HOTBROWSER USER GUIDE

火特浏览器用户手册

从第一个窗口开始，到管理账号、备份数据和团队协作。每一步都说明在哪里操作、需要填写什么，以及如何确认成功。

适用版本 **0.9.0-dev** | Windows 64 位 | 更新于 2026-10-04

本手册以 hotBrowser 当前客户端和服务端为准。界面会根据账号权限、窗口状态和已安装内核显示不同操作；升级后按钮位置可能有小幅调整。

阅读目录

先完成快速上手，再按任务查阅。电子 PDF 可通过下面的目录链接或阅读器书签跳转。

1. 十分钟快速上手
2. 下载安装与升级
3. 注册、登录与密码
4. 界面、编号与列表
5. 创建一个窗口
6. 合理随机指纹
7. 代理与地区联动
8. 批量创建与账号文件导入
9. 迁移 BitBrowser 环境
10. 日常管理与批量操作
11. 密码、绑定网站与 2FA
12. 备份、导出与恢复
13. 跨机器云同步
14. 员工与团队权限
15. 扩展中心
16. 窗口同步器
17. RPA 与自动化接管
18. 内核选择与更新
19. 网站管理后台
20. 常见问题与排查

附录：术语与操作检查单、编写依据。

十分钟快速上手

hotBrowser 把每个账号的浏览器设置和网站数据放在独立的“窗口环境”中。关闭后再打开同一个编号，会继续使用该环境保存的指纹和数据。第一次使用，先完成下面这一条流程。

1. **安装客户端。**在官网点击“下载 Windows 64 位版”，运行安装包，完成后从桌面“火特浏览器”图标启动。
2. **注册并登录。**打开左侧“会员中心”，用可收信的邮箱注册；收到邮件后粘贴验证令牌，完成验证。已有账号可直接登录。
3. **准备代理。**需要代理时，先在“代理库”保存代理，或在创建窗口时直接填写。点“检测当前代理出口”，确认出口、国家和时区能正常返回。
4. **创建第一个窗口。**在“浏览器窗口”点“创建窗口”。名称可以留空；选择网站，填写账号、密码和可选的 2FA 密钥。
5. **生成并保存指纹。**在“内核与指纹”选择内核与系统类型，点“随机生成”；需要语言、时区随代理匹配时，选择“按代理出口 IP 匹配”。
6. **打开并检查。**点“保存并打开”。确认浏览器标题和工具栏中的编号，查看环境控制台的代理出口；首次登录网站仍要完成网站自己的验证。
7. **关闭并备份。**通过管理器“关闭”或浏览器关闭按钮正常关闭窗口。基础同步会自动上传，请确认成功；需要更多网站存储时开启完整同步，并按需另做本地备份。

> **判断是否完成**
>
> 窗口列表中有新编号，浏览器可以正常加载目标网站，关闭后重新打开仍能找到原数据。显示“云同步已开启”还不够，上传记录必须显示成功，另一台电脑才能下载。

1
建窗口
账号与独立数据

2
配代理
检测真实出口

3
定指纹
保存后持续使用

4
关窗同步
检查成功状态

下载安装与升级

新用户安装

1. 进入 hotbrowser.cc 官网，下载 Windows 64 位安装包。当前公开下载版为 `0.9.0-dev` 内测版，面向 Windows 10/11。
2. 运行安装包，按照向导完成安装。若出现安装许可提示，核对安装来源与文件名称后继续。
3. 从桌面或开始菜单的“火特浏览器”快捷方式启动。正常情况下先出现管理器，再由管理器打开具体环境浏览器。
4. 打开“会员中心”登录，然后检查“内核设置”。缺少所需内核时先检测并下载安装。

安装版运行不需要另行安装开发工具或在 WSL 中执行编译命令。macOS Apple Silicon 和 Intel 属于后续发行目标；截至本手册更新日，官网没有可供用户安装并验收的正式 Mac 版本。

升级已有客户端

1. 正常关闭所有环境；已开启云同步的环境等待上传完成。
2. 对重要数据做一次备份，尤其是尚未上传的本地环境与账号凭据。
3. 安装新版并重新启动；核对版本、环境数量、常用编号、代理和内核。
4. 先打开一个环境确认正常，再恢复批量运行。

升级后环境列表变空，怎么办？

安装目录与数据目录是两回事。新安装版默认使用当前 Windows 用户的 `%LOCALAPPDATA%\hotBrowser` 数据区；旧独立部署可能使用 `C:\hotBrowser-native\data\manager`。启动到了另一套目录，界面就会显示另一套环境库。换会员账号也会改变可见记录。

> **先确认数据位置**
>
> 先核对 Windows 用户、登录会员和管理器正在读取的数据目录。不要因为列表空就删除旧目录或重新导入同一批账号。沿用旧数据需保留环境库、账号密钥和用户目录；如需绑定旧部署，按安装维护人员提供的迁移方案操作。

旧独立部署的启动方式

此前部署在 `C:\hotBrowser-native` 的源码管理器，可双击该目录里的 `start-hotbrowser.cmd` 或 `start-hotbrowser-native.cmd`。这是已有开发部署的入口；安装版用户应优先使用桌面快捷方式。避免同时启动两套管理器读写同一套环境数据。

---

03 / 账号

注册、登录与密码

用邮箱注册

1. 打开左侧“会员中心”，点“邮箱注册”。
2. 填写可正常收信的邮箱、至少 12 位密码和确认密码，点“发送验证邮件”。
3. 查看收件箱和垃圾邮件。将邮件中的一次性验证令牌粘贴到“验证注册邮箱”页面，点“验证并登录”。
4. 会员中心显示当前会员、有效期和额度，才表示账号已创建并登录。新注册团队永久免费获得 200 个环境和 3 个成员名额（含本人，可再添加 2 名员工）。环境额度由团队共享；已有其他授权保留，以会员中心显示为准。

发送验证邮件不等于注册完成。令牌失效时回到注册页重新填写密码发信，使用最后一次收到的令牌；重新提交注册会更新尚未验证的密码。

已有账号登录、切换和退出

在会员中心输入会员邮箱和密码，点“登录或切换会员”；历史用户名账号可继续使用原用户名登录。退出时点“退出登录”。切换、退出和改密前先关闭所有运行环境，并完成待上传的同步。

会员登录决定环境可见范围、启动授权和团队权限。**会员密码不是环境内 Gmail、Facebook 等网站的密码**，也不是网站管理后台的管理员密码。切换会员不会把旧会员的环境自动转给新会员。

忘记密码

1. 点“忘记密码”，填写已验证的注册邮箱，发送重置邮件。
2. 收到邮件后点“已有重置令牌”，粘贴令牌，填写并确认新密码。
3. 重置成功后重新登录；该会员在所有设备上的旧登录令牌都会失效。

页面对存在和不存在的邮箱显示相同提示，不能仅凭“已发送”判断账号是否存在。重置令牌有效期为 30 分钟，一次有效；重复申请后应使用最新邮件。没有绑定邮箱的旧用户名账号，需要联系管理员处理。

主动修改密码

登录后点“修改密码”，输入当前密码和至少 12 位的新密码。完成后全部设备需重新登录。此操作修改 hotBrowser 会员密码；不会自动修改各网站的登录密码。

> **收不到邮件**
>
> 确认邮箱拼写、垃圾箱与最后一次提交时间，避免连续重复提交。若提示“邮件服务不可用”，需要管理员检查发信服务；客户端无法生成一个可替代邮件令牌的验证码。

---

04 / 界面

界面、编号与列表

左侧页面	主要用途
首页	查看概览、最近使用，进入创建、导入等常用操作。
浏览器窗口	创建、搜索、打开、编辑、批量操作、导出和查看云环境。
分组与标签	按项目、用途或状态整理本机窗口。
代理库	保存、导入、搜索和选用代理。
窗口同步器	把主控窗口的操作发送给选定的被控窗口。
RPA 自动化	保存流程、执行任务和设置本机定时计划。
扩展中心	选择、导入、安装、更新和分配扩展。
会员中心	注册、登录、退出、查看会员状态、修改密码。
员工与权限	管理团队成员、团队组和授权。
内核设置	查看已安装内核和检测在线更新。

编号是日常识别的主线

名称可以留空。列表、浏览器标题、工具栏编号和 Windows 任务栏标识帮助你分辨不同环境。新建和批量导入按当前活动环境的空缺编号优先分配，例如当前有 1、2、3、4、7、8、9、11，下一批依次使用可用的 5、6、10、12……。移入回收站后原编号可以被新建环境使用；恢复时原编号若已被占用，会重新分配空缺编号。

