

Proxifier v3 for Microsoft Windows

Standard and Portable Editions

User Manual

Introduction	2
What's New in Version 3	2
Proxifier v2 Migration Notes.....	6
Quick Start.....	6
Proxy Server Settings	8
Proxification Rules	11
Manual Proxification <i>Standard Edition only</i>	14
Profiles.....	15
User Interface	18
System Tray Icon.....	20
Name Resolution Through Proxy	21
Proxy Chains.....	22
Proxy Server Redundancy	23
HTTP Proxy Support	25
Advanced Proxy Server Settings	27
Profile Auto Update.....	29
Direct Connections	30
Log Files	30
Services and Other Users <i>Standard Edition only</i>	31
Connection Loop Detection.....	31
Proxifier Editions.....	32
Run as Windows Service <i>Standard Edition only</i>	33
Portable Network Engine <i>Portable Edition only</i>	34
Proxy Checker	35
Proxifier System Settings <i>Standard Edition only</i>	36
Network Error Codes.....	38
Order Proxifier.....	38
Trial Version.....	39
Technical Support.....	39
End-User License Agreement.....	39

Introduction

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

With Proxifier you can easily tunnel all TCP connections on the system or the selected ones only.

Proxifier allows you to:

- Run any network applications through a proxy server. No special configuration is required for the software; the entire process is completely transparent.
- Access the Internet from a restricted network through a proxy server gateway.
- Bypass firewall restrictions.
- “Tunnel” the entire system (force all network connections including system connections to work through a proxy server).
- Resolve DNS names through a proxy server.
- Use flexible Proxification Rules with hostname and application name wildcards.
- Secure privacy by hiding your IP address.
- Work through a chain of proxy servers using different protocols.
- View information on current network activities (connections, hosts, times, bandwidth usage, etc.) in real-time.
- Maintain log files and traffic dumps.
- Get detailed reports on network errors.
- ... and much more.

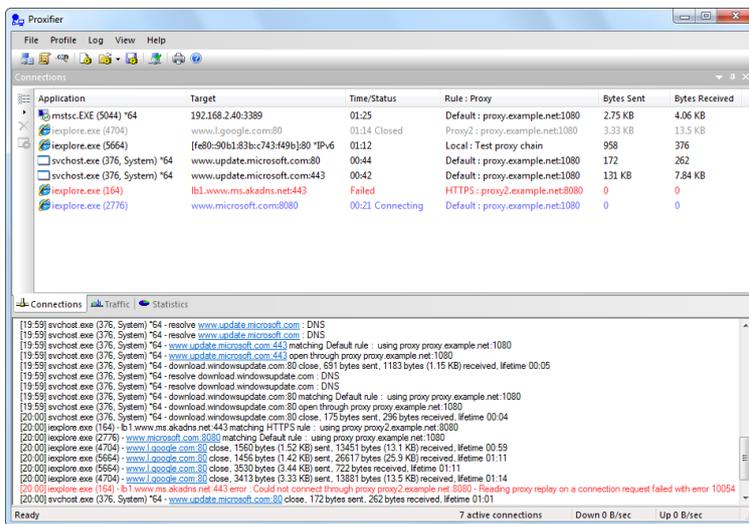
Specifications:

- Proxy protocols: SOCKS v4, SOCKS v4A, SOCKS v5, HTTPS and HTTP (HTTP connections only).
- Authentication: SOCKS5 Username/Password Authentication (RFC 1929), HTTP Basic, NTLM (including transparent mode).
- Full IPv6 support
- Full 64 bit applications and systems support.
- Profile password encryption up to AES 256 bit.
- Windows 2000/XP/Vista/7/8/10, Server 2003/2008/2012/2016.

What's New in Version 3

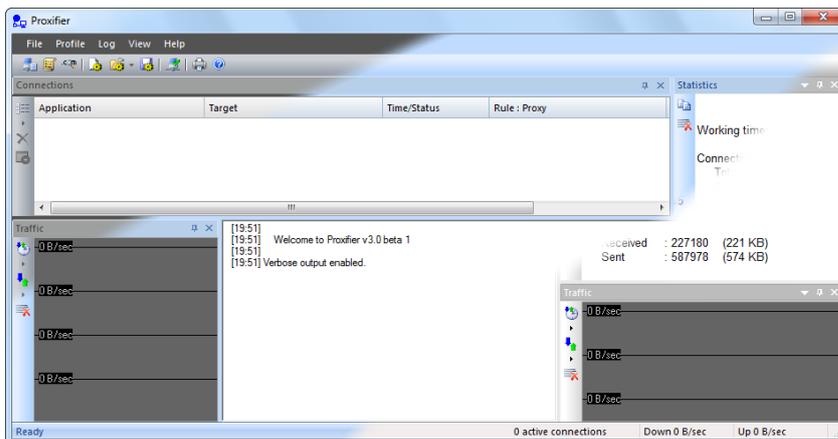
Improved UI and New Visual Style

The new version features a significantly improved user interface. The connection list provides much more detailed information about the connections including: selected proxy server, matched rule, connection status with color indication, x64 and IPv6 mark, user name and process ID. All additional information is displayed only when needed so UI remains clean and easy to read.



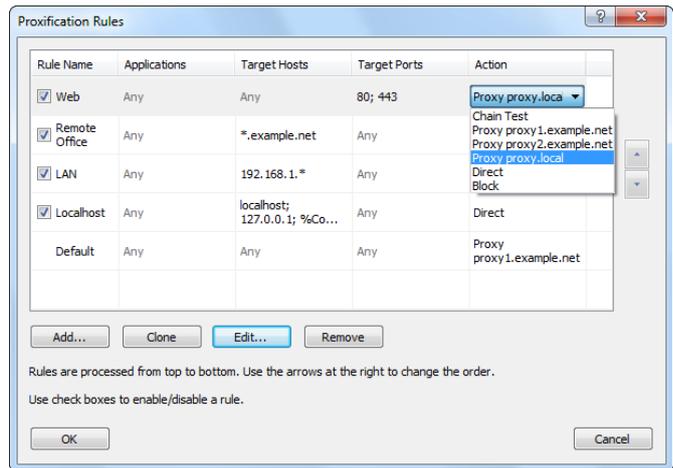
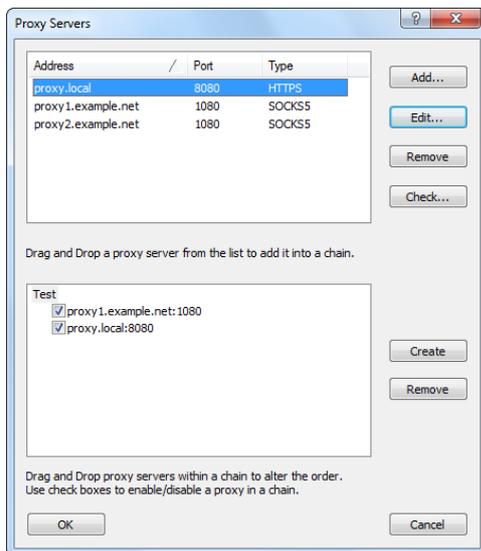
Proxifier log messages are now more detailed, including all new parameters listed in the above paragraph. Additionally a number of new messages were introduced. Now Proxifier can be configured to output DNS requests, rules processing messages and more. Verbosity of the output can be changed via the **Log** menu. It is possible to set different log levels for screen and file output and the log file directory is also configurable.

The new version features a new, fresh and much more flexible user interface. You can even create your own configuration of panels or change visual appearance (**View->Application Look**).



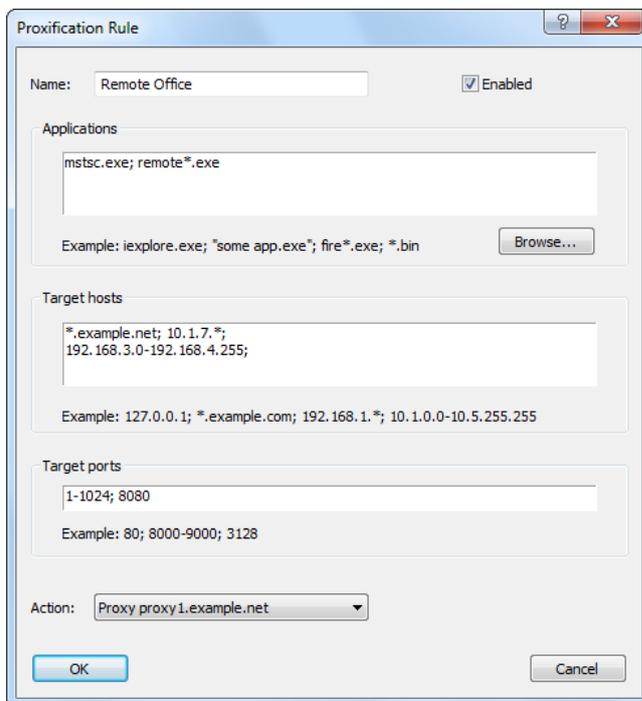
Brand New Concept for Proxy Settings and Rules

The core Proxifier configuration has been significantly redesigned and improved. Now you can specify independent multiple proxy servers in (**Profile->Proxy Settings...**). It is also possible to create multiple proxy chains and manipulate them via the new UI.



The new version allows you to assign different proxies/chains for different **rules** (**Profile->Proxification Rules...**). Thus each rule has an individual action that tells Proxifier to process the connections through a proxy or chain, to block the connection or to open it directly.

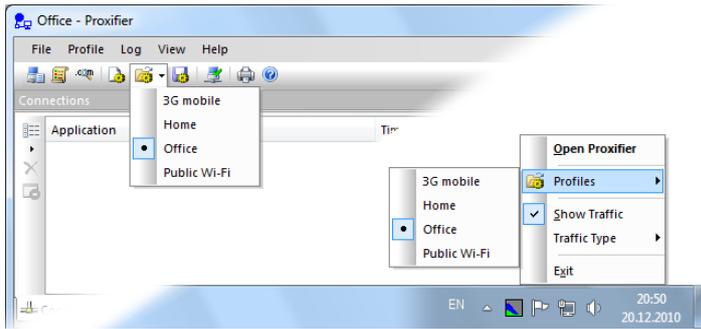
Rule configuration has been redesigned to be much more comprehensive and flexible. Applications and target hosts can be specified as wildcards (e.g. inet*.exe, 192.168.1.*, etc.). Another very important improvement is DNS name support. Thus the target can be specified by its host name mask such as *.example.com



Profiles

Management and organization of Proxifier configuration files (*.prx) has been improved and the function has been renamed to **Profiles**. The key features of the new approach are:

- Fast switching between profiles.
- Password encryption (**Profile->Advanced->Password Encryption**).
- XML format of profile files (*.ppx).



Support for New Technologies

Proxifier v3 fully supports IPv6 protocol and x64 applications and systems. Everything works out of the box. No additional configuration is required.

Transparent NTLM authentication with current user credentials is supported.

All character processing is now based on Unicode. Proxifier works well with any international strings and fonts.

The new version is fully compatible with the latest versions of Windows operating system and benefits from the features available on Windows Vista, Windows 7 and Windows Server 2008.

We also did our best to ensure maximum backward compatibility. It is still possible to run Proxifier on Windows 2000.

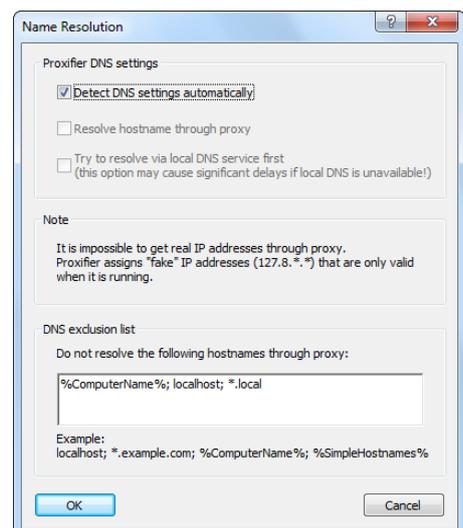
Services and Other Sessions Proxification

Standard Edition only

The Proxifier network module has been rewritten to support **Windows Services** and applications being run by other users on the computer (**Profile->Advanced->Services and Other Users...**).

DNS over Proxy Improvements

Now you can specify the hostnames that should be resolved with local DNS when Proxifier is configured to process **hostnames through a proxy**. This feature is useful when you need to work with LAN and Internet connections at the same time.



Other

Version 3 features a number of other improvements. Overall the user experience has been significantly improved. We did our best to ensure maximum compatibility with third-party software, especially firewall and antivirus packages. The new version is much less likely to cause software conflicts.

Proxifier v2 Migration Notes

Proxifier v3 does not import old settings automatically. To convert an old configuration file from Proxifier v2 (*.prx) please use the **File->Import Profile...** command.

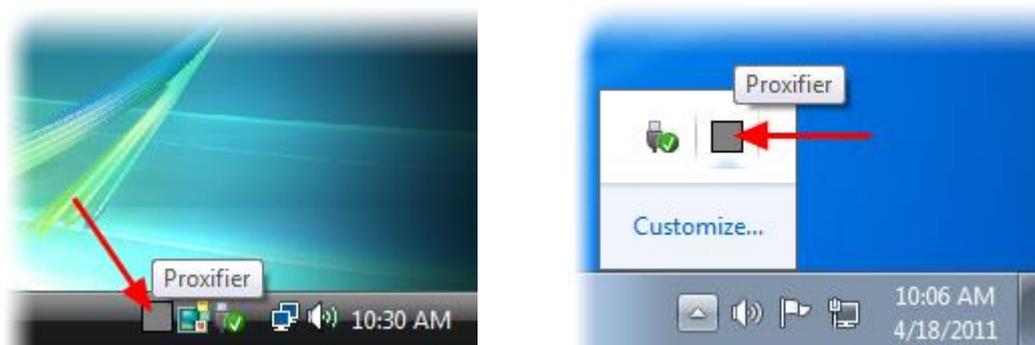
We do not expect any problems with migration, but to avoid any trouble please be aware of the following changes:

- Each **Proxification Rule** now has a specific action that tells Proxifier to connect through a proxy or chain, connect directly or block the connection.
- Proxifier examines the rules from top to bottom. The order of the rules now matters and can be changed.
- If a connection matches no rules, it is processed according to the special default rule located at the bottom of the list.
- Direct connections are not processed by default. To change this, please enable **Profile->Advanced->Handle Direct Connections**
- Multiple **proxy servers** are not chained automatically. The order of the proxies in the list is not relevant. You should implicitly create a proxy chain from the specified proxies.

