

SSLTurbo 服务安装配置手册（Mac OSX 平台）

对应 SSLTurbo 版本 V0.14.4

IGVPN SSLTurbo 服务是 IGVPN 最新研发的加速服务，提供独立客户端，主要功能如下：

- 1、跨平台独立客户端支持，提供 Windows 和 Mac OSX 平台全平台支持，将来扩展到 Linux 和部分移动平台等，目前提供一键自动安装程序。
- 2、一键记忆密码登录，提供开机自启动和客户端自动登录功能。
- 3、自动同步最新服务器列表，可以随时选择任意服务器。
- 4、目前提供高性能 SSL 协议、ShadowSocks 协议和 StealthVPN 等协议，将来可扩展到更多的协议。
- 5、支持自定义黑白代理名单，用户可自定义多个黑白名单组，自行维护域名清单，黑白名单提供外部文本文件导入功能，提供黑白名单云端保存和同步。
- 6、提供多种代理策略选择：
 - a) Tunnel all sites 策略，即全代理模式
 - b) Tunnel these sites 策略，即仅代理用户自定义黑名单组中定义的域名
 - c) Exclude these sites 策略，即除了用户自定义白名单组中定义的域名，其他全部代理
 - d) Unblock sites 策略，即 IGVPN 预定义的代理策略，采用白名单模式，国内的主流网站不代理，其余全部代理，域名清单不一定全面，但基本满足日常使用，推荐。
- 7、自带代理策略 PAC 服务器，提供唯一的 PAC URL 地址，可供 IE 自动代理、Chrome 代理插件，FireFox 代理插件使用。
- 8、本地提供高性能 HTTP 代理（使用 SSL 协议时）或者 SOCKS5 代理（使用 ShadowSocks 协议时，请灵活变通），免密码认证，供高级用户扩展使用。
- 9、在使用 SSL 和 Shadowsocks 协议的情况下，提供局域网高性能加速代理的功能。
- 10、提供 StealthVPN 协议，系统级别的加速服务，提供国内外路由分离开关功能。
- 11、提供服务包内容、到期时间和流量信息显示功能。
- 12、提供在线检查更新功能（Beta 测试）。
- 13、提供本地无污染 DNS 解析功能，当选择 SSL 协议即可使用，服务端口固定为 10053 支持本地和局域网的 TCP 协议 DNS 解析请求，仅供高级用户使用。

以下仅以 Mac OSX 10.10.2 平台环境，介绍 SSLTurbo 服务的配置使用。

一、在 IGVPN 会员区下载页面找到并下载 SSLTurbo 客户端安装包（.pkg 格式）到本地，双击启动：

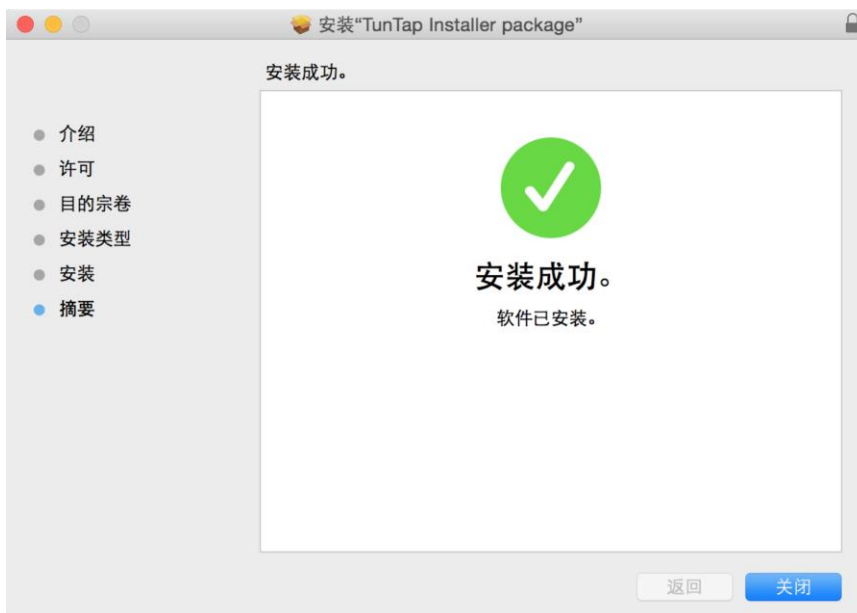
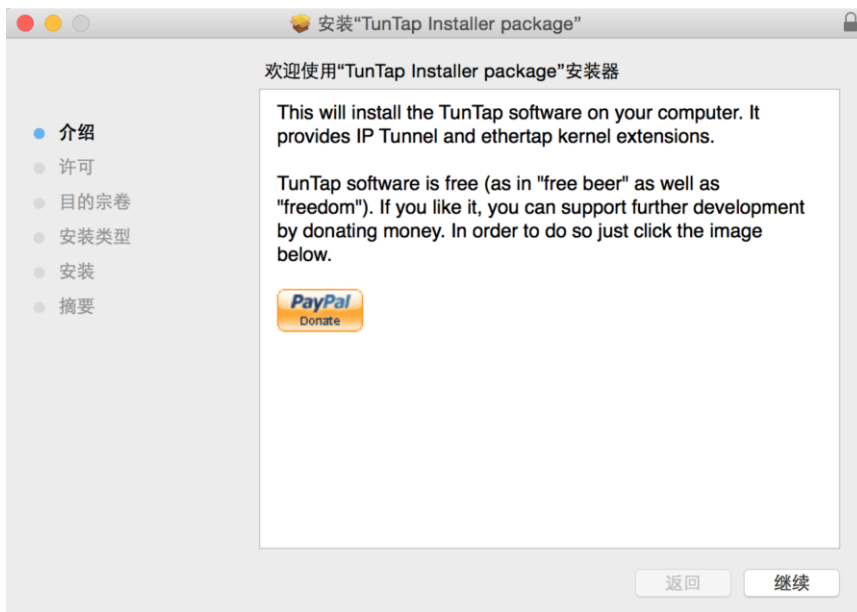
按界面提示安装，关键截图如下：



务必选择所有的安装组件（含 TunTap 虚拟网卡驱动）：



在弹出的 TUNTAP 驱动安装窗口，按提示安装即可：



在弹出的 SSLTurbo 卷窗口,和其他 Mac OSX 的一般程序安装方式一样,把 SSLTurbo 程序拖拽到 Applications 目录即可完成安装,如提示覆盖老版本是可以点击确认覆盖。

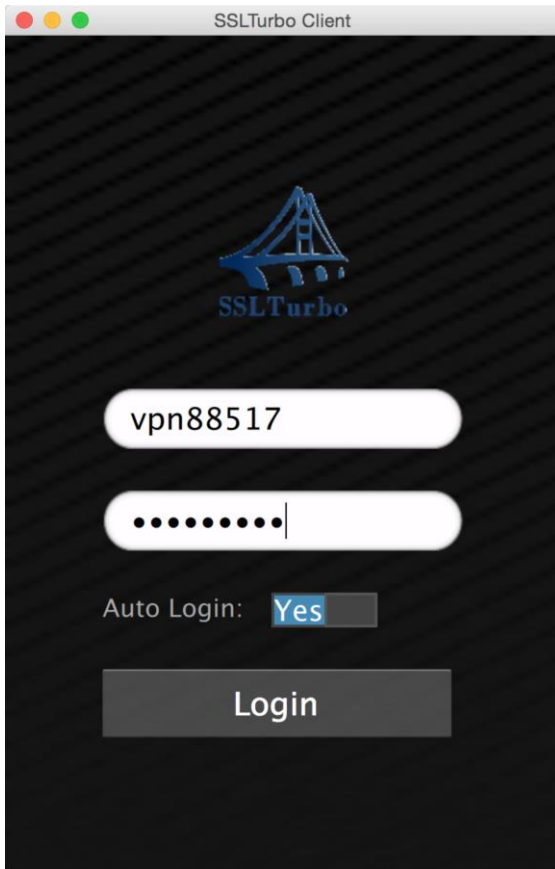


SSLTurbo.app

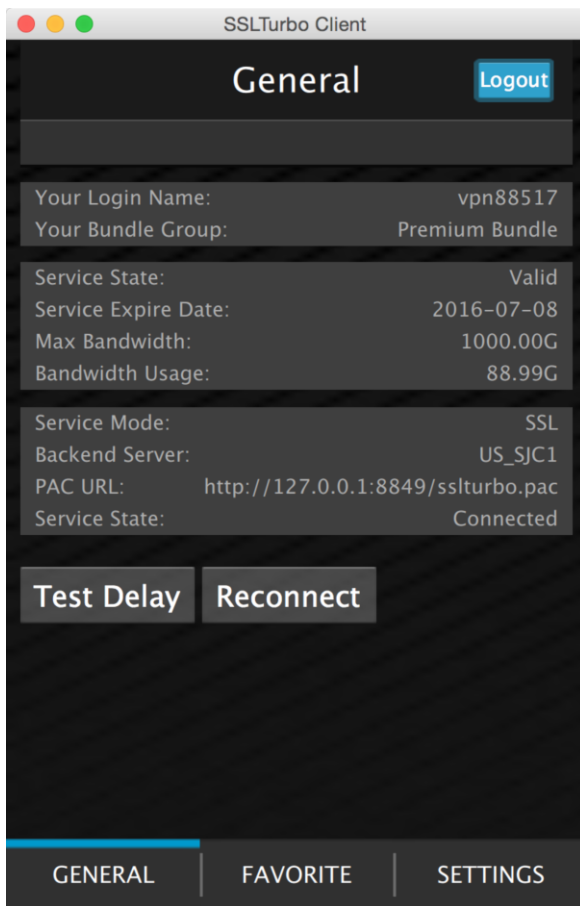


Applications

然后，和其他 Mac OS X 程序一样，在 LaunchPad 中找到并启动 SSLTurbo 程序，启动界面上输入你的 VPN 账号和密码：



Auto Login 可以选成 Yes，密码默认自动保存，然后点击 Login 即可登录，登录成功后，程序会最小化到右上角状态栏常驻，点击 SSLTurbo 的图标，即可打开程序登录后的主信息页面，显示登录账号相关的一些关键服务信息，截图如下：