本机编号、原版来源编号和环境唯一 ID 用途不同。“原版 9 号”导入后可能显示为 hotBrowser 的另一个编号；跨机器同步通过环境唯一 ID 对应数据，两台电脑显示的本地编号可以不同。

搜索、分页和选择范围

1. 先选择“全部”“已打开”“已关闭”或“常用”，再按分组、标签和代理筛选。
2. 高级筛选可按编号范围、平台账号、代理主机和平台检索；起始编号不要大于结束编号。
3. 列表翻页只改变当前显示页。勾选可能跨页保留，执行批量操作前核对“已选数量”和筛选外已选提示。
4. 表头全选用于当前页；“选择当前筛选全部”用于整个筛选结果。要重新选一批记录，先“清空选择”。
5. 使用列设置隐藏次要列，保留编号、窗口、状态和操作。显示设置记在当前设备上。

首页“最近使用”用于快速定位某个环境。若看起来只剩一条，先检查当前搜索和筛选，点“重置全部筛选”，再确认当前会员。

浅色和深色主题

使用客户端顶部“外观”选择浅色、深色或跟随系统。主题改变界面颜色，不修改指纹、代理或网站数据。

---

05 / 环境

创建一个窗口

入口：浏览器窗口 → 创建窗口

创建页分为“窗口信息”“代理网络”“内核与指纹”“高级设置”“确认配置”五步。可以逐步填写，也可返回前面的步骤调整。

第一步：窗口信息

项目	怎么填写	填完后有什么作用
窗口名称	可留空；需要说明用途时再填写。	编号始终用于辨识环境。
分组、标签、备注	例如“美国项目”“待登录”。	方便筛选和批量管理。
平台 / 网址	选预设网站，或选择自定义平台并填完整 HTTPS 网址。	绑定账号，作为平台页和辅助填入的匹配依据。
账号、密码	填写该网站的真实登录资料。	保存到 hotBrowser 账号记录；开启原生密码保存后写入该环境密码管理器。
2FA 密钥	填写 Base32 密钥或受支持的 `otpauth://totp` 地址。	生成动态验证码；不能填一个临时的六位验证码作为密钥。

项目	怎么填写	填完后有什么作用
校验重复项	新建默认开启。	阻止重复平台账号；检查报错后再决定是否确实需要重复环境。
打开指定网址	每行一个完整网址，可填写多个。	启动时打开工作页面。
Cookie	仅在有合法、有效数据时导入；不了解时留空。	预置网站数据，是否能登录由网站决定。

第二步：代理网络

选择代理库记录或填写协议、主机、端口、用户名、密码。点“检测当前代理出口”，检查结果。需要语言和时区联动时选择自动地区模式，详见代理设置。

第三步：内核与指纹

选择已支持的内核系列和设备系统，再点“随机生成”。检查系统、UA、CPU 线程数、内存、屏幕、语言、时区等是否符合用途。这里生成的是一组保存参数，重新启动不会重新抽取，除非你主动编辑或再次随机。

第四步：高级设置

按需设置窗口尺寸、标签页恢复、下载目录、密码管理器、图片与 JavaScript、通知、声音等。**普通新建默认使用自动模式，保留本地自动化通道；手动登录模式是用户可选择的特殊模式。**勾选手动登录后，CDP 自动化、窗口网页同步、自动 2FA 辅助和管理器标签恢复将不可用；原生密码管理器仍可使用。

“启动前清 Cookie”会删除登录 Cookie；“清理缓存”主要针对可重建文件，两者影响不同。要保留网站状态，不要把清 Cookie 当作日常加速按钮。

第五步：确认并保存

1. 检查平台、网络、指纹和高级设置摘要。摘要不会显示明文密码或密钥。
2. 点“保存”只建记录；点“保存并打开”先保存，再尝试启动。
3. 若提示“已保存，但打开失败”，该环境已经存在。修正错误后重试打开，避免再次创建重复记录。

编辑已有环境

先关闭环境，再点“编辑”。密码和 2FA 字段留空表示保留旧值；要删除需勾选对应的清除选项。填写新值并保存后，后续启动使用新配置。指纹、代理、内核的大幅变更可能让网站重新验证登录，调整前先备份。

---

06 / 指纹

合理随机指纹

随机指纹需要一组相互匹配的参数。例如 Windows 的系统标识应与 Windows UA 搭配，移动设备的触摸、屏幕和移动 UA 需要相互一致。hotBrowser 从当前可用的指纹样本与生成规则中组合设备参数，并为各环境保存独立噪声种子。

推荐的生成顺序

1. 先选择内核系列，例如 153 或 148。
2. 选择 Windows、Android 或 iOS 设备类型；移动类型属于桌面 Chromium 的移动模拟。
3. 确定代理和地区策略，再点“随机生成”。
4. 检查 CPU 线程数、内存、屏幕与 GPU 搭配；需要固定某项时手动调整并检查合理性。
5. 保存环境，并从真实浏览器中打开“指纹检测页”查看实际返回值。

参数	用户应了解的含义
UA、platform、vendor	网站看到的浏览器与系统身份，需要与所选内核、系统类型协调。
CPU / 硬件并发	表示网站可见的逻辑线程数；不是给环境限制 CPU 使用率。
设备内存	网站可见的设备内存参数；不是预先为环境分配同等大小的内存。
屏幕与像素比	包括屏幕尺寸、可用区域、DPR 和色深；浏览器窗口实际大小是另一个设置。
语言、时区、地区	可手动指定或随启动前检测的代理地区联动；不是网站显示语言的绝对保证。
Canvas、WebGL、Audio、ClientRects	按该内核支持的方式施加持久参数或噪声；是否生效要看浏览器检测结果。
WebRTC、公开 IP	控制相关网络暴露策略；不能通过填写一个 IP 替代真实代理出口。
触摸参数与移动屏幕	用于 Android / iOS 模拟；仍在电脑上的 Chromium 中运行。

什么时候可以重新随机？

为一个全新账号准备环境时可以多次随机挑选。已经长期登录的环境应尽量保持已保存身份；不要每次启动都重新随机，也不要认为指纹越频繁变换越稳定。克隆时“同指纹”与“随机指纹”用途不同，创建另一套独立设备时选择随机克隆。

指纹库和真实结果

客户端登录后可更新服务端提供的样本库。样本总数、所选系统和内核筛选后可用数量会随库更新变化，本手册不把某个数量写成永久值。创建页预览是配置，检测页才是当前浏览器对网页暴露的结果；发现不一致时记录编号、内核版本和检测字段。

> **移动环境的含义**
>
> Android / iOS 模式用于移动网页的设备模拟，不会安装 Android 系统或真正的 iPhone Safari。iOS 的系统服务、Safari WebKit 行为、硬件证明和原生 App 能力不能由 Chromium 参数完全等同替代。

---

07 / 网络

代理与地区联动

先分清代理端点和真实出口

代理端点是你连接的服务器地址，例如 `global.rotgb.711proxy.com:10000`；真实出口是网站看到的公网 IP。同一个网关可以按连接轮换很多出口。因此“固定代理”只表示主机和端口固定，不保证整个浏览过程使用同一公网 IP。

填写一条代理

入口：创建 / 编辑窗口 → 代理网络；或代理库 → 保存后选用

1. 选择 HTTP、HTTPS、SOCKS5 或受支持的 SSH 代理类型。协议必须与供应商给出的连接方式一致。
2. 主机填域名或 IP，端口单独填数字。例如主机 `global.rotgb.711proxy.com`，端口 `10000`，开头的 `g` 不要漏掉。
3. 认证用户名、密码分别填写；供应商允许白名单免认证时才可留空。
4. 也可以在“粘贴代理”中输入下方格式，然后核对自动解析结果。
5. 点“检测当前代理出口”；需要联动时点“检测并匹配指纹地区”。成功后再保存。

```
proxy.example.net:10000
proxy.example.net:10000:代理用户名:代理密码
http://代理用户名:代理密码@proxy.example.net:10000
socks5://代理用户名:代理密码@proxy.example.net:1080
```

