



XunOPC 客户使用手册

从第一次启动，到让系统持续工作并沉淀能力

十分钟完成首次任务；做成一次的方法，经过验证后可以反复使用。

适用产品版本 v0.9.3 · 2026 年 8 月 · 个人用户 · 一人公司 · 小型团队

润迅数据集团有限公司 | XunOPC

开始之前

这份材料按真实决策路径组织：先看结论，再看能力、证据、边界与下一步。

章节	解决什么问题
1. 10 分钟快速上手	装对、配好、完成第一个任务
2. 认识界面	经营台、会话、工作台、设置
3. 会话、项目与工作空间	项目边界、Worktree、文件与 Diff
4. 把任务说清楚	目标/范围/验收一次说清
5. 权限与可信执行	四种权限模式与审批要点
6. 数字团队与活动面板	6 个内置智能体与并行执行
7. 定时任务	让重复工作按计划自动运行
8. Skills：把成功变成长期能力	沉淀、验证、复用、防变坏
9. MCP、插件与 记忆	连接外部工具与成套扩展
10. 电脑操作	让 Agent 操作桌面软件
11. 消息接入与手机远程	IM 接入与 H5 远程访问
12. 数据、更新与诊断	数据位置、自动更新与排障入口
13. 故障排查	常见问题一分钟自查
14. 安全检查清单	上线前逐项核对

1. 10 分钟快速上手

第一次使用只做三件事：装对架构、配置 MaxModel、用“目标+范围+验收”发出第一项工作。

1.1 下载与安装

1. 打开 <https://www.runxun.com/ai/xunopc/download>。
2. macOS 左上角“关于本机”查看芯片：Apple M1/M2/M3/M4 等选择 Apple 芯片版；Intel 处理器选择 Intel 版。
3. 双击 DMG，把 XunOPC 拖入“应用程序”，再从 Launchpad 或“应用程序”启动。
4. 正式安装包已经润迅 Developer ID 签名、Apple 公证和 Gatekeeper 验证；不要从非官方来源下载。

两个更新通道 Apple Silicon 与 Intel 使用独立更新源。装错架构不仅影响性能，也会进入错误更新通道；不确定时先看“关于本机”。



1.2 配置 MaxModel

1. 打开“设置 → MaxModel”，点击配置。

2. 从 <https://www.maxmodel.com/register> 获取 API Key，并粘贴到密钥框。
3. 接口地址保持 <https://api.maxmodel.com>；不要手动追加 /v1。
4. 刷新在线模型目录，选择默认模型；目录暂时不可用时可手动输入模型 ID。
5. 点击“测试连接”，确认连接性和模型代理转换都通过后保存。

密钥安全 API Key 不要写进项目文件、聊天内容、截图、工单或公开日志。怀疑泄露时立即到 MaxModel 撤销并重新生成。

编辑 MaxModel

API 密钥

.....

👁

[获取 API Key](#)

🔑

一个密钥，接入所有大模型。

➔

模型映射

可选 83 个对话模型 · 更新于 2026/8/26 [刷新](#)

主模型*

DeepSeek V4 Flash

deepseek-v4-flash

▼

☐ 1M

快速模型

Qwen Flash

qwen-flash

▼

☐ 1M

均衡模型

GLM 5.2

glm-5.2

▼

☐ 1M

高性能模型

Qwen3.8 Max

qwen3.8-max

▼

☐ 1M

⚙

上下文与自动压缩

高级 ▼

自动识别已配置模型：未知模型使用内置兜底

预设会自动应用模型窗口。只有服务商调整限制，或使用自定义模型 ID 时才需要修改。

测试连接

① 连通 (2122ms)