For complete information about each option above please see the corresponding topic in this document.

Quick Start

Install and launch Proxifier. The Proxifier icon showing traffic (information flow) will appear on the system tray. On Windows 7, the icon can be hidden.

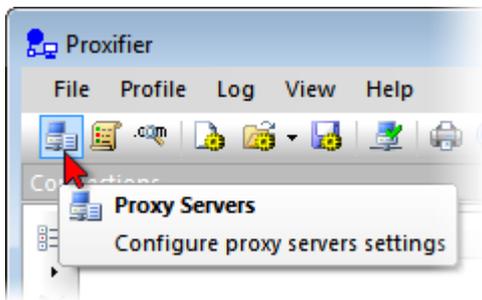


Double click the system tray icon to open the main window of the program. Alternatively, you can start Proxifier again from the start menu and the existing running instance will be detected and will activate the main Proxifier window.

By default, Proxifier is configured to bypass all network connections. You can still see connections and DNS requests if you enable verbose output **Log->Output Level->Verbose**.

Proxifier can process the connection directly (without a proxy server). To enable this mode, set **Profile->Advanced->Handle Direct Connections**. It can be useful to troubleshoot problems and utilize some features of Proxifier like traffic dumps, bandwidth and connection monitor, etc.

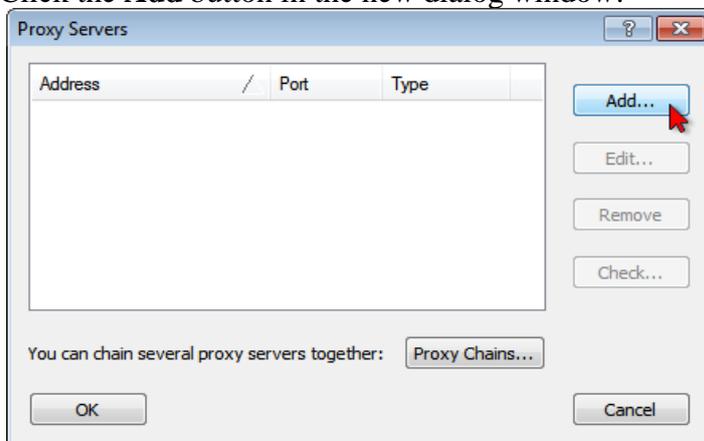
To make the connections work through a proxy server or a chain of proxy servers, you must first define a proxy server in Proxifier. Click **Proxy Servers...** in the **Profile** menu or click on the icon located on the toolbar:



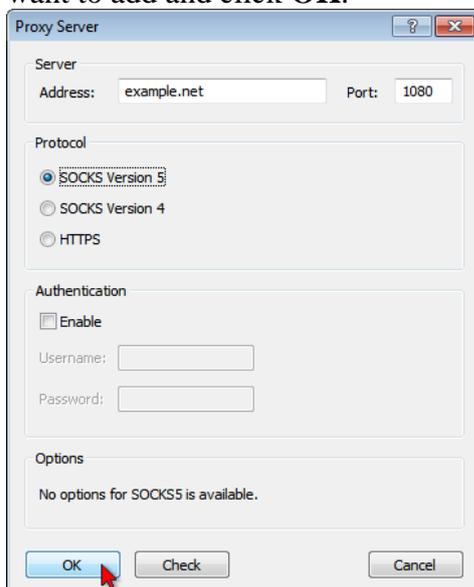
WARNING!

If you were using proxies before you installed Proxifier you should disable any built-in proxy settings. Your applications should then be configured to connect “directly” to the Internet (rather than through proxies).

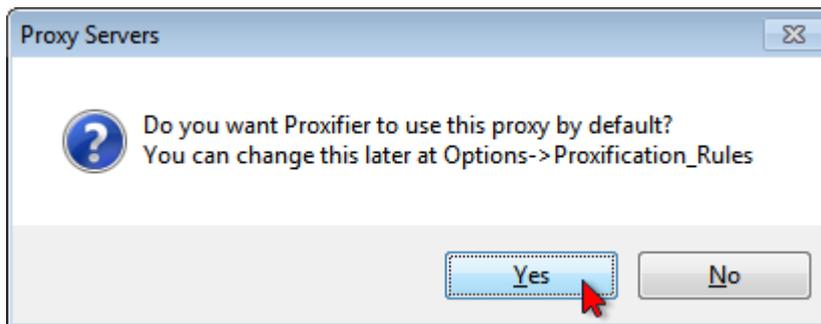
Click the **Add** button in the new dialog window:



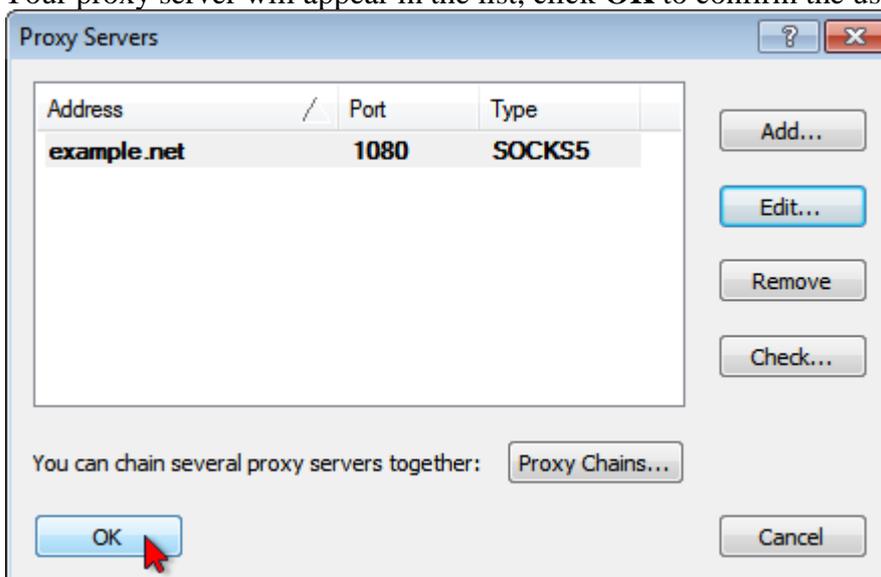
Fill in the form specifying the details of the **proxy server** (address, port, protocol, etc.) that you want to add and click **OK**:



Proxifier will ask you whether or not you want to use this proxy by default. Click **Yes** to set it as the target for the Default Proxification Rule. You can change this anytime later at **Proxification Rules**.



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



From now on all new connections (TCP/IP) will be established through the specified proxy server while Proxifier is running.

If you only want to tunnel specific connection, not all of them, use **Proxification Rules** and/or **Manual Proxification Mode**.

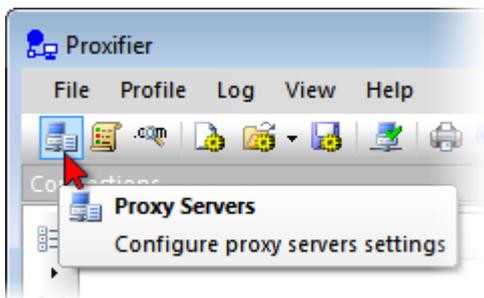
By default, Proxifier gets minimized to the **System Tray** when you close its window. You can change this behavior at **View->Icon in the System Tray**.

To exit Proxifier when the System Tray icon is enabled right-click on the icon and select **Exit**.

To make Proxifier start automatically on user login, enable **File->Autostart** option.

Proxy Server Settings

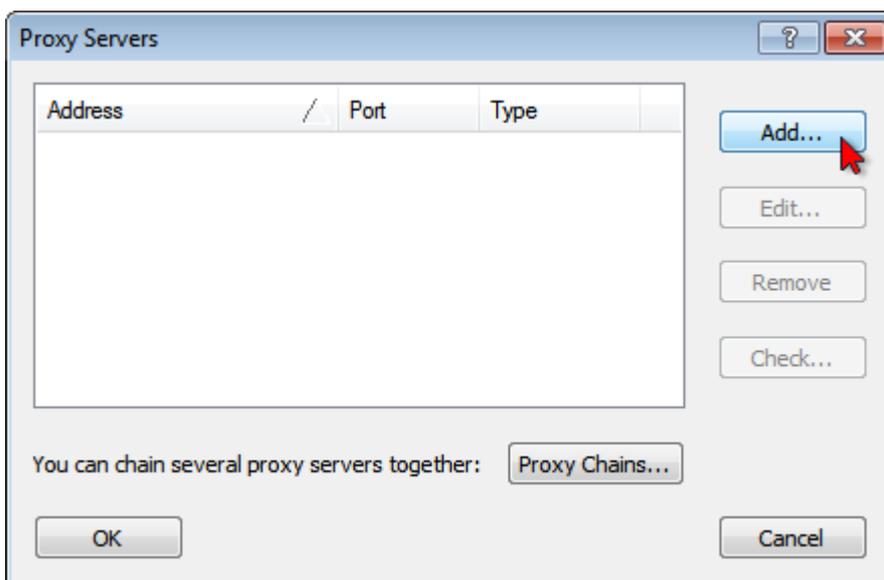
To add a proxy server, click either **Proxy Servers** in the **Profile** menu or the corresponding item on the toolbar:



WARNING!

If you were using proxies before you installed Proxifier you should disable any built-in proxy settings. Your applications should then be configured to connect “directly” to the Internet (rather than through proxies).

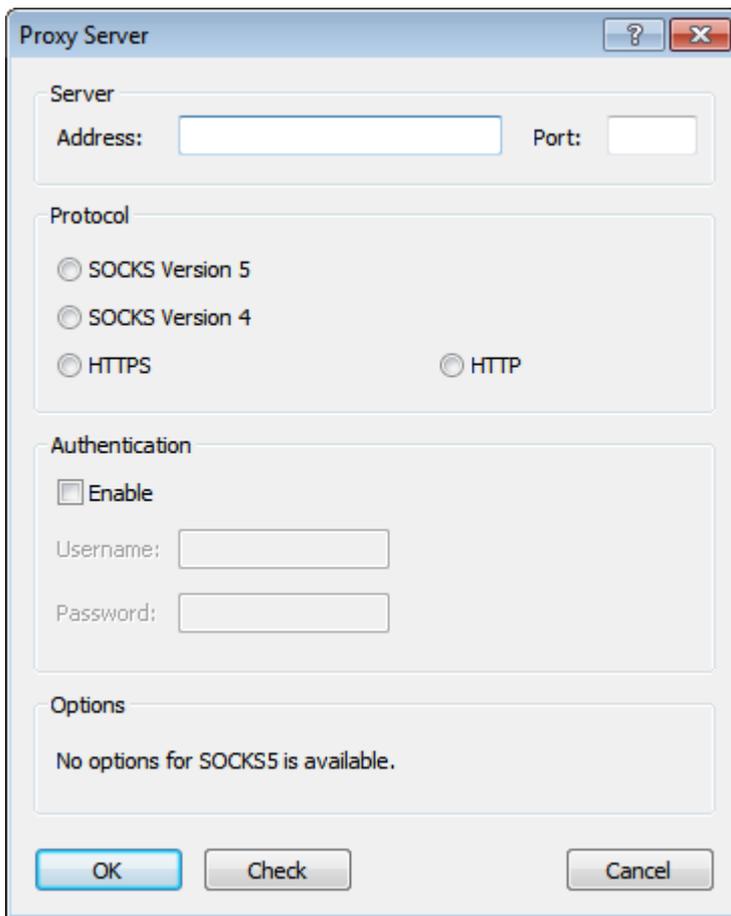
This will open a dialog window where you can add, edit or remove proxy servers and **proxy chains** used by Proxifier. If several proxy servers are specified, you can create a **proxy chain**.



A proxy server will be displayed in bold if it is defined as the **Action** for the **Default Proxification Rule**.

The order of the proxy servers in the list is not relevant. You can sort the list by address, port and type (protocol).

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



Address

The address of the proxy server can be a hostname or IPv4/IPv6 address.

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 four types of protocols:

- **SOCKS version 4(A)** — a widely used proxy server protocol that does not support authentication.
You can specify only User ID.
- **SOCKS version 5** — has more features than version 4 and supports authentication. You can specify a username and password.
Technical documentation can be found at: <http://www.ietf.org/rfc/rfc1928.txt> and <http://www.ietf.org/rfc/rfc1929.txt>
- **HTTPS** — HTTP proxy with SSL support for arbitrary ports.
Technical documentation can be found at: <http://www.ietf.org/rfc/rfc2817.txt>
HTTP proxy with SSL tunnel support is also known as:
 - CONNECT proxy
 - SSL proxy

WARNING!

Many **HTTP proxy** servers do not support SSL tunneling; therefore, they cannot be used as HTTPS. If an **HTTP proxy** works properly in the browser but fails in

Proxifier, it most likely means that SSL support is unavailable. You can also check the proxy with the **Proxy Checker** tool.

- **HTTP** — the most common type of proxy servers. Unfortunately, such proxies can only be used for **HTTP connections**. You can enable this protocol at **Profile->Advanced->HTTP Proxy Servers...** Please make sure that you have read and understood the **HTTP proxy servers** topic before using this option!

Authentication and Options

The options available depend on the proxy server protocol.

- **SOCKS version 4(A)**
User ID — used for the purposes of authentication.
SOCKS 4A extension — allows remote **name resolving** (“DNS through proxy” feature) for SOCKS v4 proxy.

- **SOCKS version 5**
Username and Password — user authentication.

- **HTTPS**
Username and Password — user authentication.

Appear as Internet Explorer 6.0 — if checked, Proxifier emulates browser’s environment and appears as Internet Explorer 6.0 (some firewalls deny all requests that do not come from a browser).

Use NTLM — it is a widely used authentication protocol using encryption for secure transmission of login credentials.

