Proxifier for Mac v2

User Manual

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.

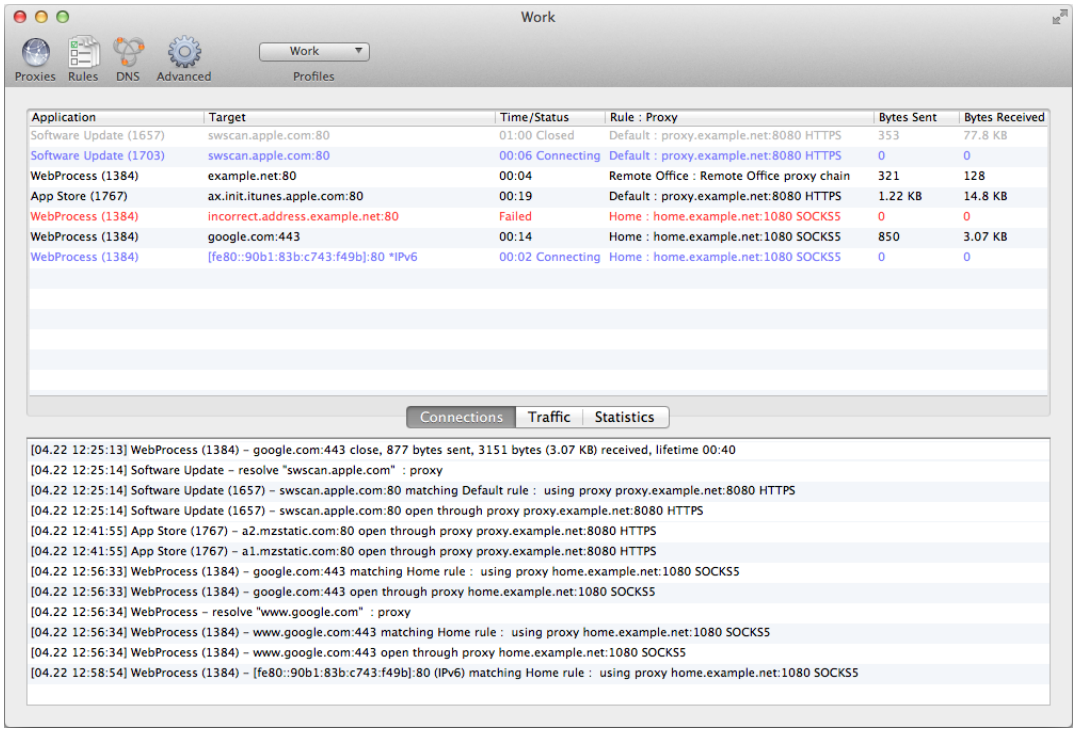
Specifications:

- Proxy protocols: SOCKS v4, SOCKS v4A, SOCKS v5, HTTPS and HTTP (HTTP connections only).
- Authentication: SOCKS5 Username/Password Authentication (RFC 1929), HTTP Basic.
- Full IPv6 support
- Full 64 bit applications and systems support.
- Profile password encryption up to AES 256 bit.
- macOS 10.8-10.13

What's New in Version 2

Improved UI

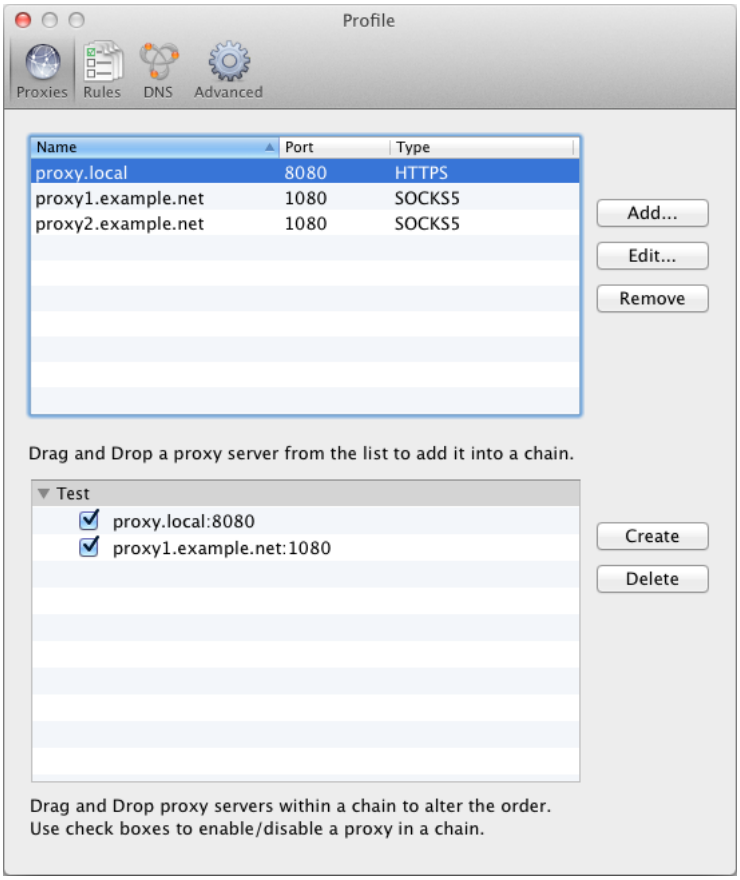
The new version features a significantly improved user interface. The connection list provides much more detailed information about the connections including: selected proxy server, matched rule, connection status with color indication, user name and process ID. All additional information is displayed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