可以看到一些关键信息，如：

Your login name: 当前登录的 VPN 账号

Your Bundle Group: 服务包级别，主要是 Pro Bundle 和 Premium Bundle（额外服务器）

Service State: 服务包有效状态

Service Expire Date: 服务包到期时间

Max Bandwidth: 服务包月度流量使用限制（单位 GB）

Bandwidth Usage: 单月流量使用（单位 GB）

Service Mode: 当前使用的通道协议

Backend server: 当前连接的远端服务器

PAC URL: 自动代理配置 URL 地址（选择 SSL 协议或者 ShadowsSocks 协议时有效）

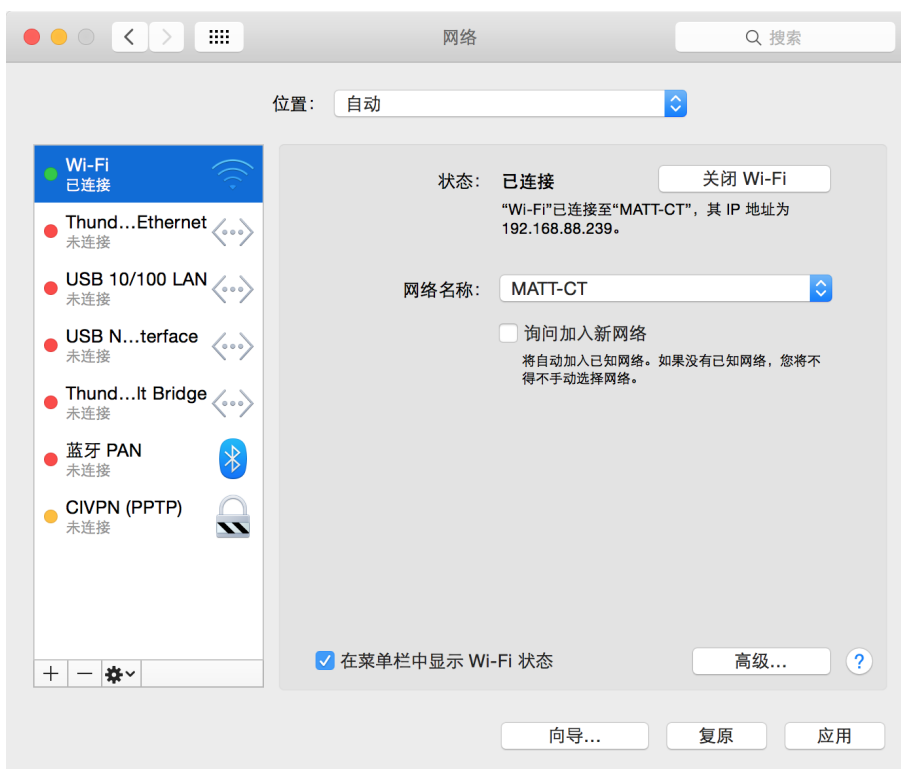
Service state: 服务连接状态

二、快速使用指南：

我们的预制客户端默认选择我们预定义的代理策略，即“Unblock sites”策略，稍作配

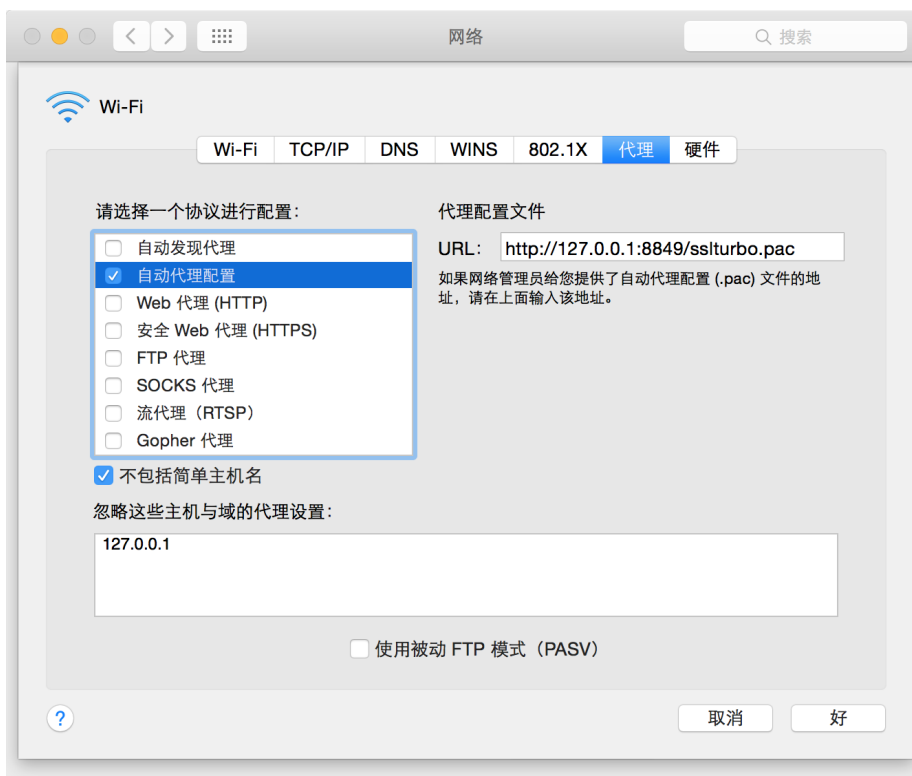
置即可实现科学上网，方法如下，**适合懒人：**

打开 Mac OSX『设置』程序，选择『网络』，左边栏选择当前活动的网络，如 WiFi，然后点击『高级』，再点击『代理』，进入代理设置页面：



勾选『自动代理配置』，在 URL 地址栏中输入：

<http://127.0.0.1:8849/sslturbo.pac>



点击『应用』退出，然后在 Safari 浏览器中输入你想访问的网站地址，比如 <https://twitter.com>，应该就可以打开了。

注意：设置 MacOSX 系统自动代理地址，实际是设置了系统级别的代理，因此一旦设置完成，Mac OSX 系统中的其他程序一般选择自动或者设置成使用系统代理，比如 Chrome 浏览器，Firefox 浏览器，DropBox 客户端，Google Earth 客户端等。

懒人配置到此结束！再次提醒，**懒人配置必须使用的是 SSL 协议**，如果修改协议，需要阅读高级用户部分。

以下设置供高级用户耐心看完，没有耐心的用户不建议阅读！

三、SSLTurbo 客户端的一些常见设置

1、授权启用 SSLTurbo 的 StealthVPN 协议

由于 MacOSX 的权限设计原因，此版本的 SSLTurbo 如需启用 StealthVPN 协议，暂时只能通过命令行手工授权以管理员权限启用 SSLTurbo 客户端，才能正常使用 StealthVPN 协议，而 SSL 和 Shadowsocks 协议无需命令行授权启动的。

打开『终端』应用：

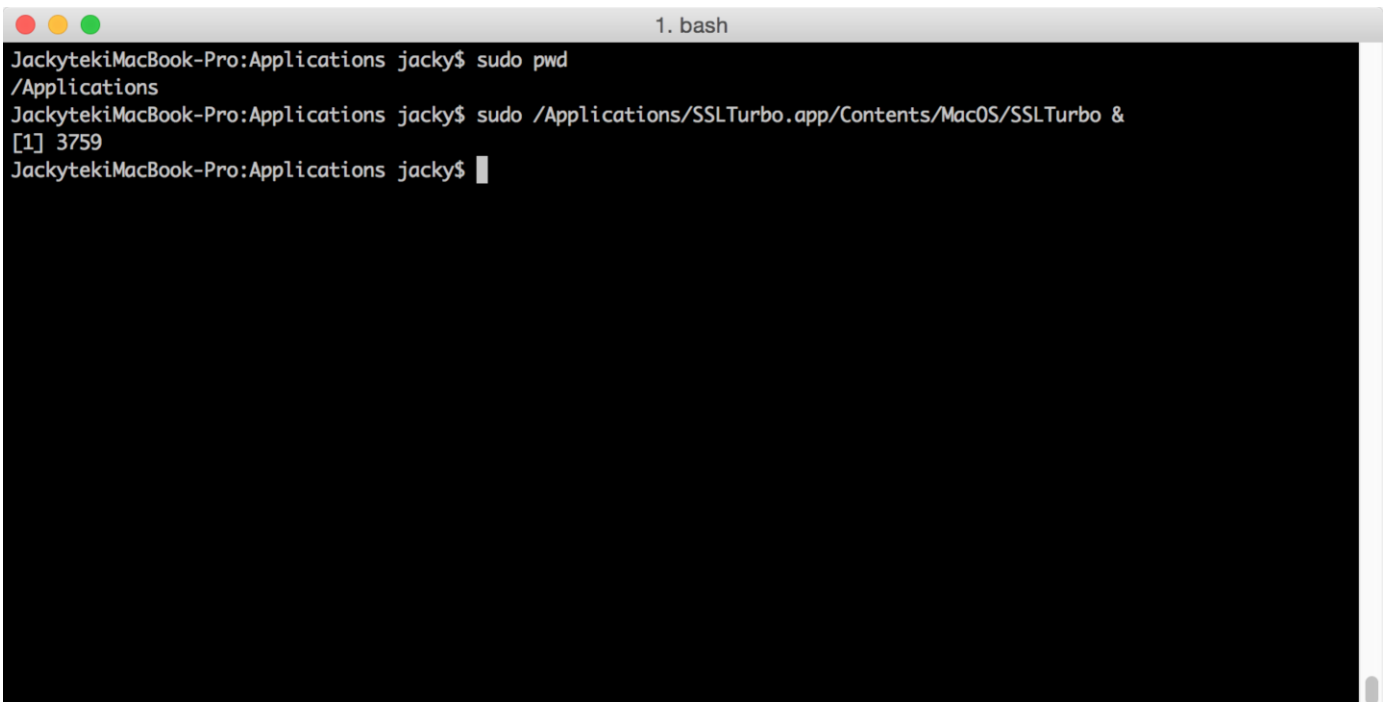
输入以下命令并回车：

```
sudo pwd
```

按提示输入登录用户的密码，然后再输入以下命令并回车：

```
sudo /Applications/SSLTurbo.app/Contents/MacOS/SSLTurbo &
```