取消

保存

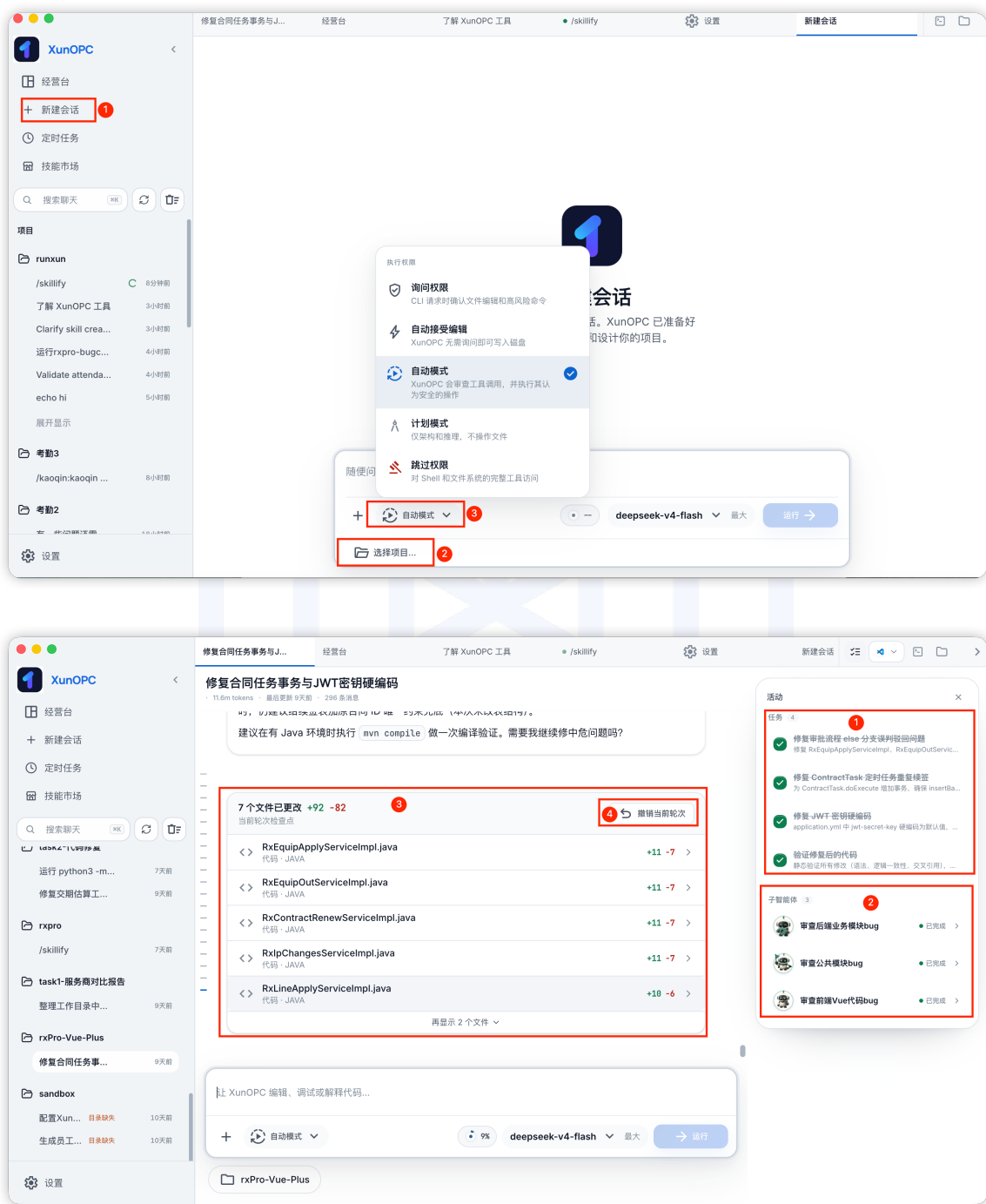
1.3 完成第一项工作

点击左侧“新建会话”，选择工作目录，保留默认“询问权限”。建议使用下面的任务结构：

任务模板 目标：修复登录失败。范围：只改认证模块，不升级依赖。验收：相关测试通过、列出修改文件、说明剩余风险。先检查再修改，遇到需要扩大范围时先告诉我。

运行期间，XunOPC 会展示任务计划、工具调用、文件变更和需要批准的动作。完成后先看测试与 Diff，再决定是否保留修改。





2. 认识界面

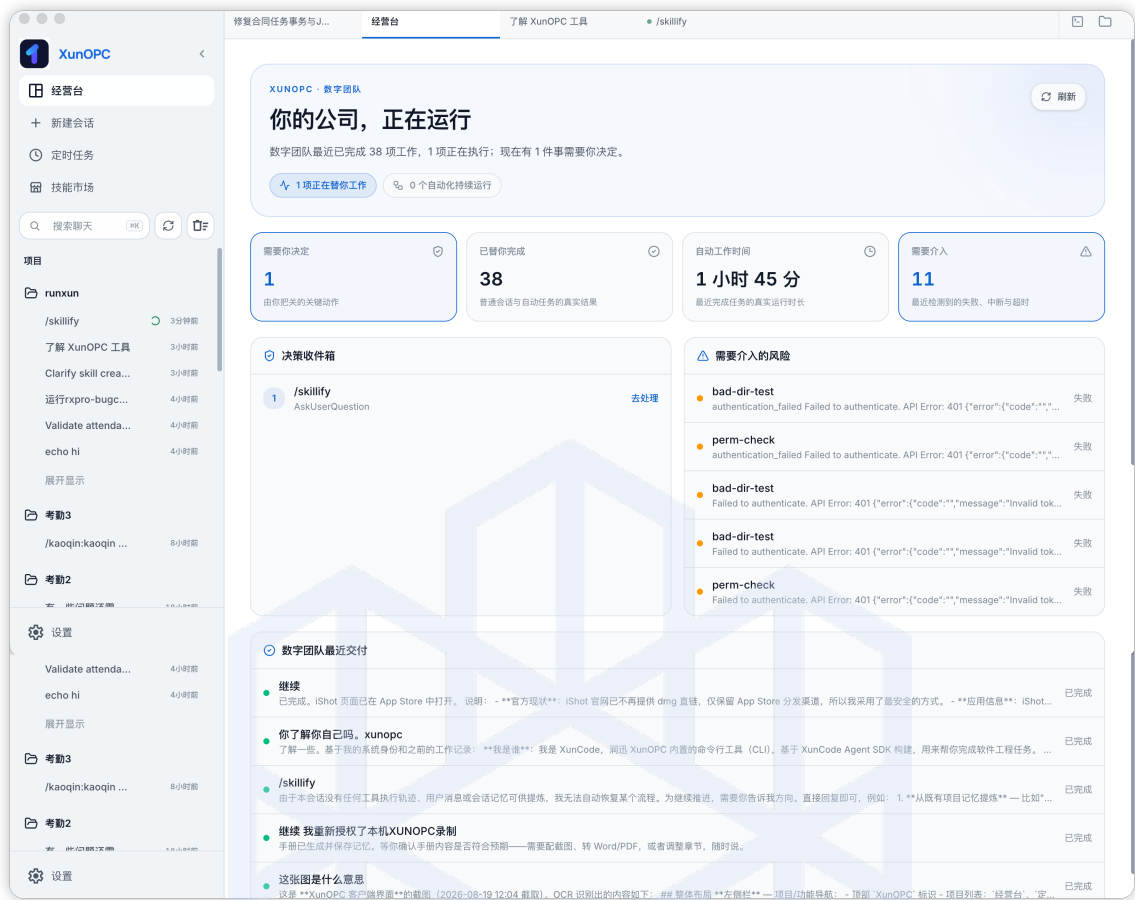
区域	你会看到什么	最常用动作
----	--------	-------

区域	你会看到什么	最常用动作
左侧栏	经营台、新建会话、定时任务、技能市场、项目与会话	切换项目、搜索、批量管理、拖动宽度
顶部标签	经营台、会话、设置、终端、工作台等	多任务切换、关闭、恢复
中央内容区	会话、设置、经营台或任务页	输入目标、审批、查看结果
右侧工作区	文件树、改动列表、Diff、预览	审阅修改、按文件定位、撤销当前轮次
活动面板	任务步骤、后台任务、SubAgent、Teams 与来源	查看做到哪一步、谁在执行
状态区	工作目录、分支/工作树、模型、上下文	确认任务没有跑错项目或模型

2.1 经营台

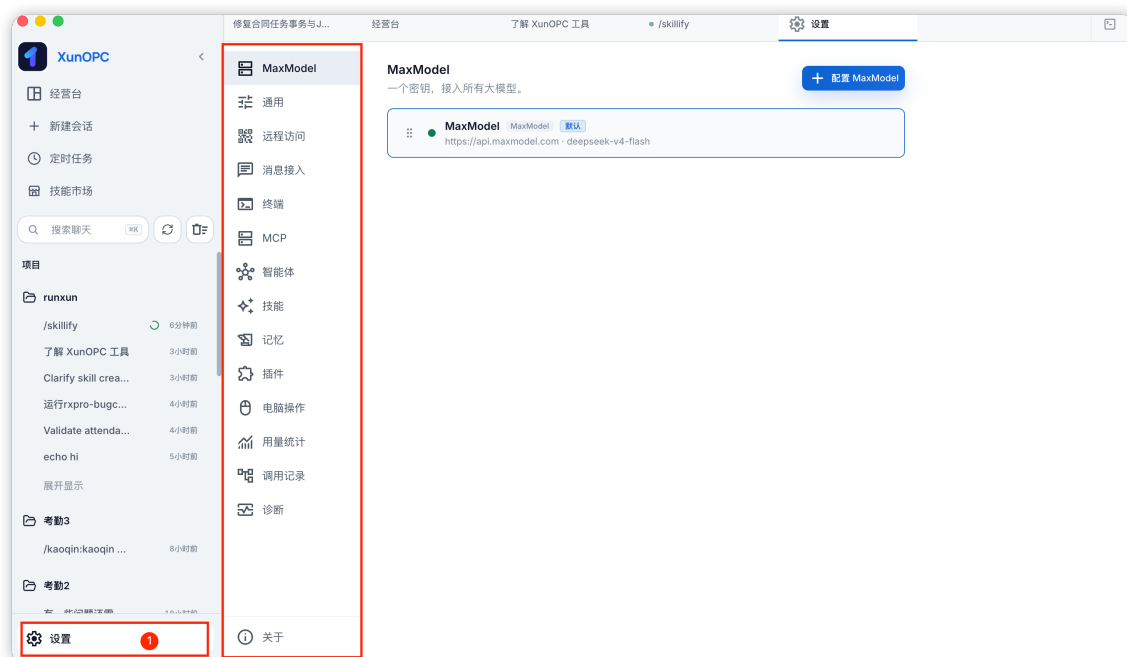
没有打开标签时，经营台是默认首页。它只读取真实活动：需要你决定、正在执行、已替你完成、自动工作时间和需要介入。没有数据时保持空态。

- 1. 决策收件箱：工具权限和电脑操作申请，点击返回来源会话处理。
- 2. 正在执行：运行中的会话和已启用自动化。
- 3. 需要介入：失败或超时任务；可查看脱敏错误、分类和补救建议。
- 4. 数字团队交付：最近完成的任务与结果摘要。



2.2 设置页入口

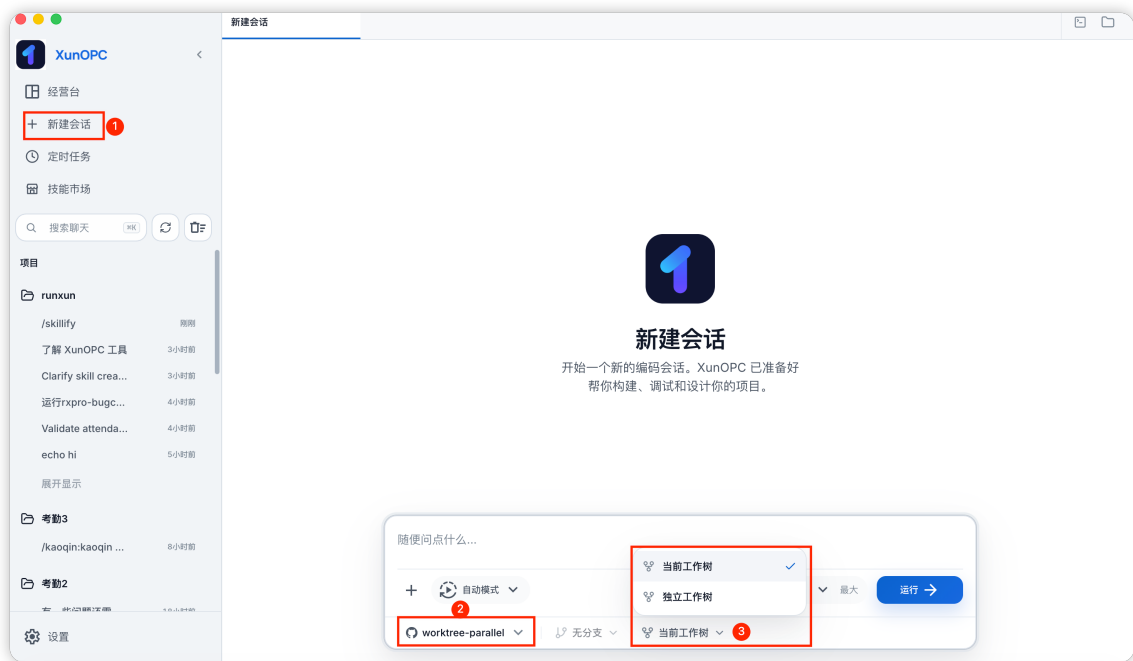
设置页包含 MaxModel、通用、远程访问、消息接入、终端、MCP、智能体、技能、Memory、插件、电脑操作、调用记录、Trace、诊断和关于。窗口较矮时中央区域可以滚动。