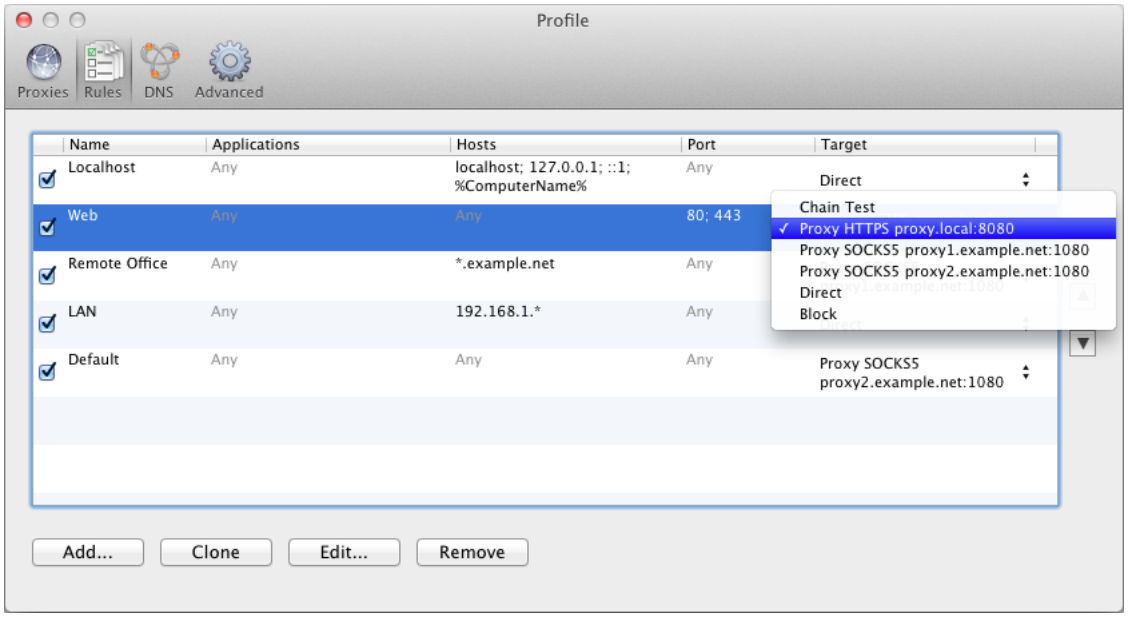
Proxifier log messages are now more detailed as well. They include all new parameters listed in the above paragraph. Additionally a number of new messages were introduced. Now Proxifier can be configured to output DNS requests, rules processing messages and more. Verbosity of the output can be changed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

Brand New Concept for Proxy Settings and Rules

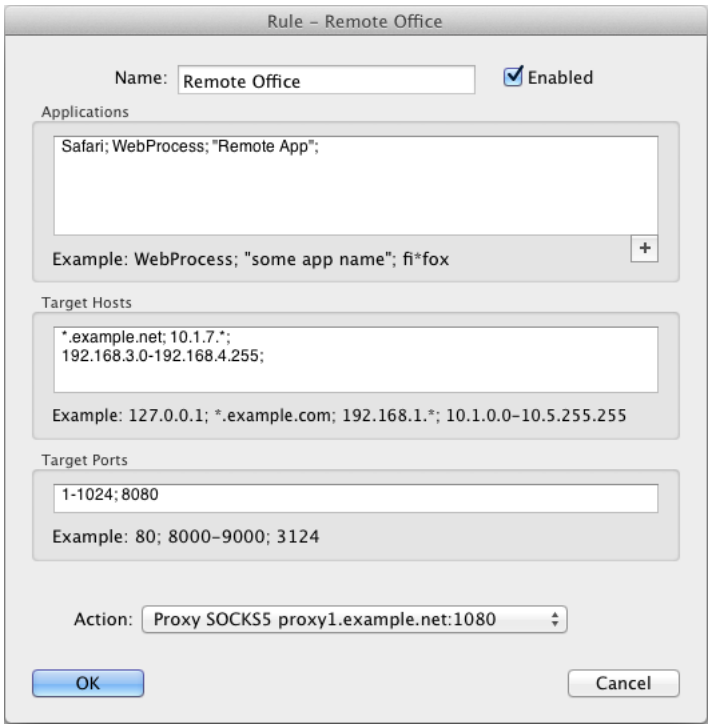
The core of Proxifier configuration has been significantly redesigned and improved. Now you can specify independent multiple proxy servers in **Profile->Proxy Settings...** It is also possible to create multiple proxy chains and manipulate them via the new UI.



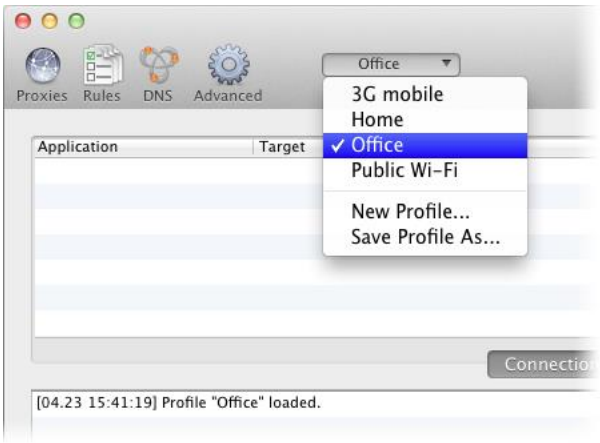
The new version allows you to assign different proxies/chains for different rules **Profile->Proxification Rules...** Thus each rule has an individual action that tells Proxifier to process the connections through a proxy or chain, to block the connection or to open it directly.



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

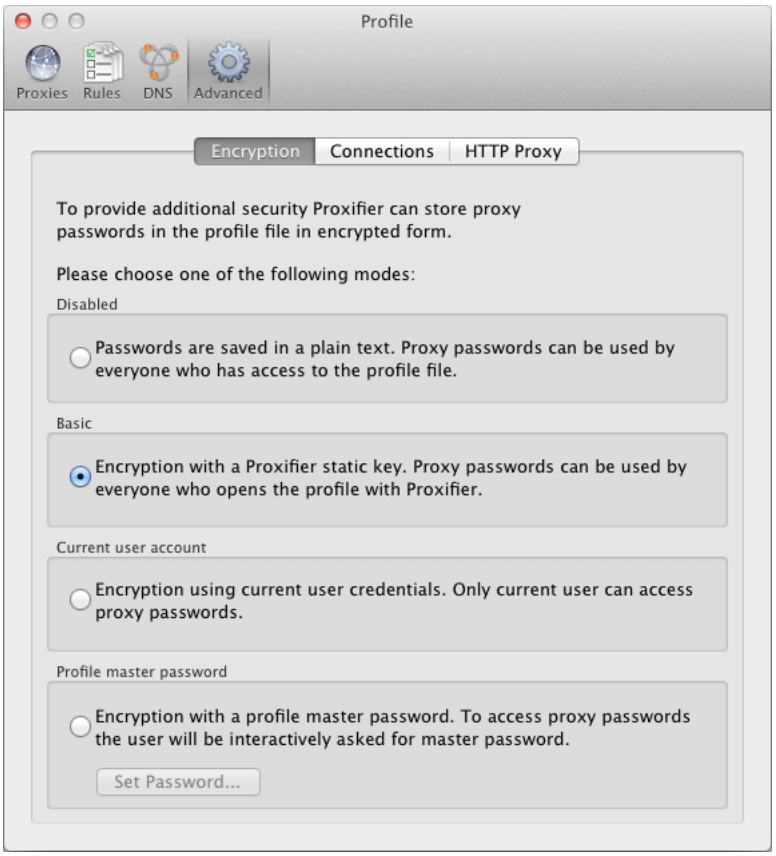


Profiles



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->Encryption...**
- XML format of profile files (*.ppx).