Use current user login — proxy authentication will be done with current user credentials. Also known as transparent NTLM authorization.

- **HTTP**
Username and Password — user authentication.

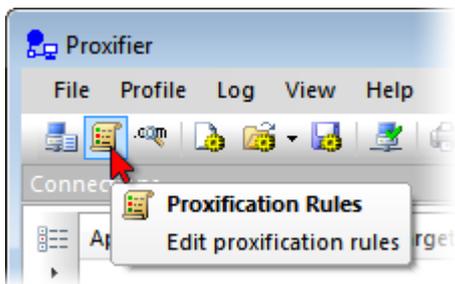
You can check any proxy with the **Proxy Checker** tool using the **Check** button.

Proxification Rules

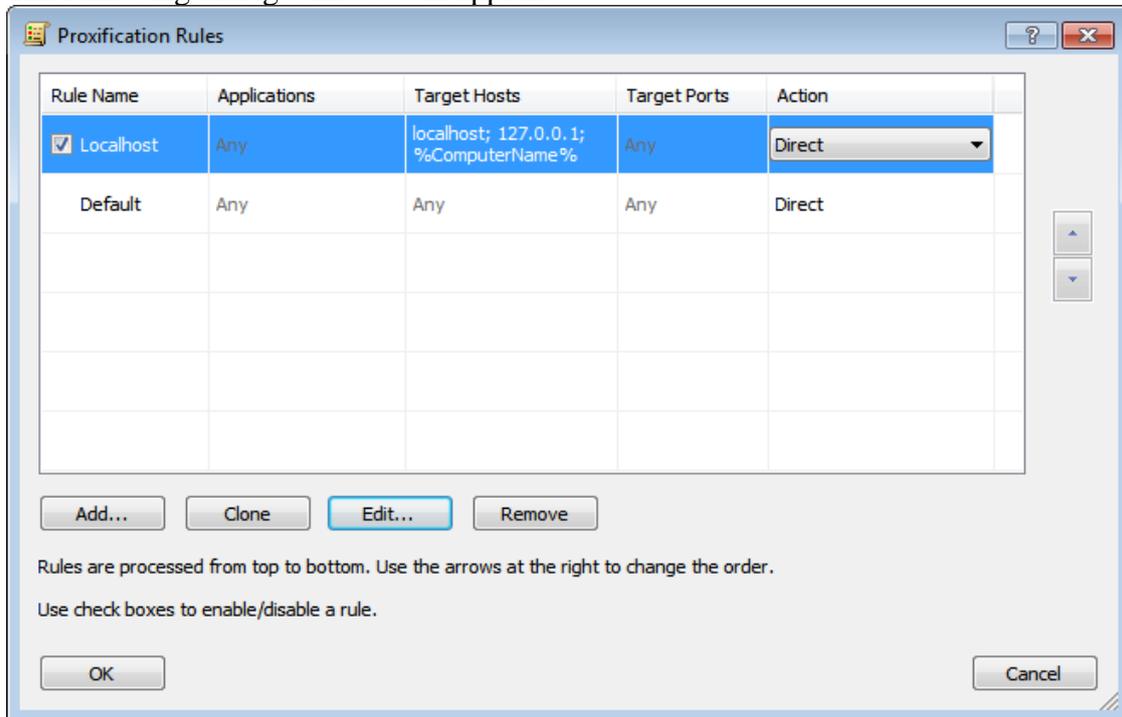
This feature allows you to define how certain connections should be processed by Proxifier. Each connection can be **processed directly**, through a **proxy/chain** or blocked.

The rules can be based on application names, the target host IP or address and port numbers. Applications and targets can be specified as wildcards. Ports can be specified as ranges.

To access this feature, click **Proxification Rules** in the **Profile** menu or the corresponding item on the toolbar:



The following dialog window will appear:



The “Default” rule cannot be changed. It is a special rule. Proxifier uses it when no other rules match the connection. You can only change the **action** for this rule.

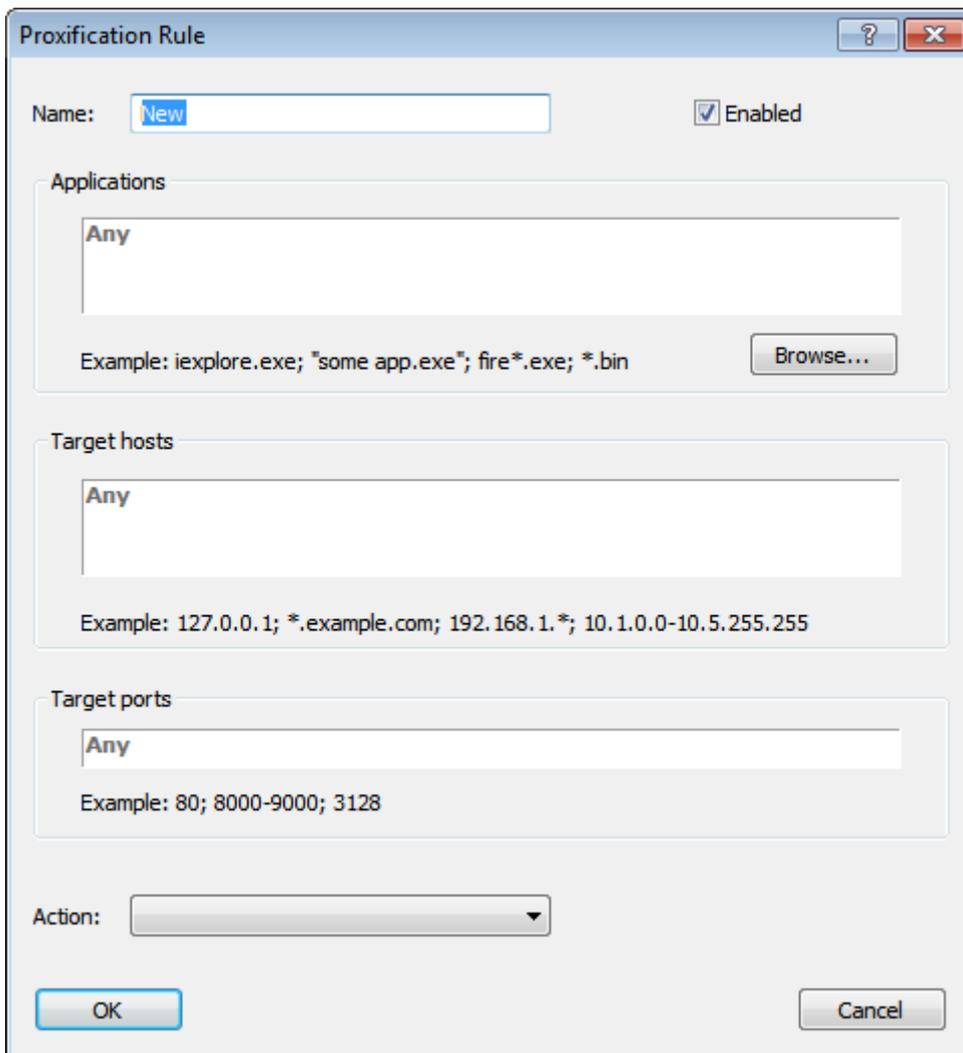
For example, if you assign a **proxy server** as an action for the “Default” rule and you have no more rules defined, Proxifier will process all connections through this proxy.

By default each profile also has a predefined rule called “Localhost.” When this rule is enabled, Proxifier does not tunnel local connections (loopbacks) on the computer. Some applications like Firefox can depend on the loopback connections. You can edit or remove this rule, but it is recommended to keep it enabled unless you are absolutely sure that you need to tunnel connections to 127.0.0.1 through a proxy.

Proxifier scans rules from top to bottom. Thus, the rule order is important. You can change the order with the arrow-like buttons on the right side of the window.

You can **enable/disable** the rules with the check box and change the rule’s **action**. With the corresponding buttons it is possible to **Add** a new rule, **Clone**, **Edit** or **Remove** an existing rule. Alternatively, you can use double-click to edit a rule or the “Del” key to remove it.

When you edit a rule or add a new one the following window appears:



Name — the name of the rule. You can use any text that is meaningful for you.

Enable — use this check box to enable/disable the rule. When the rule is disabled, Proxifier simply ignores it.

Applications — a list of executable file names that correspond to the programs which connections should match the rule.

Separate individual names with a semicolon (;). Use double quotes (“”) for names containing spaces.

You can use wildcards (masks) where “?” matches any symbol and “*” matches any substring. The path of the file is not relevant.

With the **Browse...** button you can browse for the file and add it to the list.

Target hosts — to match the rule a connection should connect to a host from this list. You can specify host names (DNS names), IPv4 or IPv6 addresses.

Separate individual addresses with a semicolon (;). Wildcards (masks) are supported and you can use wildcards (masks) where “?” matches any symbol and “*” matches any substring.

IPv4/IPv6 addresses can be specified as a range. Use a minus sign (-) to define the range.

%ComputerName% constant is automatically swapped with the local computer name during the processing.

Target ports — to match the rule a connection should connect to a port from this list.

You can use any integer from 1 to 65 535 ($2^{16}-1$). Separate individual ports with a semicolon (;).

Use a minus sign (-) to define a range.

Action — defines how Proxifier should process the connection if it matches the rule.

Possible options:

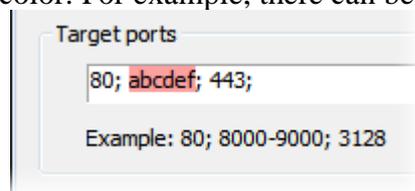
Proxy <name> — process the connection through the **proxy server**. You can define **proxy servers** at **Profile->Proxy Servers...**

Chain <name> — process the connection through the **proxy chain**. You can create **proxy chains** at **Profile->Proxy Servers...**

Direct — process the connection directly (skip any processing). The connections will be connected to the original target.

Block — the connection will be blocked.

Proxifier applies certain filtering for the text fields. Incorrect symbols are indicated with red color. For example, there can be no letters in **Target ports** field:



To match the rule a connection should satisfy all three criteria: **Applications**, **Target hosts** and **Ports**. If you have nothing defined in a field, the word “Any” in gray color is displayed and it will then match all possible values for certain criteria. This effectively means that this criterion will not be used for rule valuation.

For example, if you specify **Applications** only and leave **Targets** and **Ports** empty, Proxifier will process all connections of the specified applications regardless of the target hosts and ports.

Note:

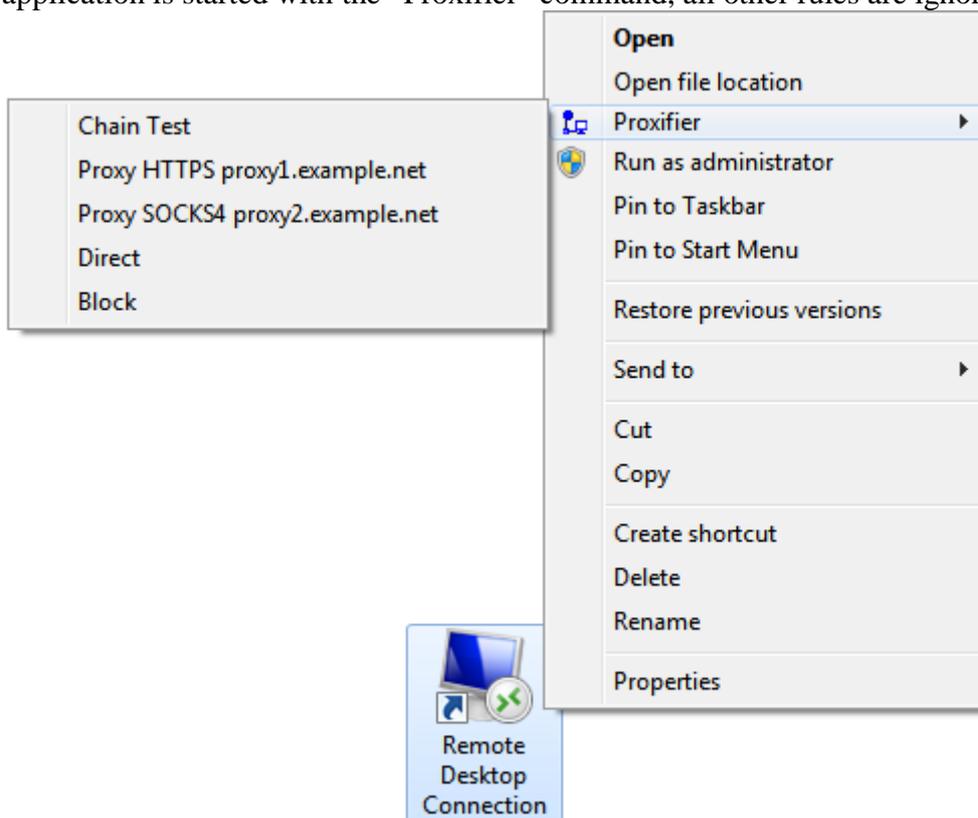
The rules have no effect on **manually proxified applications** (“Proxifier” command in the context menu of exe-files). In other words, applications started by the “Proxifier” command will always be redirected through a proxy server.

Manual Proxification

Standard Edition only

Apart from **Proxification Rules** you can set proxification options manually for certain applications. When Proxifier is installed and running, Windows adds a “Proxifier” command to the exe-file context menu.

The “Proxifier” submenu shares the same actions with the **Proxification Rules**. You can select a proxy or a chain, block connections or process them directly. When an instance of the Proxifier application is started with the “Proxifier” command, all other rules are ignored for this instance.



Please note that the “Proxifier” command is only available for exe-files or shortcuts (lnk-files) that point to exe-files. Different versions of Windows can use different kinds of surrogate shortcuts that technically are not links to exe-files. If you do not see the “Proxifier” command in the context menu of an application, it is recommended that you find its executable file and create a direct link to it.

On Windows 7, to display the context menu for application icons located on the task bar, hold down the “Shift” key when you right-click on them.