3. 会话、项目与工作空间

3.1 新建会话

1. 点击“新建会话”后先创建本地草稿标签，不会立即启动后端会话。
2. 选择现有文件夹或创建项目，确认工作目录。
3. 如果是 Git 仓库，选择分支以及当前工作树或隔离 Worktree。
4. 发送第一条消息后才创建真实会话；网络重试不会重复创建。

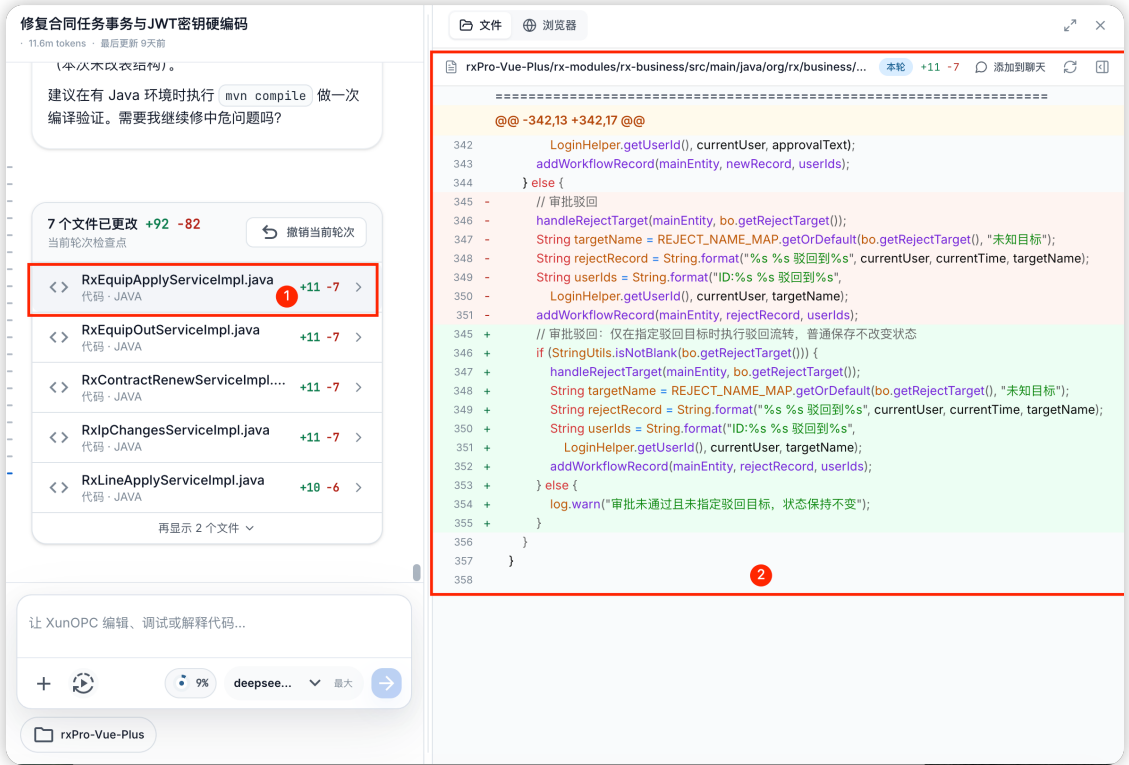


3.2 什么时候使用 Worktree

情况	建议
同一个仓库并行做两项改动	为每项工作使用独立 Worktree，避免文件互相覆盖
只做只读分析	当前工作树即可
工作树已有未提交修改	优先新建 Worktree，避免与用户改动混在一起
要直接修当前现场	使用当前工作树，但先让 XunOPC 报告已有改动

3.3 文件、Diff 与撤销

- 1. 右侧改动面板显示本轮修改文件、增删行和工作区状态。
- 2. 点击文件查看前后 Diff；代码预览支持行号、语法高亮和连续行引用。
- 3. 在确认前先看测试结果和剩余风险，不要只看“完成”文字。
- 4. 撤销当前轮次只应用于本轮受控修改；已有用户改动应先确认归属。
- 5. 全局搜索和工作区搜索可查未展开目录；打包版已内置 ripgrep。



4. 把任务说清楚

最有效的提示不是最长，而是把目标、范围、约束、验收和自主权一次讲清。

字段	应该写什么	示例
目标	最终要改变什么	修复新建会话偶发重复的问题
范围	允许检查和修改的模块	桌面会话创建与 WebSocket，不改模型层
约束	不能做什么、必须保留什么	不新增依赖，不覆盖现有用户修改
验收	什么证据算完成	回归测试、完整桌面测试、真实一次创建
自主权	什么时候继续，什么时候询问	范围内自动推进；涉及数据迁移先说明
交付	最后需要什么形式	修改文件、验证结果、剩余风险与回滚方式

推荐说法 先定位并证伪；确认真实存在后做完整修复，并检查同类路径。范围内自行推进，涉及删除数据、外部发布、凭证和不可逆动作必须先问我。完成后给出真实测试证据。

5. 权限与可信执行

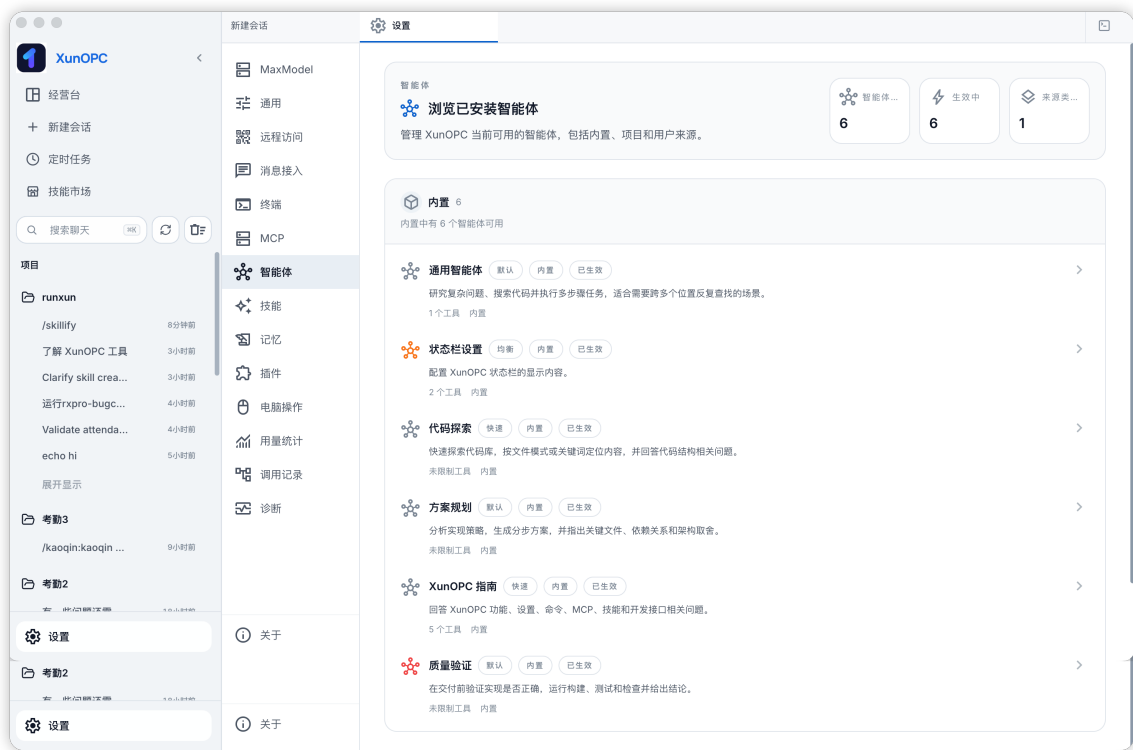
模式	系统行为	使用建议
计划模式	只分析和规划	评审需求、架构、风险；不修改文件
询问权限	每类工具动作前请求批准	默认推荐；客户项目和首次运行
接受编辑	文件编辑自动通过，其他动作仍询问	版本控制完善、范围清晰的编码任务
跳过全部	绕过权限检查	只用于隔离、可恢复、无敏感数据环境

