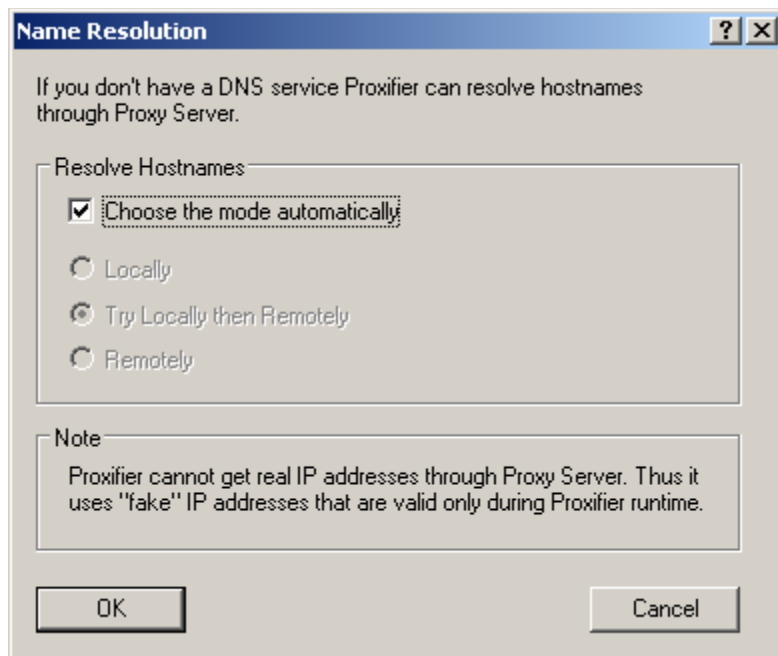
You can easily switch between the variants of the icon. To do it, right-click the icon and either check or uncheck the **Show Traffic** item. You can also do the same with the **Show Traffic on The Tray Icon** item in the Options menu of the main program window.

Using the **Incoming Traffic** and **Outgoing Traffic** items of the context menu, you can specify the graph type to be displayed.

Name resolution through proxy server

This feature is useful when there is no DNS server running on the LAN or access to the server is restricted.

To configure name resolving please click **Name Resolution** in the **Options** menu or the corresponding icon on the toolbar. **Name Resolution** dialog will appear:



There are three available modes:

Locally

Applications resolve hostnames independently from Proxifier (Proxifier doesn't capture DNS requests). In this mode the local computer should be configured to resolve hostnames.

Remotely

Proxifier will resolve hostnames through the proxy server (or through the last proxy server in the chain). Unfortunately, proxy servers cannot just return an IP address for a hostname, thus Proxifier assigns a 'fake' IP address for each hostname (e.g. 0.0.0.123) that is valid only during Proxifier runtime.

Warning:

If you restart Proxifier, all applications that used Remote Name Resolution should be restarted as well, because their DNS cache becomes invalid.

Try Locally then Remotely

Applications will try to resolve hostname through a local DNS service and then through Proxifier (if the local DNS failed).

To let Proxifier detect the mode automatically please enable the **Choose the mode automatically** option.

Notes:

Proxifier will process DNS requests only for the applications which connections are also processed. (You can use **Proxification Rules** to specify it).

Proxifier captures DNS request of the applications that use only standard Windows functions to resolve hostnames. Programs that implement specific DNS capabilities will not be proxified. For example 'nslookup' tool will not be proxified.