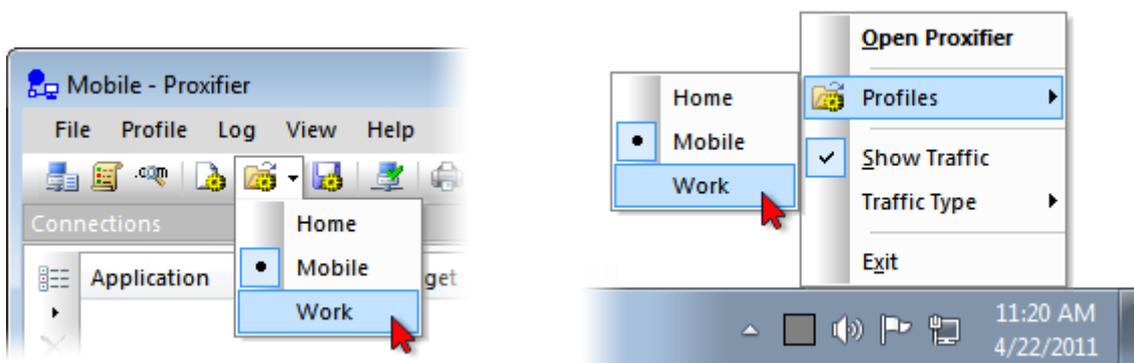
Another problem can be caused by applications that use launchers and multiple instances. If you start a program that starts another one, only the original one will be processed accordingly to the “Proxifier” command. A good example of this is Internet Explorer. When Protected Mode is enabled it starts a new instance of its own each time you run it so you cannot perform manual proxification for it.

Profiles

Proxifier settings located in the **Profile** menu together are referred to as a profile. This includes **Proxy Servers**, **Proxification Rules**, **Name Resolution** and others. Settings available under **Log** and **View** menus are not included in a profile. Mostly they represent settings related to the Proxifier user interface and appearance.

Proxifier automatically saves the current profile (without prompting) on any change. You can save the profile with a specific name by **File->Save Profile As...** and load it later with **File->Load Profile**. The name of the active profile is displayed at the title of the main window.

You can easily navigate and load profiles with the toolbar button or the context menu of the **system tray icon**:



To import or export a profile from/to a file use the **Import Profile** or **Export Profile** commands of the **File** menu respectively. With **Import Profile** you can import settings from the old versions of Proxifier (prx-files).

You can also manage profiles at the file level with **File->Manage Profiles...** command.

Proxifier profiles are user specific. Each user account on the computer has its own private set of profiles.

However, it is possible to specify one global profile for all users on the computer. To do this, just export the profile as “Default.ppx” (**File->Export Profile**) and place it into: “C:\Users\All Users\Application Data\Proxifier\” or its equivalent on your system. Proxifier checks this path on start and if there is “Default.ppx” file, it loads it automatically.

Proxifier v3 uses XML for profile files. The format is human readable and self-explanatory. You can edit the content with any third party tools and scripts.

You can load a profile via command line using the following command:

Proxifier.exe profile-file-name.ppx

If Proxifier is not running it will be started with specified profile. If Proxifier is already running, the profile will be loaded into the running instance.

In order to load a profile silently (without user prompt) use “*silent-load*” flag:

Proxifier.exe profile-file-name.ppx silent-load

Profiles can contain passwords for proxy servers. To protect this information Proxifier supports encryption. You can change encryption options at **Profile->Advanced->Password Encryption...**

The same settings are requested anytime you use **Export Profile**.

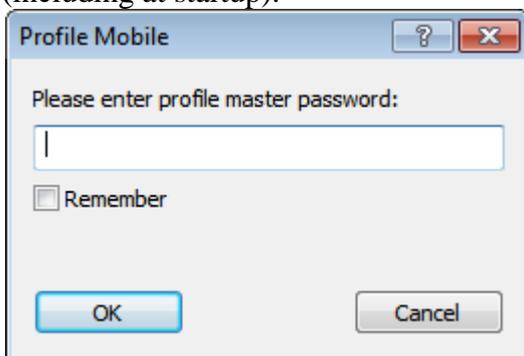


The description of each option is provided in the dialog window above.

Basic and **Current user account** uses AES 256 bits.

For **Profile master password** Proxifier uses the standard Windows Data Protection API (DPAPI). Internally it is based on Triple-DES.

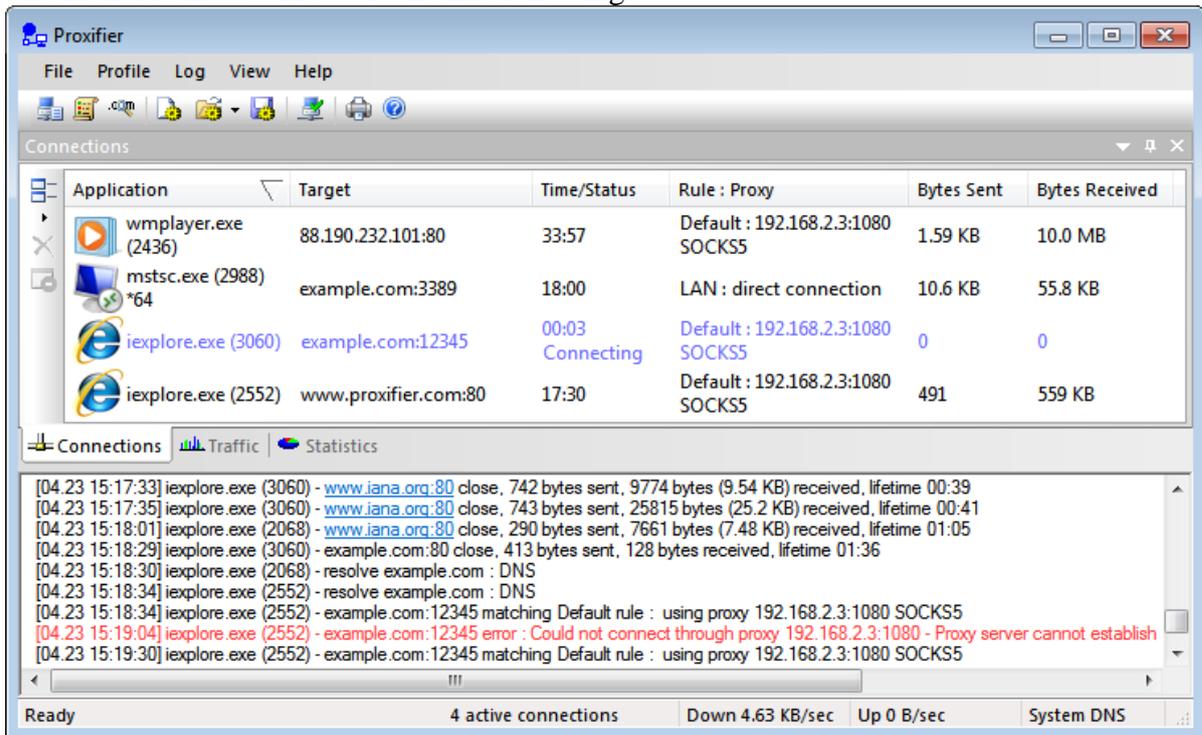
When **Profile master password** is used Proxifier asks it each time the profile is loaded (including at startup).



You can save this password within the current user account with the **Remember** checkbox. Proxifier will not load the profile until the correct password is specified. Please consider this if you are going to use Proxifier in unattended mode (e.g. with **autostart** feature). If you enter an incorrect password, Proxifier will ask you to repeat or load the profile with blank passwords.

User Interface

The main Proxifier window looks like following:



Four main parts are **Connections**, **Traffic**, **Statistics** and **Output**. The first three are panes so you can adjust their layout, drag-and-drop, dock, hide, close, etc.

To enable/disable the panes use the **View->Windows** menu. The layout is saved through the restart of Proxifier.

You can reset the entire layout with **View->Reset Layout** command.

Connections

In this window you can see a list of active connections handled by Proxifier with status. The information about each connection is divided into the following groups (columns):

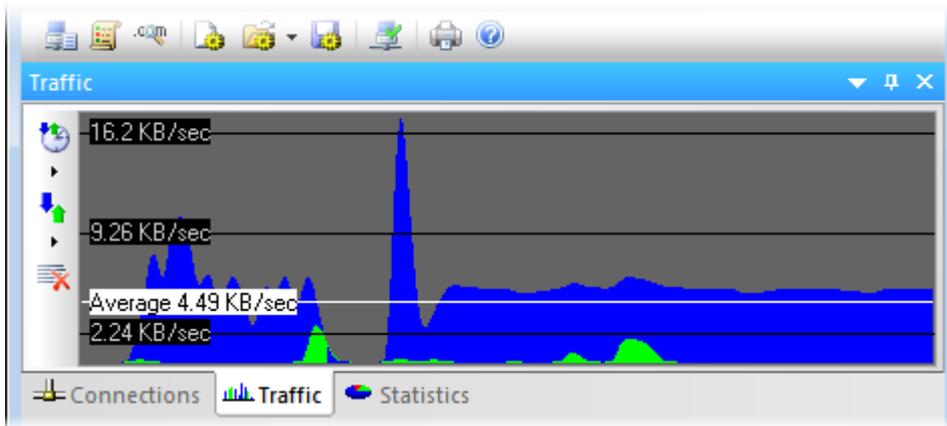
- *Applications* — program name, process ID (if **Verbose** output is enabled), “*64” mark for 64 bit applications.
- *Target* — target host address (DNS name or IPv4/IPv6) and port number.
- *Time/Status* — time elapsed from the last status change. Available statuses are Connecting (blue), Closed (gray), Failed (red) and Canceled (red). No status is displayed for an active connection.
- *Rule - Proxy* — **rule** name and **proxy** address with the protocol or **chain** name. If no proxy is assigned “**direct connection**” is displayed.

You can sort the list by any of these parameters with a click on the corresponding column header.

On the left hand side of the window there is a toolbar with three buttons. You can use it to change the size of the list elements, to close a connection or to terminate a process. The same options are available in the context menu (right-click).

Traffic

The Traffic pane allows you to view the graphic presentation of the data on the amount of information being transferred.



The blue represents incoming traffic, and green is outgoing traffic. The horizontal black lines indicate the levels of the data transfer rate. The white line indicates the average transfer rate for the displayed period of time.

With the corresponding toolbar buttons or the context menu (right-click) you can change the update rate, specify the type of the graph, and clear it.

Statistics

This pane shows various statistics on the work of Proxifier: the number of connections processed by the program (active, failed, total), the quantity of sent and received bytes, and the time Proxifier has been working. With the corresponding toolbar buttons or the context menu (right-click) you can copy the statistics to the clipboard or reset all counters.

Output

Here Proxifier outputs (logs) all message in real time. Each entry can contain the following information:

- Time/date in the following format [MM.DD HH:MM:SS].
- Application name with optional x64 mark and process ID.
- Target (hostname or IPv4/IPv6 address).
- Event description (e.g. connection opened/closed, resolve, error, etc.)
- Additional information like connection statistics or **error code**.

You can change verbosity of the output at **Log->Output Level** menu.

Three levels are available:

- **Error only** — errors and program critical messages only.
- **Normal** — errors and connection related messages (open/close). Recommended for the majority of cases.
- **Verbose** — outputs all messages. This includes **rule processing**, **DNS requests** and others. Can be useful for debugging purposes.

It is possible to write the output into a log-file with the **Log->Log Level** menu.

Miscellaneous

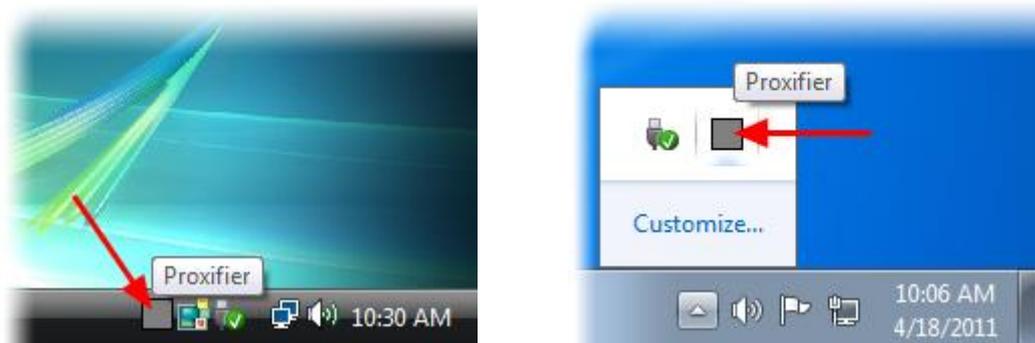
Proxifier can be hidden to the System Tray when the main window is closed (**View->Icon in the System Tray**).

At the bottom of the main window there is a special information area called the Status Bar. Here you can see the number of active connections, transfer rates and DNS status.

Proxifier supports various visual styles. You can change the style at **View->Application Look**.

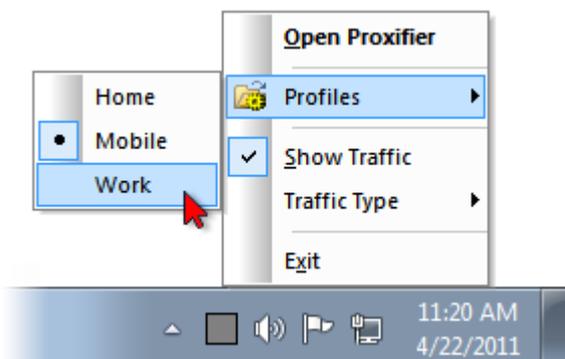
System Tray Icon

To add the Proxifier icon to the System Tray, enable the **Icon in the System Tray** item in the **View** menu. In this mode Proxifier will continue working even when the main window is closed. On Windows 7 the Proxifier icon can be hidden. Click the arrow-like button to access it. (You can drag-and-drop the icon to the System Tray to make it always visible).



To maximize the main window of the program, double-click the icon with the left mouse button or select the **Open Proxifier** command from the context menu. To close Proxifier in this mode either use the **Exit** context menu command or the **Exit** command of the **File** menu in the main window.

With the context menu you can easily navigate and switch profiles.



(SysTrayIconProfiles.png)

By default the icon shows the traffic. In fact it is a minimized copy of the Traffic pane. With the **Show Traffic** option of the context menu you can switch to the static icon and back.