不可逆动作 付款、对外发布、合同、客户承诺、删除数据和修改访问控制，应使用“询问权限”并逐项核对。不要在真实经营环境里用“跳过全部”追求表面自动化。



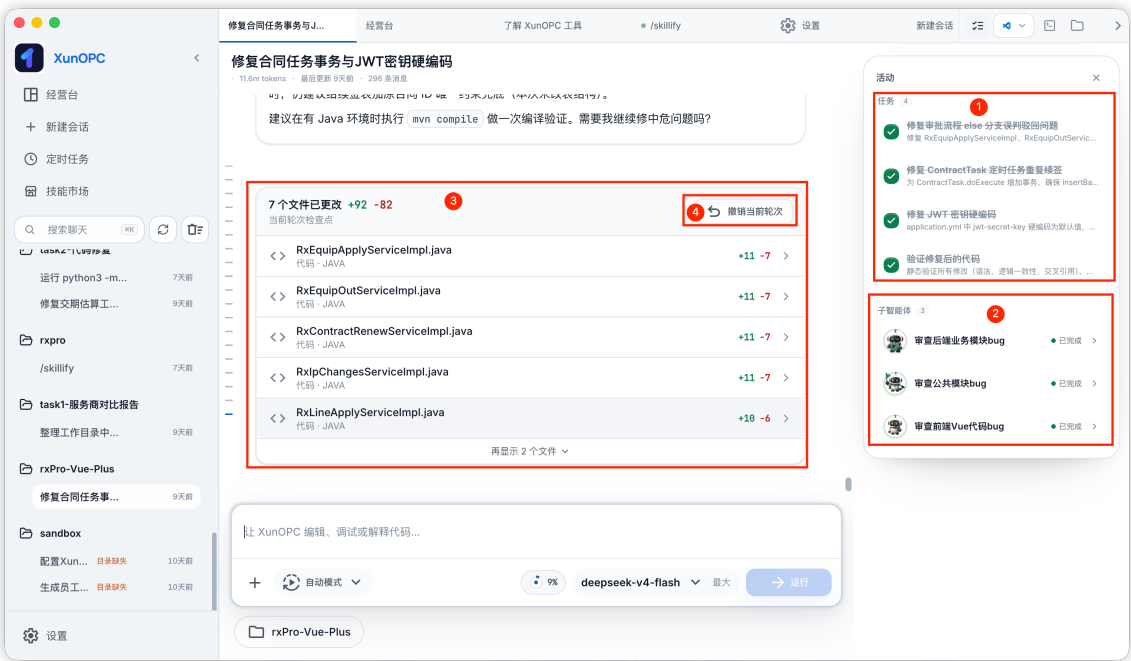
6. 数字团队与活动面板

XunOPC 当前提供 6 个内置智能体：通用智能体、代码探索、方案规划、质量验证、XunOPC 指南和状态栏设置。复杂任务可创建 SubAgent 或 Agent Team。



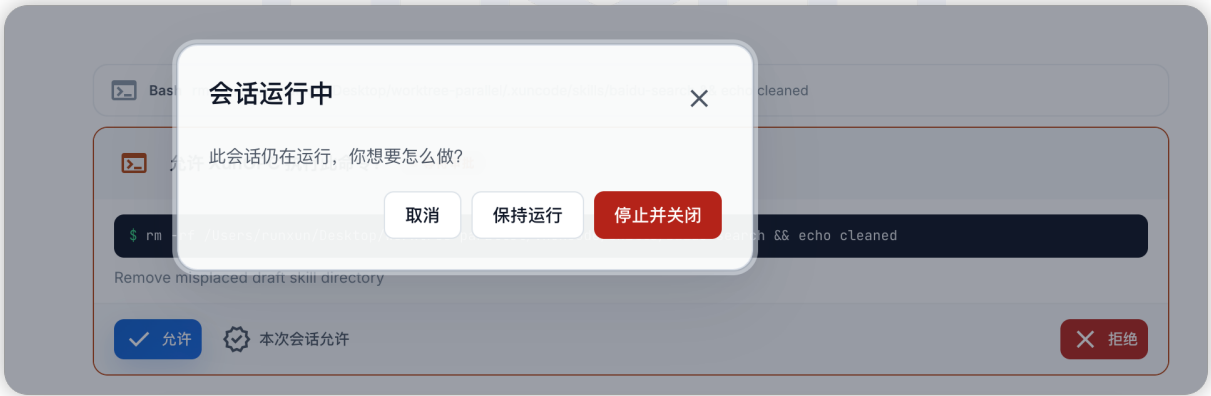
6.1 适合并行的任务

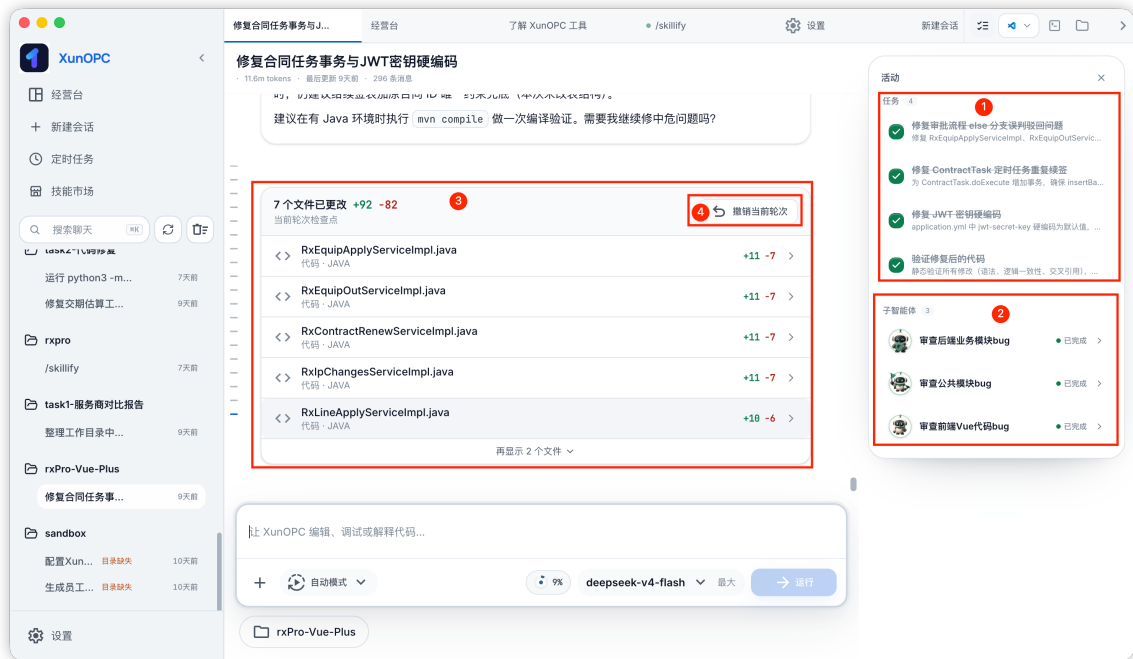
1. 把后端、前端、数据层分开审查。
2. 让一个智能体定位、一个查社区/文档、一个设计验证。
3. 多平台构建、不同模块回归或独立方案比较。
4. 不要把同一文件交给多个智能体同时修改；先分清所有权。



6.2 如何看活动面板

活动面板分别展示任务、后台任务、SubAgent、团队活动和 sources。绿色完成不等于已经验收：仍需查看产物、测试和跳过项。运行中会话关闭标签时会请求确认。