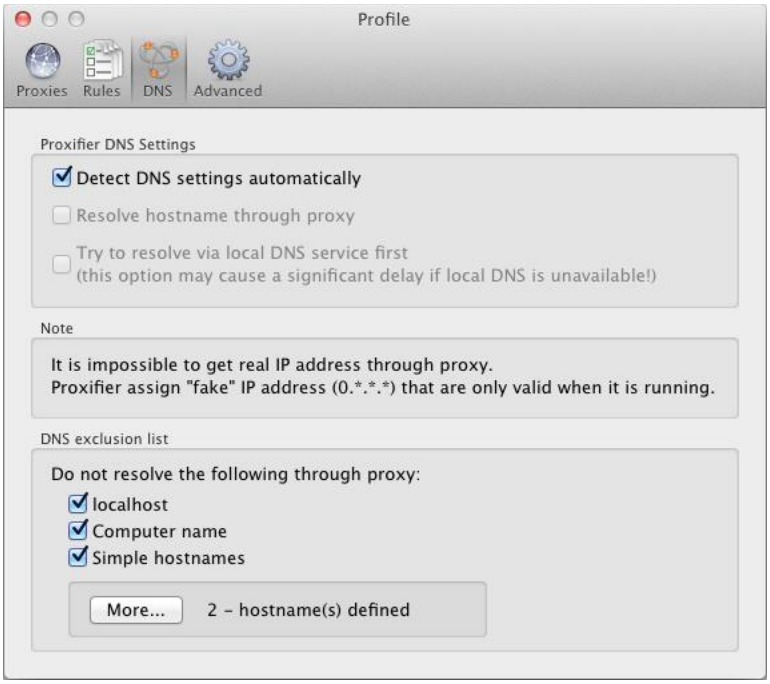
Proxifier Profiles of Windows and Mac versions are compatible so you can easily move configuration between the platforms.

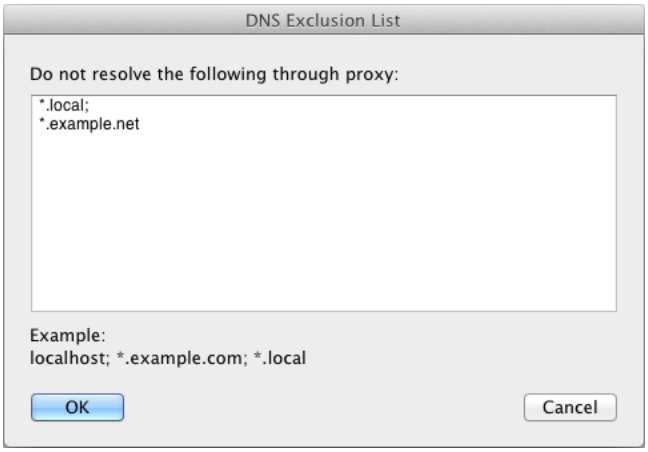
New Network Engine

The network engine of Proxifier for Mac has been completely rewritten. It improves the overall performance of the program, provides full IPv6 support and better hostname processing. No installation is needed anymore. You can simply unpack Proxifier to any folder on your Mac and you are all set.
The new version features a number of other improvements. They significant improve user experience.

DNS over Proxy Improvements

Proxifier can now automatically detect DNS settings and select an appropriate mode that matches the current network environment. I.e. it will resolve hostname through proxy if local DNS is unavailable and vice versa.





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.

Proxifier Migration Notes

Proxifier v2 does not import old settings automatically. To convert an old configuration file from Proxifier v1 (*.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.

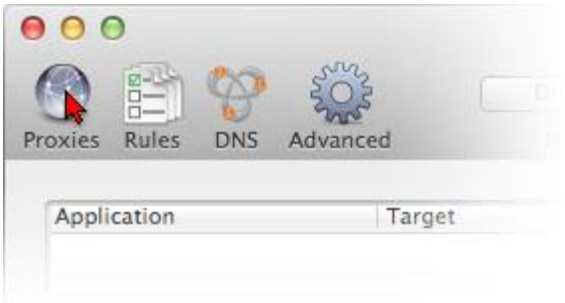
Quick Start

Copy Proxifier.app to Applications folder and launch Proxifier.

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 **Handle Direct Connections** option under **Profile->Advanced**. It can be useful to troubleshoot problems and utilize some features of Proxifier like traffic dumps, bandwidth and connection monitor, etc.

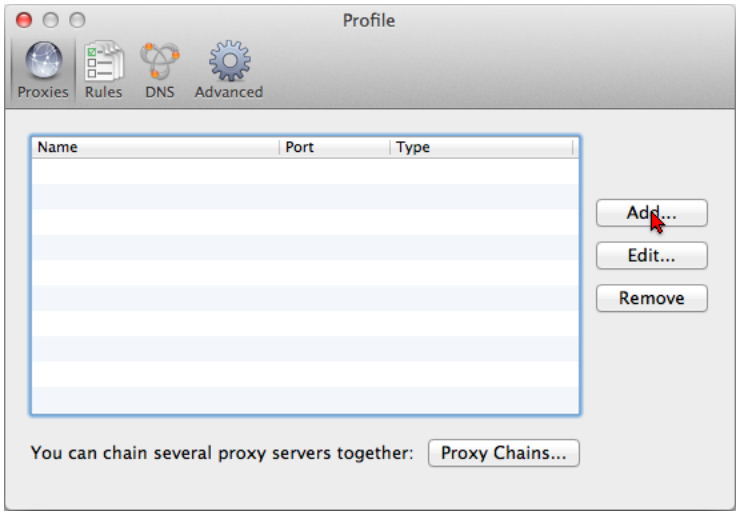
To make the connections work through a proxy server or a chain of proxy servers, you must first define a proxy server in Proxifier. Click **Proxy Servers...** in the **Profile** menu or click on the icon located on the toolbar:



