ProxySandbox 使用说明

简单易用的代理隧道与网络沙箱启动工具

支持系统：macOS · Windows 10/11 · Linux

一、安装与打开

系统	安装包	打开方法
macOS	`ProxySandbox.zip`	解压后将 `ProxySandbox.app` 拖入「应用程序」文件夹双击打开。 首次打开若提示无法验证开发者，可右键点击「打开」，或在终端执行 `xattr -cr /Applications/ProxySandbox.app` 后再双击。
Windows	`ProxySandbox-windows-x86_64.zip` `ProxySandbox-windows-arm64.zip`	解压整个文件夹后直接双击 `ProxySandbox.exe`（无需管理员权限）。 若系统弹出保护提示，点击「更多信息」→「仍要运行」即可。
Linux	`ProxySandbox-linux-x86_64.tar.gz` `ProxySandbox-linux-arm64.tar.gz`	解压后在终端运行 `./ProxySandbox`，程序会自动打开操作界面（也可复制终端显示的本地网址在浏览器中打开）。

二、功能展示与操作指南

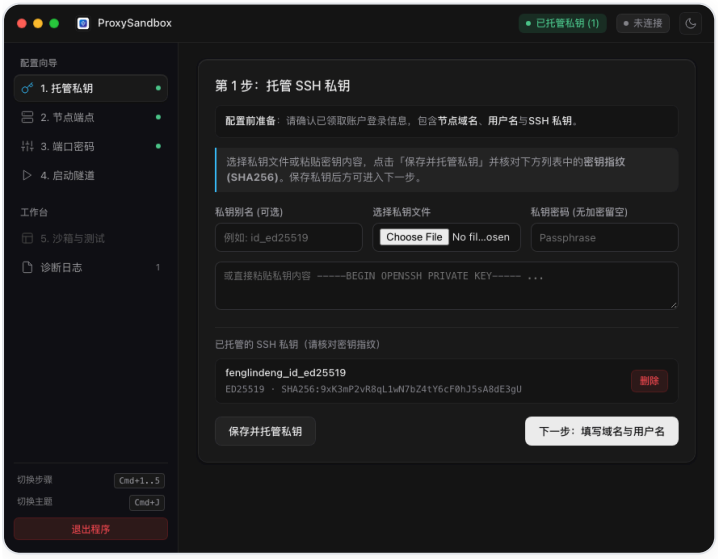

图 1：私钥托管、隧道映射与实时监控主界面

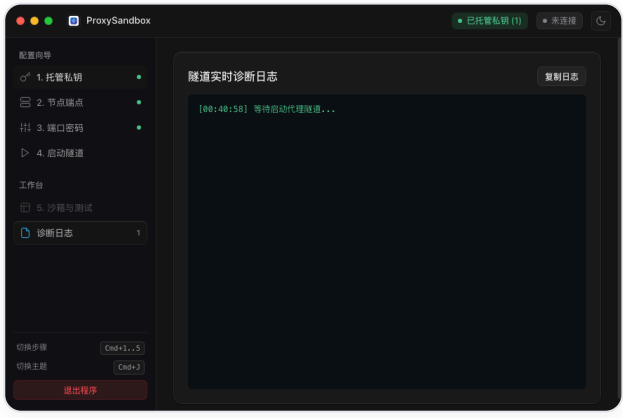

图 2：独立的「诊断日志」标签页

1. 第 1 步：托管 SSH 私钥

- **配置前准备**：请先确认已领取账户登录信息，包含：**节点域名**、**用户名**与 **SSH 私钥**。
- **添加私钥并核对指纹**：填写私钥别名，选择私钥文件或直接粘贴私钥文本；若有密码保护则填写私钥密码，点击**「保存并托管私钥」**。保存成功后请在下方列表核对密钥指纹（SHA256），确认无误后点击「下一步」。

2. 第 2 ~ 4 步：节点端点、端口密码与启动隧道

- **填写域名与用户名**：在第 2 步填写账户分配的节点域名（SSH Host）和用户名（SSH User），并确认已选中的私钥。
- **确认端口与密码**：第 3 步默认远端端口为 SOCKS5 `1080`、HTTP `8443`、SS `8388`；SOCKS5 与 HTTP 用户名密码默认留空；SS 默认加密方式 `aes-128-gcm`，密码默认 `your_secure_password`。
- **启动隧道与连通性测试**：在第 4 步核对配置摘要并点击**「启动隧道」**。连接成功后界面会自动进入第 5 步，在「隧道实时连接状态」卡片中可查看本地端口、延迟 RTT、速率与累计流量，建议点击**「测试各端口连通性」**确认端口与密码无误。