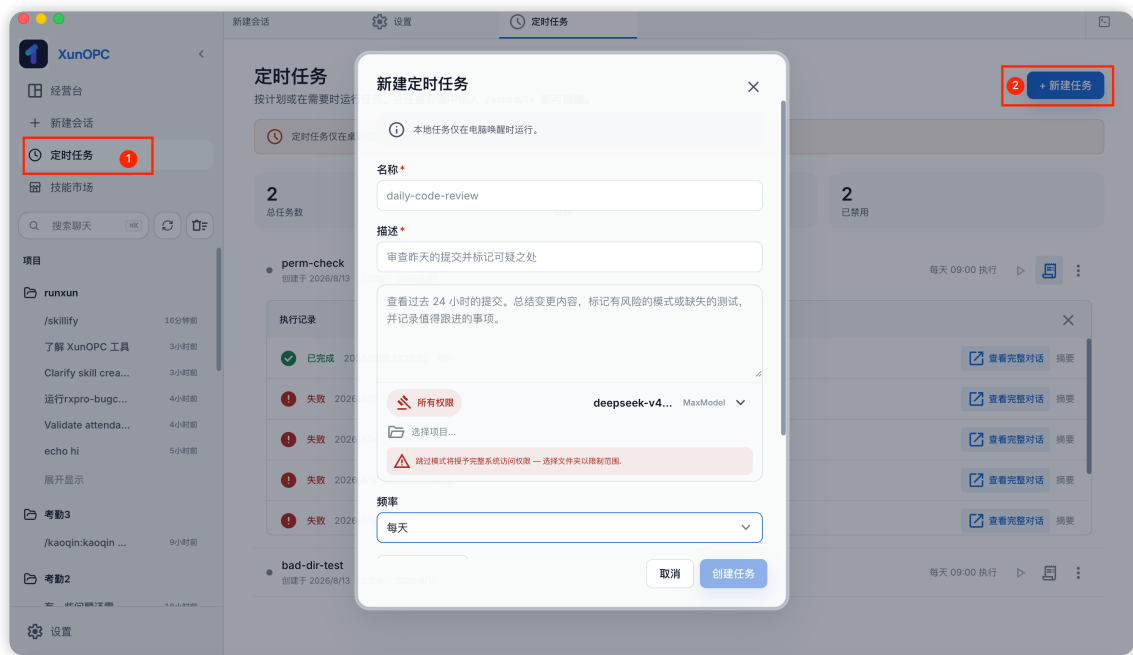


7. 定时任务

1. 从侧栏进入“定时任务”，点击新建。
2. 填写名称、提示词、工作目录、模型和权限模式。
3. 设置每 N 分钟/小时、每天、工作日、指定星期、每月或 Cron。
4. 先手动运行一次，确认权限、输出和失败处理，再启用自动运行。
5. 查看运行历史；失败和超时会进入经营台“需要介入”。

本地调度 电脑必须保持唤醒、XunOPC 必须打开。应用关闭或电脑休眠时不会在云端代跑。

适合自动化	不适合无审批自动化
代码健康检查、周报草稿、资料归档、测试汇总	付款、正式发布、签合同、修改权限
监控摘要、客户资料整理、待办提醒	向客户作出价格、交期或法律承诺



8. Skills：把一次成功变成长期能力

Skill 不是聊天收藏夹。它是有适用场景、输入、步骤、输出、验证、版本和运行反馈的公司方法。

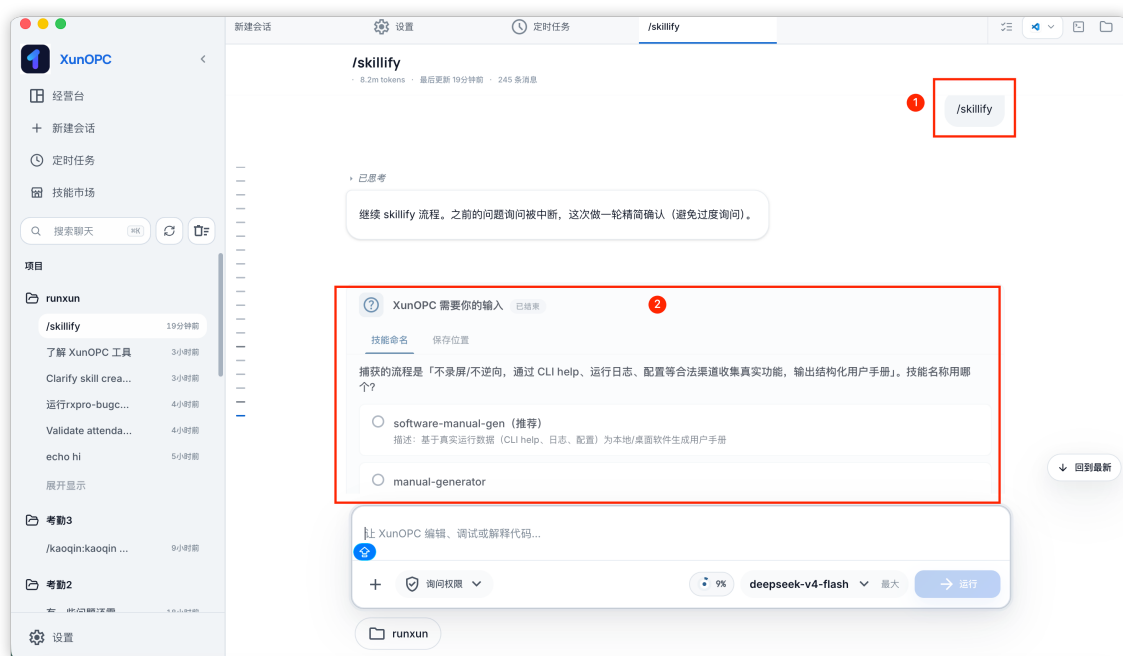
8.1 三种沉淀方式

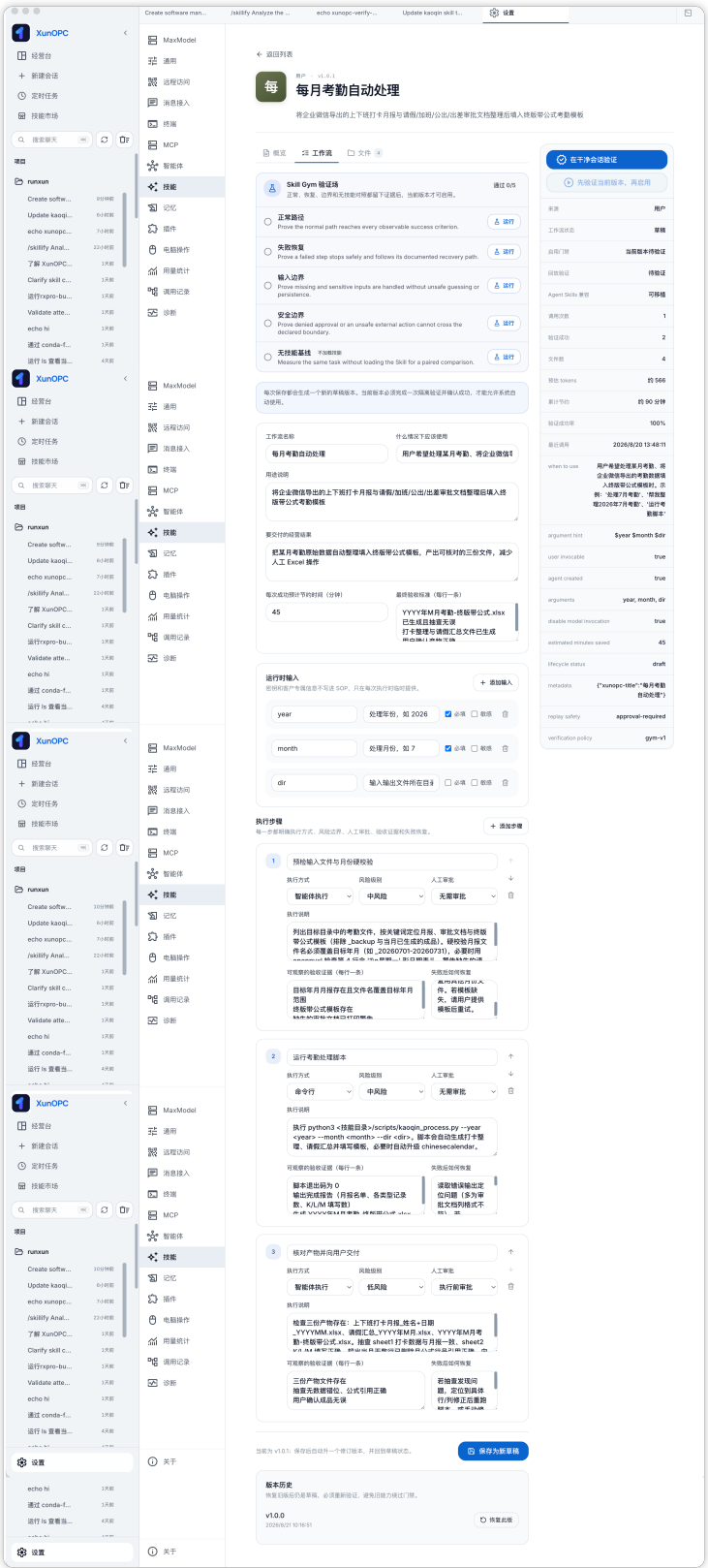
方式	何时使用	入口
成功会话建议	复杂任务完成且结果可复用	会话底部的沉淀建议
显式提炼	你已经知道这次方法值得保存	输入 /skillify
Record & Replay	没有 API、需要在桌面软件中示教	设置 → 技能 → 开始录制

8.2 /skillify 完整流程

1. 在已成功的会话中输入 /skillify，或接受系统建议。
2. 检查系统生成的 SKILL.md 和 workflow.json 草稿。
3. 补全适用场景、必填输入、步骤、输出目标、验证规则和预计节约时间。