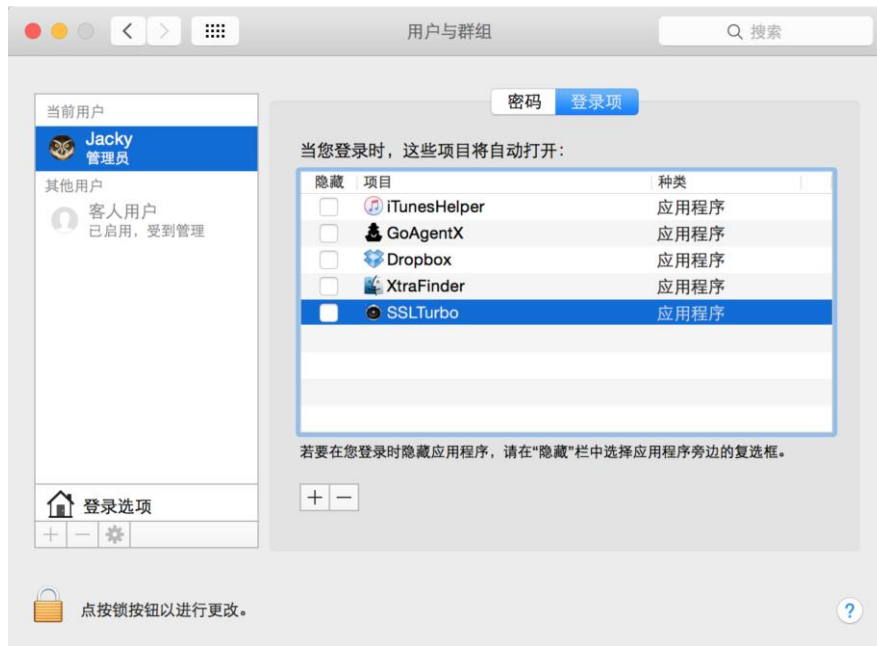
即可授权管理员用户权限启动 SSLTurbo 客户端，后续通过 SSLTurbo 客户端的图形界面按正常使用即可。参考如下图：



```
1. bash
JackytekiMacBook-Pro:Applications jacky$ sudo pwd
/Applications
JackytekiMacBook-Pro:Applications jacky$ sudo /Applications/SSLTurbo.app/Contents/MacOS/SSLTurbo &
[1] 3759
JackytekiMacBook-Pro:Applications jacky$
```

2、设置开机自动启动

SSLTurbo for Mac 开机启动需要利用 MacOSX 的用户登录启动功能，在『系统设置』->『用户和群组』，点击你的登录用户，选择『登录项』，点击+号，找到 SSLTurbo.app，添加到系统开机项里面，参考如下图：



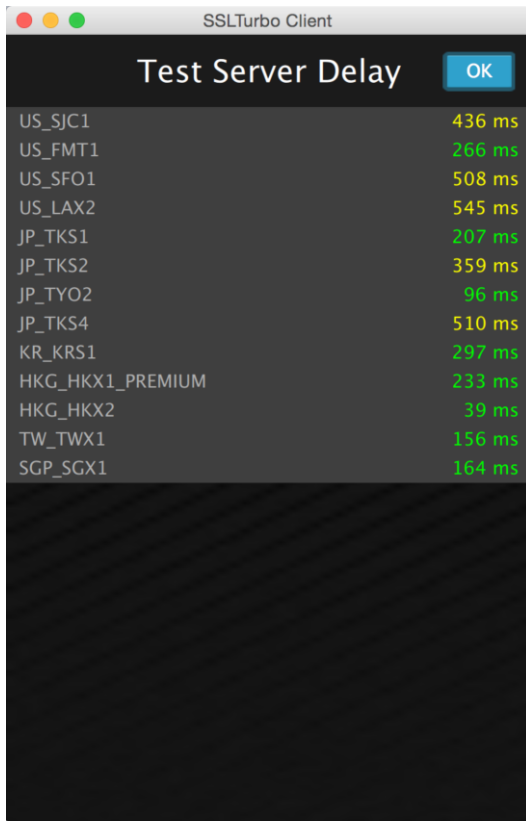
3、检查更新版本的 SSLTurbo（目前仅供测试）

0.14.4 版本开始，SSLTurbo 支持在线更新，方法如下：

在/Applications/SSLTurbo 目录找到名为 Maintenance 的应用，这是 SSLTurbo 的组件维护程序，双击启动，在弹出的窗口中选择第二项“更新组件”来检查更新即可。

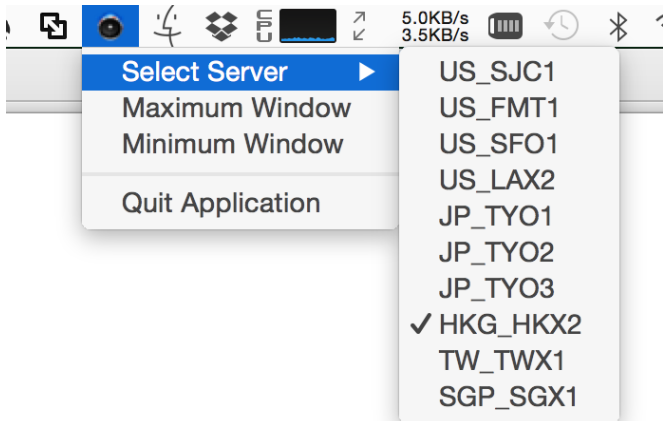
4、服务器测速

在主界面，点击『Test Delay』按钮，等待测速结果，即可了解哪台服务器对你当前的网络更为友好，测试结果不是简单的 ping 测试，而是用我们自己的算法进行测试，测试结果供参考（在使用过程中随时可以测速了解服务器的友好度）：



5、在线切换服务器

客户端每次登录成功会自动同步当前可用的服务器清单，可以在 MenuBar 菜单栏中找到 SSLTurbo 的图标，点击，通过“Select Server”来切换服务器：



服务器切换完成后，SSLTurbo 客户端会自动重连新的服务器，一般过几秒即可使用。

6、切换加密协议

目前 SSLTurbo 加速服务支持 SSL 协议、ShadowsSocks 协议和 StealthVPN 协议，可以根据需要进行选择，区别如下：

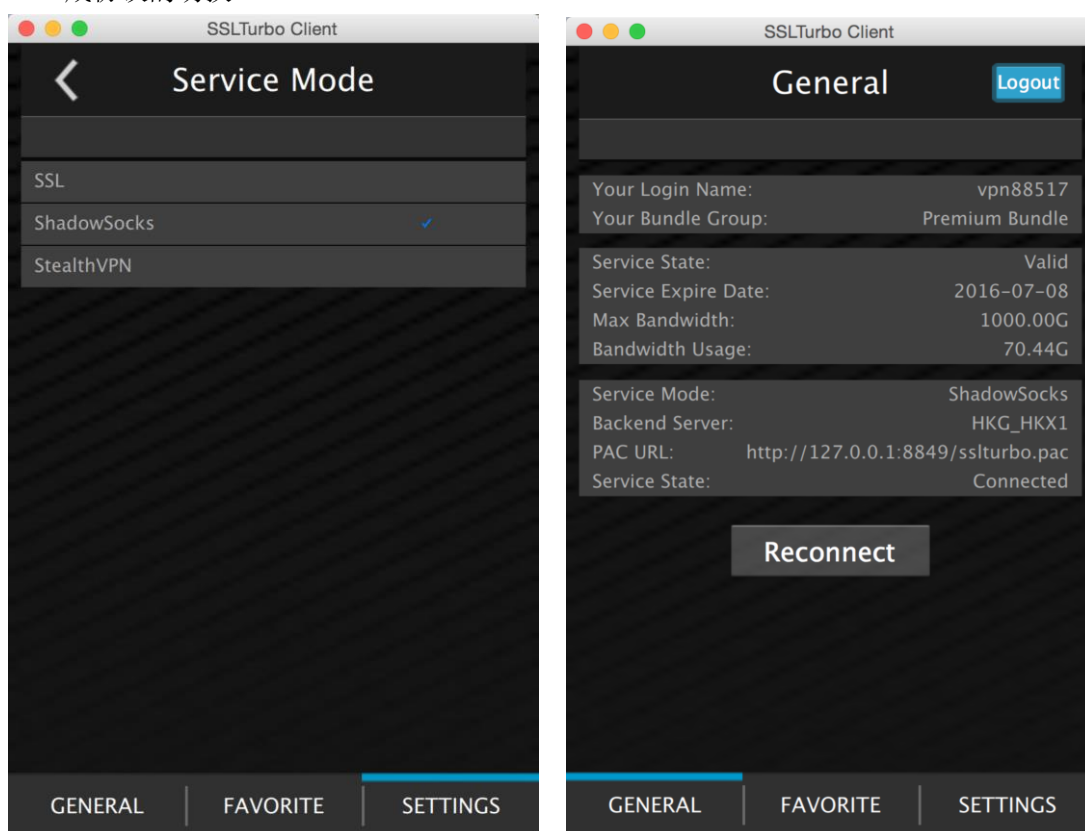
- 1) 如果选择 SSL 协议（推荐），启用 256 位的 SSL 加密通道，本地生成的是独立

的 HTTP 代理，自动生成的 PAC 自动代理中的代理定义也是 HTTP 的。

- 2) 如果选择 ShadowSocks 协议，启用的是 128 位加密通道，本地生成的是独立的 SOCKS5 代理，自动生成的 PAC 自动代理中的代理定义也是 SOCKS 的。
- 3) 如果选择 StealthVPN 协议（测试阶段），那么启动的是混淆 SSL VPN 连接，连接成功后会修改系统本地路由，系统整体将处于翻墙状态，还可以按需启用国内外路由分离功能，且无需设置任何浏览器的代理设置。