以上示例中的地址和凭据需替换成你的真实代理。URI 形式中若用户名或密码含 `@`、`:` 等特殊字符，使用供应商提供的正确转义链接，或改用分开的字段填写。

从代理库使用

1. 在“代理库”保存或导入代理，设置易辨认的名称。
2. 创建单个窗口时点“从代理库选用”，搜索后确认，字段会复制到窗口配置。
3. 批量创建或账号导入时，选择统一使用、逐个分配或循环分配；逐个分配的代理数需与账号数相等。

库代理保存到窗口时会复制参数。以后修改或删除代理库记录，不会自动覆盖已有窗口的代理；已有窗口需要单独或批量编辑。

语言、时区随出口匹配

选择“按代理出口 IP 匹配”后，保存和启动时通过环境代理检测国家和时区，更新对应语言、地区参数并用于该次启动。GeoIP 结果来自检测服务的地区库，可能存在供应商标注和地理库之间的偏差。

选择“手动设置”时使用你保存的语言和时区。导入原版环境需要保留原身份时，先确认其地区策略，不要把自动联动当作默认必须开启的选项。自动模式检测失败或缺少有效时区时会提示错误，需要修正后继续。

粘性会话、动态代理与启动拦截

如果登录操作需要出口稳定，在代理供应商处生成粘性会话凭据。例如 711Proxy 可使用供应商定义的 session 与 sessTime 参数设置 30 分钟会话；相同窗口保留相同 session。到期、线路故障或供应商策略变化仍可能换 IP，hotBrowser 不会替供应商永久锁住出口。

动态提取模式填写供应商 API 提取链接；启动前提取并检查有效的端点，可按设置复用上次端点。不要把提取 API 链接填到固定代理的“主机”里。SSH 当前支持密码认证，不能在密码字段填 SSH 私钥文件。

“网络异常阻止启动”“IP 变化阻止启动”“国家变化阻止启动”分别针对不同问题。启用后触发规则会停止启动并说明原因；配置了代理时不应通过静默直连掩盖连接失败。

看懂环境控制台的代理信息

- **代理端点：**保存的网关连接信息。
- **启动前检测的出口：**最近启动检测得到的公网 IP。
- **地区、出口时区、检测时间：**该次检测返回的结果。
- **未检测：**还没有有效结果；不能解释为“代理肯定可用”。关闭后检查并重开，必要时手动检测。

这个结果是启动前最近一次检测，不代表后续每个网页请求都使用同一 IP。旋转代理尤其要区分这两件事。

---

08 / 批量

批量创建与账号文件导入

入口：浏览器窗口 → 创建窗口右侧下拉箭头

选择适合的创建方式

方式	适合什么情况
批量创建窗口	准备一批新环境，统一设置平台和规则，每个环境生成独立指纹。
导入账号文件	已有每行一个账号的 TXT / CSV / TSV，识别账号、密码与可选的 2FA。
批量导入表格	已有符合导入列定义的 CSV / XLS / XLSX / XLSM 配置表。
导入现有环境	已有 hotBrowser 备份或 BitBrowser 的配置及用户数据。
克隆选中窗口	复用已有配置，选择保留或重新随机指纹；复制网站数据需另看备份范围。

按行导入账号：完整步骤

1. **选择文件或粘贴。**支持 UTF-8、带 BOM 的 UTF-8 和 GB18030；一次最多 100 个账号、1 MB。先用几条测试格式，再处理大批次。
2. **检查识别。**预览显示账号、密码是否识别、2FA 是否识别和错误行号。密码与原始密钥不会直接展示。
3. **选择要导入的行。**默认选择成功识别的账号；可单选、全选、取消全选、反选。最终勾选数就是本次创建数。
4. **确认平台。**常见邮箱可给出平台建议；普通账号和其他域名应主动选择正确平台。一个批次使用所选平台，需要多个平台时分批处理。
5. **配代理。**可统一一条、逐行一对一、循环分配，或从代理库选择并分配。逐行模式数量必须与勾选账号数一致。
6. **生成指纹。**选择系统、内核、地区策略，生成并检查每条预览。重新随机后以最终预览为准。
7. **确认默认选项。**账号文件导入默认使用自动模式、校验重复账号，并启用首次打开保存到浏览器密码管理器。若选手动登录，则自动化及 2FA 页面辅助不可用。
8. **创建并检查。**提交后核对新增编号、账号、代理和指纹；首次打开时检查密码管理器写入。登录会员后，符合权限条件的环境会自动进行基础云同步，可在任务与云环境中查看进度。

可直接使用的文本格式

简单三列可以不带表头；复杂文件建议加表头，明确哪一列是 2FA，避免把辅助邮箱、国家码或应用密码识别为密钥。

```
username,password,twoFactorSecret
person1@example.com,"示例密码-A",JBSWY3DPEHPK3PXP
person2@example.com,"示例密码-B",
```

```
账号|密码|2FA密钥
账号|密码|辅助邮箱|2FA密钥|其他附加列
账号----密码----2FA密钥
```

示例账号、密码和密钥仅用于演示格式，不对应可登录账户。支持 Tab、分号等分隔符；可手动选择分隔符。Base32 密钥或受支持的 SHA1、6 位、30 秒 TOTP 地址均可使用。

哪些列不会导入？

供应商文件中的辅助邮箱、国家标注、尾部应用密码等附加列会按当前解析规则忽略，预览说明忽略项数。主账号、网站登录密码和 2FA 才是账号记录的核心字段。必须保存附加业务资料时，先整理成备注或另建工作表。

重复或识别失败怎么处理？

文件内重复、无效密钥、格式错误或超限会阻止整批提交，不会悄悄跳过坏行。出现“多个可能的 2FA 字段”时，加上 `username,password,twoFactorSecret` 表头并只保留明确字段，或调整列布局。已有同平台同账号默认去重，确实要重复创建时才主动允许已有账号。

取消勾选某行后，代理按剩余账号的原文件顺序重新分配。比如选第 1、3 行，第一条代理给第 1 行，第二条给第 3 行；不是继续给未选行占位。

普通批量创建与表格导入

普通批量创建可设置数量、分组、平台、代理、内核与指纹生成规则；一次最多 100 个。名称前缀可留空，系统按可用编号分配。表格导入先查看当前客户端提供的列定义与预览，核对内核、代理和地区设置再提交；配置表不是浏览器用户数据备份。

---

09 / 迁移

迁移 BitBrowser 环境

入口：创建窗口下拉 → 导入现有环境 → 自动扫描 BitBrowser；或选择配置 / 压缩包

导入前准备

1. 在原版客户端正常关闭要迁移的窗口，确保用户数据已保存；不要两个管理器同时读写原目录。
2. 先在原版导出或复制一份原数据备份，保留来源编号和账号对应表。

3. 在 hotBrowser 登录有权限的会员，并安装目标内核。首次先迁移一个窗口验证，再批量迁移。

自动扫描与选中导入

1. 运行本机 BitBrowser 扫描，查看识别到的环境列表。
2. 按原版来源编号、账号或名称找到目标，勾选需要的记录。来源编号 9 和“列表顺数第 9 个”不是同一种选择方式。
3. 核对平台、代理认证、指纹、目标内核以及用户数据路径。
4. 确认导入范围。只有配置就只能恢复设置；要迁移网站数据，必须同时取得对应用户数据。
5. 导入后查看 hotBrowser 新分配编号与来源信息，在新窗口检查网络、密码库、Cookie 和必要页面。

扫描不到时先检查：是否在安装 BitBrowser 的同一 Windows 用户下、是否有可读取的原目录、数据是否只在原厂云端、本机是否曾下载过该环境。hotBrowser 的本机扫描不能代替登录原厂云端下载所有记录。

导入以后使用哪套服务？

可转换的 BitBrowser 配置会转为 hotBrowser 环境配置，后续由 hotBrowser 的会员、签名和内核服务管理。来源配置、账号保险库和浏览器用户数据在迁移中承担不同作用，缺少必要部分都可能影响恢复结果。

BitBrowser 桌面环境导入当前默认使用手动登录模式，关闭 CDP、账号自动填入和管理器标签恢复，以保留原生用户数据中的会话。需要自动化、窗口同步器或 2FA 页面辅助时，关闭环境后在高级设置取消手动登录模式并重新打开。移动模拟需要控制通道，不使用这个桌面导入默认值。

为什么网站仍然要求重新登录？

“标签页恢复”“Cookie 成功复制”“网站认可原会话”是三个不同结果。网站可能因 Cookie 过期、IP 变更、设备参数、内核变化、风险检查或机器绑定数据，要求新登录。hotBrowser 不能保证 Gmail 或其他网站把 148 到 153、或跨电脑访问判定为同一台设备。