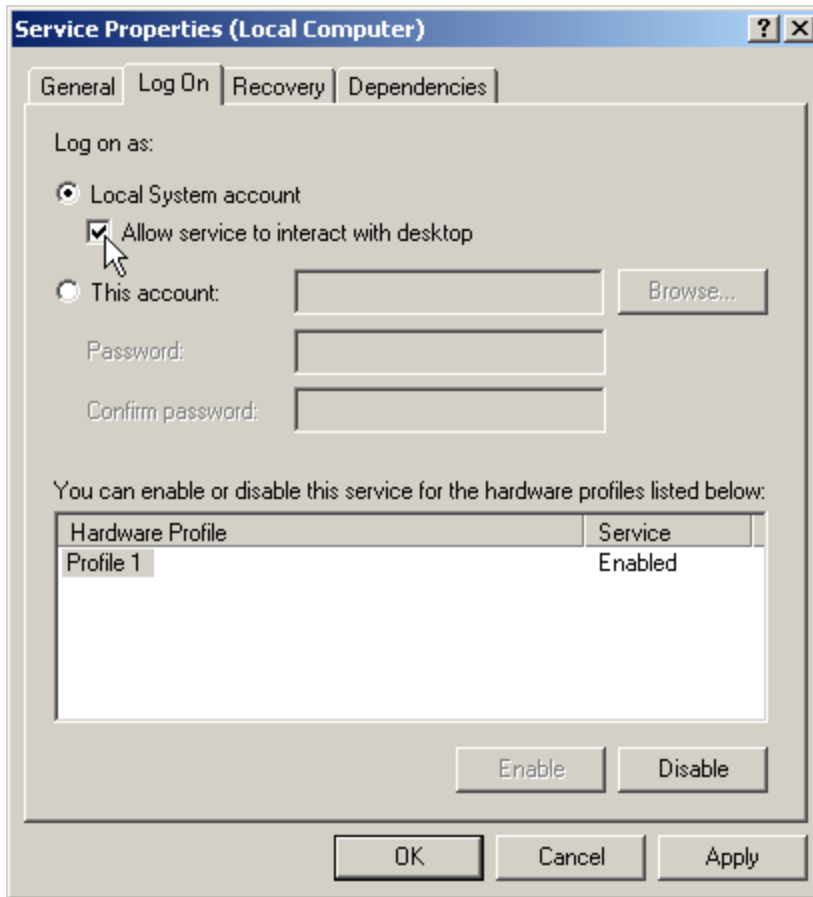
Proxification of Windows Services

Important This article is for advanced users only. If you do not understand the topics in this article, we recommend that you do not perform the described actions.

Warning Changing the Windows Services configuration may be dangerous. We do not recommend proxification of Services that are part of Windows (all Services of services.exe, lsass.exe and other).

Windows Services are special programs that usually run in the background from the Local System account. By default Proxifier don't process Windows Services. If you want to tunnel TCP/IP connections of a certain service – you should do the following:

1. Open Windows Services Manager. To do this please click **Start -> Settings -> Control Panel -> Administrative Tools -> Services**.
2. Double-click on the Service that you want to process. Click **Log On** tab. Check **Allow service to interact with desktop**. (See screenshot).



3. Restart the Service.

Windows will save the settings, so there is no need to repeat the configuring after the computer restarts.

From this moment, the service can be proxified as a regular application. Proxifier will examine Proxification Rules for the service as well, so the connections of the service should match the rules if you want to redirect it through a proxy.

Notes

Some services have the **Allow service to interact with desktop** option enabled by default. Thus these services can be proxified without any modifications.

If a service logs on from non **Local System** account - it can be proxified without modifications as well.

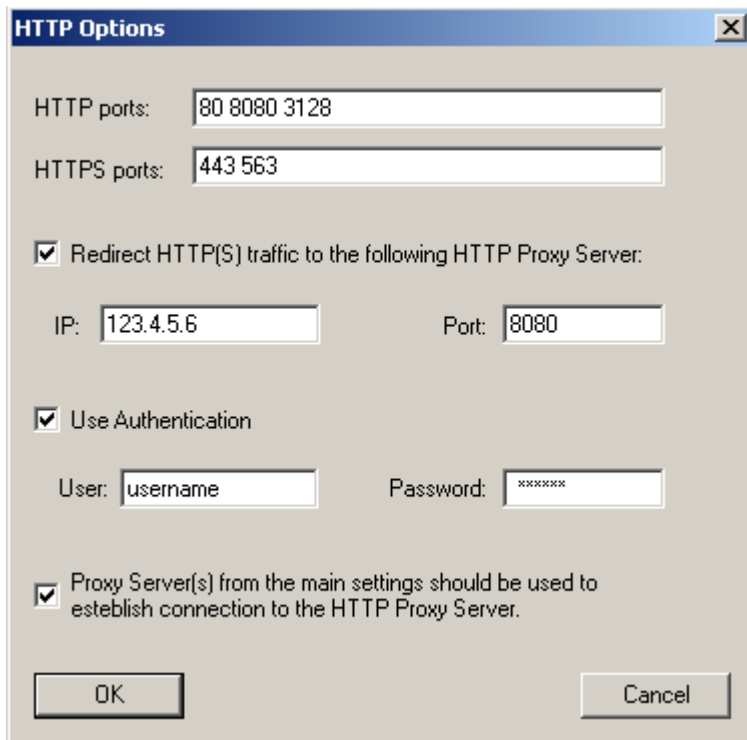
Processing of HTTP traffic

This function can be useful when you have access only to an HTTP proxy server that allows HTTP connections only, or you would like to redirect HTTP traffic through a certain proxy server.

Note:

You can redirect HTTPS traffic as well.