以下以 SSL 和 Shadowsocks 等代理协议切换介绍如下：

点击 SSLTurbo 客户端主界面的 SETTINGS，选择 Service Mode，选择你希望使用的协议，然后马上点击 GENERAL 界面，点击 Reconnect 重连，一般需要等若干秒钟，即可完成协议的切换。



特别特别要注意的是：

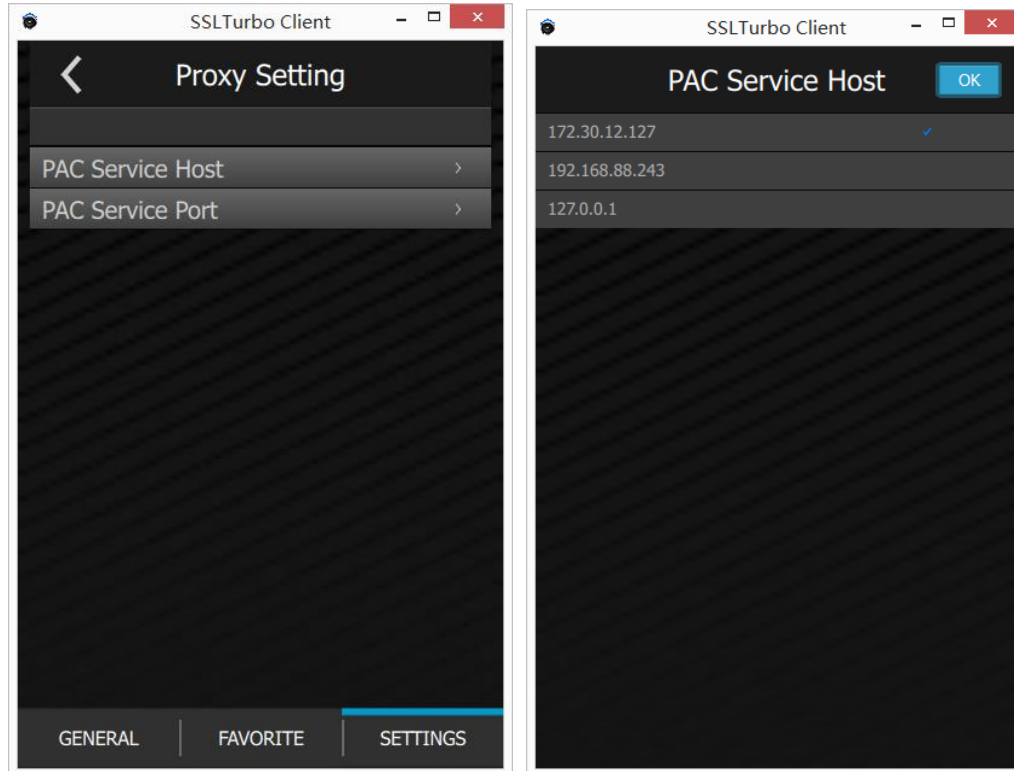
① 由于 SSL 协议和 Shadowsocks 协议生成的代理类型不一样，因此切换协议后，需要关闭再重新启用一下系统或者浏览器的自动代理设置（包括使用插件的情况下，也要重新启用下），因此我们不推荐经常切换协议，避免带来问题，我们推荐用户使用 SSL 协议。

② 如果使用 StealthVPN 协议，首先是需要用命令行 `sudo` 授权启动 SSLTurbo 客户端，另外由于目前在测试阶段，可能存在不稳定，连接或者断开连接的时间可能也会比较长。

7、局域网共享代理设置（仅选择 SSL 协议或者 Shadowsocks 协议时有效）

SSLTurbo 如果选择了 SSL 协议或者 Shadowsocks 协议，连接成功后，不仅为本机提供加速代理服务，还可以为局域网内的其他设备提供高速代理服务，设置方法如下：

连接成功后，在 SSLTurbo 客户端中选择 SETTINGS 页面，点击“Proxy Service Host”，选择 SSLTurbo 服务所在机器的局域网 IP 地址，然后点击 OK 返回即可，如图：



通过以上设置，如果已顺利连接上了 SSLTurbo 服务，系统本地生成的高性能 HTTP 代理（选择 SSL 协议时）或者 SOCKS5 代理（选 ShadowSocks 协议时）服务在满足本地使用之外，还可以提供给局域网其他机器使用。

以截图为例，局域网中其他机器可使用的高性能 HTTP 代理或者 SOCKS5 服务地址：

172.30.12.127:8848

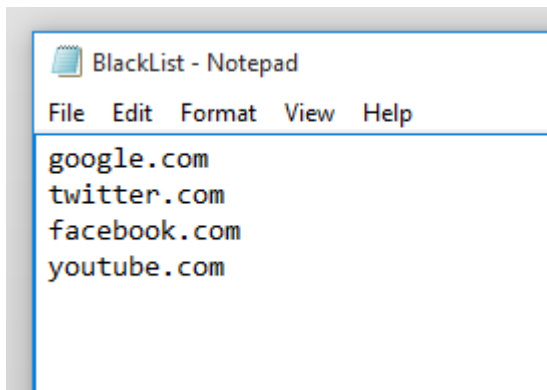
以截图为例，局域网其他机器可使用的自动代理策略 PAC URL 地址：

<http://172.31.12.127:8849/sslturbo.pac>

目前平台 iOS 系统，Android 5.1+以上版本、Windows Phone 7+和 BlackBerry10 的机器都可以在 WiFi 情况下使用 SSLTurbo 的高速代理共享服务。

8、自定义黑名单组（仅选择 SSL 协议或者 Shadowsocks 协议时有效，StealthVPN 协议无需设置）

黑名单设置支持文件导入，可以将你自己定义的黑名单放在一个 txt 文本文件中，每行一个黑名单域名：

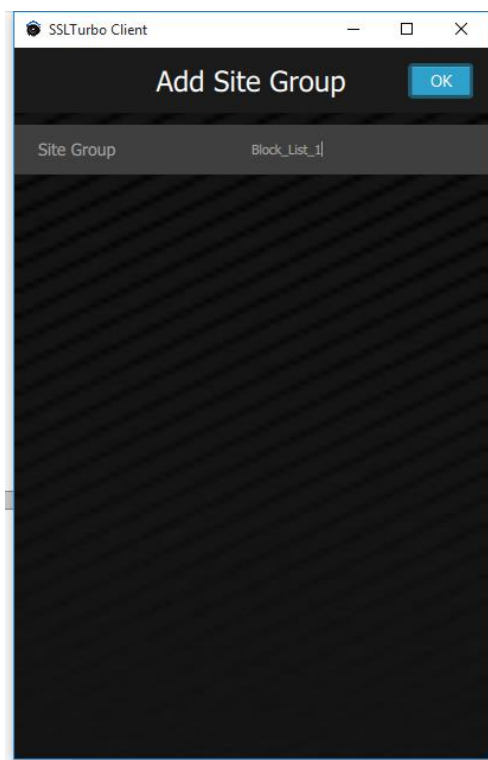


黑名单域名简单来说就是你希望代理的网站域名，一般就是被墙而你又想访问的网址，域名不需要输入全，输入域名主体加后缀即可，比如：

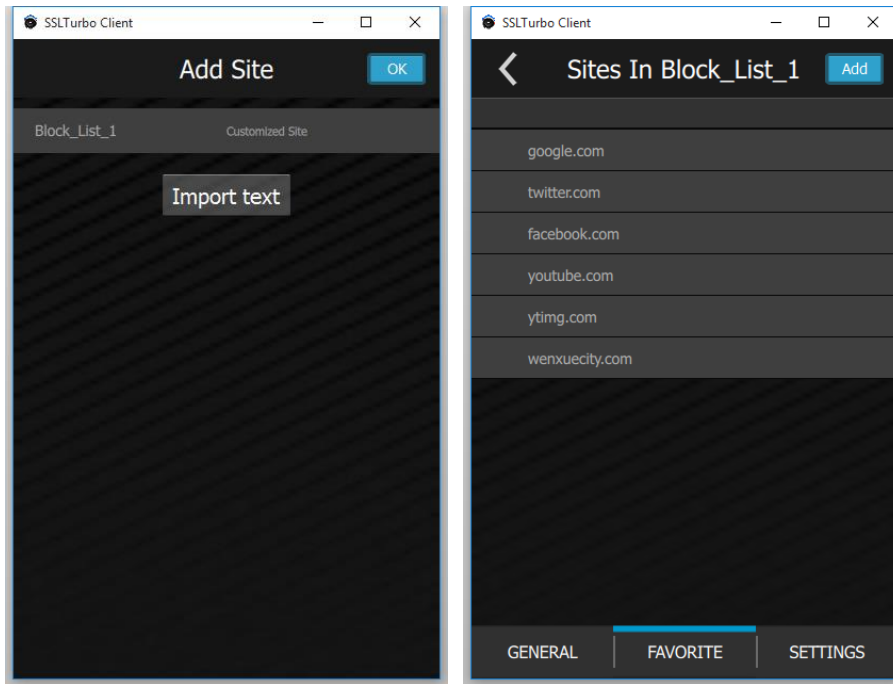
google.com

代表：*.google.com 都会被代理，但 *.google.com.hk 就不会

在 SSLTurbo 客户端，选择 FAVORITE 页面，点击“Add”，在“Site groups”这里输入黑名单的名字，比如 Block_List_1，如图：