为提高可恢复性，迁移时尽量保留整个必要持久化范围、原代理会话和稳定指纹；先用相同主版本验证。切换主版本不应直接共用同一个浏览器数据目录，详见内核更新。

> **保留原数据直到验收完成**
>
> 确认网站能正常使用、需要的账号资料和业务状态存在、重新打开后仍正常，再决定清理旧环境。一次启动成功并不能代表原账号登录和全部应用数据已经恢复。

日常管理与批量操作

单个窗口的常用操作

列表右侧“打开 / 关闭”“编辑”和“⋯”提供当前可用动作。运行中的窗口可置前、重开；自动模式还可管理标签页、打开网址、读取 Cookie、保存会话、截图。更多菜单提供账号复制、2FA、指纹检测、备份、云同步、克隆和移入回收站。

同一环境不能重复打开。正常关闭后，等状态显示“已关闭”；云同步环境还要等待上传完成。配置修改建议关闭后进行，运行中的窗口不会自动应用所有编辑结果。

批量操作的顺序

1. 先筛选，再选择目标；需要所有页时点“选择当前筛选全部”。
2. 核对选中数量，确认有没有筛选之外仍被选中的窗口。
3. 执行打开、关闭、编辑、云同步、导出、分组、标签、排列或回收站操作。
4. 查看逐条结果，区分成功、失败、跳过；只针对失败记录重试。

批量打开使用启动队列，可设置间隔。停止队列只阻止后续启动，不会关闭已启动窗口；正在进行的单次启动可能完成。电脑资源不足时减少同时运行数，不要把网页卡顿都归因于指纹参数。

批量编辑不会默认覆盖所有字段

批量编辑一次最多 100 个环境。勾选要修改的字段，先预检，再提交；未勾选字段保留原值。目标窗口必须关闭。统一改代理会替换所选连接和凭据；批量改平台名称 / 地址不等于给每条窗口写同一个账号密码。

分组、标签、常用与窗口排列

本机分组用于分类，一个窗口可配合多个标签。设为常用后在“常用”筛选中快速查看。平铺、对角线和统一大小用于整理已运行窗口，可设置起点、尺寸、列数和间距；Windows 屏幕缩放和浏览器最小尺寸可能限制实际布局。

清理哪些数据？

缓存清理主要处理网页资源、脚本编译、GPU 缓存等可再生成数据。Cookie、Local Storage、IndexedDB、扩展数据和 Service Worker 中可能有登录状态或未同步业务数据，不能一律当作垃圾。先看类别和占用，再选择清理范围。

回收站：删除与永久删除

1. 关闭目标窗口，在更多菜单或批量工具栏选择“移入回收站”。
2. 回收站可按编号、名称或备注搜索，勾选后批量恢复。
3. 确认不再需要时才永久删除；永久删除会清理对应用户目录，不能靠本机回收站再次恢复。

移入回收站保留数据，不等于释放磁盘；本机回收站恢复、云历史版本恢复和独立 ZIP 备份是不同的恢复路径。

密码、绑定网站与 2FA

账号资料分别保存在什么地方？

位置	保存什么	用来做什么
hotBrowser 窗口账号记录	平台、用户名、网站密码、原始 2FA 密钥。	绑定网站、受控复制、动态码生成和凭据导出。
环境浏览器密码管理器	浏览器保存的网站用户名与密码。	网站登录表单的原生密码选择与填入。
Cookie 与站点存储	网站登录令牌、设备标识、业务数据。	由网站判断是否保留登录和其他状态。

输入账号密码无法生成一份已经登录的 Cookie。首次登录必须完成网站的真实身份验证。更改网站密码后，不要假定浏览器密码管理器与 hotBrowser 账号记录会同步更新；检查两处保存内容，必要时编辑窗口记录。

原生密码保存与辅助填入

1. 创建或导入时启用“首次打开时将账号密码保存到浏览器密码管理器”，并保持高级设置里的密码管理器开启。
2. 首次启动由内核写入原生密码记录。到网站登录页，可使用浏览器提供的用户名 / 密码选项。
3. “填入平台账号”用于当前可识别、与绑定网站匹配的登录表单；填写后由用户检查并提交。

这不是全网站自动登录承诺。网站分步登录、自定义表单或风险策略可能要求手工输入。浏览器仍提示“保存密码”时，确认实际登录用户名、网址范围和保存记录；不要因为密码字符串相同，就假定浏览器认定它是同一登录项。

环境控制台 / 绑定页面

入口：窗口“⋯” → 环境控制台（绑定网站与 2FA）

管理器为当前运行环境生成本机控制台入口。页面展示绑定网站、可复制的账号、代理检测和 2FA 动态码等；敏感操作需要有效的环境授权。不要把带临时授权的完整链接当作可长期保存的公共网址，窗口关闭或管理器重启后，应从管理器重新打开。

本机控制台的 `127.0.0.1` 地址只代表当前电脑。它不是官网管理后台，也不能复制到另一台电脑直接访问该环境。

保存并查看 2FA

1. 创建或编辑窗口时填写该网站的 TOTP 密钥；编辑留空保留旧值。

2. 从控制台或窗口更多菜单复制当前六位验证码，在有效期内提交给网站。
3. 要备份原始密钥，点“查看/复制原始 2FA 密钥”；可以短时显示或复制。
4. 需要批量保存账号资料时使用凭据导出，详见备份与导出。

六位码约每 30 秒改变；原始密钥才是能持续生成验证码的数据。电脑系统时间明显偏差会导致验证码无效，先校准 Windows 时间。

登录时辅助输入验证码

自动模式、有效的绑定网站及已保存密钥是前提。辅助程序检查受支持的登录挑战页和账号身份，找到明确的空验证码输入框后，尝试以键盘输入方式填入当前码。普通登录挑战使用**已经保存并生效的密钥**，不会使用之前取消的修改候选密钥。

它不会自动提交整个登录流程。页面不匹配、身份不明确、多个输入框或已有内容时，可能拒绝填入；可手动从控制台复制当前码继续。

修改 2FA：新密钥什么时候保存？

1. **进入网站设置。**在受支持的绑定网站中开始重新设置验证器。出现二维码时，辅助功能可在匹配页面点击“Can’t scan it?”打开文本密钥方式；当前页面自动检测以文本密钥为主。
2. **取得新候选密钥。**识别到新文本密钥后，暂存在本次修改流程中；此时旧密钥仍是已保存值。
3. **填入新验证码。**明确识别验证输入框后，使用候选密钥生成码并尝试输入。由用户点 Verify / 验证。
4. **确认网站成功。**只有识别到验证通过结果并有编辑权限，才把新密钥写入 hotBrowser 记录。第一次失败后可重新填码再次验证；不要把点击按钮本身当作成功。
5. **检查并备份。**修改后查看已保存的原始密钥或导出凭据，确认确实更新，再依靠新密钥登录。

取消、未提交、验证失败或没有明确成功结果时，候选密钥不会覆盖旧值。页面 DOM、导航与 CDP 事件驱动检测，并有连接维护；外部 Puppeteer/CDP 会话通常可共存，但导航、焦点争用、连接断开和网站页面改版都可能影响辅助识别。

> **手动兜底**
>
> 若网站已成功更改而管理器未确认保存，立即复制网站显示的真实新密钥，编辑该窗口的 2FA 字段并保存。不能继续依赖旧码；关闭前核对保存状态。自动识别只覆盖匹配的页面流程，不能视为所有网站、所有 2FA 方法都已兼容。

备份、导出与恢复

先选择要导出什么

导出方式	包含什么	适合用途
选择数据备份 / 环境 ZIP	环境设置与所选浏览器数据类别；普通 ZIP 清单不包含管理器保存的账号密码和 2FA。	本地备份、复制或作为新环境导入。
批量导出环境 ZIP	所选窗口的环境备份，按类别压缩。	批量备份浏览器数据。
配置表 CSV / XLSX	可编辑配置列；不包含账号密码、代理密码、2FA 和用户目录。	查看、整理、记录参数；不是完整恢复包。
导出账号 / 密码 / 2FA 密钥	所选记录当前保存的明文网站账号、密码和原始 2FA 密钥，JSON 格式。	单独备份账号资料；新密钥修改成功后重新导出。
Cookie 导出	运行中的自动模式窗口 Cookie，可用 JSON、Header、Netscape 等支持格式。	指定范围的数据交换；不能替代完整站点存储。
云同步快照	管理器账号资料、代理凭据及所选浏览器数据，由服务器加密保存。	相同云环境跨机器恢复，详见下一章。