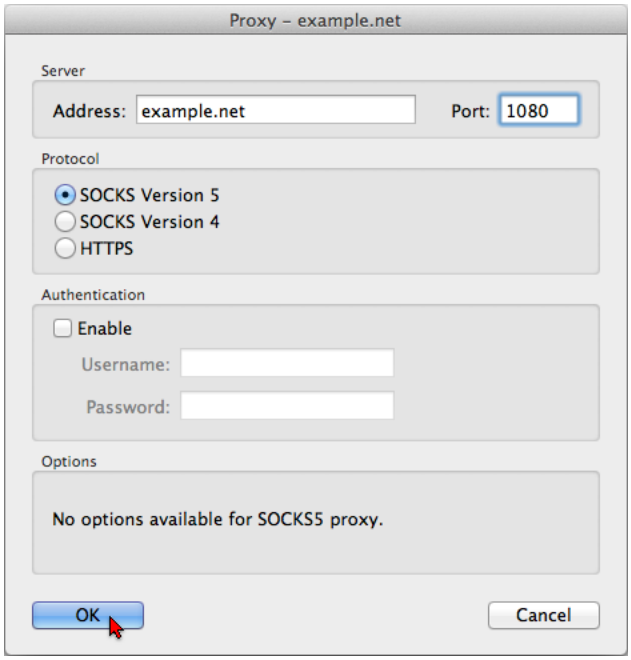
WARNING!

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:

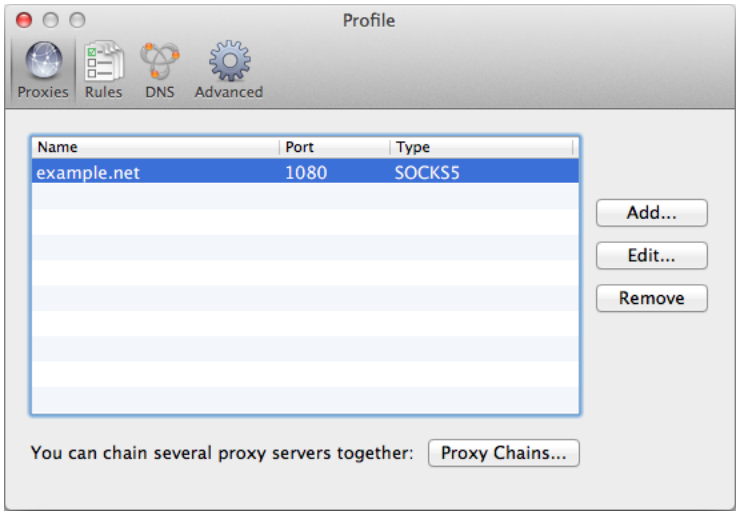


Fill in the form specifying the details of the **proxy server** (address, port, protocol, etc.) that you want to add and click **OK**:



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:



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**.

Proxy Server Settings

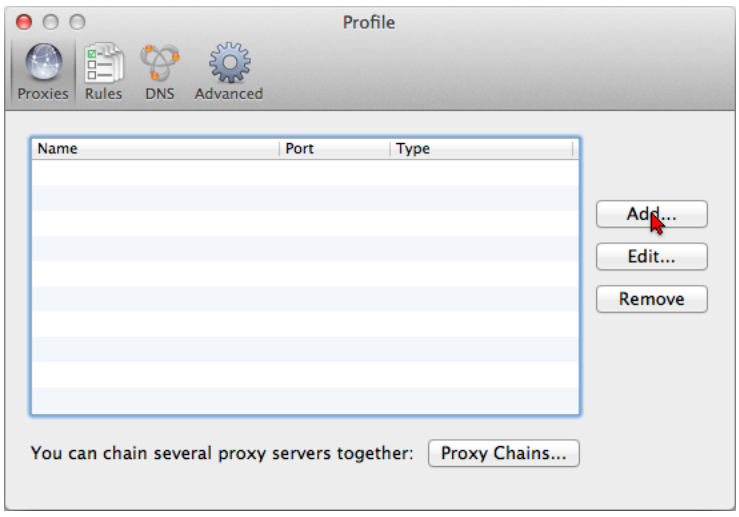
To add a proxy server, click either **Proxy Servers** in the **Profile** menu or the corresponding item on the toolbar:

WARNING!

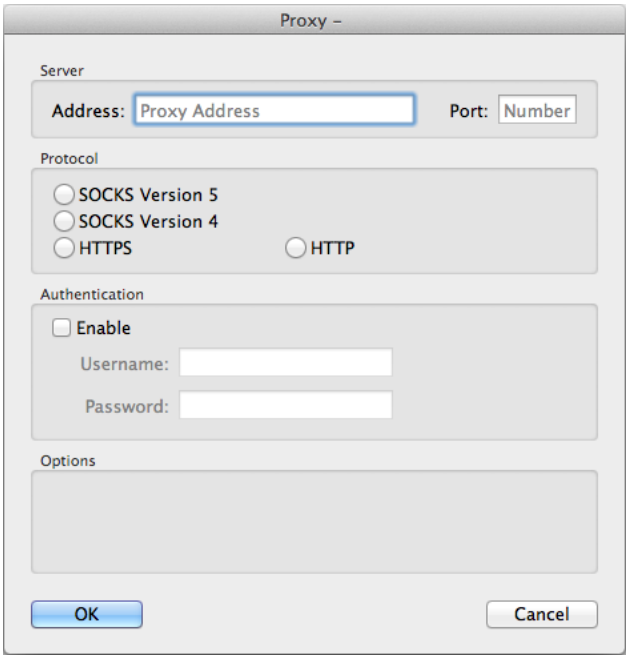
If you were using proxies before you installed Proxifier you should disable any built-in proxy settings. Your applications should then be configured to connect "directly" to the Internet (rather than through proxies).

This will open a 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**.

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.

- **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** on **HTTP Proxy** tab**.** 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.

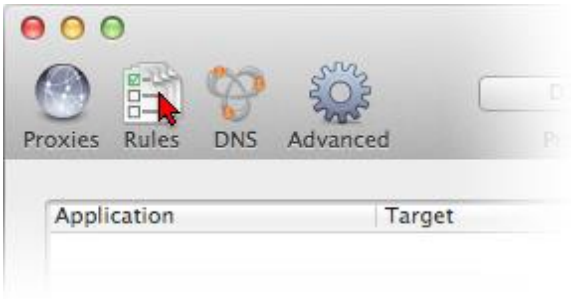
- **HTTPS**
  Username and Password — user authentication.