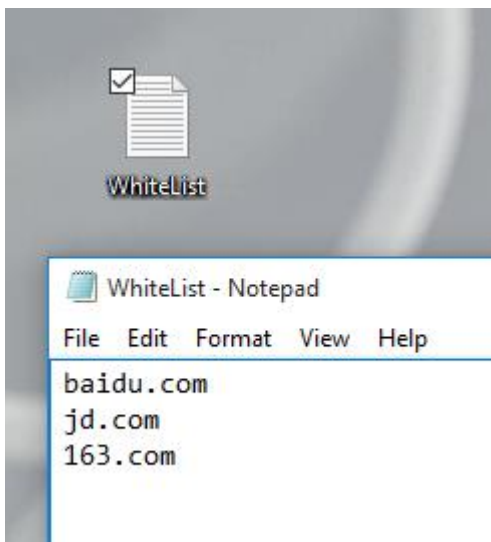
点击 OK 保存，点击刚建立的 Block_List_1 组，进入域名定义界面，点击 Add，然后再点击 Import text，选择你的黑名单文件即可导入，导入完成点击 OK 即可看到导入的域名列表。



可以根据需要建立多个黑名单组。建立的黑名单组在“Tunnel these sites”代理策略设置时可以指定使用。

9、自定义白名单组（仅选择 SSL 协议或者 Shadowsocks 协议时有效，StealthVPN 协议无需设置）

自定义白名单设置支持文件导入，可以将你自己定义在白名单放在一个 txt 文本文件中，每行一个白名单域名：



白名单域名简单的说就是你希望直接访问而不是不通过代理访问的网站域名，一般是国内的网站，域名不需要输入全，输入域名主体加后缀即可，比如：

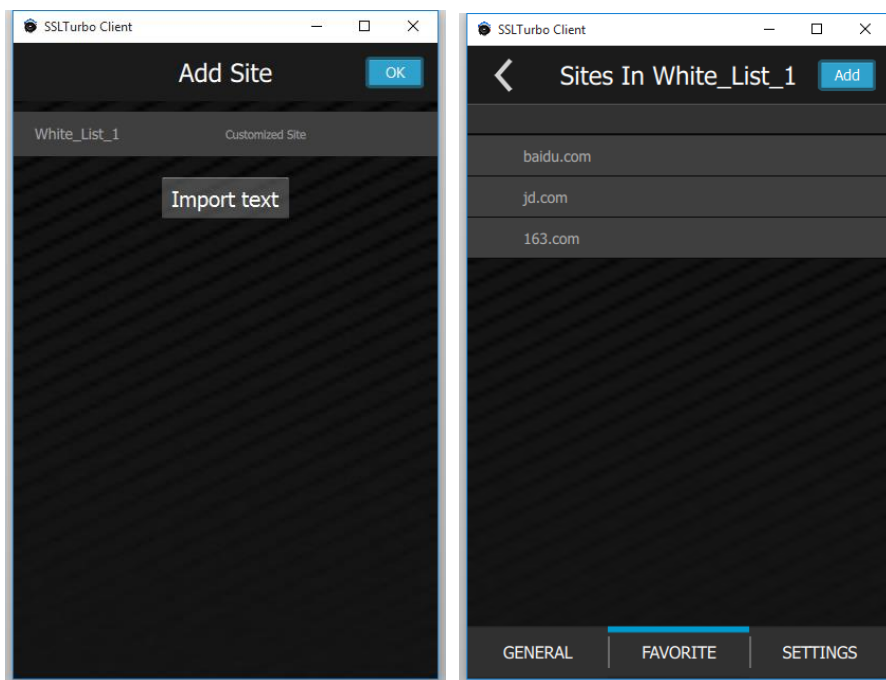
baidu.com

代表: *.baidu.com 都会被代理, 但 *.baidu.com.hk 就不会

在 SSLTurbo 客户端, 选择 FAVORITE 页面, 点击 “Add”, 在 “Site groups” 这里输入白名单的名字, 比如 White_List_1, 如图:



点击 OK 保存, 点击刚建立的 White_List_1 组, 进入域名定义界面, 点击 Add, 然后再点击 Import text, 选择你的白名单文件即可导入, 导入完成点击 OK 即可看到导入的域名列表。



可以根据需要建立多个白名单组。建立的黑名单组在“**Exclude these sites**”代理策略设置时可以指定使用。

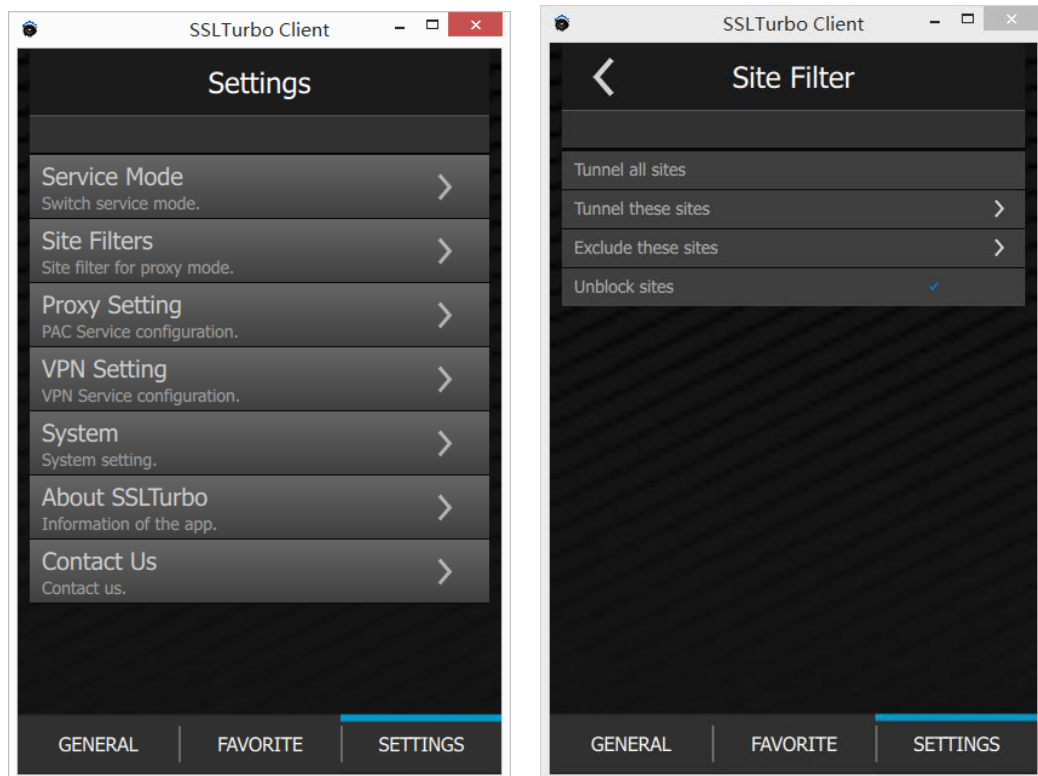
10、代理策略设置（仅选择 SSL 协议或者 Shadowsocks 协议时有效，StealthVPN 协议无需设置）

SSLTurbo 客户端提供以下 4 种代理策略选择：

- a) Tunnel all sites 策略，即全代理模式
- b) Tunnel these sites 策略，即仅代理用户自定义黑名单组中定义的域名
- c) Exclude these sites 策略，即除了用户自定义白名单组中定义的域名，其他全部代理
- d) Unblock sites 策略，即 IGVPN 预定义的代理策略，采用白名单模式，国内的主流网站不代理，其余全部代理，域名清单不一定全面，但基本满足日常使用，推荐。

设置方法：

在 SSLTurbo 客户端，选择 SETTING 页面，点击“Site Filter”，进入代理策略设置页面：



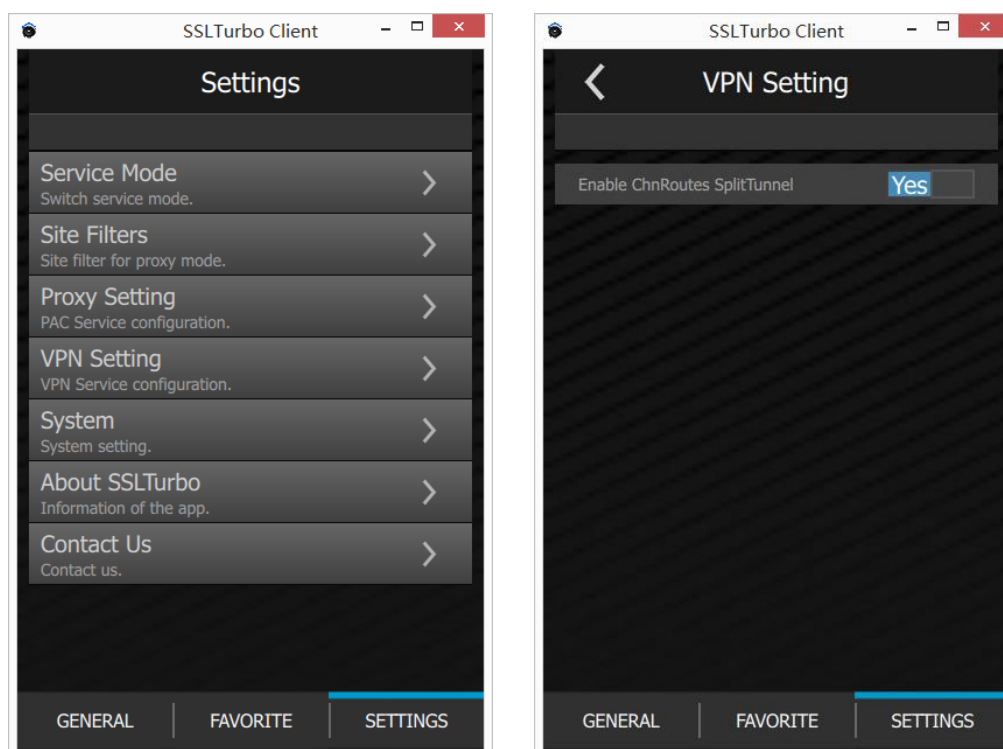
可以根据需要选择代理策略，再次特别说明：

- a) Tunnel these sites 策略，请选择前面定义的黑名单组
- b) Exclude these sites 策略，请选择前面定义白名单组

11、设置国内外路由分离（仅选择 StealthVPN 协议时有效，目前提供测试）

当使用 SSLTurbo 的 StealthVPN 协议时，默认是国内外路由分离设置的，即访问国内不通过 VPN，访问国外统一通过 VPN，仅供高级用户测试，介绍如下。