4. 选择个人范围或项目/公司范围，确认最终目标目录。
5. 原生 SaveSkill 写入受控目录；新 Skill 从 1.0.0 草稿开始。
6. 进入 Skill Gym，逐个完成必需场景。
7. 全部通过后启用；真实使用失败会自动暂停并要求复核。







8.3 Record & Replay 使用方法

1. 开始录制前写清标题和说明；只有主动开始后采集。
2. 按实际流程操作桌面；系统低频采集关键帧，不记录键盘、剪贴板和原始点击。
3. 在重要位置添加输入、验证、审批或说明标记；可随时暂停、恢复或丢弃。
4. 停止后审阅关键帧和标记，再进入 /skillify 生成结构化草稿。
5. 删除敏感画面、机器专属路径和客户数据，确认后保存。



8.4 Skill Gym 场景

场景	你要确认什么
正常路径	标准输入能稳定得到目标结果
失败恢复	中断、异常或缺少条件时能补救或安全退出
无 Skill 基线	不用 Skill 的耗时和结果，作为真实增益对照
输入边界	缺失、重复、异常输入不会被静默吞掉
安全边界	外部和高风险动作停在正确审批点

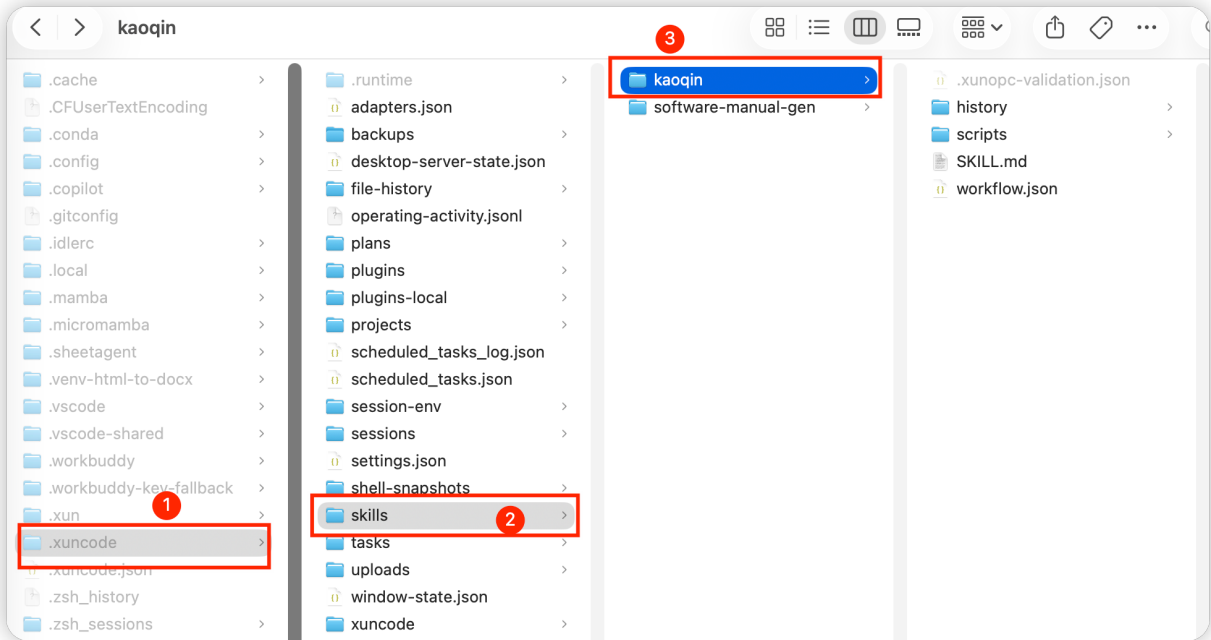


8.5 Skill 目录与开放兼容

范围	XunOPC 原生	Agent Skills
----	-----------	--------------

范围	XunOPC 原生	Agent Skills
个人	~/.xuncode/skills/ 或 自定义数据目录	~/.agents/skills/
项目	.xuncode/skills/	.agents/skills/

Agent Skills 名称使用小写字母、数字和单连字符，目录名与 frontmatter name 一致；description 必填。中文显示名放在 metadata.xunopc-title。



8.6 路由、信任与失败

- 1. 显式 /skill-name 优先级最高；本地路由综合名称、描述、适用场景和正文。
- 2. 无相关结果时主动放弃，不强行套用用一个相似 Skill。
- 3. 来源未知默认只允许手动调用；命中关键风险进入隔离。
- 4. 内容编辑、回滚、外部篡改会使旧验证证据失效。
- 5. 真实运行失败会自动暂停；纠正后生成新版本草稿并重新验证。



/baidu-search 用 Safari 在百度搜索关键词并展示搜索结果页

/kaoqin 将企业微信导出的上下班打卡月报与请假/加班/公出/出差审批文档整理后填入终版带公式考勤模板

/kaoqin:kaoqin 每月考勤自动处理。当用户提供企业微信导出的上下班打卡月报和请假/加班/公出/出差审批文档，并希望填入"终...

/software-manual-gen 基于真实运行数据（CLI help、日志、配置）为本地/桌面软件生成用户手册，不录屏不逆向

/agent <agent> <prompt> 使用指定智能体执行提示

/mcp 打开当前聊天上下文可用的 MCP 工具

+

自动模式

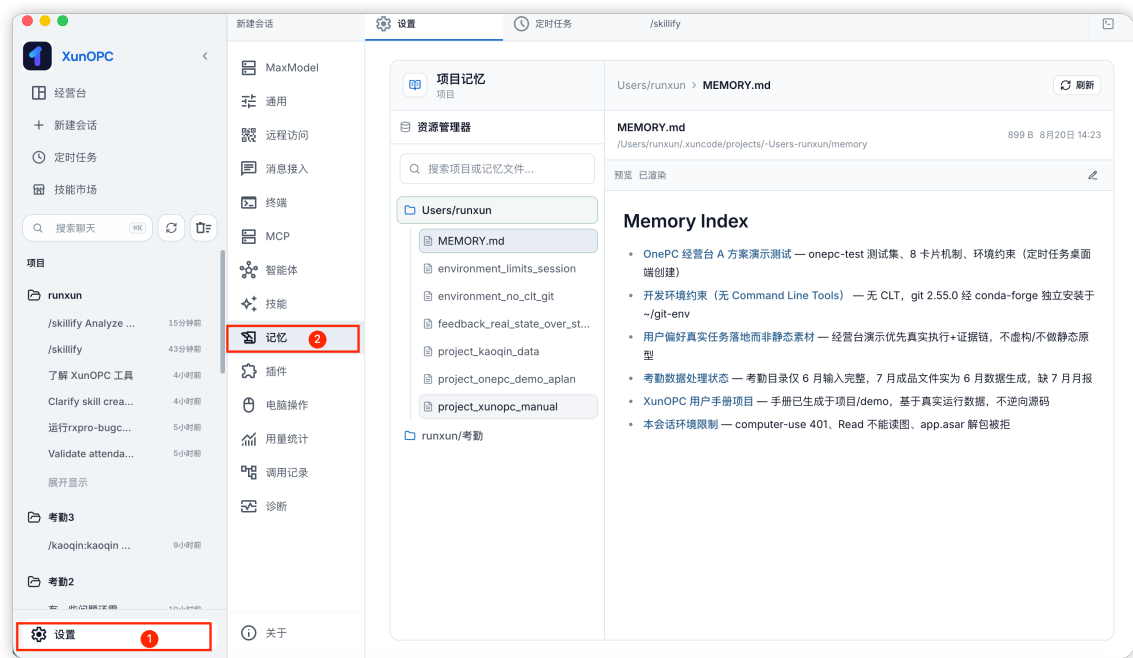
deepseek-v4-flash

最大

运行

选择项目...