  Appear as Web Browser — if checked, Proxifier emulates browser's environment (some firewalls deny all requests that do not come from a browser).

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

Proxification Rules

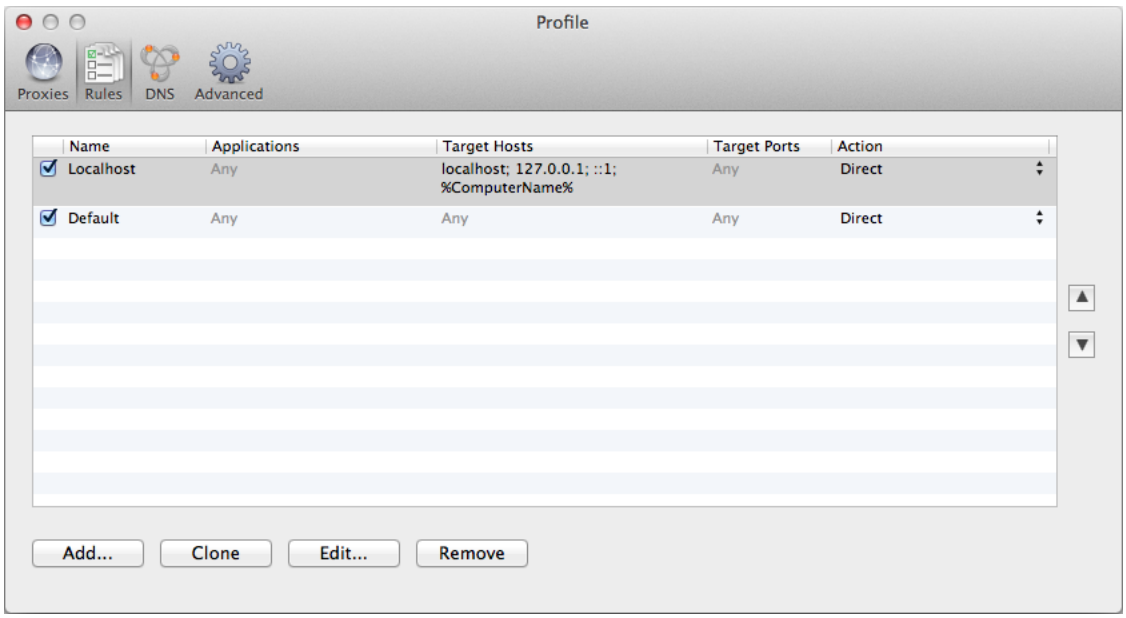
This feature allows you to define how certain connections should be processed by Proxifier. Each connection can be **processed directly**, through a **proxy**/**chain** or blocked.



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 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.

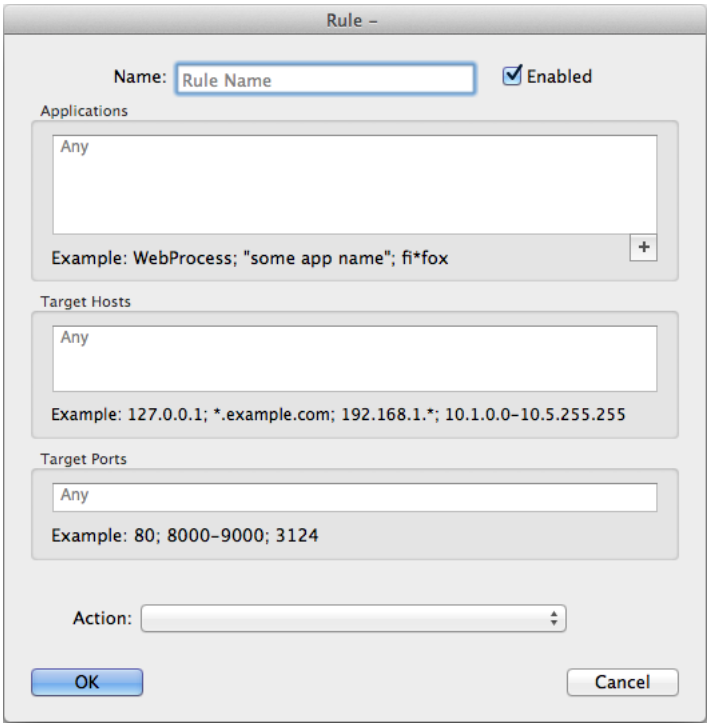
For example, if you assign a **proxy server** as an action for the "Default" rule and you have no more rules defined, Proxifier will process all connections through this proxy.

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 system applications like System Preferences can depend on the loopback connections. ***It is not recommended to edit or remove “Localhost” rule 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.

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 **“+”** 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.

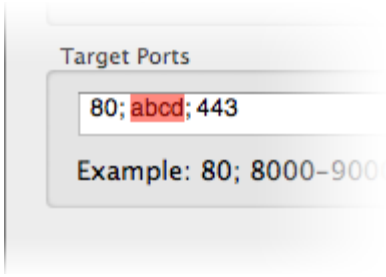
You can use any integer from 1 to 65 535 (2^16-1). Separate individual ports with a semicolon (;).

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:



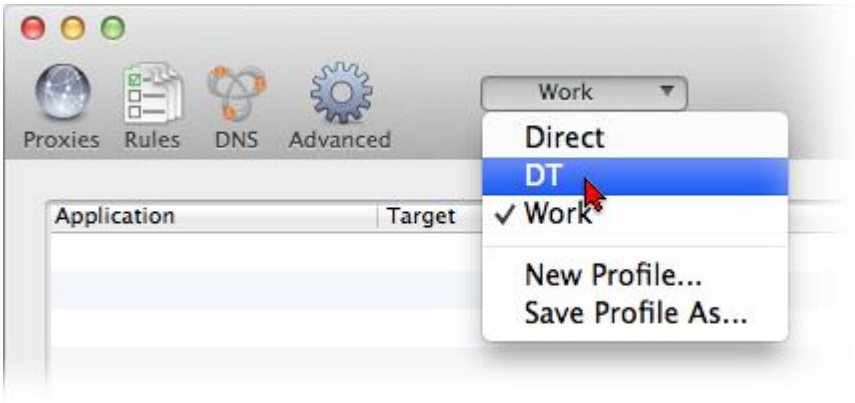
To match the rule a connection should satisfy all three criteria: **Applications**, **Target hosts** and **Ports**. If you have nothing defined in a field, the word "Any" in gray color is displayed and it will then match all possible values for certain criteria. This effectively means that this criterion 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.