哪些浏览器数据建议保留？

这里的 Cookie 和站点数据覆盖**整个环境的所有网站**，不限于 Gmail 或某一个应用。为了最大限度保留业务状态，推荐保留持久化类别，排除可重建缓存和诊断数据。

类别	通常选择	为什么
基础设置	必选	环境指纹、代理、浏览器设置与必要本机状态。
Cookie	保留	常见登录凭据，但网站仍可撤销会话。
Local / Session Storage、IndexedDB	保留	网站令牌、设备标识、账号业务状态。
其他持久化、Service Worker / Cache Storage	保留	可能有离线业务、后台任务和未提交数据，不能按名称一概视为缓存。
标签页	按需，通常保留	恢复网址和窗口会话；不等于网站登录会话有效。
书签、历史、密码、自动填充	按需保留	用户资料；密码解密仍受平台密钥兼容性影响。
扩展运行数据	需要扩展状态时保留	扩展本地与同步存储、规则和运行状态。

类别	通常选择	为什么
其他未分类持久化文件	通常保留	避免漏掉尚未明确归类的业务数据。
网页 / 脚本 / GPU 缓存	通常排除	可重新下载或生成，能显著缩小很多环境的备份。
日志、崩溃报告	通常排除	主要用于排查，不是常规业务恢复数据。
运行锁、调试端口文件、符号链接	始终排除	属于当前运行实例，不能带到新实例。

备份单个或多个环境

1. 先关闭目标窗口，避免数据库正在写入。
2. 单个窗口点“⋯ → 选择数据备份”；多个窗口勾选后点“批量导出环境 ZIP”。
3. 选择推荐、完整或自定义类别。预览显示每类文件数和大小、包含与排除总量。
4. 导出后保存 ZIP；如需恢复管理器中的网站密码和 2FA，另做凭据导出，或使用云同步。

“原版默认”类别方案只包含基础设置、Cookie 和标签页，体积可能较小，但会遗漏某些网站所需的持久化数据。它是类别选择预设，不是“保证原会话完整恢复”的开关。

单独或批量导出账号与密钥

单个窗口点“⋯ → 导出账号/密码/2FA 密钥”；多个窗口勾选后点批量工具栏“更多操作 → 导出所选凭据”，一次 1–100 条。确认内容提示后下载 JSON，里面是当前已保存的密码和原始密钥，不是短期六位验证码。尚未成功保存的 2FA 候选值不会导出；每次改密钥后重新导出才得到新值。

导入 ZIP 与恢复

从“导入现有环境”选择包，检查声明的数据范围后导入。普通 ZIP 导入为独立新环境，编号重新分配；旧包若没有类别清单，界面只能说明范围未知。不同 Windows 用户或电脑上的密钥兼容性，可能影响浏览器密码和 Cookie 解密。

为什么一个环境有几十或几百 MB？

除了配置，它还可能包含多个网站数据库、离线存储、扩展、历史、会话和缓存。只记录账号参数的表格很小；真正的浏览器环境并不是几行配置。排除缓存后体积常会下降，但长期使用、离线应用、IndexedDB 和扩展仍可能让持久化备份达到数百 MB，以预览统计为准。

> **文件内容要看清楚**
>
> 凭据 JSON 包含明文密码与原始 2FA 密钥；普通环境 ZIP 本身不加密，浏览器文件也可能含敏感数据。把它们保存到你控制的备份位置。做整套客户端灾难恢复时，还需保留管理器数据库、账号保险库密钥、未上传用户数据和同步状态文件。

---

13 / 云端

跨机器云同步

> **先区别两种“同步”**
>
> **云同步**保存环境配置和浏览器数据，用于备份及另一台电脑继续使用；**窗口同步器**复制当前鼠标键盘等操作，用于同时控制多窗口。它们各有独立入口和作用。

基础同步自动进行

登录会员后，当前会员有编辑或管理权限的自主内核环境自动使用基础同步，无需逐条点击开启。新建、导入和已有的已关闭环境会进入上传队列；运行中的环境在正常关闭后上传。尚未认领的旧记录、其他会员的本机记录不会自动上传。首次启动需要先完成首版同步；网络或权限异常会显示失败原因，恢复后重试。

档位	同步内容	操作方式
基础同步	环境配置、管理器保存的账号 / 密码 / 2FA、Cookie、标签页、浏览器保存的密码。	自动执行，不需要额外开启。
完整同步	包含基础档，并增加 Local / Session Storage、IndexedDB、其他网站存储、书签、历史、自动填充和扩展数据。	关闭环境后，在云同步设置中打开“开启完整同步”。关闭此开关则回到基础档。

两档均排除网页 / 脚本 / GPU 缓存、Service Worker / Cache Storage 离线资源、日志、崩溃报告和未分类文件；“完整同步”并非整个目录逐文件复制。依赖离线资源或其他未包含数据的应用，另做本地分类备份。旧版自定义同步范围会保留，主动切换档位后才按新范围同步。

批量同步与调整档位

关闭目标环境后，在窗口列表勾选，再点“批量云同步”，一次最多 100 条。可立即同步，也可选择基础或完整档后同步；每条单独显示结果。超过 100 条分批处理，失败记录修复后重试。自动队列会逐条处理已有记录，可以在任务与云环境中核对进度、版本、时间和实际大小。

在另一台电脑继续工作

1. 安装 hotBrowser、登录自己的会员、准备所需内核。
2. 同一会员可访问自己的云环境；员工需获得相应团队组的编辑或管理权限。
3. 打开“浏览器窗口 → 云环境”，找到环境并点“下载到本机”。
4. 核对来源与数据范围，本地编号可能不同，但云环境唯一 ID 对应同一记录。
5. 从管理器打开，正常使用后关闭，确认回传成功。

只授权“查看”或“打开”不足以下载含凭据的云快照。如果只是普通 ZIP 导入，它通常是一条新环境，不能当作已经加入原云环境的共同版本链。

为什么不允许两台电脑同时改一个环境？

系统通过单写租约避免覆盖。已有电脑持有有效使用锁时，另一台打开同一云环境会被拒绝。应先在第一台正常关闭并上传，等使用锁释放后，再在第二台启动。不要删除锁文件或复制正在运行的数据目录强行并用。

待同步、失败与冲突

- **待同步：**本地有尚未成功上传的变化，先恢复网络并重试。
- **云端已有新版本：**不会直接用旧版本覆盖。先判断哪边数据应保留。
- **本地有未上传修改：**普通下载会拒绝替换；需要明确选择“保留本机副本并恢复云端”。
- **锁失效 / 续约失败：**停止冲突写入，必要时尝试正常关闭窗口，随后检查同步状态。
- **加密格式不兼容：**不能仅复制文件就完成跨机解密；保留原电脑数据，按提示处理。

历史版本与容量

云端保留最近 3 个版本。恢复历史版本前保留当前本机副本；确认恢复后，“立即同步”发布为新版本。本机恢复副本不会自动等同云端版本保留，也不会自动清理。

当前单个快照压缩包上限为 512 MB，文件数上限 300,000，解压 / 本地计划上限 20 GB。超限时先检查缓存和不必要的诊断数据，不能为缩小体积随意删除网站数据库。

关闭后上传的正确做法

通过管理器关闭或浏览器正常退出，等待上传结果。退出管理器时也需要让关闭和回传完成。强制结束进程、断电、休眠或网络断开可能留下待同步数据，下次启动后检查并重试。云快照通过 HTTPS 传输，在服务端以 AES-256-GCM 加密保存；这属于服务端加密存储。

员工与团队权限

会员和团队是什么关系？

每个人先有自己的会员身份。团队关系决定谁是上级、可以访问哪些团队组、可做哪些操作，以及有效期与窗口额度。给员工授权后，员工仍使用自己的账号登录；共享文件夹或共用密码不能替代团队授权。

本机“分组与标签”用于整理列表，远端“团队组”用于服务端授权。只有本机分组名称相同，不代表两个会员已经共享同一环境。

免费团队名额怎么算？

免费团队共 3 人：本人占 1 个名额，还可添加 2 名员工。所有成员共享 200 个环境；员工再创建下属也计入同一团队的 3 人总数。已加入但被禁用或到期的账号仍占名额。待接受的邀请暂不占位，接受时会重新检查人数；名额已满时不会把对方加入团队，也不会改动对方原有账号和数据。