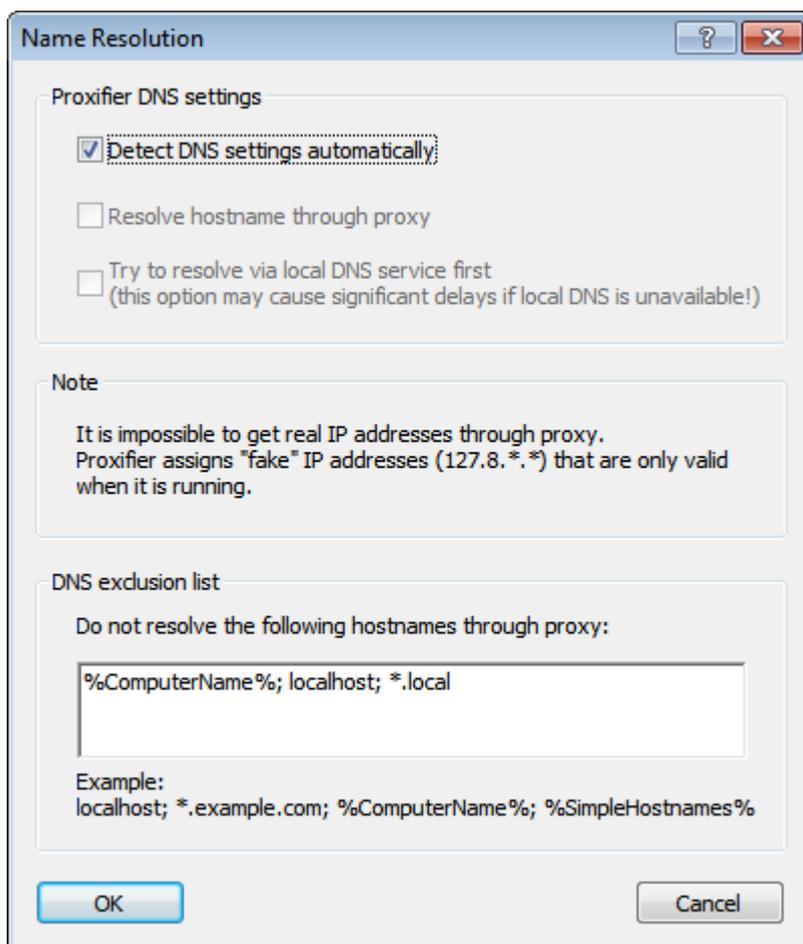
You can also do the same with the **Show Traffic on the Tray Icon** toggle in the **View** menu of the main program window.

Using the **Traffic Type** submenu, you can specify the graph type to be displayed.

Name Resolution Through Proxy

Proxifier can resolve hostnames through a **proxy server**. This feature is useful when a DNS server is not available or restricted. Generally speaking, it is not recommended to use this feature in all other cases as it has some limitations versus the normal way of resolving. For example, it is impossible to get a real IP address through a **proxy** so Proxifier has to assign placeholder (fake) IP addresses like 127.8.*.* which are only valid within the local computer. **Proxification rules** based on IP addresses will also not work in this case.

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



By default the **Detect DNS settings automatically** mode is enabled. In this case, Proxifier continuously tracks the network condition and if system DNS is unavailable Proxifier automatically enables the **Resolve hostnames through proxy** option.

You can disable automatic mode and enable/disable this option manually.

When Proxifier changes DNS mode automatically the following message is output: *(Automatic DNS mode detection) Local DNS service is available/unavailable. Name Resolution through proxy is disabled/enabled.* The current DNS mode is also indicated at the **Status Bar** of the main window.

It is also possible to enable a combined approach with the **Try to resolve via local DNS service first** option. In this mode Proxifier will try to resolve the name with system facilities first. If this attempt fails the name is resolved through a **proxy**

server. Use this approach very carefully as it can result in significant delays, for example, if a non-existent hostname is requested!

DNS exclusion list contains the names that should not be resolved through **proxy**. If a hostname matches an entry of the list, the name is resolved by system facilities.

You can use wildcards (masks) where “?” matches any symbol and “*” matches any substring.

%ComputerName% constant is automatically swapped with the local computer name during the processing.

%SimpleHostnames% constant defines all names that do not contain a domain/subdomain (i.e. there are no dot-separated parts). Usually such hostnames are used with a local network so it makes no sense to resolve them through a **proxy**.

Proxifier will output DNS requests if **Verbose** output mode is enabled (**View->Output Level->Verbose**), which can be useful when investigating DNS related problems.

Name resolving settings are stored in Proxifier **profiles**. So you can save/load them like the other settings.

Proxy Chains

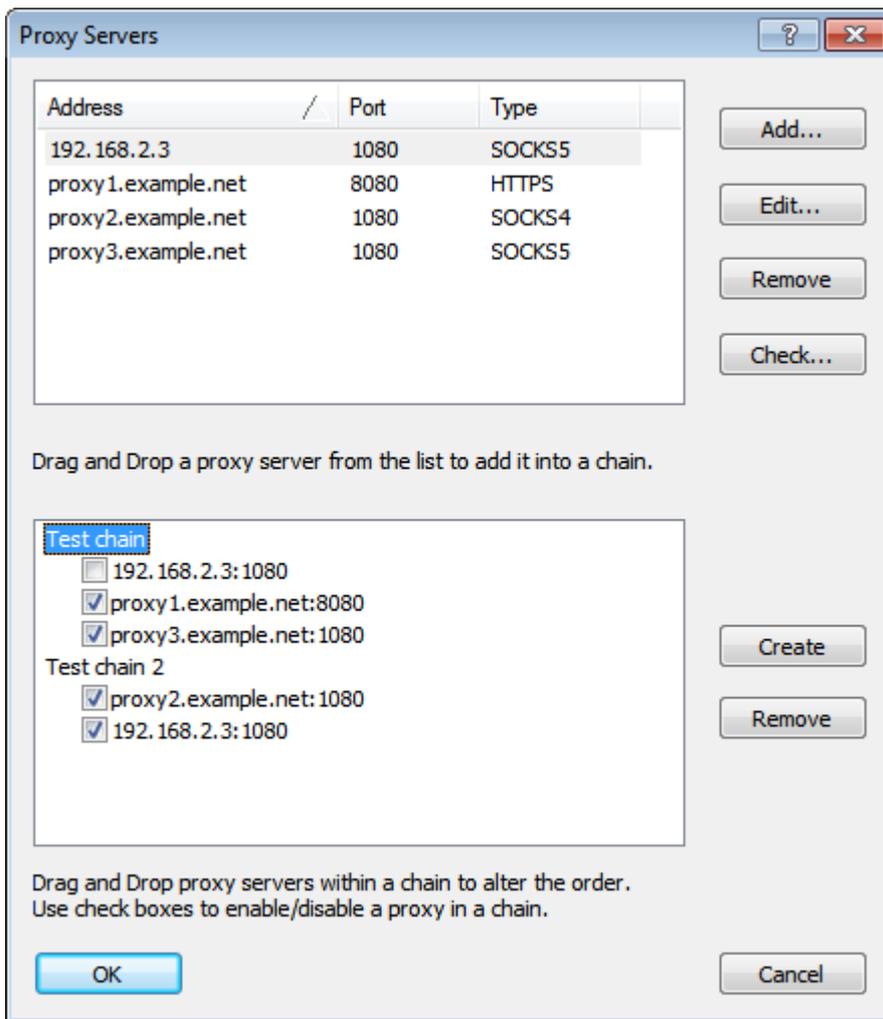
With Proxifier you can work through a chain of **proxy servers**. Connecting to a remote host will be performed sequentially from one proxy server to another.

This mode can be useful when a remote host is only accessible through multiple proxies or when Proxifier is used to ensure a high level of anonymity.

When working through a proxy chain, keep in mind the following:

- A chain can contain proxy servers of **different types**: SOCKS v4, SOCKS v5, HTTPS. If you use HTTP proxy it must be the last one in the chain.
- 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 broken at one proxy, the entire connection to the remote host is lost.

To create a chain of proxy servers, click **Proxy Settings** in the **Profile** menu and **add two or more proxies**. If the proxy chains area is not visible click the **Proxy Chains...** button and then click **Create** to create an empty chain. Now you can populate this chain with proxy servers from the list by drag-and-drop operation.



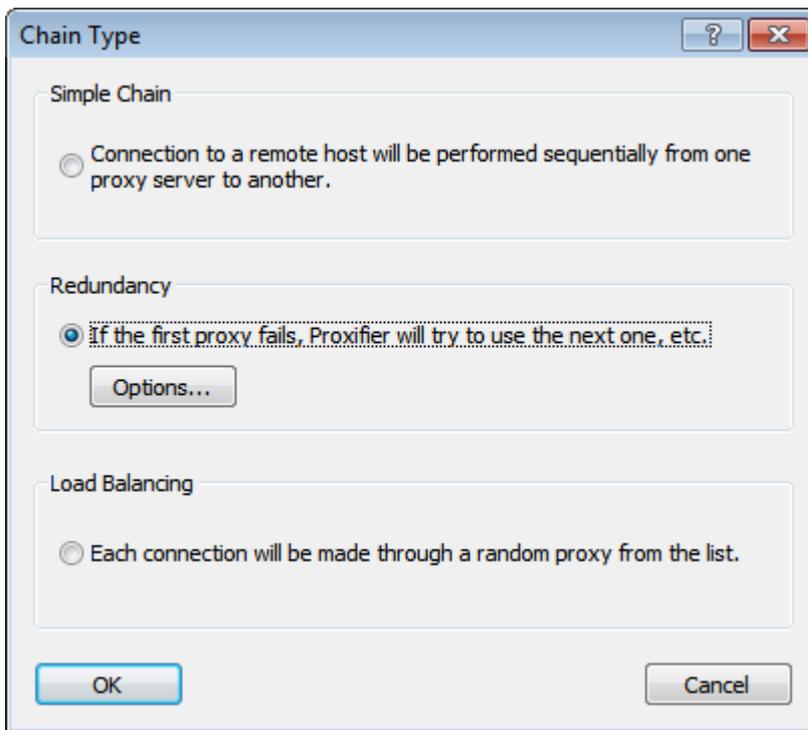
Connections between proxy servers will be established in the order they are displayed in the list (from top to bottom). You can change the order using the drag-and-drop operation on proxies within the chain. Uncheck a proxy to disable it.

To rename a chain left-click its label. Use the **Remove** button to remove a selected chain.

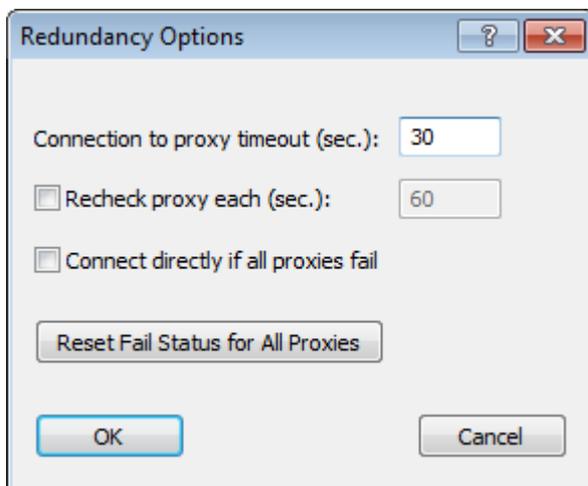
If a chain contains no proxies the connection will be made **directly**.

Proxy Server Redundancy

Redundancy can be useful when you need to provide proxy server failover or load balancing. To enable this feature, you need to create a **proxy chain** and set chain type to **Redundancy** or **Load Balancing**.



Options... button allows you to configure failover options.



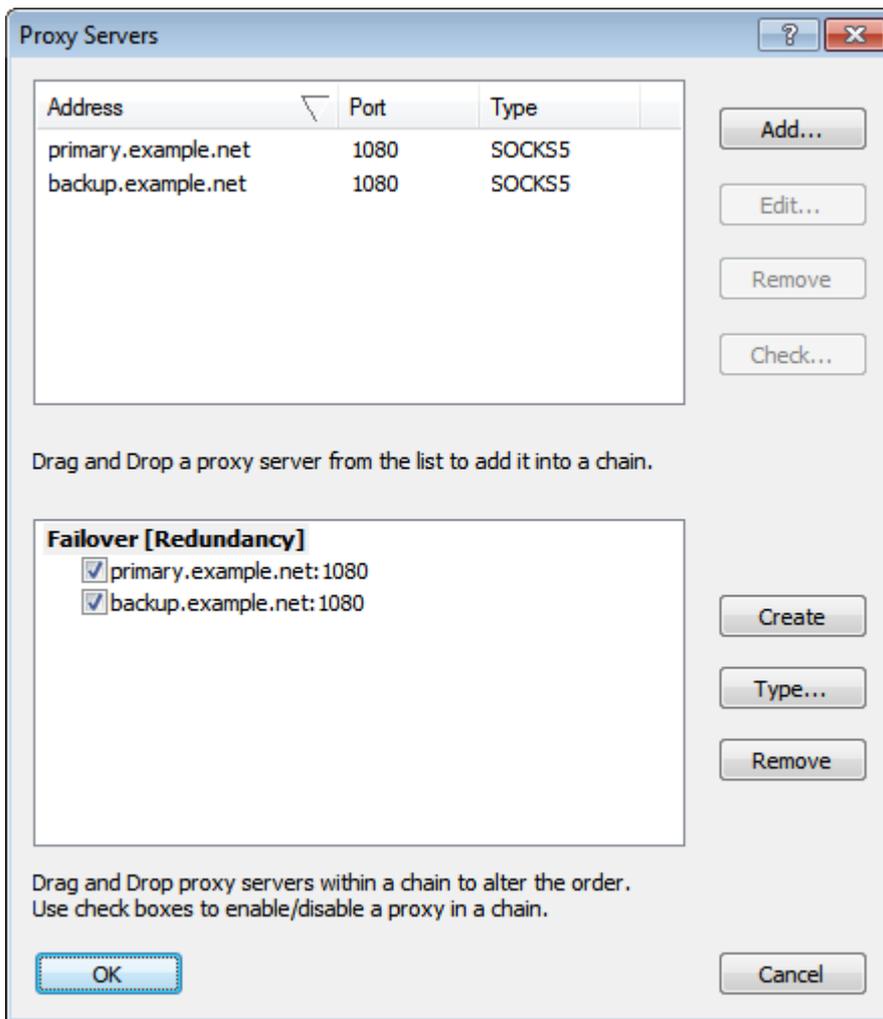
Here you can set **Connection to proxy timeout** in seconds and make Proxifier to **Connect directly if all proxies fail**.