首先确认选择了 StealthVPN 协议，然后点击 SSLTurbo 客户端主界面的 SETTINGS，选择 VPN Setting，将“Enable ChnRoutes SplitTunnel”设置成 Yes，即可完成 StealthVPN 协议下的国内外路由分离设置，更改设置需要点击主界面的 Reconnect 重连生效，如下图：



12、 本地无污染 DNS 解析服务（仅选择 SSL 协议时有效，目前提供测试）

SSLTurbo 0.14.4 以上版本提供了本地无污染 DNS 解析功能，当选择 SSL 协议即可使用，DNS 服务端口固定为 10053，支持本地和局域网解析请求，仅支持 TCP 协议 DNS 解析请求，仅供高级用户扩展使用。

简单通过局域网内的其他 Linux 系统的 dig 工具测试如图：

```
root@vpnsrv:~# dig twitter.com @172.30.12.127 -p 10053 +tcp
; <<>> DiG 9.9.5-4-Debian <<>> twitter.com @172.30.12.127 -p 10053 +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13089
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags;; udp: 4096
;; QUESTION SECTION:
;twitter.com.                IN      A

;; ANSWER SECTION:
twitter.com.                1450    IN      A      199.16.158.179
twitter.com.                1450    IN      A      199.16.158.168

;; Query time: 146 msec
;; SERVER: 172.30.12.127#10053(172.30.12.127)
;; WHEN: Wed Aug 12 04:57:00 PDT 2015
;; MSG SIZE rcvd: 72
root@vpnsrv:~# █
```

四、浏览器相关设置（仅选择 SSL 协议或者 Shadowsocks 协议时有效，StealthVPN 协议无需设置即可直接翻墙）

如果已顺利连接上了 SSLTurbo 服务，系统本地会生成了高性能 HTTP 代理（选择 SSL 协议时）或者 SOCKS5 代理（选 ShadowSocks 协议时）服务，也提供了自动代理策略 PAC URL 服务，无论选择哪台服务器，选择那种代理策略，信息都统一如下：

本地高性能免密码输入的 HTTP 代理或者 SOCKS5 服务地址：

127.0.0.1:8848

本地自动代理策略 PAC URL 地址（PAC URL 在程序主界面也有显示）：

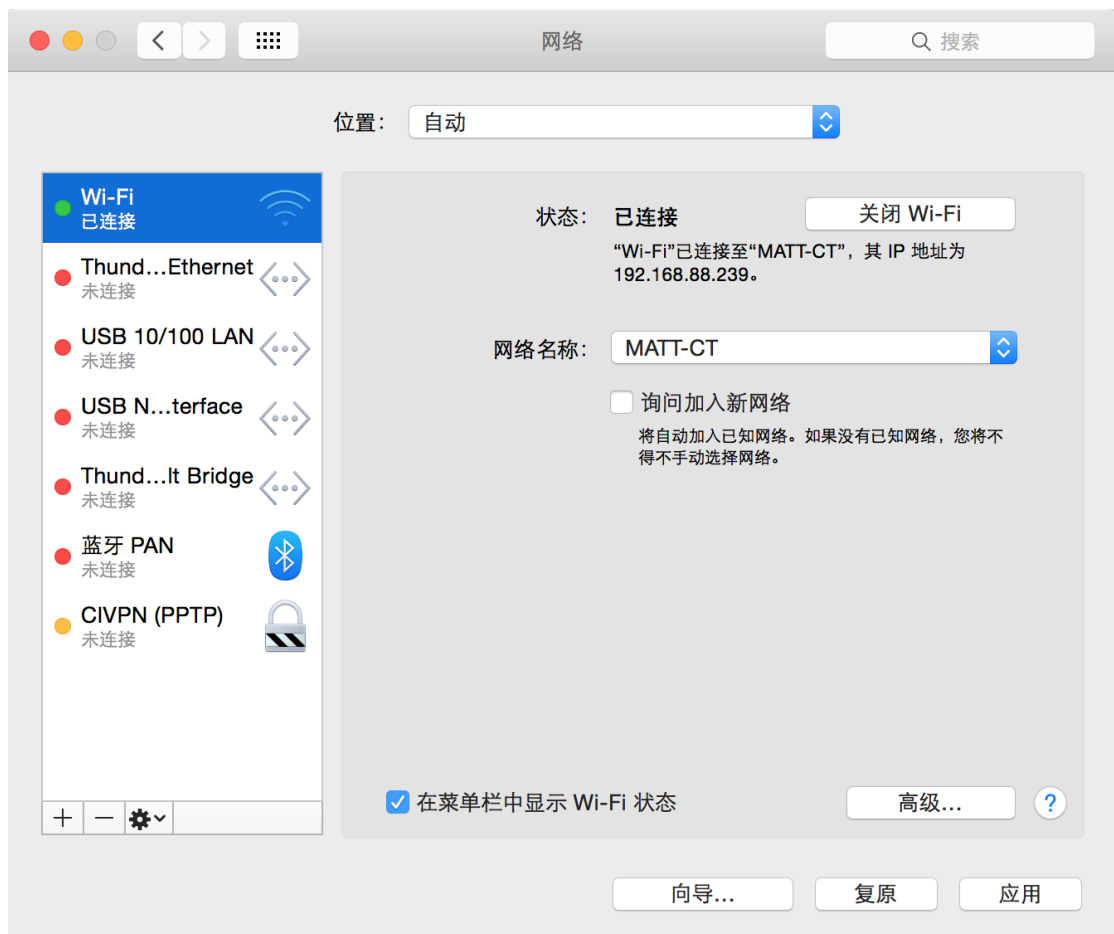
<http://127.0.0.1:8849/sslturbo.pac>

预制的 SSLTurbo 客户端默认选择了我们预定义的代理策略，即“Unblock sites”策略，稍作配置即可实现科学上网，以下分别讲述主流浏览器的配置：

（1）Safari 浏览器（系统级别自动代理）：

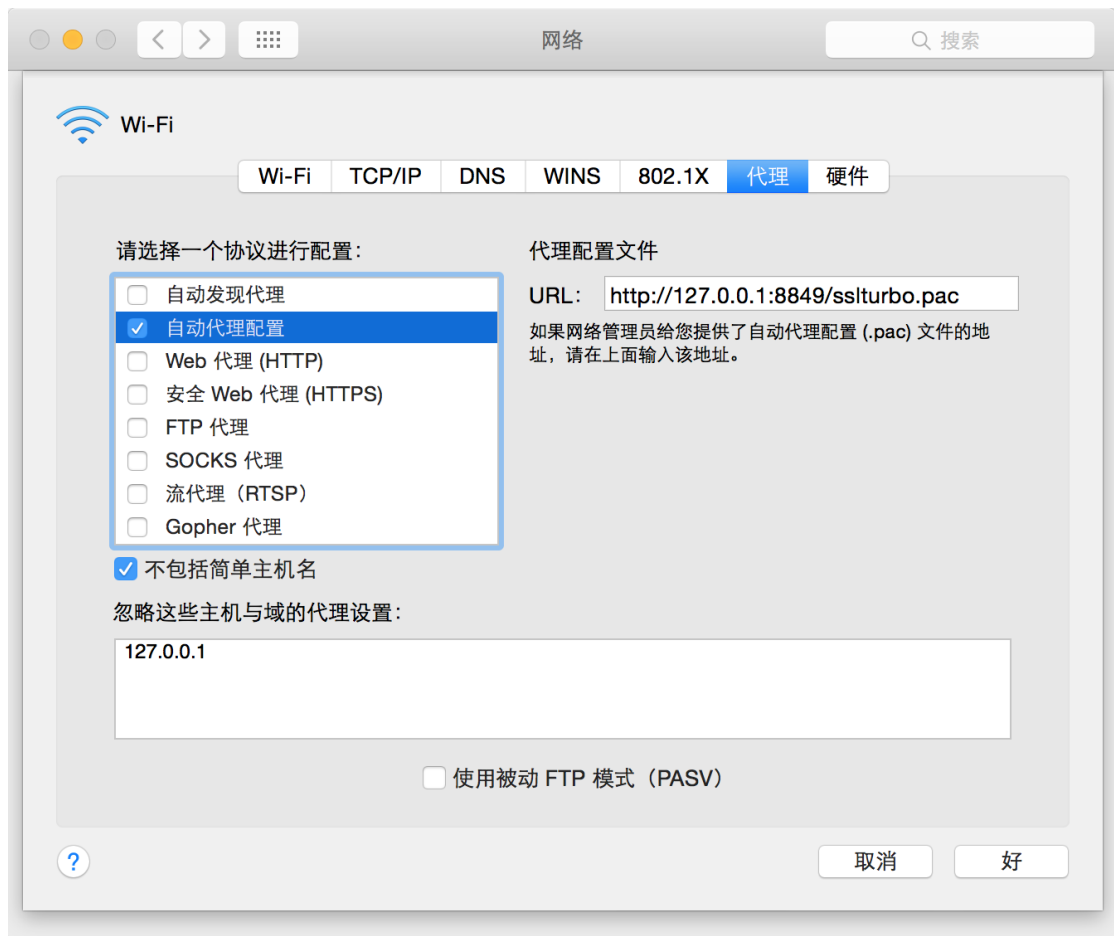
我们可以设置 Mac OSX 系统级别的自动代理，因此一旦设置完成，Mac OSX 系统中的其他程序一般可以选择自动或者可以设置成使用系统代理。