推荐使用邮箱邀请

1. 员工先自助注册并验证邮箱。
2. 有权限的经理进入“员工与权限”，发送团队邀请，填写已验证邮箱、角色、有效期和额度，可选择团队组。
3. 员工在客户端登录自己的会员，查看收到的邀请，输入邮件中的邀请令牌后接受。
4. 经理核对成员状态，并在团队组中授予需要的权限。
5. 要跨电脑共享数据，确认环境基础同步已上传，并分配到已授权团队组。

邀请有效期为 7 天，可拒绝或由发起者撤销。已属于其他上级的会员不能直接接受新团队归属；需要先由有权限人员处理原关系。旧用户名员工创建仍存在，但它不等同邮箱邀请与验证注册流程。

四种分组权限

级别	适合用途	关键边界
查看	查看授权范围内的环境记录。	不能仅凭此权限打开、编辑或下载凭据快照。
打开	运行已有授权环境。	不等同可以编辑核心配置或下载云快照。
编辑	修改环境、按授权范围同步或下载数据。	含敏感数据访问能力，按业务需要分配。
管理	管理团队组及其授权范围。	可执行更高层管理操作，仍以服务端校验为准。

角色与有效期

`member` 是成员，`manager` 是受范围约束的团队经理。`owner` 和 `admin` 属于平台级角色，可管理更广范围；不要把平台管理员角色当作普通团队主管的默认角色。

员工自己的有效期、禁用状态、窗口额度，以及上级链的有效状态都会影响使用。上级到期或停用可能影响下属登录和启动；先在团队和会员页面核对，不要只修改环境设置。

给员工共享一个环境的检查单

1. 员工账号可登录，邀请已接受。
2. 环境属于正确的远端团队组，员工至少具备所需权限。
3. 环境云同步已启用，首版上传成功。
4. 员工电脑有对应内核，能在“云环境”看见并下载。
5. 原电脑已关闭该环境，不占用云使用锁。

共享授权不会自动转移环境所有权，不能把“员工看见记录”当作“完整数据已经在员工电脑上”。

---

15 / 扩展

扩展中心

入口：左侧 → 扩展中心

页面有“扩展库”“已安装”“团队共享”三个栏目，可按名称、开发者、分类、状态搜索，并按服务端分页查看。扩展的程序包、目标窗口分配和每个环境的运行数据是三个独立部分。

从扩展库安装

1. 找到扩展，打开详情查看版本、发布者、权限与更新说明。
2. 点“选择窗口”，指定安装目标；可搜索、筛选和跨页选择。
3. 执行安装或保存分配策略，检查逐窗口结果。
4. 正常关闭并重开目标窗口，让内核加载新的扩展或配置。

导入自己的扩展

1. 点“导入本地扩展”。
2. 选择 ZIP / CRX，或选择根目录包含 `manifest.json` 的已解压文件夹，也可按页面提供的商店链接 / ID 入口解析。
3. 检查名称、版本、权限和身份，再确认导入。
4. 导入完成后仍需指定目标窗口安装；导入仓库不等于已加载到所有浏览器。

商店访问或包下载失败时，可先取得有权使用的本地扩展包再导入。上传和发布受到会员、分组与发布权限约束，普通用户不会因此自动成为公共发布者。

启停、更新、卸载和工具栏

可单个或批量启用、停用、更新、卸载。范围可设为全部窗口、指定窗口或停用；更新不会热替换正在运行的浏览器，应关闭目标窗口后操作，再重开检查。

工具栏策略可保留浏览器当前状态、启动时固定或启动时取消固定。卸载与关闭扩展不是同一件事；需要保留扩展的账号状态时，备份中包含“扩展运行数据”。

跨电脑如何恢复扩展？

扩展中心负责按身份和版本获取程序包与安装策略。环境云快照里的扩展类别负责保存浏览器用户目录中的 Local / Sync / Managed 存储、规则和运行状态。只下载扩展程序包，不代表已经恢复扩展里面登录的账号。

“火特浏览器链接助手”等扩展的实际用途应查看该扩展详情与当前版本说明；不要仅凭名称判断它能访问哪些数据。

---

16 / 效率

窗口同步器

把一个主控窗口里的操作同步到勾选的被控窗口，适合多个环境执行相近操作。它不会把各环境的账号、Cookie 或指纹合并。每个被控仍是独立浏览器环境。

第一次开始同步

1. **准备窗口。**在窗口列表或同步器里选择环境，批量打开。网页同步需要自动模式；手动登录窗口没有所需 CDP 通道。
2. **设置主控。**明确选定一个主控窗口，其余需要接收动作的窗口勾选为被控。只是出现在控制列表中还不够。
3. **对齐页面。**进入相似页面，尽量统一窗口大小、缩放和滚动位置。位置点击在布局不同的页面可能点到不同元素。
4. **保存同步设置。**选择需要同步的鼠标、键盘、滚动、导航和标签等选项，以及坐标映射、延迟与排列策略。
5. **开始并观察。**先用两三个窗口测试普通动作，确认只有预期窗口响应，再增加数量。
6. **暂停后调整。**修改被控集合、做独立输入或执行其他批量动作前先暂停或停止，完成后再继续。

> **这三个按钮意义不同**
>
> “暂停”临时停止事件分发；“停止”结束本次同步；“移出控制列表”只移除同步目标，不删除环境。批量关闭才会关闭对应浏览器。

窗口与标签操作

可批量激活、最小化 / 还原、统一大小、重叠、宫格、对角线或自适应排列。标签动作包括统一网址、当前 / 新标签打开、关闭当前、刷新和强制刷新。关闭最后标签前可能保留空白页，避免环境直接退出。

统一标签是统一网址，不会复制主控的登录 Cookie。网站有不同权限或登录状态时，相同网址可能显示不同内容。

相同文本和差异文本

1. 暂停实时同步，在每个目标页面确认输入框焦点。
2. 相同文本填入一段共用内容；差异文本给每个窗口配置左 / 右列，按当前窗口映射检查。
3. 可从 TXT 按起始行与列规则导入，或按字符集、前后缀、大小写与随机数规则生成。
4. 设置输入速度和是否先清空，再点击对应的输入动作；多个候选页面或焦点变化时会拒绝或停止，检查后重试。

支持匹配焦点链的同源、跨域和嵌套 iframe 文本输入，不意味着每个第三方页面结构或系统输入框都可处理。导入文本、剪贴板和随机生成内容是当前操作资料，不能依赖同步器偏好设置保存来长期存储。

截图、预览和快捷键

可预览所选页面、调整预览列数、放大画面和下载截图 ZIP。截图为网页可视区域，不包含浏览器地址栏和任意系统弹窗。查看后台标签时可能短暂切换并尝试恢复焦点。

快捷键可配置开始、停止、暂停、排列、文本动作等；需要启用对应设置并保存。先检查与系统和其他软件的快捷键冲突，离开同步页面后部分注册会释放。

超级鹰验证码识别

这是第三方图形验证码识别功能，与 TOTP 六位 2FA 不同。按页面配置超级鹰账号、软件 ID 和验证码类型；先定位图像区域并测试截图，再发送识别请求。查看各窗口返回结果，确认验证码输入框已获得焦点后再分发。

请求会把选定验证码截图发送给答题平台，并受其账户余额、接口可用性和支持类型影响。识别返回不等于网站已接受；它也不能当作所有滑块、交互验证或网站安全挑战的通用处理器。

浏览器工具栏与系统弹窗

Windows 原生顶部鼠标桥接为实验选项，默认关闭，对 DPI、窗口数量与工具栏尺寸有额外要求。地址栏原生键入、系统文件选择器、完整标签跨窗口拖动等仍不能按网页同步的方式保证一致。普通用户优先使用已支持的网页、标签和窗口动作。

RPA 与自动化接管

先确认窗口处于自动模式

普通新建与账号文件导入默认保留自动化通道。已启用“手动登录模式”的环境，需要关闭后取消该选项并重新打开，才可用网页自动化、Cookie API、同步器和页面 2FA 辅助。调试接口只面向本机回环地址。