If timeout is too big, client applications can consider that the target host is down and they can close connection before Proxifier will try the next proxy. If timeout is too short, Proxifier can mistakenly detect proxy failure.

You can make Proxifier to recheck failed proxies in background after a certain amount of time using **Recheck proxy each (sec.)** option.

Failed proxy servers are marked as *[failed]* at the proxy list. The fail status is not saved through Proxifier restart. You can **Reset Fail Status for All Proxies** thus Proxifier will try to connect the proxies all over again.

A redundancy proxy chain can look like this.



You can use checkboxes to enable/disable particular proxies in the chain. This option has nothing to do with the failure status. If a proxy is unchecked, Proxifier will simply ignore it. On the other hand, a checked proxy can be marked as *[failed]* and ignored.

If the first proxy in such chain fails, Proxifier will mark it as failed and it will try the next one. You will be provided with detailed messages that will render the status of the process. The entire process is completely transparent for the client application. Proxifier can try several proxies without losing the initial connection request from the application.

Here is a typical session for failover procedure:

```
[02.01 11:18:37] iexplore.exe (2972) - proxifier.com:80 matching Default rule : using Failover proxy chain
[02.01 11:18:46] (Redundancy Chain) Failover - Could not connect to proxy primary.example.net:1080 - connection timeout (10 sec)
[02.01 11:18:46] (Redundancy Chain) Failover - New active proxy is backup.example.net:1080
[02.01 11:18:46] (Redundancy Chain) Failover - Trying next proxy.
[02.01 11:18:47] iexplore.exe (2972) - proxifier.com:80 open through Failover proxy chain
```

HTTP Proxy Support

(This topic is about HTTP proxy servers. Please do not confuse this with **HTTPS**).

It is a common misconception to confuse HTTP proxy and HTTPS proxy. HTTP proxy servers can process HTTP connections (port 80). They can also support HTTPS connections (SSL) but usually such connections are only allowed on port 443 (the standard port for HTTPS). For example this is the default configuration for Squid and Microsoft ISA proxy servers. If an HTTP proxy allows HTTPS connections on arbitrary ports, it can be called HTTPS proxy server (also called CONNECT or SSL proxy). In this case it can be used for generic TCP connections like SOCKS v4/5 proxy.

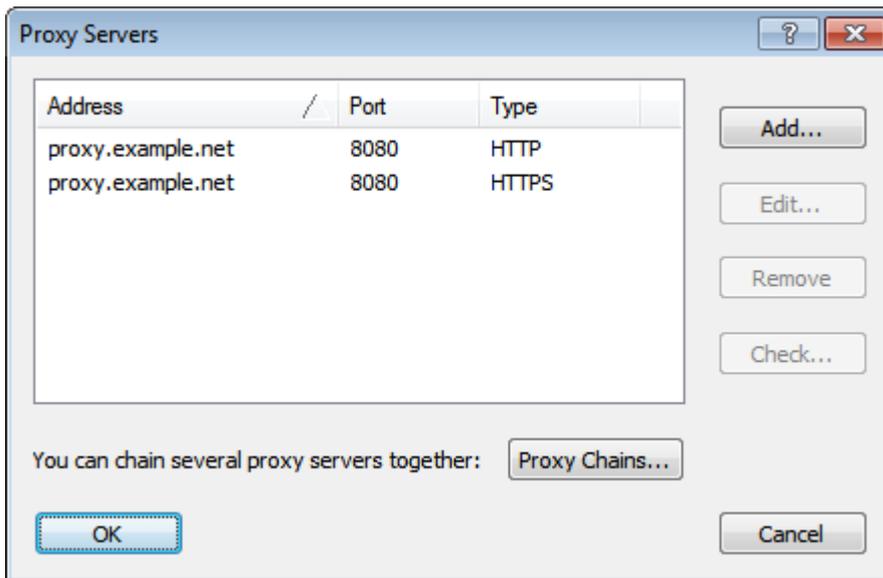
Proxifier can work with HTTP proxy servers that do not support HTTPS on arbitrary ports. Due to the technical limitation of this protocol it is only possible to process HTTP connections with such proxy servers. This means that you must configure the **Proxification Rules** accordingly.

You can enable HTTP proxy support at **Profile->Advanced->HTTP Proxy Servers...** After that you will be able to **add HTTP proxy server** just like any other type of proxies. Once HTTP proxy server is added, make sure that you properly set the **Proxification Rules**. If you want to process HTTPS connections through this proxy also, you should add this proxy separately as HTTPS.

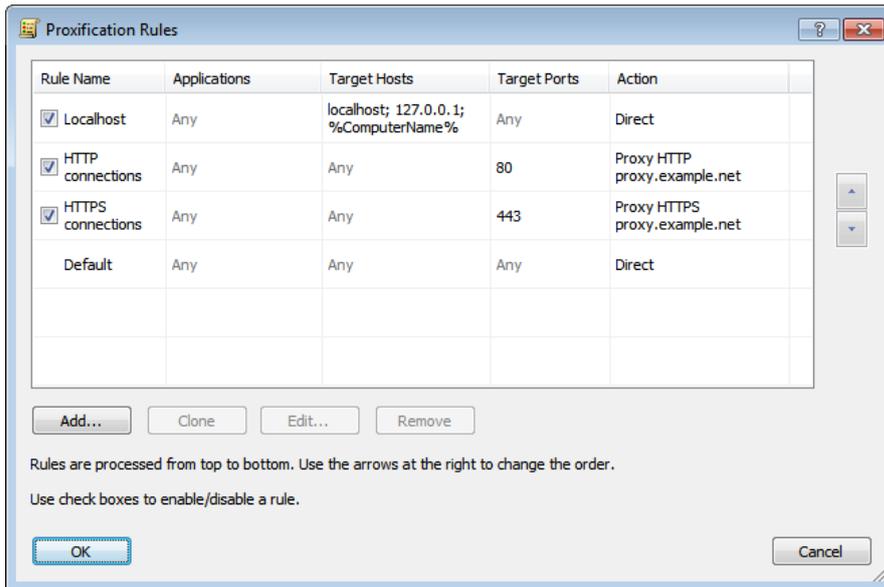
Suppose *proxy.example.net:8080* is a usual HTTP proxy and supports HTTP on port 80 and HTTPS on port 443 and we want to configure Proxifier to process HTTP/HTTPS connections (web browsing) through it.

The following images illustrate the correct setup.

Proxy Settings:



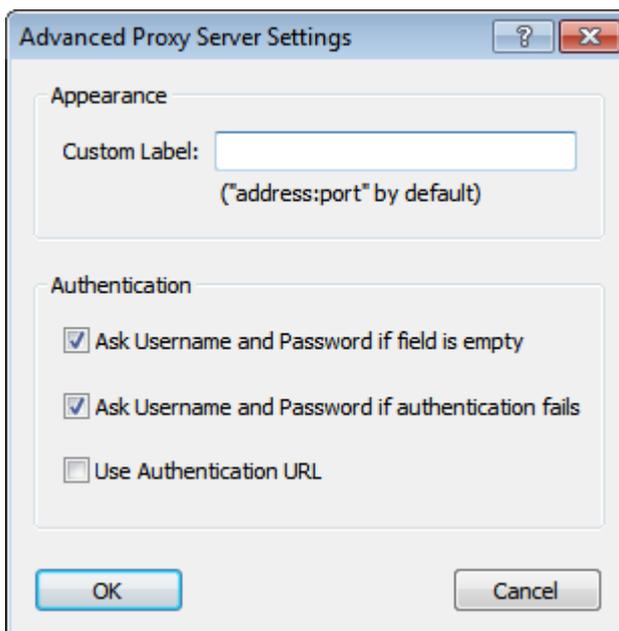
Proxification Rules:



You can check HTTP proxy servers with the [Proxy Checker](#) tool.

Advanced Proxy Server Settings

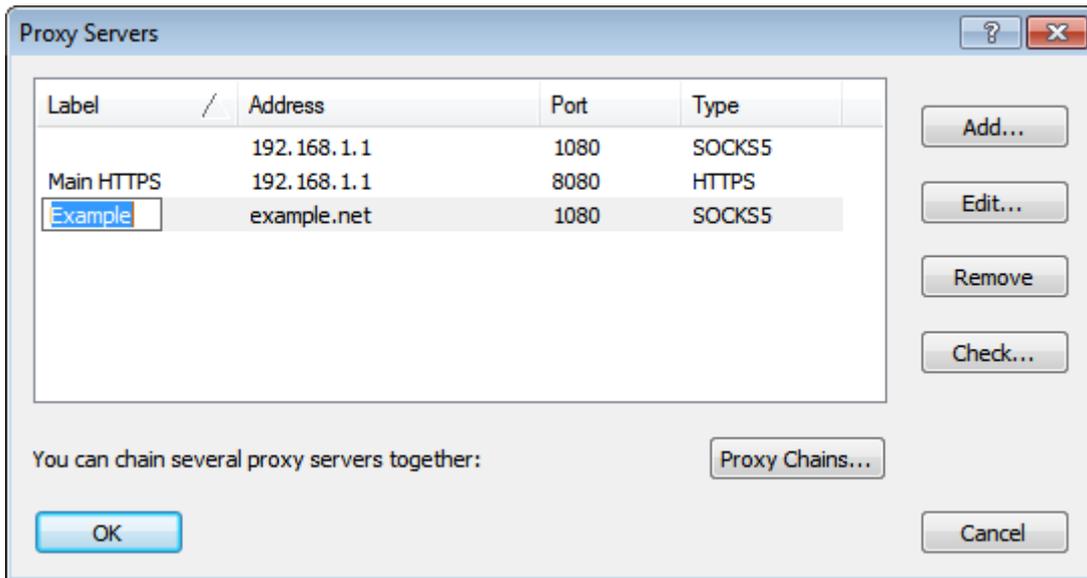
To access advanced settings of a proxy server, click **Advanced...** button at the [Proxy Server](#) dialog of Proxifier.



Custom Label

You can define a custom label (short name) for the proxy server. Proxifier will use this name instead of proxy address in all parts of the program (rules, logs, etc). This option can be convenient when you have multiple proxy servers with the same or similar addresses.

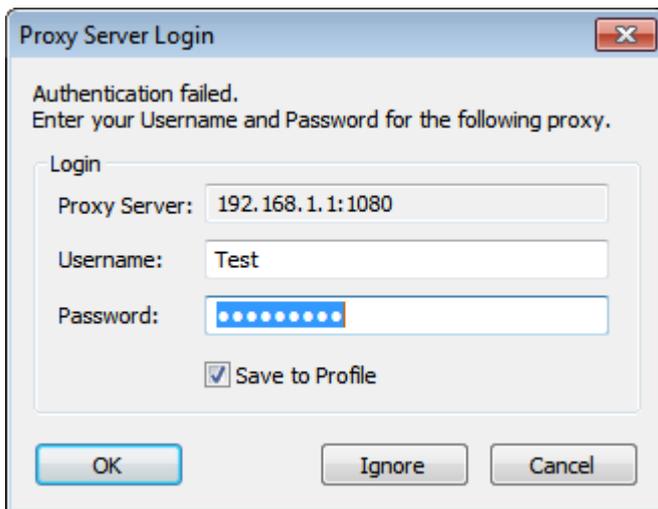
If at least one of proxy servers has a label, Proxifier will display a new *Label* column at the **proxy list**. You can edit labels right there.



Authentication

Proxifier can interactively ask the user for proxy server login and password if **one of these fields is empty** or **authentication fails**.

When a condition specified in one of these options is met, Proxifier displays the following form.



It is possible to specify and/or correct login details, **Cancel** or permanently **Ignore** (within the current Proxifier session) this message so it will not be displayed again and authentication will silently fail each time.

If **Save to Profile** option is not enabled, new login details will be used during the current Proxifier session only. No changes will be saved on disk to **profile** in this case.

When this popup form is active, all connections are put on hold. Proxifier will continue processing when authentication succeeds. The entire process is completely transparent for client applications.

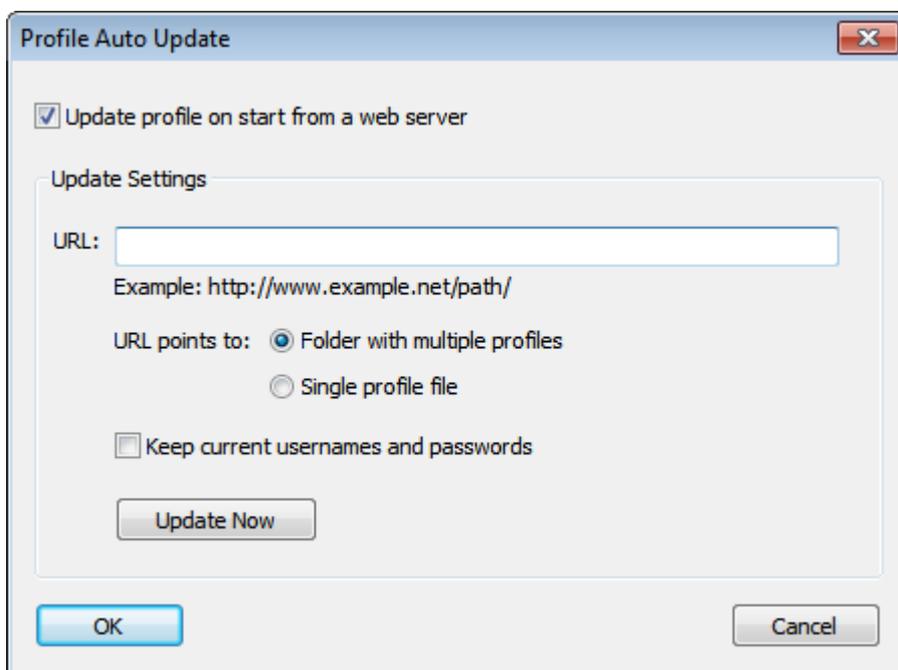
Authentication URL

If this mode is enabled, you can specify Authentication URL instead of username/password in the **main proxy settings**. Proxifier will use this URL to be authorized on the proxy server.