9. MCP、插件与记忆



9.1 MCP 服务

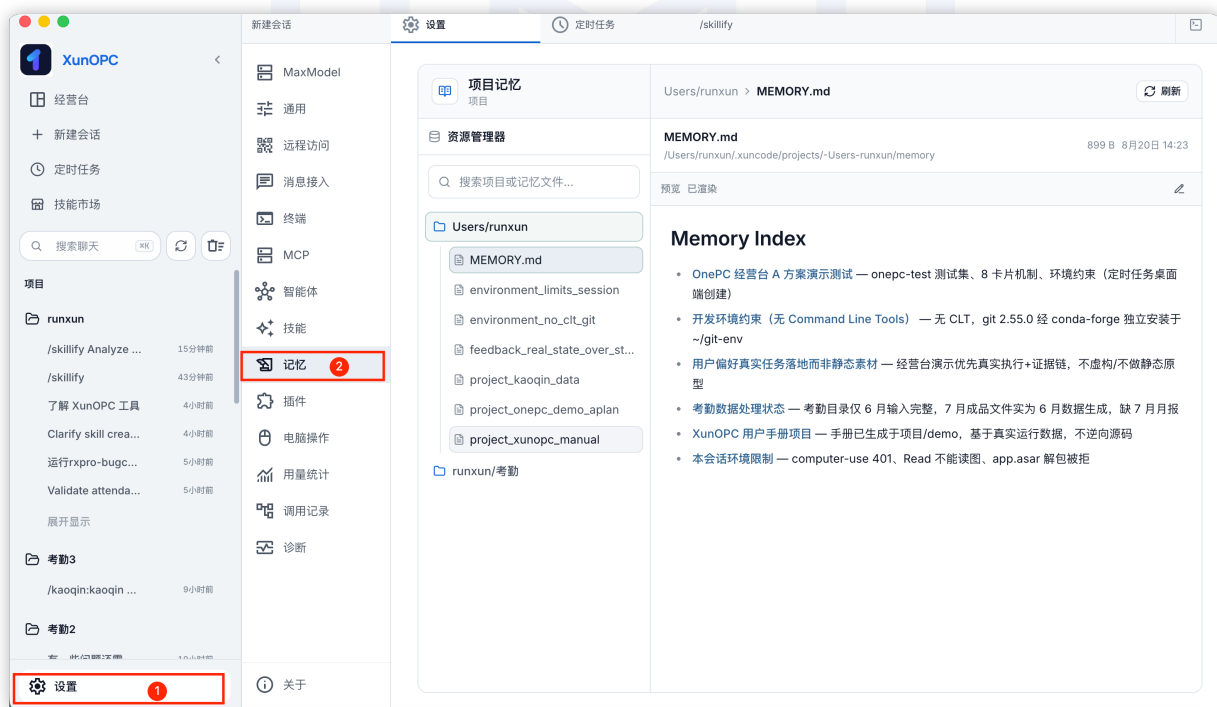
打开“设置 → MCP → 添加服务”，可连接 STDIO、Streamable HTTP 或 SSE。配置范围分为项目私有、项目共享和全局用户。

类型	注意事项
STDIO	直接在宿主主机运行；Node.js、Python、Bun、uv 等必须能从 PATH 找到
HTTP/SSE	核对 URL、请求头、OAuth 与证书；敏感字段展示时脱敏
项目共享	写入项目配置；不要把个人 API Key 放进会随仓库分发的文件



9.2 记忆

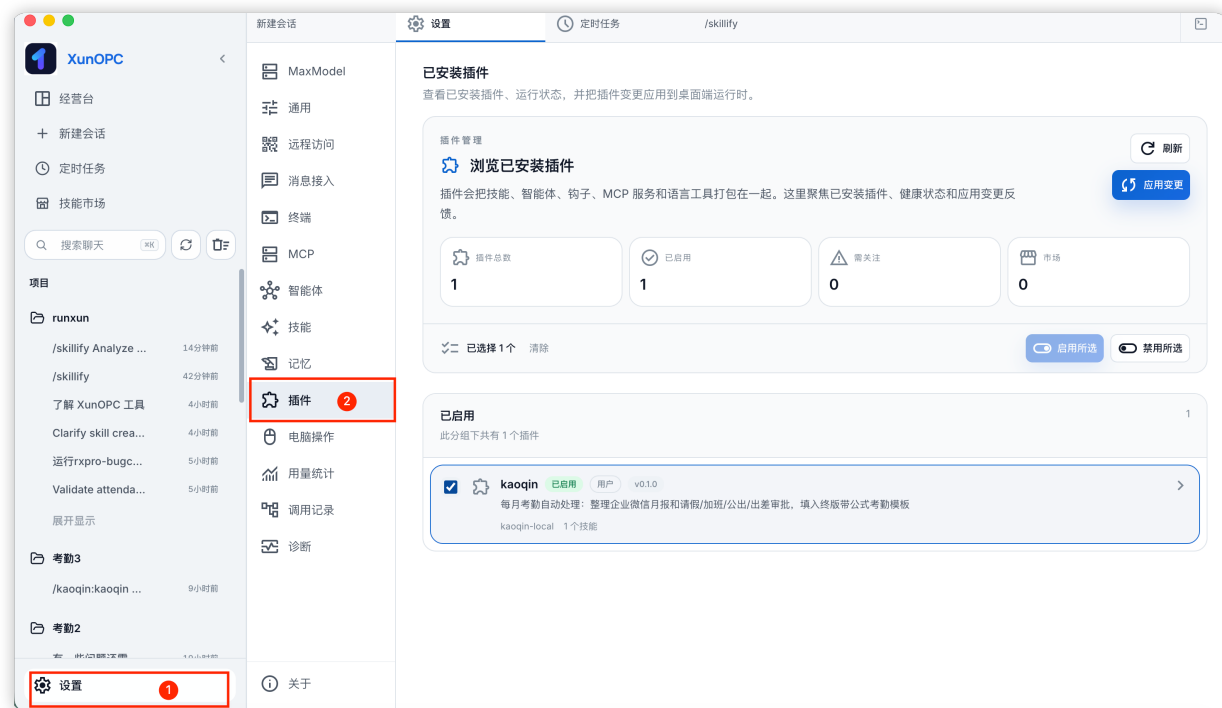
记忆 用于保留项目长期上下文、约定和决策。把稳定事实写进 Memory，把可执行方法写进 Skill：前者回答“我们是谁、为什么这样做”，后者回答“这件事具体怎么做”。