打开 Mac OSX『设置』程序，选择『网络』，左边栏选择当前活动的网络，如 WiFi，然后点击『高级』，再点击『代理』，进入代理设置页面：



勾选『自动代理配置』，在 URL 地址栏中输入：

<http://127.0.0.1:8849/sslturbo.pac>



点击『应用』退出，然后在 Safari 浏览器中输入你想访问的网站地址，比如 <https://twitter.com>，应该就可以打开了。

(2) Chrome 浏览器：

场景一：Chrome 浏览器没有安装或者禁用了任何代理类插件，比如 switchysharp 等，**适合一般用户**

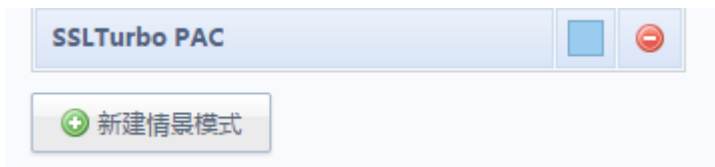
请设置 Mac OSX 系统自动代理设置，Chrome 浏览器直接就可以翻墙，网站访问限制或代理行为由 SSLTurbo 客户端中的代理策略设置而定。

方法二：Chrome 浏览器已安装了代理类插件，比如 switchysharp，**适合高级折腾用户**

在 switchysharp 插件选项设置中，选择“情景模式”：



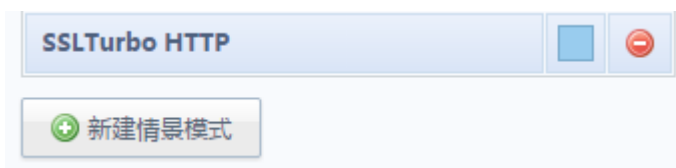
增加一个代理配置，命名为 SSLTurbo PAC:



在自动配置处填入 SSLTurbo 服务的本地 PAC URL 即可:



也可以再新增一个非自动配置的全局 HTTP 代理（如 SSLTurbo 客户端选择 Shadowsocks 协议，则为 SOCKS5 类型的代理，请注意变通），如 SSLTurbo HTTP



手工配置处，填写如下:



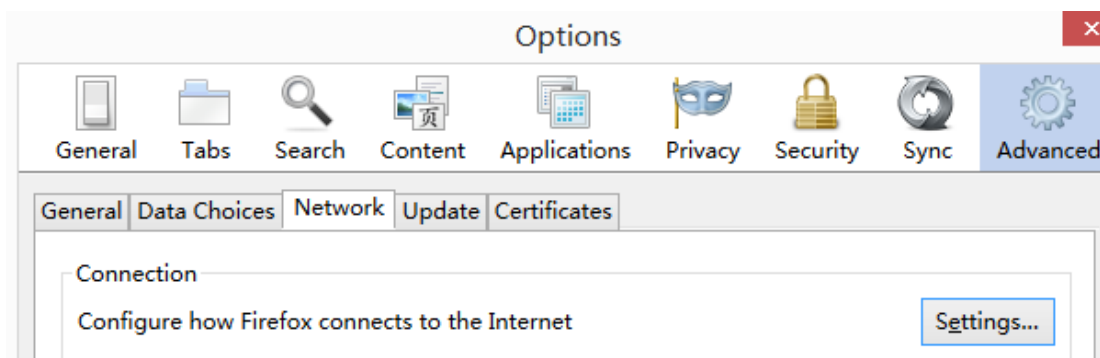
保存退出，然后通过插件选择 SSLTurbo PAC 或者 SSLTurbo HTTP 即可实现翻墙。

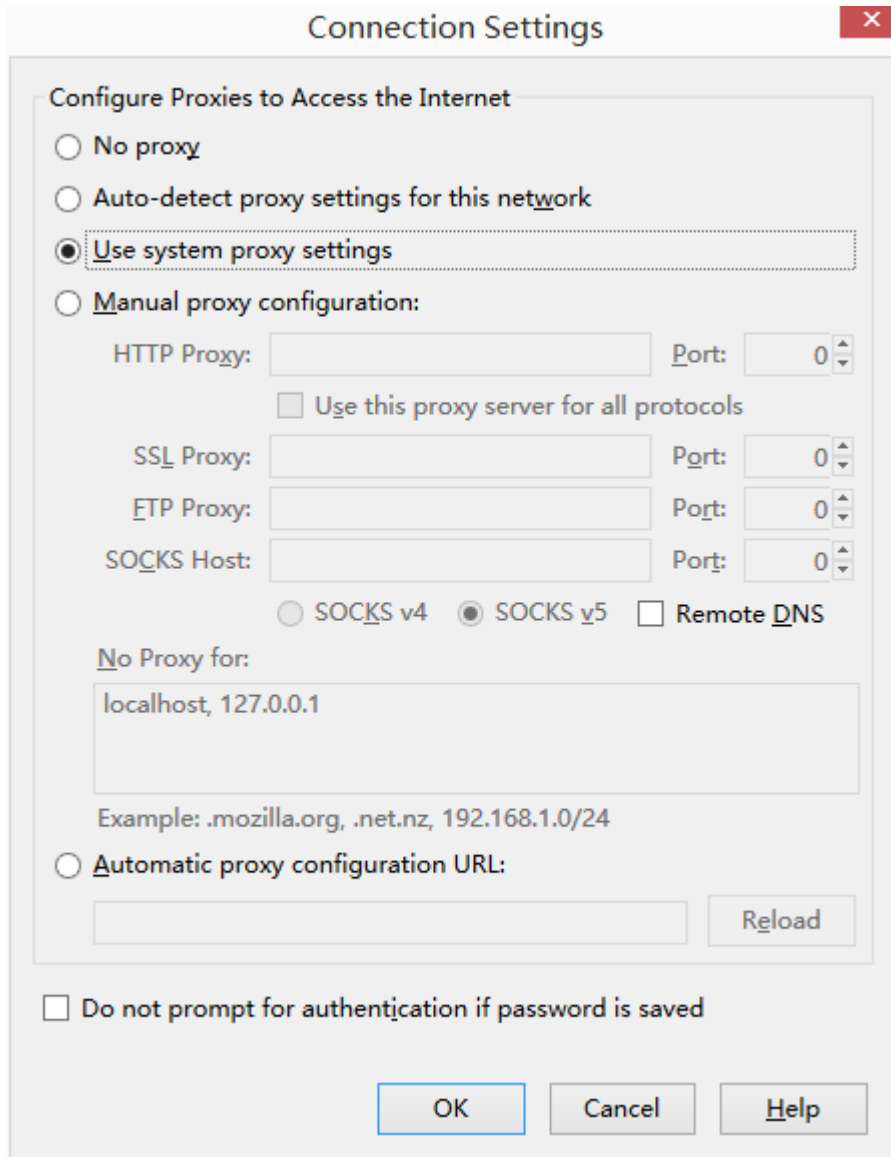
(3) Firefox 浏览器

场景一：Firefox 浏览器没有安装或者禁用了任何代理类插件，比如 AutoProxy 或者 FoxyProxy 等，**适合一般用户**

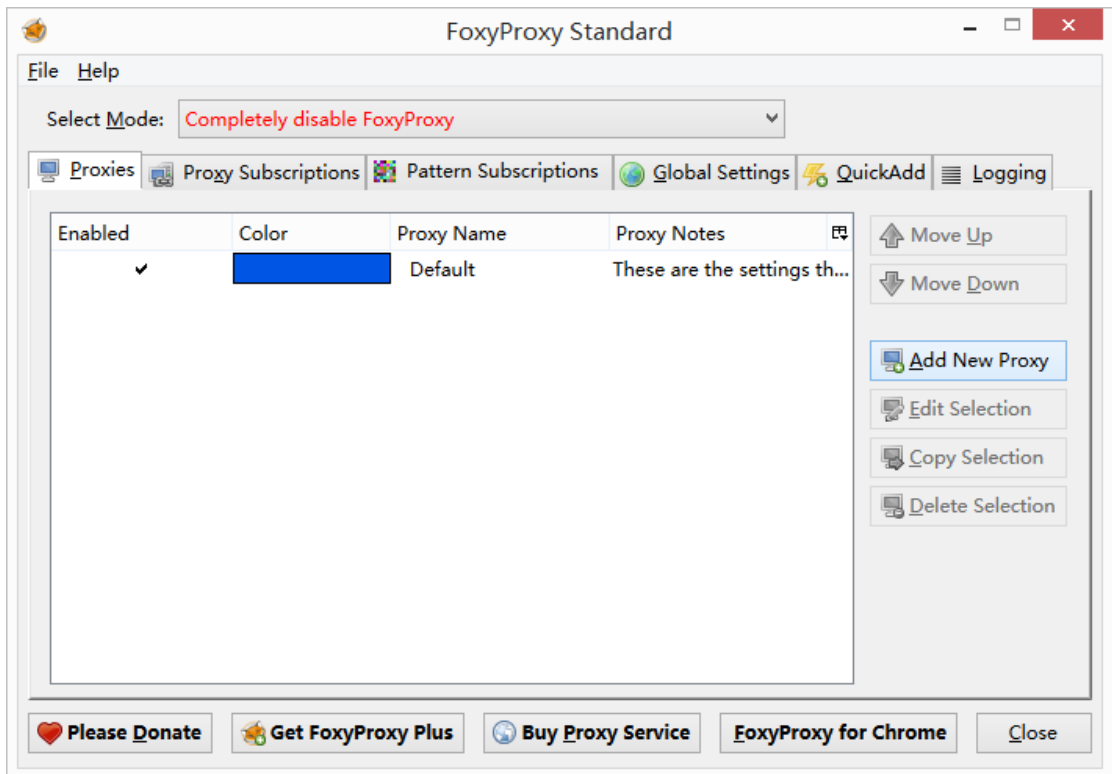
请设置 IE 浏览器自动代理地址，Firefox 浏览器直接就可以翻墙，网站访问限制或代理行为由 SSLTurbo 客户端中的代理策略设置而定。