This option can work only with specific proxy servers like Blue Coat. Additional configuration is required on the server side.

Profile Auto Update

Proxifier can update profile automatically on start. To enable this feature, please go to **File->Profile Auto Update...** and check **Update profile on start from a web server**.



Here you can specify a **URL** that will be used for update. It should start either with *http://* or *https://*

HTTP Redirects are supported.

Update Now button starts the update immediately. When the update is working, **Stop** button becomes available to stop the process.

There are two update modes available:

Folder with multiple profiles. The **URL** points to a folder. Proxifier will search for the currently used profile in this folder. Update is performed if there is a profile file with the exact name.

Single profile file. The **URL** points to a single file. Proxifier performs automatic update only if the file name matches current profile name. **Update Now** button updates the profile regardless the name.

Keep current usernames and passwords option allows keeping login information during the update. Proxifier checks for the same proxy servers in the new profile. If the same proxy is found – login information for this proxy gets copied to the updated profile.

A typical auto update session looks like the following:

(**Log->Output Level->Verbose** enabled).

[12.13 15:10:29] (Profile Auto Update) - Update started.

[12.13 15:10:29] (Profile Auto Update) - New profile has been downloaded.

[12.13 15:10:29] (Profile Auto Update) - Profile Work has been successfully updated from the remote server.

[12.13 15:10:29] (Profile Auto Update) - Saving login details for proxy 192.168.1.1:1080

Direct Connections

Proxifier can process connections without a proxy server. You can enable this with **Profile->Advanced->Handle Direct Connections** option. If this mode is enabled Proxifier will handle the connections that match **Proxification Rules** with action set to “Direct.” The connection will be added to the connection list, the traffic will be counted, etc.

This working mode does not differ in any way from working through a proxy server, except that the connection is established directly from the local computer to the remote one. In this mode Proxifier can be used as a tool for monitoring network connections and traffic. You can use it to log network activity and make and analyze traffic dumps of network applications.

Log Files

Proxifier can save its **output (log)** into a file. You can enable this feature on the **Log->Log to File** menu.

The following options are available:

- *Disabled* — do not write a log file.
- *Errors Only, Normal, Verbose* — write the output in the log file. The levels are the same as for **Output Level**.
- *Verbose and Traffic* — write verbose log into a file and save traffic into dump files.

You can set the log directory with the **Log->Log to File->Set Log Directory...** command. The messages are saved into a “Log.txt” file in this directory. Traffic dumps (if enabled) are saved into a “Traffic” subdirectory as files with “.dmp” extension. For each connection Proxifier creates two files — one for incoming and one for outgoing traffic. The name consists of application name, “TO” or “FROM” mark, date (year, month, day) and time (hour, minute, millisecond).

For example, a dump of an HTTP connection can look like the following:

```
“iexplore.exe (4472) TO www.google.com_80 AT 20110424 131552072.dmp”
```

```
“iexplore.exe (4472) FROM www.google.com_80 AT 20110424 131552359.dmp”
```

WARNING!

Saving traffic on fast networks may require a lot of space on the hard disk. Proxifier checks the Traffic directory on each start and warns you if there are more than 1000 files or the total size is more than 500 Mb.

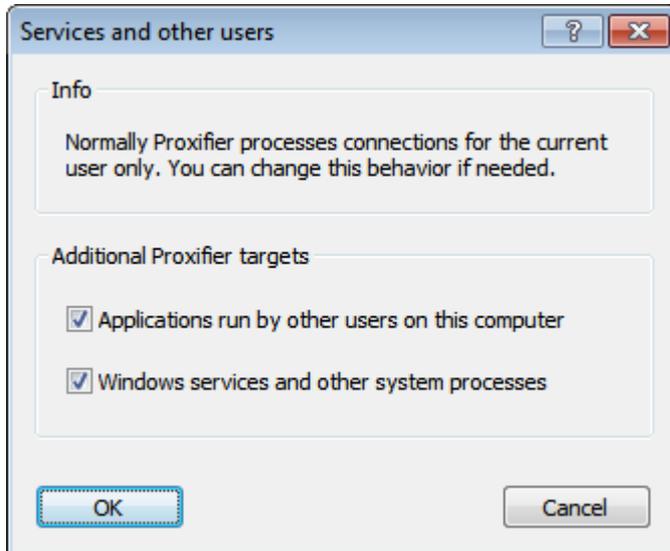
Services and Other Users

Standard Edition only

Starting from version 3 Proxifier can process applications run by other users and Windows Services like Windows Update.

Both features are disabled by default. You can enable them at

Profile->Advanced->Services and Other Users...



NOTE: These settings are recommended for advanced users only!

Connection Loop Detection

Working with Proxifier you can get into a situation where a connection gets to an infinite loop. Such situations can cause serious stability problems. In the worst case, network access can be completely blocked.

This can happen when there is a local proxy server running on the system (e.g. tunneling software or antivirus).

Suppose the following scenario:

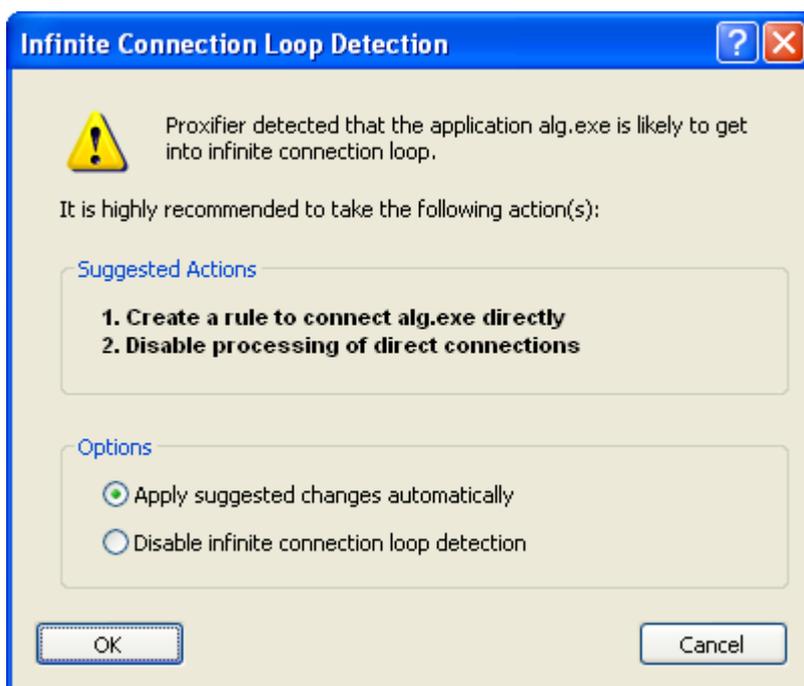
1. Application initiates a connection.
2. Proxifier captures it and redirects to the local proxy server.
3. Local proxy server forwards the connection to the Internet.
4. Proxifier captures this connection and redirects to the same proxy again.
5. Step 3 is repeated.

System will repeat steps 3 and 4 forever (while the system can still handle new connections).

You can easily prevent this problem with proper **Proxification Rules**. Basically, Proxifier should be configured to bypass connections made by local proxy and **Handle Direct Connections** options should be disabled.

Proxifier v3 also has a built-in mechanism to detect and prevent such dangerous situations. You can enable/disable this feature with **Profile->Advanced->Infinite Connection Loop Detection** option.

Using some adaptive logic Proxifier continuously monitors connections on the system. If an infinite connection loop is detected the following window appears and all new connections are automatically blocked until the user responds.



Proxifier will suggest one or two actions to prevent a connection loop from happening in the future. You can either apply the actions automatically or disable the loop detection logic. If you click **Cancel** or close the window nothing will be changed and the loop detection logic stays active. You are advised to take some action manually to address the problem; otherwise the logic will likely be triggered again soon.

It is recommended that you disable the **Infinite Connection Loop Detection** feature only in the case of false positive detections.

Proxifier Editions

(Information about Proxifier for Mac is available in a separate document).

There are two different editions of Proxifier for Windows:

- **Proxifier Standard Edition**
- **Proxifier Portable Edition**

The main goal of the **Portable Edition** is to help people who have no opportunity to install the software on a computer or deal with multiple computers and would like to save time on installation. The **Portable Edition** requires no installation and can be run from a USB stick. You can work from an Internet cafe or on a computer with guest access only.

Standard Edition is more suitable for users who have their own PCs at home, at work, or in a corporate environment.

A comparison chart of the main features is listed below.

Feature	Standard Edition v3	Portable Edition v3
Installation and System Requirements		
Install/Uninstall	Yes (Administrator rights are required)	No installation is required
Run from "Guest" account	Yes	Yes
Run from removable media (USB stick, card, etc)	No	Yes
Supported operating systems	Windows XP/Vista/7/8/10 Server 2003/2008/2012/2016 32/64-bit	Windows XP/Vista/7/8/10 Server 2003/2008/2012/2016 32/64-bit
Settings storage	File and System Registry	File
Proxy Servers		
Protocols	SOCKS v4(A); SOCKS v5; HTTPS	SOCKS v4(A); SOCKS v5; HTTPS
HTTP proxy	HTTP connections only	HTTP connections only
Authentication	Basic/NTLM	Basic/NTLM
Proxification		
User applications	All	Applications with graphical user interface only
Services	Yes	No
Other user sessions	Yes	No
Proxification mode	Auto/Manual	Auto
Proxification rules	Yes	Yes
Miscellaneous		
DNS through proxy server	Yes	Yes
Auto run on Windows startup	Yes	No
File log and traffic dump	Yes	Yes
Help system	Online/Help file	Online

Profiles of **Standard** and **Portable** editions are absolutely compatible. You can export a **profile** from the **Standard** version and load it into the **Portable** version and vice versa.

Run as Windows Service

Standard Edition only

You can run Proxifier as Windows Service with SrvAny tool from Microsoft.

<https://support.microsoft.com/en-us/help/137890/how-to-create-a-user-defined-service>

This allows you run Proxifier in the background when there is no active user logged on the system.

To configure Proxifier as a Windows Service, please do the following:

1. Register **Proxifier for All users on this computer** (enable this option at registration form) with a registration key. If you do not have a key – we can provide you with a test one.
2. Download <https://www.proxifier.com/distr/Service.zip> and unpack into the working folder of Proxifier (where Proxifier.exe is located).
3. Run InstallService.bat as administrator. This will create Proxifier service.

For the service mode, it is necessary to make sure that both options at **Profiles->Advanced->Services and Other Users** are enabled in Proxifier.

Configuration

Please note that Proxifier Service will be running under System account by default. It means that its configuration (**profile**) will be empty as the profiles are individual for each user account.

You can either configure the service to run under a user account that has Proxifier configured or enable system wide global Proxifier profile. To do this, just export a profile as "Default.ppx" (**File->Export Profile**) and place it to: "C:\Users\All Users\Application Data\Proxifier\" or its equivalent on your system. On Windows Server, the location is "C:\ProgramData\Proxifier\Default.ppx"

From this moment, Proxifier will use this profile-file for all users on the computer.

Log File

If you need to enable log file for Proxifier Service, please create the following entries in the system registry:

HKEY_USERS\S-1-5-18\Software\Initex\Proxifier\Settings

LogPath (REG_SZ) = path to the log file folder e.g. D:\Temp

LogLevelFile (REG_DWORD) = 3

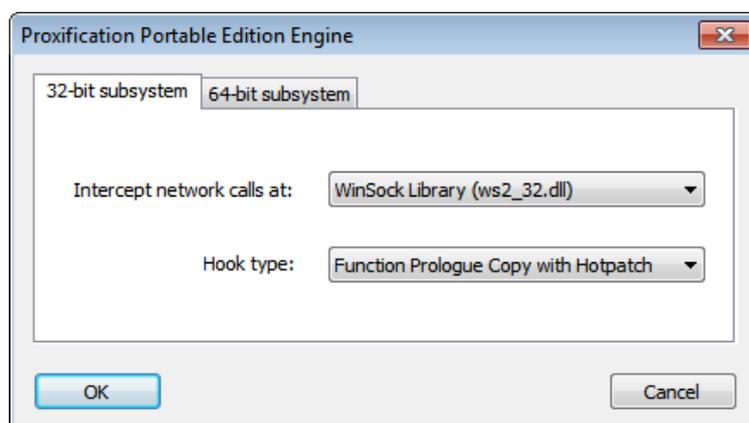
This will enable Proxifier file log at "D:\Temp" when Proxifier Service is running under System account. If you run it from another account please replace "S-1-5-18" in the registry path with an appropriate user SID.

Portable Network Engine

Portable Edition only

The Proxifier Portable Edition v3 features a completely new network engine. Along with better reliability and robustness, it provides support for 64-bit applications and significantly increases compatibility with third party software.

Some settings of the engine are configurable and can be accessed at:



Profile->Advanced->Proxification Engine... Proxifier menu.

Here you can choose the point in the network API stack where Proxifier intercepts network calls and the hook type to use.

The default settings should be OK for the vast majority of users. However on some systems the default settings can cause conflict with third party software (especially antivirus and firewall software).

In this case you can try to change engine configuration in order to bypass the conflict.

On 64-bit versions of Windows it is also possible to configure the 64-bit engine. The 32- and 64-bit subsystems and engines are completely isolated.