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** menu are not included in a profile.

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:



To import or export a profile from/to a file use the **Import** or **Export** commands of the **File** menu respectively. With **Import** 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.

Proxifier v2 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.

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

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

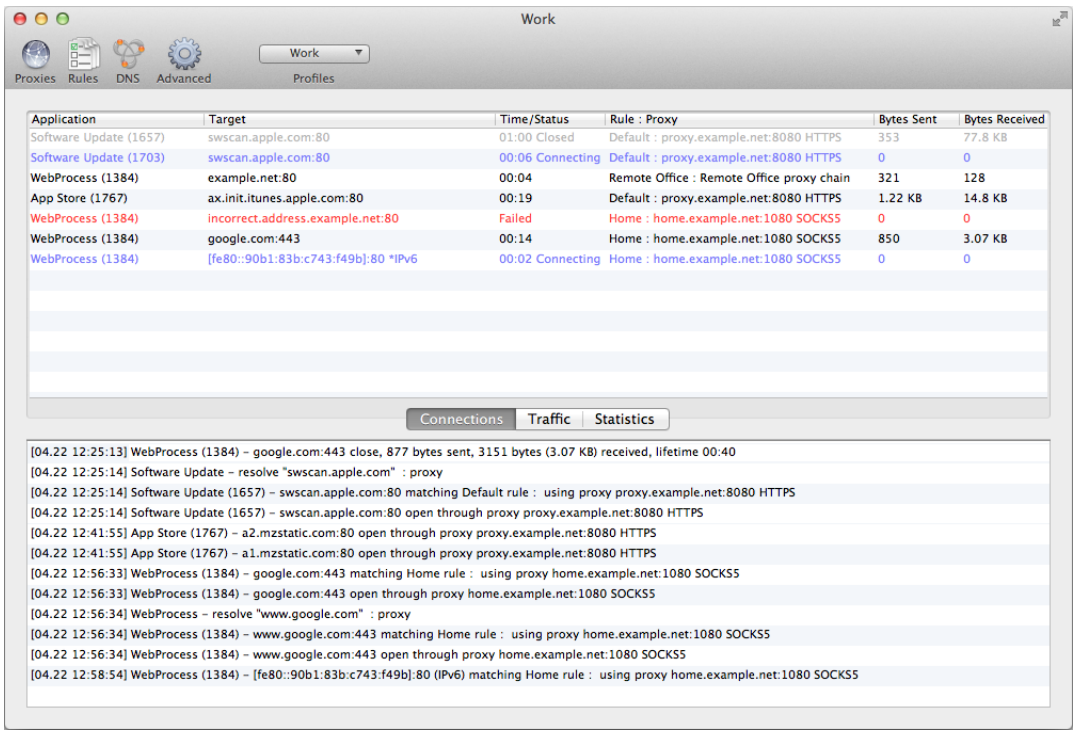
The description of each option is provided in the dialog window.

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.
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**.

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):

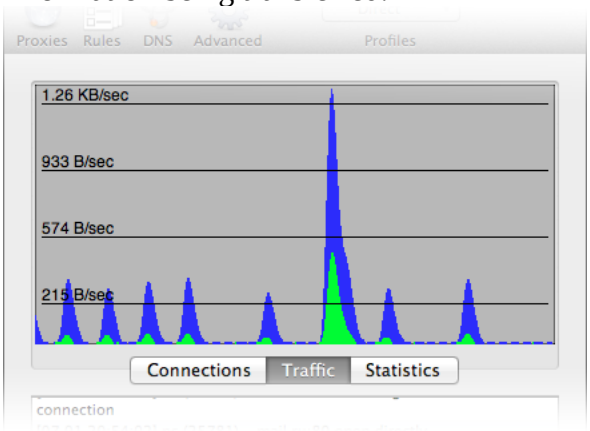
- *Applications* — program name, process ID (if **Verbose** output is enabled).
- *Target* — target host address (DNS name or IPv4/IPv6) and port number.
- *Time/Status* — time elapsed from the last status change. Available statuses are Connecting (blue), Closed (gray), Failed (red) and Canceled (red). 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.

Traffic

The Traffic tab 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.

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 context menu you can 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 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

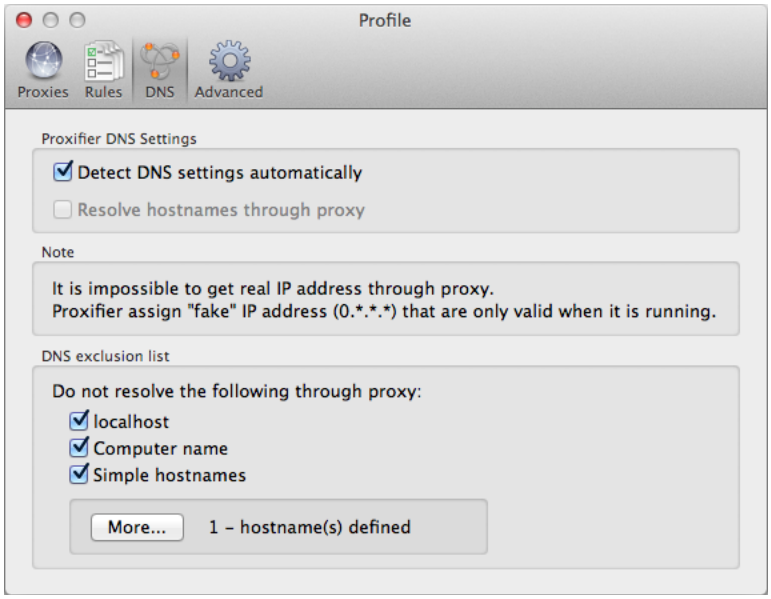
If you quit Proxifier when the main window is closed, it will not be opened automatically on the next start.

To reopen main window please click on Proxifier dock icon.

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 0.*.*.* which are only valid within the local computer while Proxifier is working. **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. The **Name Resolution** settings 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.

DNS exclusion list defines the names that should not be resolved through **proxy**.

localhost – "localhost" DNS name.

Computer Name - the local computer name.

Simple Hostnames - 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**.

More – allow to edit a custom DNS exclusion list. 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.

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.