To access this function please click **HTTP Settings** on the **Options** menu or the corresponding icon on the toolbar. **HTTP Options** dialog will appear:



The screenshot shows the "HTTP Options" dialog box with the following settings:

- HTTP ports: 80 8080 3128
- HTTPS ports: 443 563
- Redirect HTTP(S) traffic to the following HTTP Proxy Server:
 - IP: 123.4.5.6
 - Port: 8080
- Use Authentication
 - User: username
 - Password: *****
- Proxy Server(s) from the main settings should be used to establish connection to the HTTP Proxy Server.

Buttons: OK, Cancel

To enable the function please click **Redirect HTTP(S) traffic to the following HTTP Proxy Server** and specify **IP address** and **Port** of the proxy server.

Proxifier will redirect traffic to the proxy server only if it can find the target port in the **HTTP(S) ports** list.

Also you can enable **Authentication** on the proxy server.

The bottommost option allows you to redirect the HTTP traffic through the proxy server(s) from the main settings. It can be useful when you cannot access the HTTP proxy server directly.

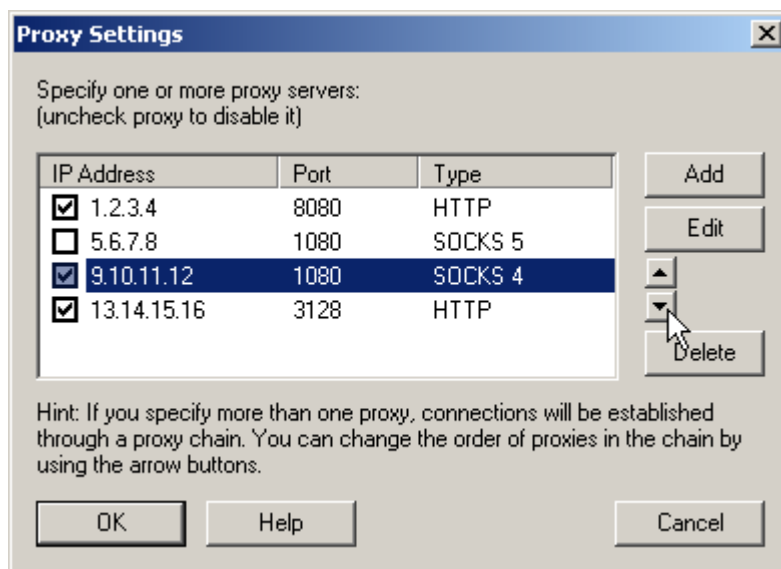
Note:

If an HTTP proxy server is already used by a client application (e.g. web browser) – Proxifier will redirect the traffic to the HTTP proxy server that is specified in the Proxifier settings.

Working through a chain of proxy servers

With Proxifier you can work through a chain of proxy servers (SOCKS4, SOCKS5, HTTP). Connecting to a remote host will be performed sequentially from one proxy server to another, thus, you will securely hide you actual IP address from the remote host.

To create a chain of proxy servers, click **Proxy Settings** in the **Options** menu and add two or more proxies. Connections between proxy servers will be established in the order they are displayed in the list. You can change the order using the arrow buttons in the right-hand part of the window:



(These are not real proxies, only a sample)

Hint: uncheck proxy to disable it.

When working through a chain of proxies, mind the following:

- A chain can contain proxy servers of different types (SOCKS v4, SOCKS v5, HTTP)
- If at least one proxy is not functioning, the entire chain will not work
- The total lag will be the sum of all lags at all proxy servers in the chain
- If the connection is terminated at one proxy, the connection to the remote host is lost

Working without a proxy server

Proxifier can work without a proxy server. This working mode does not differ in any ways from working through a proxy server, except that all connections will be established directly from the local computer to the remote one.

In this mode Proxifier can be used as a powerful tool for monitoring network connections, traffic (can be displayed as an icon in the System Tray); you can use it to log, save and analyze the traffic of various network applications.

Logging

Proxifier allows you to save the entire information about all the events taking place during its work to a special log file, and also all the traffic passing through it. The content of the log file is the same as the content of the message window.

To start logging, click **Log Level** on the **View** menu and select the necessary logging level:

- 0** – logging is off
- 1** – only errors are logged
- 2** – all events are logged
- 3** – all events are logged and the entire traffic is saved

The log file is saved to the Logs subdirectory of the directory where Proxifier is installed. Traffic is saved to the Traffic subdirectory as files with names of the following type *to(from)_IP address_N.dmp*. Each connection has two files created for it: the incoming traffic is saved to one of them, while the outgoing traffic is saved to the other one.

Attention! Saving traffic on fast networks may require a lot of space on the hard disk.