Proxy Checker

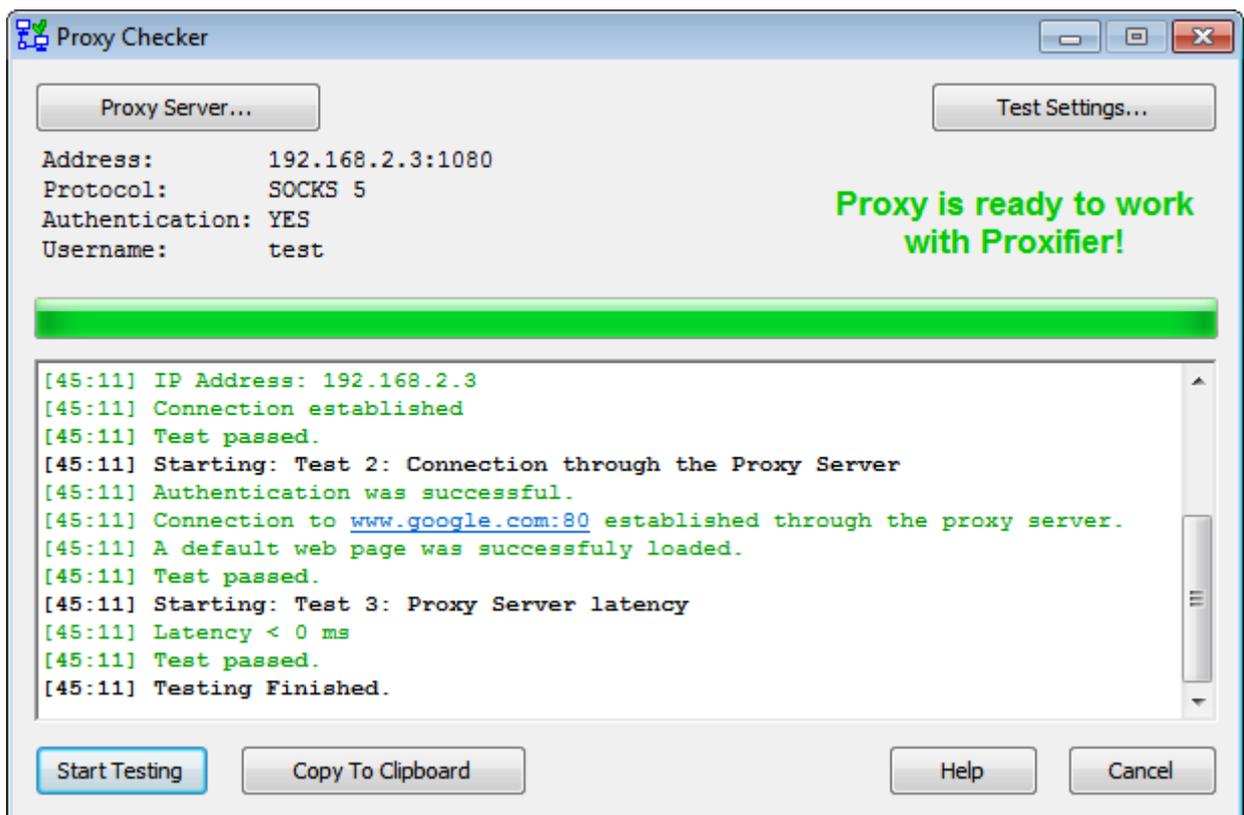
Proxy Checker tool is integrated into Proxifier, but it can be useful on its own. It allows you to test proxy servers and check whether they can work with Proxifier or not.

With Proxy Checker you can:

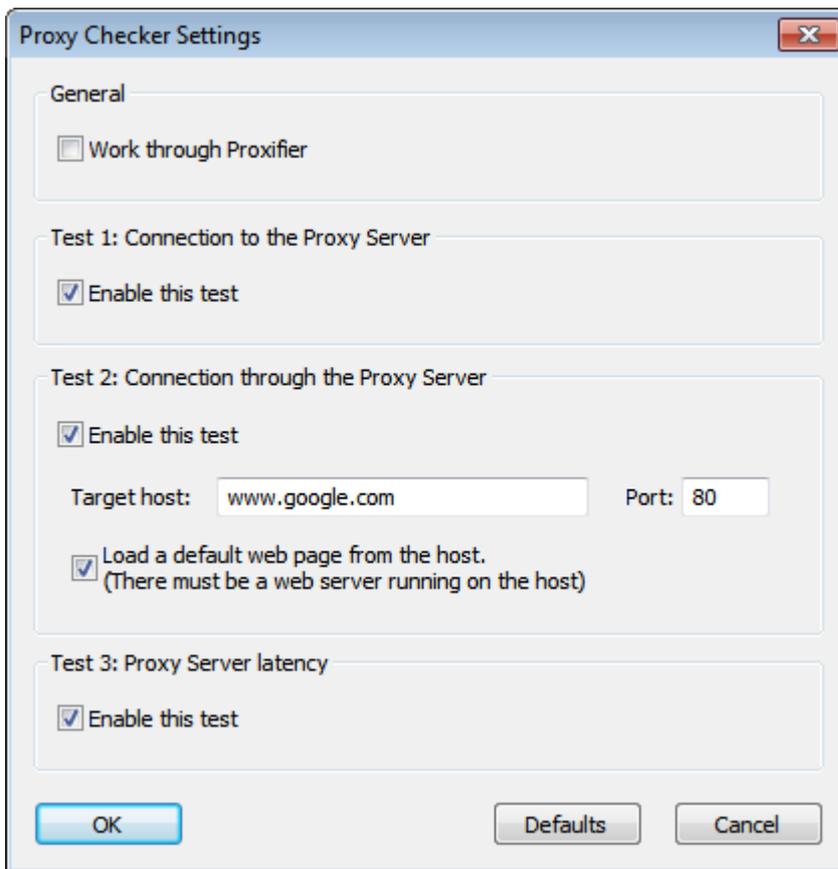
- Test SOCKS v4(A), SOCKS v5, HTTPS and HTTP proxy servers.
- Get an easy-to-understand report with recommendations that can help to solve a problem (if any).
- Measure proxy server response time (latency).

To check a proxy with Proxy Checker, click the “**Check**” button in **Proxy Settings** dialog. Alternatively you can run Proxy Checker manually in Proxifier with the toolbar button, **View->Proxy Checker...** or **Start->Programs->Proxifier->Proxy Checker** (Windows Start menu) and specify proxy details with the “**Proxy Server...**” button.

Use the “**Start Testing**” button to begin the test.



To adjust Proxy Checker settings click the “**Test Settings...**” button.



The following options are available:

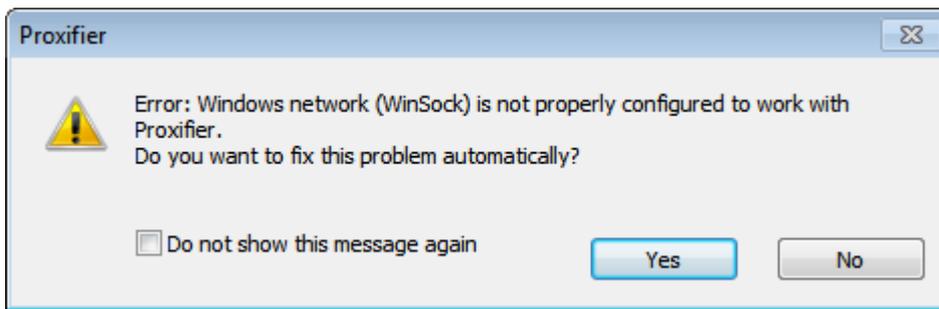
- *Work through Proxifier* — Proxy Checker will bypass Proxifier when this option is disabled. This is the default value and it should only be changed in a very special scenario (e.g. the target proxy is not directly accessible).
- *Target host* and *Port* — set the target host for the test connection.
- *Load a default web page from the host* — enable to test data transfer.
- You can enable/disable particular tests.

You may use and distribute Proxy Checker as a standalone application (ProxyChecker.exe). Proxy Checker is free for personal and noncommercial use.

Proxifier System Settings

Standard Edition only

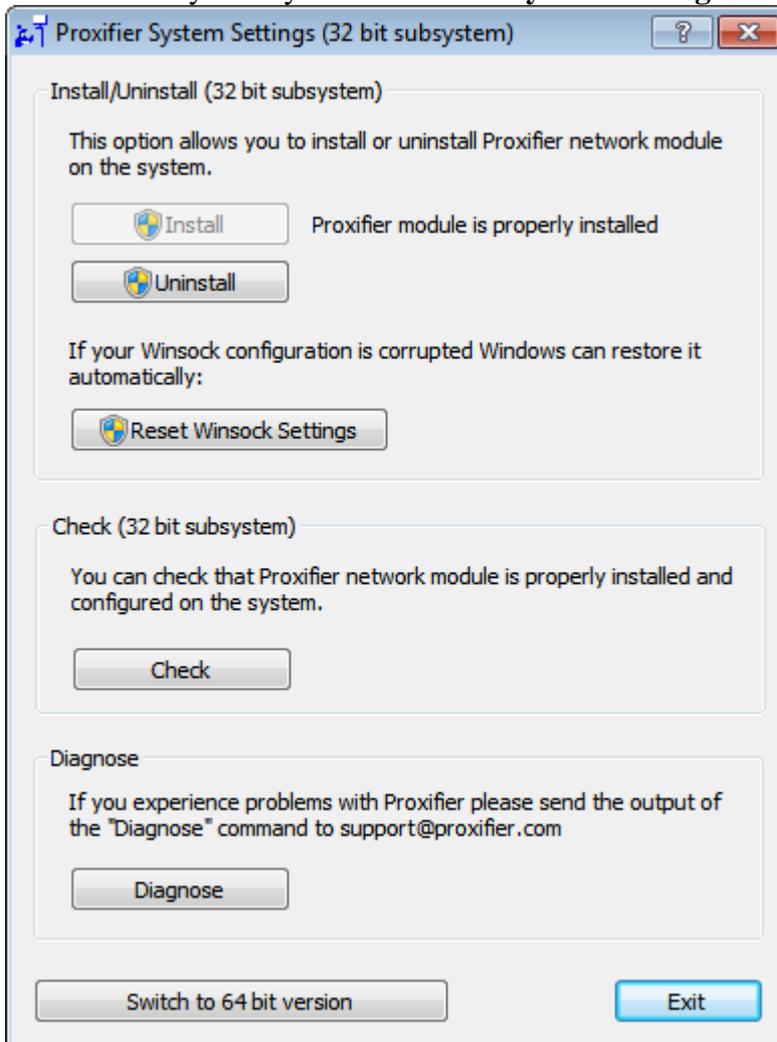
Proxifier Standard Edition uses Winsock Layered Service Provider (Winsock LSP) to capture TCP connections and Winsock Name Space Provider (Winsock NSP) to handle name resolution over proxy. Both providers have to be properly installed in the system. Normally this is done once automatically during Proxifier installation. Proxifier checks the configuration on each start. If a problem is detected you will be prompted to resolve it automatically. It is highly recommended to fix the problem before using Proxifier.



All Proxifier system settings are done with the **System Settings** tool (**Star->Programs->Proxifier->System Settings**). Technically the tool consists of the SysSettings32.exe and SysSettings64.exe programs for the 32- and 64-bit subsystems respectively.

Most commonly the cause of the problem is a third-party software that uses Winsock LSP and conflicts with Proxifier. We did our best to maximize Proxifier compatibility in v3, but, unfortunately, some conflicts may still exist.

In some cases you may need to run the **System Settings** tool manually.



Depending on the current state of the system settings you can **Install**, **Uninstall** and **Repair** the Proxifier module.

If your Winsock configuration is corrupted you can use the **Reset Winsock Settings** button. This will run a built-in Windows mechanism to address this problem (“netsh winsock reset” command).

The **Check** button will provide you with a brief report on the status of Proxifier subparts.

Finally, if you experience problems you can get a detailed report on your Winsock configuration with the **Diagnose** button. Please include this report if you contact support with system settings related problems.

On the 64 bit version of Windows you need to configure settings for both 32- and 64-bit subsystems. Use the **Switch to 64(32) bit version** button to switch to 64 subsystem and vice versa.

SysSettings32.exe and SysSettings64.exe can be used in command line (silent) mode. This option can be useful for custom made installation packages and unattended deployment.

Available parameters are:

silent-check — checks current status of system. Process exit code is zero if Proxifier settings are correct.

silent-install and *silent-uninstall* — install/uninstall Proxifier settings from the system. Process exit code is zero on success. Requires Administrator rights.

Network Error Codes

In the case of network errors (e.g. a connection to a proxy server fails) Proxifier outputs error code numbers. These are the standard Winsock error codes. To get the full list of the codes and their description please go to: <http://www.proxifier.com/docs/win-v3/errors.htm>

Order Proxifier

You can purchase the full version of Proxifier at our web site: <https://www.proxifier.com/buy/>

Registration benefits:

- Fully functional, unrestricted copy of the software.
- All future minor version UPDATES for FREE!
- Free technical support.

We provide a 30-day money back guarantee. If you are not completely satisfied with Proxifier, just let us know and you will receive a full refund promptly. Orders are delivered to your email instantly. Our ecommerce partner, Avangate, processes every order using only the absolute safest SSL encryption.

Please contact sales@proxifier.com with order related questions.

Trial Version

The trial (unregistered) version of Proxifier has the following limitations:

- It will work for only 31 days after installation.
- On start, Proxifier displays the information window.

These are the only differences between the trial and registered version.

When you purchase the full version of Proxifier, you will receive a registration key (serial number) which will remove all limitations.

Technical Support

Please contact our support team using the following e-mail:

support@proxifier.com

Before you contact us, please do the following:

- Read through the document: it may already contain an answer to your question.
- Ensure that you are using the latest version of Proxifier available at <http://www.proxifier.com>

If you contact Technical Support, please provide as much information as possible about the problem, including:

- Proxifier version and edition (**Help->About**) (e.g. “Proxifier Portable Edition v1.5”).
- Windows version including service pack and edition (e.g. Windows Vista Ultimate 64-bit Edition SP1.)
- Your Network Configuration (your IP address*, proxy server IP and Port, proxy server protocol (e.g. SOCKS), proxy server name (e.g. Squid or Microsoft ISA).
- The description of your problem (be as detailed and comprehensive as possible), exact steps to reproduce the problem.
- Proxifier registration information (if you are a registered user) — registered users get higher support priority.

* We need the first byte of an IP address only. So you can specify IP addresses like 10.x.x.x, 192.x.x.x and etc.

End-User License Agreement

You can view End-User License Agreement for Proxifier here:

<http://www.proxifier.com/docs/win-v3/eula.htm>