运行一个 RPA 流程

1. 在窗口列表勾选目标，打开“RPA 自动化”。
2. 选择已保存流程或新建，填写任务名和步骤 JSON。
3. 先用一个窗口、并发数 1 验证；查看每步结果，修正网址和选择器。
4. 保存流程，再按需扩大目标范围与并发。并发越大，CPU、内存和网络压力越高。
5. 运行后查看任务记录；停止任务时，已经执行的网页操作不会自动撤回。

```
[
  {"action":"open","url":"https://example.com"},
  {"action":"waitFor","selector":"body"},
  {"action":"screenshot"}
]
```

此示例打开测试页面、等待正文并截图，不包含任何账号操作。支持的动作有打开、导航、等待、等待元素、点击、输入、按键、滚动、提取文本、截图、刷新与关闭标签。输入动作通常需要先让目标输入框获得焦点。

定时任务与保存

可设置下次执行时间和重复间隔。流程、任务记录与计划按会员保存在本机；管理器必须运行并保持登录、网络和目标环境权限有效。退出、断电或强制停止后，不要把它当作已部署在云端的常驻任务，重开后查看计划状态。

Puppeteer / CDP 与 BitShell

外部程序应先通过当前管理器 API 打开环境并取得实际 CDP 地址，再连接该环境。管理器 API 地址与环境调试地址不是同一个端口；不要把官网 API、会员验证地址或环境控制台端口当作 CDP。

本机默认管理 API 常见为 `127.0.0.1:55432`，实际值以当前管理器健康接口和启动信息为准；不同部署和显式配置可能使用其他端口。BitShell 连不上时，先检查它配置的端口是否与当前运行的管理器一致，再检查环境是否自动模式，以及是否配置了具备 read、launch、automation 权限的本地 API 密钥。新版受保护接口的匿名调用会返回 401。

技术用户的最小接管示例

环境 ID 使用本机 `GET /api/environments` 列表接口返回的唯一 ID，不是显示编号。以下示例需安装 `puppeteer-core`，替换实际端口和 ID；普通用户无需执行。

```
import puppeteer from 'puppeteer-core';
const base = 'http://127.0.0.1:55432';
const id = '替换为环境唯一ID';
const response = await fetch(`${base}/api/environments/${encodeURIComponent(id)}/open`, {
  method: 'POST', headers: {'Content-Type':'application/json'}, body: '{}'
});
const opened = await response.json();
if (!response.ok) throw new Error(opened.error?.message || '打开失败');
const endpoint = opened.devtools?.browserWebSocketUrl;
if (!endpoint) throw new Error('自动化通道未就绪，请检查登录模式');
const browser = await puppeteer.connect({browserWSEndpoint:endpoint});
try {
  const page = await browser.newPage();
  await page.goto('https://example.com');
  console.log(await page.title());
  await page.close();
} finally {
  browser.disconnect(); // 断开接管，保留环境浏览器运行
}
```

第三方网站可独立判断浏览器与访问行为，自动化通道可连接不代表 Google 登录一定通过。一个程序正在修改焦点、输入或导航时，另一个程序也做同样动作可能冲突；合理安排接管程序与辅助功能。

---

18 / 版本

内核选择与更新

管理器版本（如 0.9.0-dev）与 Chromium 内核版本（如 153.0.8010.37）分别更新。安装包可带一个初始内核，其他系列由已签名的服务端目录提供；没有必要在首次安装时下载所有系列。

查看和下载

1. 登录会员，打开“内核设置”。
2. 点“检测内核更新”，查看各主版本的本机版本与服务端版本。
3. 对缺失或有更新的系列执行下载安装，等待下载、完整性校验和注册完成。
4. 创建 / 编辑环境时在“环境内核”选择需要的主版本。已安装 148 不会自动删除 153。

5. 先测试一个环境，再用于大批次。

同系列更新与跨系列切换

变更	影响与正确做法
153 系列的补丁或安全重编包	沿用该系列用户目录。即使 Chromium 完整版本号相同，安全重编包也可能有更新。
从 148 切到 153	属于主版本迁移，使用另一套系列用户目录；现有 Cookie、密码和扩展不会仅因改下拉选项就自动出现在新目录。
从新主版本回退	数据库格式可能已经升级。先恢复旧版备份，避免让旧内核直接打开新格式目录。

跨主版本前先备份，再迁移需要的数据类别，确认网站和密码可用。两个主版本不要同时读写同一个用户目录。

为什么启动需要联网验证？

启动前，管理器核对会员有效期、环境权限、内核登记、必要的代理检测和云使用锁，并向 hotBrowser 服务请求当前启动配置签名。内核检查签名和配置是否匹配；失效、缺失或被修改的授权可能拒绝启动或关闭浏览器。

仅取得 `chrome.exe` 不是完整的环境启动流程。运行库、资源、受信清单、授权和数据目录都参与启动。不同版本的运行文件数、压缩包大小不能直接推导网页运行内存大小。

更新失败或开启较慢

检查会员状态、服务状态、下载网络和磁盘空间。首次下载、缓存较冷、代理认证、出口地区检测、云端下载或启动授权都会增加等待时间。看管理器当前提示定位阶段，不要在同一窗口连续反复点打开。

---

19 / 管理员

网站管理后台

入口：官网“管理后台” → https://hotbrowser.cc/hotbrowser/v1/admin/

这部分供拥有后台账号的运营管理员使用。普通用户在客户端会员中心登录；后台管理员账号由运营方单独提供，本公开手册不含任何真实凭据。

会员与团队管理

1. 查看会员姓名 / 邮箱、验证状态、角色、有效期、额度与上级。
2. 按权限调整期限、禁用状态和窗口额度；核对对下属的影响。

3. 管理团队组与查看、打开、编辑、管理授权；使用平台管理员角色时注意其权限范围。
4. 对已验证邮箱会员，应引导其使用邮箱找回和团队邀请流程；不要把旧用户名的重置 / 令牌签发方式当作邮箱会员的通用流程。

登录令牌与账号密码

令牌表示设备登录会话，可以撤销以终止其后续授权。会员改密 / 重置会使其全部设备令牌失效。管理员可修改自己的后台密码，后台会话随之失效；后台密码与会员密码各自管理。

云端环境、扩展与审计

云环境页查看版本、快照大小、类别、成员和租约，不直接展示解密后的快照内容。扩展仓库查看程序包、版本和发布状态。启动记录与操作审计用于排查权限、签名、同步和管理操作。

延长有效期或修改额度是当前运营配置方式；本版本没有完整的在线支付、自动计费与续费收款流程。实际套餐和额度以运营方说明及会员页面为准。

---

20 / 排查

常见问题与排查

打开环境失败，先查哪里？

1. 确认会员已登录、有效期和额度正常。
2. 确认对应内核已经安装并通过校验。
3. 检查代理连接和启动前地区检测；有拦截规则时看具体触发原因。
4. 云环境确认没有其他电脑占锁、下载成功。
5. 查看管理器错误，不要只根据窗口闪退推断原因。保留编号、时间、版本和错误文本。

浏览器启动慢，是代理的问题吗？

可能，但还可能是内核首次校验、云端下载、密码导入、启动签名和本机资源竞争。先看卡在哪个阶段，用同一代理检测实际延迟，再用少量窗口验证。浏览器已打开而网页慢，与浏览器还没出现属于不同阶段。

多个环境都显示相同的代理出口，怎么办？

先核对每个环境的代理端点与用户名。如果所有窗口分配同一固定出口或相同粘性 session，出口相同可能符合供应商策略；如果检测到了管理服务地址而非代理出口，应重新检测并核对检测服务结果。截图记录端点、出口、国家和检测时间，不要仅修改显示 IP。

地区有国家和城市，但没有时区？

地区服务必须返回有效的 IANA 时区，例如 `America/New_York`。国家或城市名称不能唯一替代时区；确认网络与 GeoIP 服务正常。自动地区模式缺少时区会报错，必要时按真实出口在手动模式明确配置。

Google 提示 “This browser or app may not be secure”？

这是 Google 的判断，可能与浏览器版本、页面行为、网络、风险状态和自动化相关。先确认真实使用的环境编号、内核、账号与代理，不要把另一个窗口的测试结果当作这个窗口的结果。必要时关闭后选择手动登录模式，使用网站支持的登录流程；该模式会关闭自动化辅助。任何模式都不能承诺 Google 一定接受。