3. 第 5 步：沙箱应用启动器

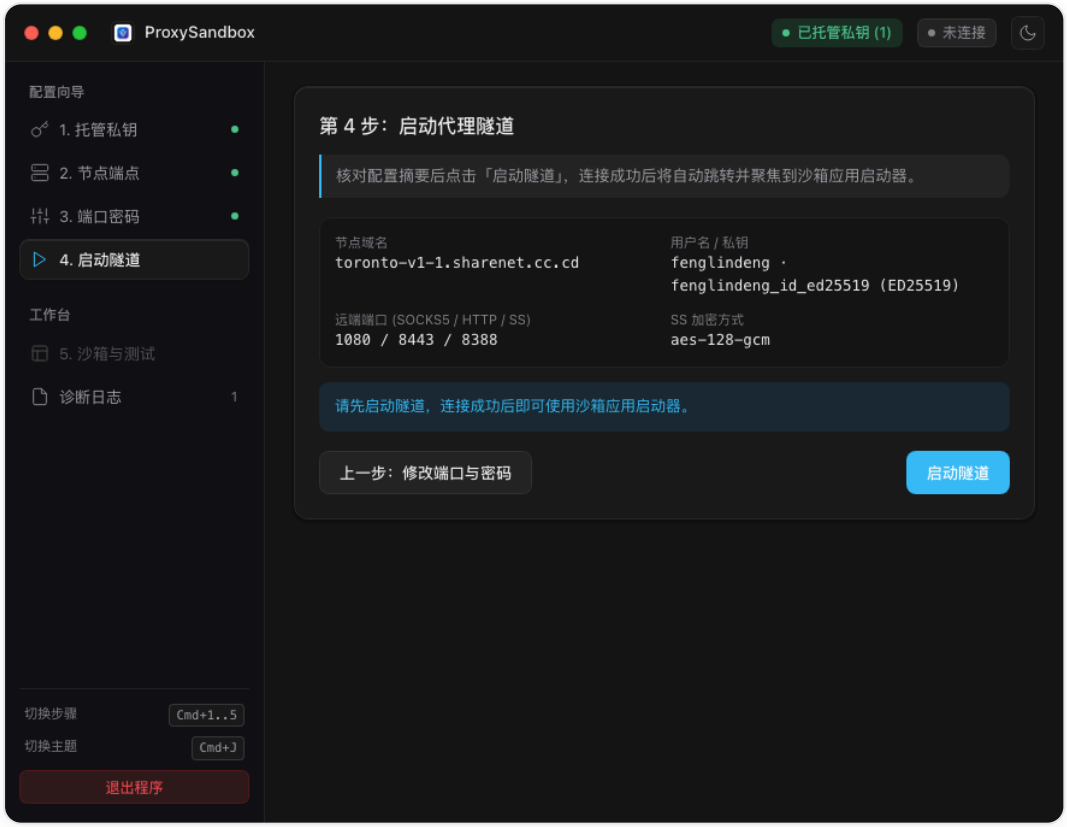

图 3：隧道实时连接状态与沙箱应用启动器（支持切换 SOCKS5 / HTTP / SS 协议）

在「沙箱应用启动器」右上角分段控制器选择沙箱应用要走的代理协议（**SOCKS5 / HTTP / SS**），然后点击对应按钮启动：

- **沙箱终端**：打开一个独立的代理终端窗口，适合在里面运行 `claude`（Claude TUI）、`curl`、`git`、`npm` 等命令，窗口内会清晰展示当前生效的代理链路。
- **沙箱 Claude Desktop**：一键以独立沙箱方式启动本机已安装的 Claude Desktop，不影响日常软件。

- **沙箱浏览器**：自动识别电脑上已安装的 Chrome、Edge、Brave、Arc、Firefox，使用独立账号与缓存目录打开，不与日常浏览器串线。
- **启动自定义程序 / 安装程序**：点击**「浏览选择...」**选择任意软件或安装包（如 `.app`、`.exe`、`.msi`、`.pkg` 等），再点击**「沙箱启动」**即可让该程序或安装过程全程走沙箱网络。

4. 诊断日志

点击左侧导航栏**「诊断日志」**，可查看连接过程、端口启动及异常提示信息，并支持点击右上角**「复制日志」**快速分享排查。

三、使用注意事项

- **先连接隧道再启动沙箱应用**：只有在隧道处于「已连接」状态时，下方的沙箱终端、浏览器、Claude Desktop 和自定义程序按钮才会启用。
- **启动沙箱版 Claude Desktop 前**：建议先彻底退出电脑上原本已打开的普通 Claude Desktop 窗口，避免新窗口被合并到未走代理的旧窗口中。
- **关闭与退出程序**：日常不使用时，直接关闭主窗口（或点击右上角红色**「退出程序」**按钮）即可自动断开所有隧道并彻底退出后台进程。
- **端口自动切换提示**：如果首选本地端口（如 1080 / 8080 / 8388）被电脑上其他软件占用，程序会自动切换到一个空闲端口，并在端口状态栏用橙色文字提示实际端口号。
- **私钥安全说明**：你托管的私钥只保存在你自己的电脑本地目录中，不会随程序安装包或压缩包传播；分享安装包给他人时，对方不会看到你的任何私钥或配置。