如何确认 Firefox 使用了系统设置的自动代理，参考截图如下：



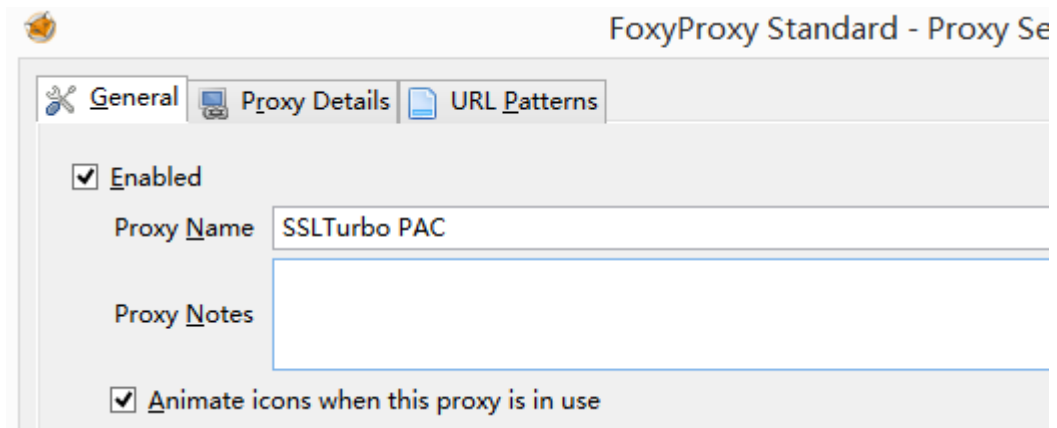


方法二：Firefox 浏览器已安装了代理类插件，比如 AutoProxy、FoxyProxy，[适合高级折腾用户](#)，以 FoxyProxy 代理插件为例，进入插件选项设置：

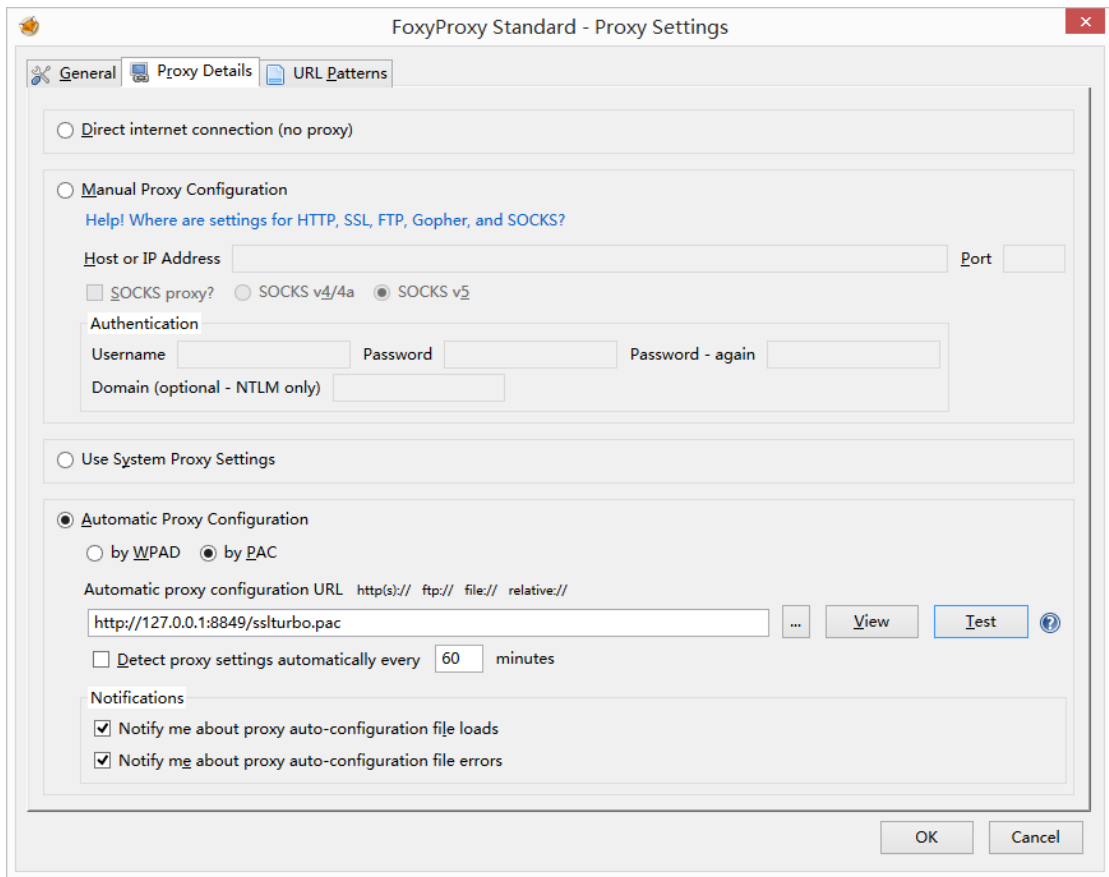


点击 “Add New Proxy”:

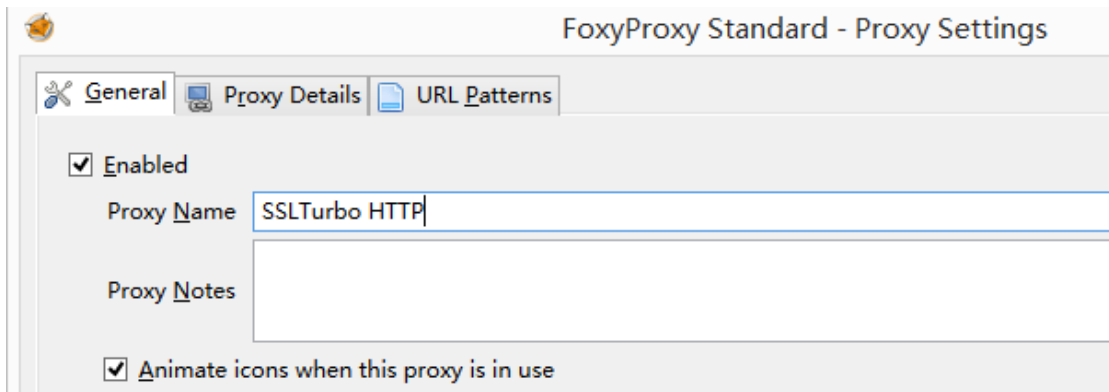
填入 Proxy Name, 如 SSLTurbo PAC



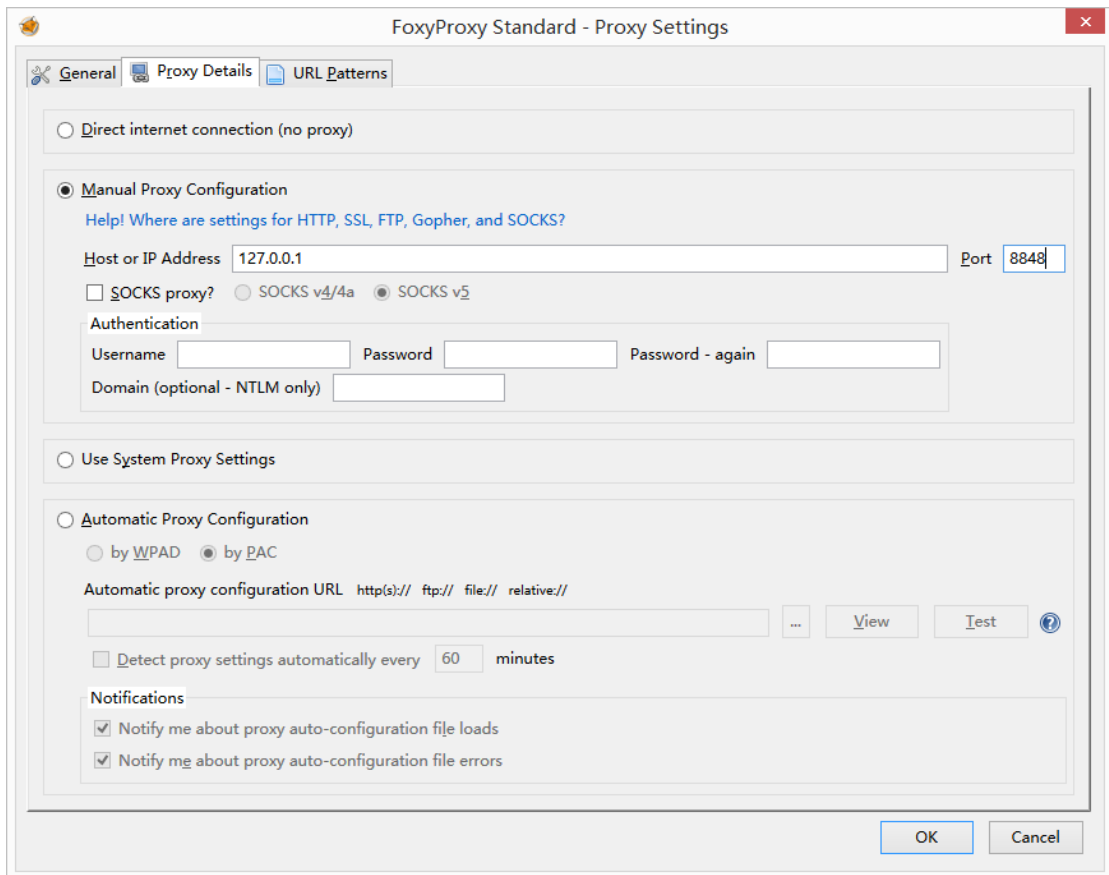
在 Proxy Detail 页面, 选择“Automatic Proxy Configuration”, 如图填入 SSLTurbo PAC URL:



也可以再新增一个非自动配置的全局 HTTP 代理（如 SSLTurbo 客户端选择 Shadowsocks 协议，则为 SOCKS5 类型的代理，请注意变通），如 SSLTurbo HTTP



在 Proxy Detail 页面，选择“Manual Proxy Configuration”，如图填入 SSLTurbo 本地 HTTP 代理地址信息即可（如 SSLTurbo 客户端选择 Shadowsocks 协议，则为 SOCKS5 类型的代理，请注意变通）：



点击确认，保存设置。

然后通过插件选择 SSLTurbo PAC 或者 SSLTurbo HTTP 即可实现翻墙。