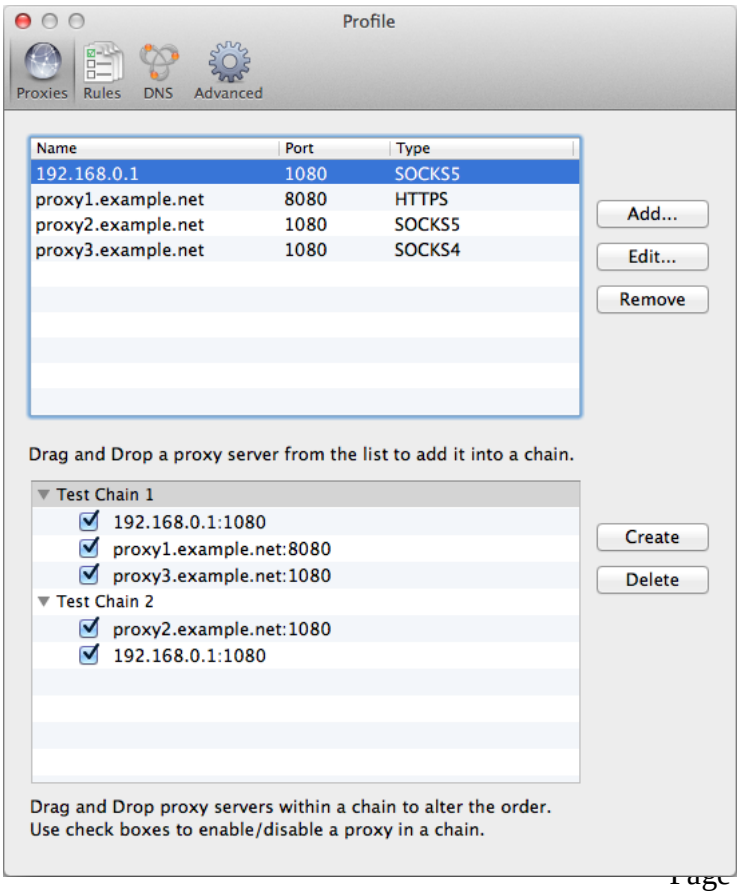
Proxy Chains

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 mouse-click its label. Use the **Remove** button to remove a selected chain.

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

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.

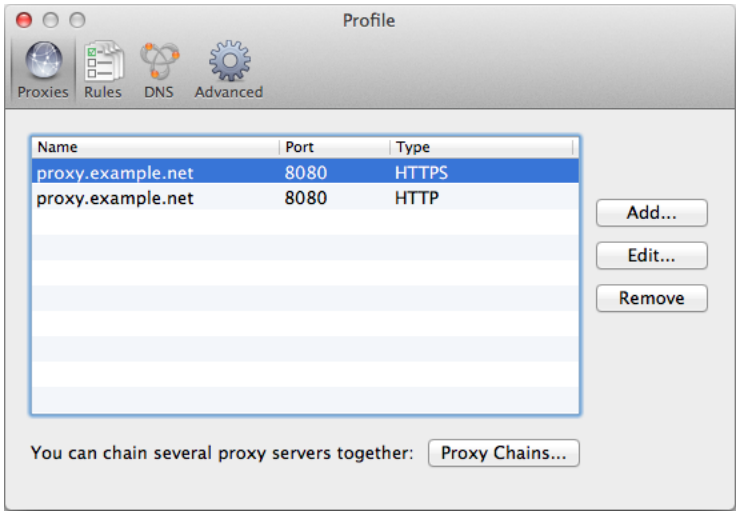
Proxifier can work with HTTP proxy servers that do not support HTTPS on arbitrary ports. Due to the technical limitation of this protocol it is only possible to process HTTP connections with such proxy servers. This means that you must configure the **Proxification Rules** accordingly.

You can enable HTTP proxy support at **HTTP Proxy** tab of **Profile->Advanced** window. 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.

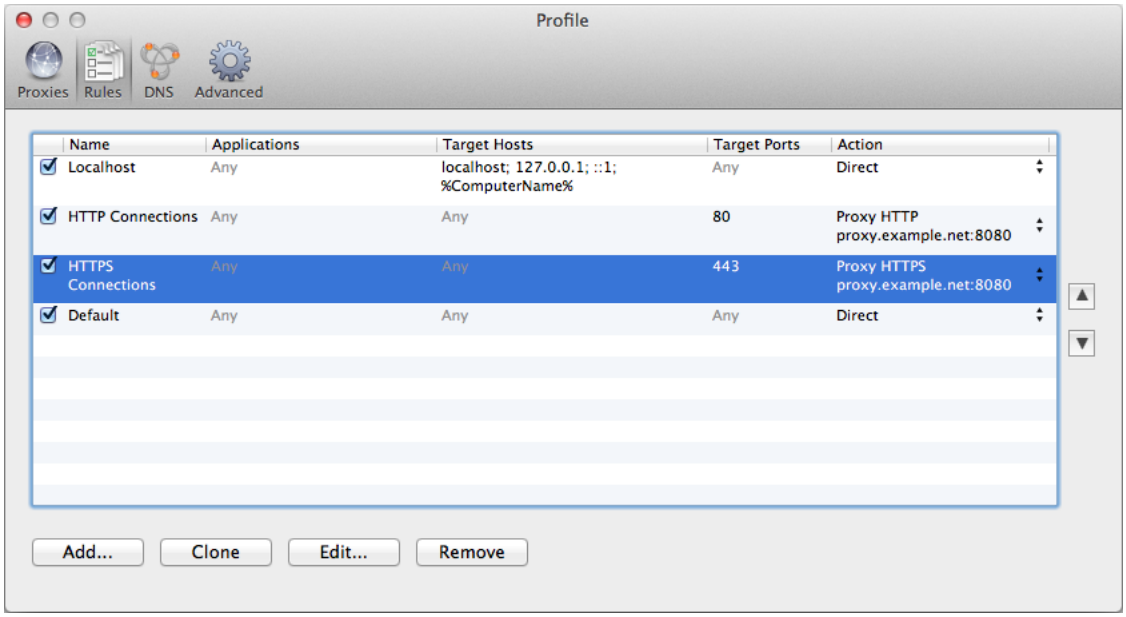
Suppose *proxy.example.net:8080* is a usual HTTP proxy and supports HTTP on port 80 and HTTPS on port 443 and we want to configure Proxifier to process HTTP/HTTPS connections (web browsing) through it.

The following images illustrate the correct setup.