同一个密码已在密码管理器里，为何还提示 Save password？

浏览器按网址、登录表单范围、用户名和保存记录匹配，不只比较密码字符串。检查当前登录账号和保存的网站记录，再确认原生导入是否成功。不要通过关闭密码管理器来掩盖尚未核对的匹配问题。

2FA 没显示或没有自动填入？

1. 确认窗口账号记录保存的是原始密钥而不是六位临时码。
2. 从当前管理器重新打开控制台，避免使用过期授权链接。
3. 检查电脑时间、平台网址、用户名与编辑权限。
4. 自动填入需要自动模式、匹配页面及空的明确输入框。
5. 修改密钥后核对保存结果，失败时手动保存真实新密钥。

点击 Can’t scan it? 后取消，会覆盖旧 2FA 吗？

不会仅因识别到候选密钥就替换。未确认修改成功时，原已保存密钥继续用于普通登录。网站成功但管理器未能识别结果时，需要你手动核对并保存，详见第 11 章。

导入后列表没刷新或看不到新记录？

先“刷新”并“重置全部筛选”，检查当前会员和编号排序。提示“已保存、刷新失败”时不应重复导入，先恢复列表请求。确认运行的是更新后的客户端；旧管理器进程未退出时仍可能是旧代码。

关窗后为什么没有自动上传？

登录会员后，有编辑或管理权限的自主内核环境会自动进入基础同步队列。先检查首版上传、权限、网络和任务进度；运行中的环境需正常关闭后上传。尚未认领的旧记录、其他会员的本机记录不会自动上传。强杀、断电或同步冲突不会被当作成功上传，需查看失败原因并重试。

员工能看到环境，却下载不了？

查看 / 打开权限不等于编辑权限，云快照含凭据，需要相应授权。检查团队组、员工状态、上级有效期、快照是否存在和内核是否可用。

备份后网站还是要求登录，是恢复失败了吗？

不一定。网站会使令牌失效或重新验证设备，标签恢复也不等于登录恢复。核对备份范围是否含所有必要站点存储、密码能否解密、IP 与身份是否变化，再按网站流程登录。

修改了设置，必须重启吗？

搜索、筛选和主题等界面设置通常即时生效；内核、指纹、代理、原生密码导入和扩展加载需要重开目标环境。升级管理器程序需正常退出再启动；有云同步的窗口先等上传完成。

如何向维护人员提供有效信息？

提供管理器版本、内核完整版本、环境显示编号及来源编号、操作时间、失败阶段、错误原文和必要截图。代理信息提供协议、脱敏端点、出口、地区和检测时间即可；不要把完整密码、2FA 原始密钥或临时授权链接放进普通报错截图。

附录 / 随时查阅

术语与操作检查单

术语	易懂解释
管理器	火特浏览器主界面，负责配置、权限、代理、启动和数据管理。
窗口 / 环境	一套独立配置与网站数据，启动后出现对应浏览器。
本机编号	你看到的 1、2、3 等序号，方便操作；不是云端唯一身份。
环境 UUID	用于 API 和跨机器对应数据的唯一 ID。
内核	实际加载网页的 Chromium 浏览器程序及运行资源。
指纹	网站可见的系统、浏览器、硬件、屏幕等参数集合。
Cookie / 站点存储	网站在环境里保存的数据，可能包含登录状态和业务内容。
TOTP 密钥 / 验证码	密钥长期生成动态码；六位验证码短期有效。
云快照	某个版本的环境配置与所选浏览器数据备份。
租约 / 云使用锁	防止同一个共享环境同时在多台电脑写入。
CDP	Chromium 的本机调试与自动化通道。
登录会话	网站对一次登录的授权与判断；打开原标签不保证原授权仍有效。

每天开始

- 会员状态和所需内核正常。
- 查看待同步与上次失败记录。
- 使用预期编号与账号。
- 检查代理出口与地区。
- 先小批次打开再扩大运行。

每天结束

- 确认需要保存的新账号资料。
- 修改 2FA 后核对原始密钥。
- 正常关闭环境。
- 等待云同步完成。
- 定期导出重要环境与凭据。

附录 / 依据

编写依据

操作名称、默认值和恢复边界依据 hotBrowser 0.9.0-dev 当前客户端与服务端代码、功能文档整理。入门、创建、导入、扩展和主控 / 被控的讲解路线参考 BitBrowser 公开帮助中心；本手册中的具体行为以 hotBrowser 的实现为准。

- BitBrowser 官方帮助中心：教程组织与常见任务
- BitBrowser 官方：新建浏览器窗口
- BitBrowser 官方：批量导入浏览器窗口
- BitBrowser 官方：扩展中心
- BitBrowser 官方：窗口群控图文指南

参考资料核对日期：2026-09-30。涉及网站登录、跨系统迁移和实验性同步的能力，应结合当前内核及实际页面验收结果使用。

免费方案、团队与自动化授权

完成邮箱验证的新注册团队永久免费提供 200 个环境和 3 个成员名额（含本人，即本人 + 2 名员工）。团队成员共同使用环境额度；成员自己的操作范围仍由团队管理员分配。创建员工、发送邀请和接受邀请时由服务端检查人数，多个请求同时提交也不能超出名额。已有其他授权保留；已存在的超额成员或环境不会被自动删除，但免费团队不能继续新增超额记录。

在客户端的会员中心可以查看组织、额度和登录设备，并撤销其他设备会话。修改密码或停用成员会使旧会话失效。组织隔离不等同于删除员工此前已下载到本机的数据。

新版管理器的本地 API 要求应用密钥。在设置中创建密钥，选择所需动作和环境，然后在脚本请求中添加 `Authorization: Bearer <密钥>`。密钥只显示一次；丢失后撤销并重新创建。直接连接浏览器 CDP 的方式由环境

运行状态提供，不要向其他人公开调试地址。

新建环境可先用快速模式填写代理；高级模式展开指纹和启动细节。批量导入先检查列映射和选中行；遇到网络失败，保持原批次内容重试。任务中心记录批量启动、创建、内核更新与云同步结果，可单独重试支持重试的失败项。

客户端、会员后端和内核各自有版本。更新管理器不会使尚未编译、未验收的内核能力自动生效；字体、媒体设备、网页定位和 WebGPU 的状态以客户端能力清单为准。

0.9.0 新功能说明

0.9.0-dev Windows 客户端及对应后端已发布，可从官网下载。免费团队名额由服务端执行，现有 0.9.0-dev 客户端同样适用。

会员验证器与恢复码

1. 进入会员中心的安全设置，输入会员密码开始绑定验证器。
2. 把设置密钥加入验证器，输入当前六位码确认；保存仅展示一次的恢复码。
3. 以后登录先输入邮箱和密码，再输入验证器码；丢失验证器时使用一个尚未使用的恢复码。

导出密码、原始 2FA 或完整环境时会要求再次验证会员身份，授权在当前客户端内短时有效。会员验证器和网站账号 2FA 是两回事；更改或找回会员密码不会关闭会员验证器。

加密备份

在环境备份中选择“.hbbak 加密完整备份”，设置至少 12 个字符的密码并确认，选择需要保留的数据类别。备份包含账号密码、原始 2FA、代理凭据和选定的浏览器数据。恢复时选择文件、输入备份密码，验证成功后创建独立新环境；密码错误、文件损坏或额度不足不会留下半批记录。

备份密码不会由服务器保存，丢失无法找回。支持的 Windows DPAPI 密钥可在目标 Windows 用户下重新保护；不支持的应用绑定加密会明确拒绝。恢复 Cookie 不能保证网站不再要求验证。普通 ZIP 保留旧兼容模式，不包含管理器账号密码和原始 2FA。

云上传重试

上传按分块校验；网络断开后，本机保存加密的待上传包，恢复网络后继续缺少的分块。基础自动同步会在临时网络错误后继续按退避间隔重试，也可在云环境中点击立即同步。换会员、云版本冲突、权限失效或存储额度不足会停止，避免覆盖数据。云界面显示用量、上传预留、待上传状态和下次重试时间。

自动化流程

流程支持变量、条件判断、循环、暂停/继续和逐步失败策略。失败任务可只重跑失败及未完成的环境，重跑从第一步开始；可能重复提交的业务操作应自行使用幂等设计。选择器检查只等待元素，不会点击。

扩展升级审批

新版扩展要求更多网站访问或功能权限时，自动更新先暂停并显示差异。确认授权的环境才安装新版，其余环境继续使用原包。本机可固定版本；这项本机设置不代表所有团队电脑已同步固定。