Proxy Settings:

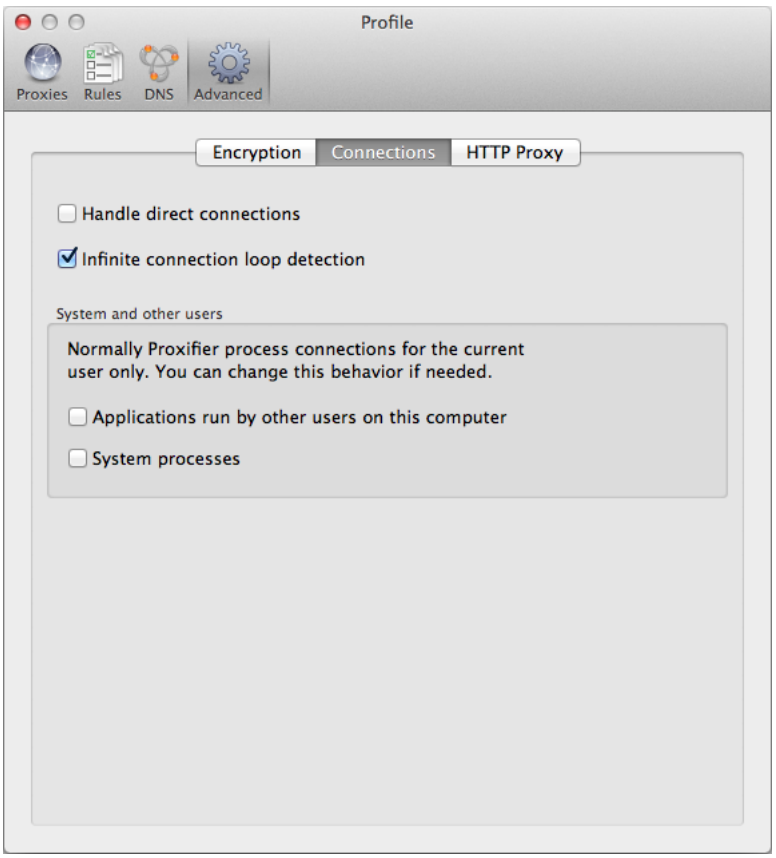


Proxification Rules:



Direct Connections

Proxifier can process connections without a proxy server. You can enable this with **Handle Direct Connections** option on **Connection** tab of **Profile->Advanced Options**. 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.

The messages are saved under ~/Library/Logs/Proxifier directory. This file can be opened with the standard Console.app using the **Log->Log to File->Open Log File** command. Traffic dumps (if enabled) are saved 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). The traffic dump directory can be opened with the **Log->Log to File->Open Traffic Log Folder** command.

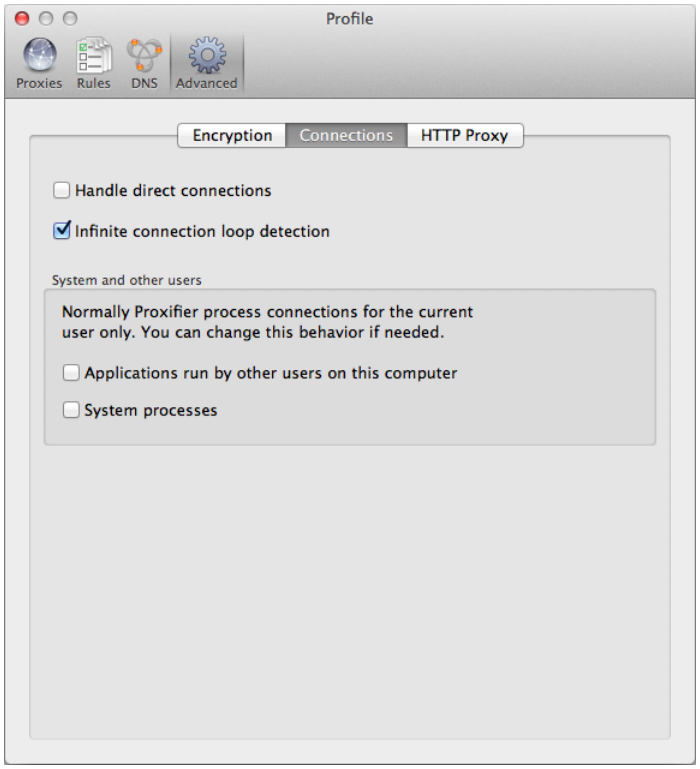
For example, a dump of an HTTP connection can look like the following:
"WebProcess (23712) TO www.apple.com_443 AT 2012_06_29 19_52_55_409.dmp"
"WebProcess (23712) FROM www.apple.com_443 AT 2012_06_29 19_52_55_721.dmp"

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.

System and Other Users' Connections

Proxifier can process system processes and applications run by other users.
Both features are disabled by default. You can enable them at **Profile->Advanced** on **Connections** tab.

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:

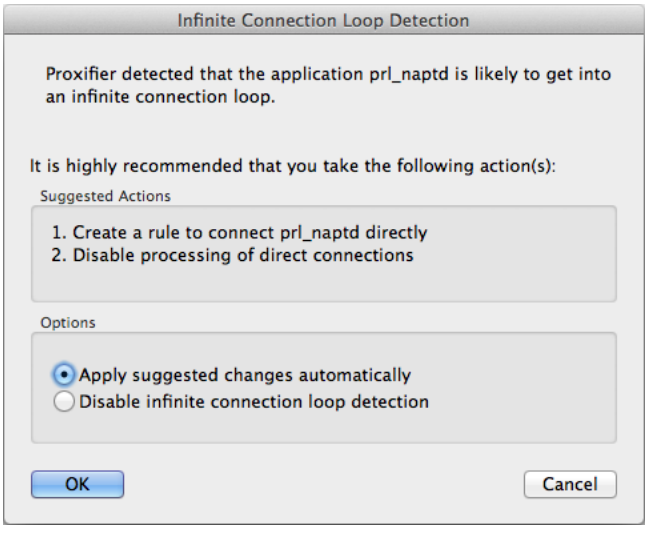
1. Application initiates a connection.
2. Proxifier captures it and redirects to the local proxy server.
3. Local proxy server forwards the connection to the Internet.
4. Proxifier captures this connection and redirects to the same proxy again.
5. Step 3 is repeated.

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

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.

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 for Mac v2.21”).
- OS version (e.g. Mac OS X 10.11.4.)
- 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/mac-v2/eula.htm