9.3 插件

插件可以打包 Skills、智能体、命令、Hooks、MCP 与语言服务。安装前核对作者、权限、目标目录和外联能力；启用、禁用或更新后点击“应用变更”重新加载。



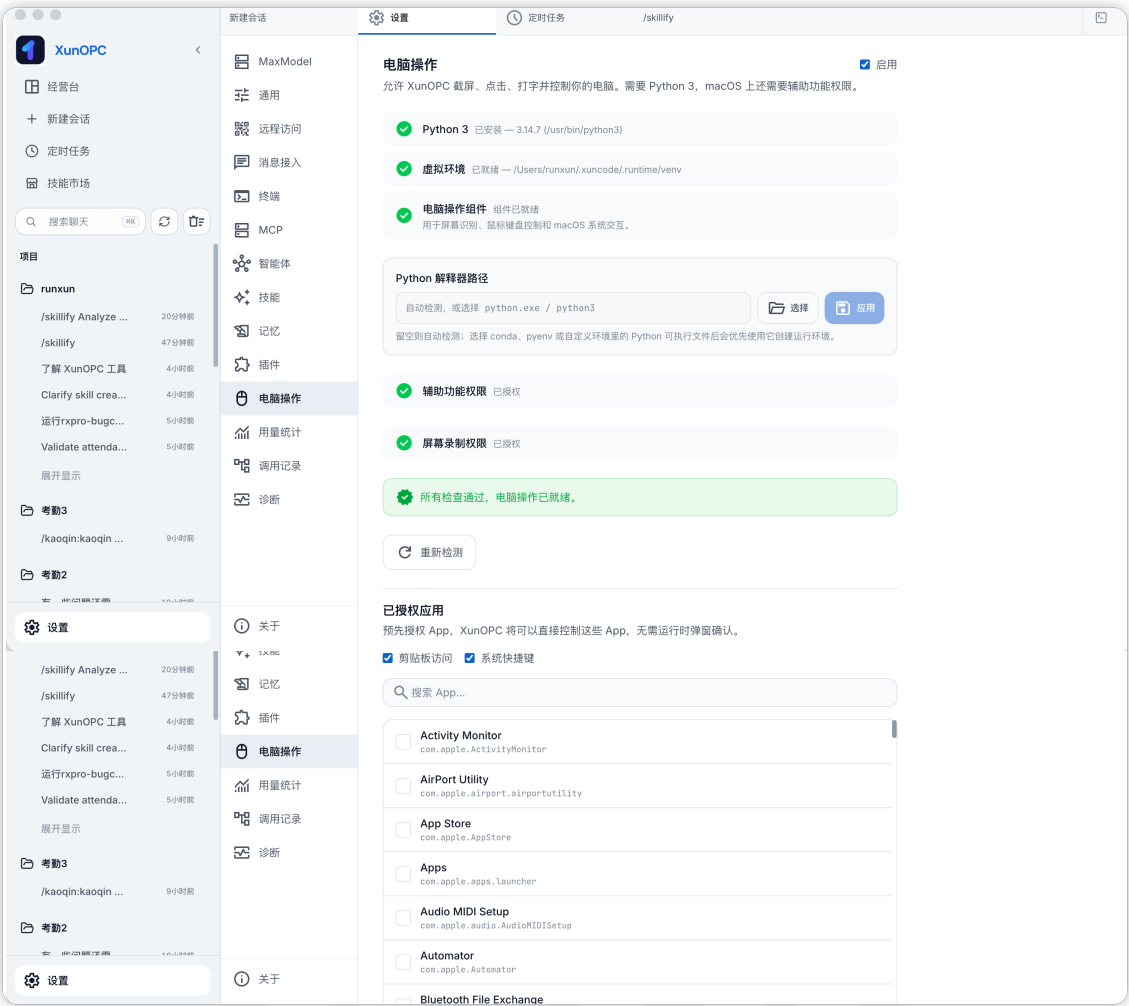


10. 电脑操作

电脑操作 让 Agent 看见并操作没有 API 的桌面应用；能力更大，也需要更严格的系统权限和应用白名单。

1. 进入“设置 → 电脑操作”，确认系统找到 Python 3。
2. 点击“环境安装”，创建独立虚拟环境并安装自动化组件。这里的“组件未安装”不代表主程序损坏。
3. macOS 在“隐私与安全性”授予辅助功能与屏幕录制权限，然后重启 XunOPC。
4. 启用电脑操作，选择可预批的应用；未预批或敏感应用仍应请求确认。
5. 先用无损任务测试，例如打开应用、搜索、截图；确认稳定后再用于正式流程。

安全建议 同一时间只让一个会话操作电脑；不要在屏幕上暴露密码、客户数据或支付页面；涉及发送、删除、发布和付款必须停在人工审批。



11. 消息接入与手机远程

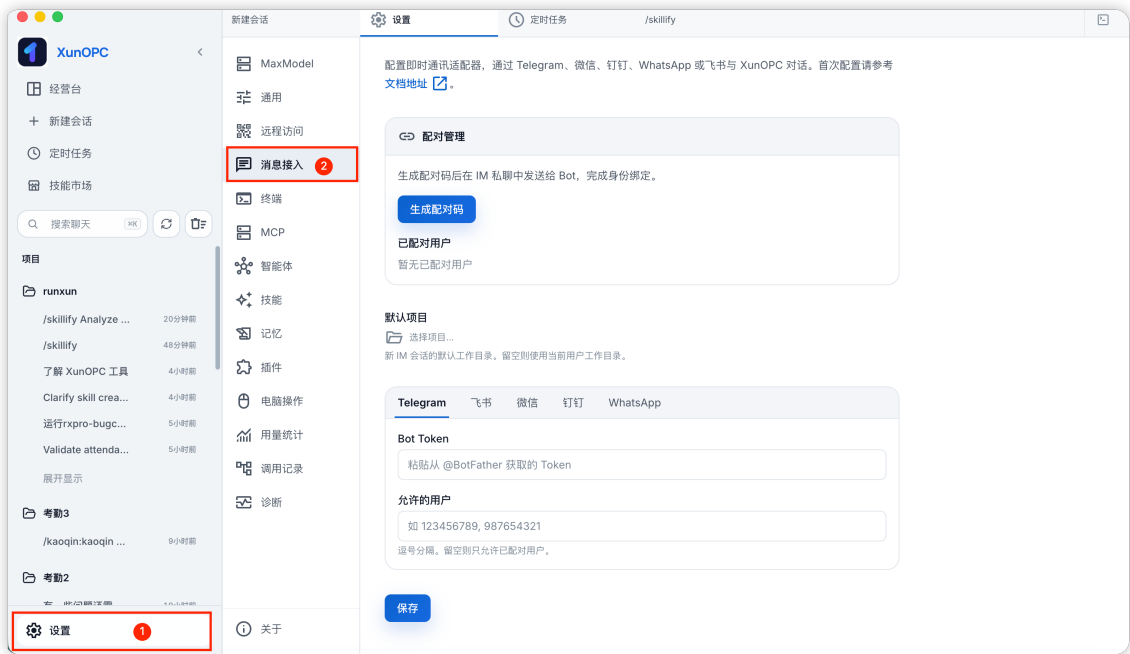
11.1 IM 接入

设置 → 消息接入支持 Telegram、飞书、微信、钉钉和 WhatsApp。发布版会在本地服务启动后拉起对应 Adapter；保存、绑定或解绑后自动重启适配器。

动作	解决的问题
扫码绑定账号	本机适配器用哪个微信/WhatsApp/钉钉账号收发消息
用户配对码	哪个具体联系人有权通过该账号调用 XunOPC
允许用户	由管理员预先授权用户 ID

动作	解决的问题
默认项目	从 IM 创建的新会话在哪个工作目录运行

最常见误解 “微信已绑定” 不等于 “用户已授权”。扫码只建立账号通道；联系人还需发送一次性配对码，或被加入允许列表。



11.2 H5 远程访问

- 1. 进入 “设置 → 远程访问”，默认保持关闭。
- 2. 在可信局域网启用，生成 Token；原文只显示一次。
- 3. 手机扫码或输入 H5 地址；需要反向代理时配置 HTTPS、允许来源和 WebSocket。
- 4. 重新生成或禁用后旧 Token 失效。二维码内含 Token，应按密码管理。



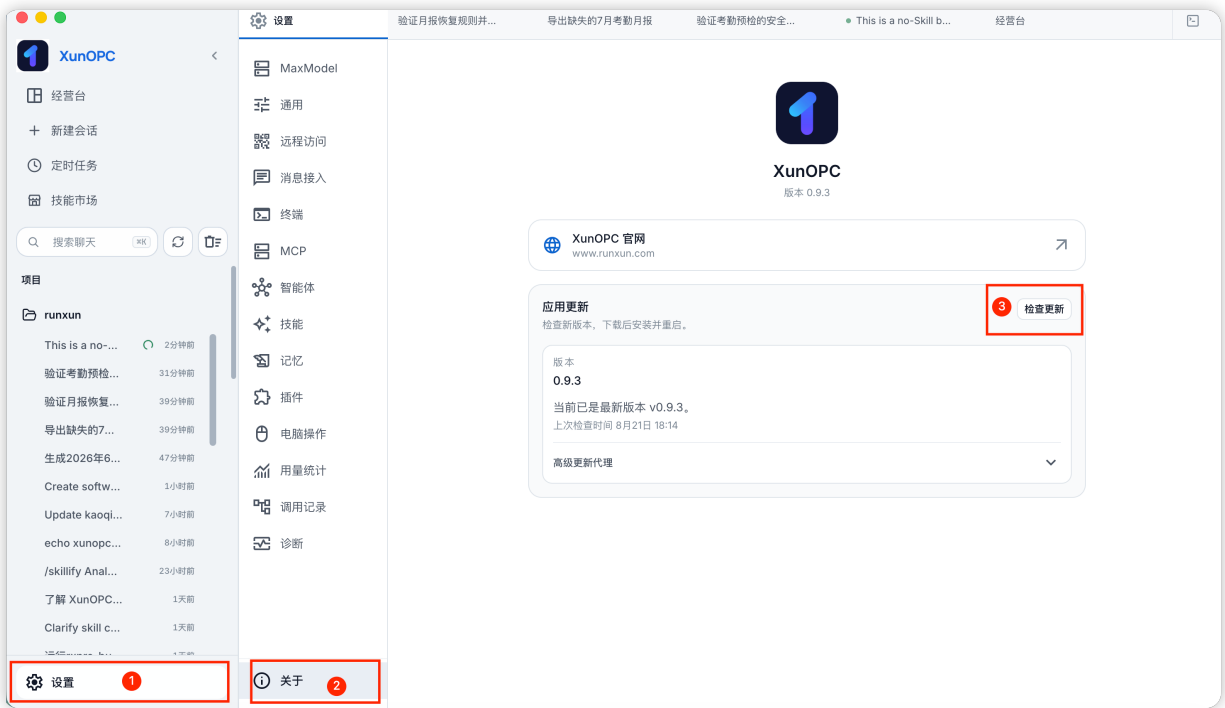
12. 数据、更新与诊断

12.1 数据在哪里

1. 默认用户数据位于本机 XunOPC/XunCode 数据目录；可在通用设置选择自定义数据目录。
2. 项目 Skill 位于项目 .xuncode/skills 或 .agents/skills。
3. SQLite 索引是可重建投影；原始会话和设置文件是权威数据。
4. 更换数据目录或升级前，等待重要任务完成并备份目录。

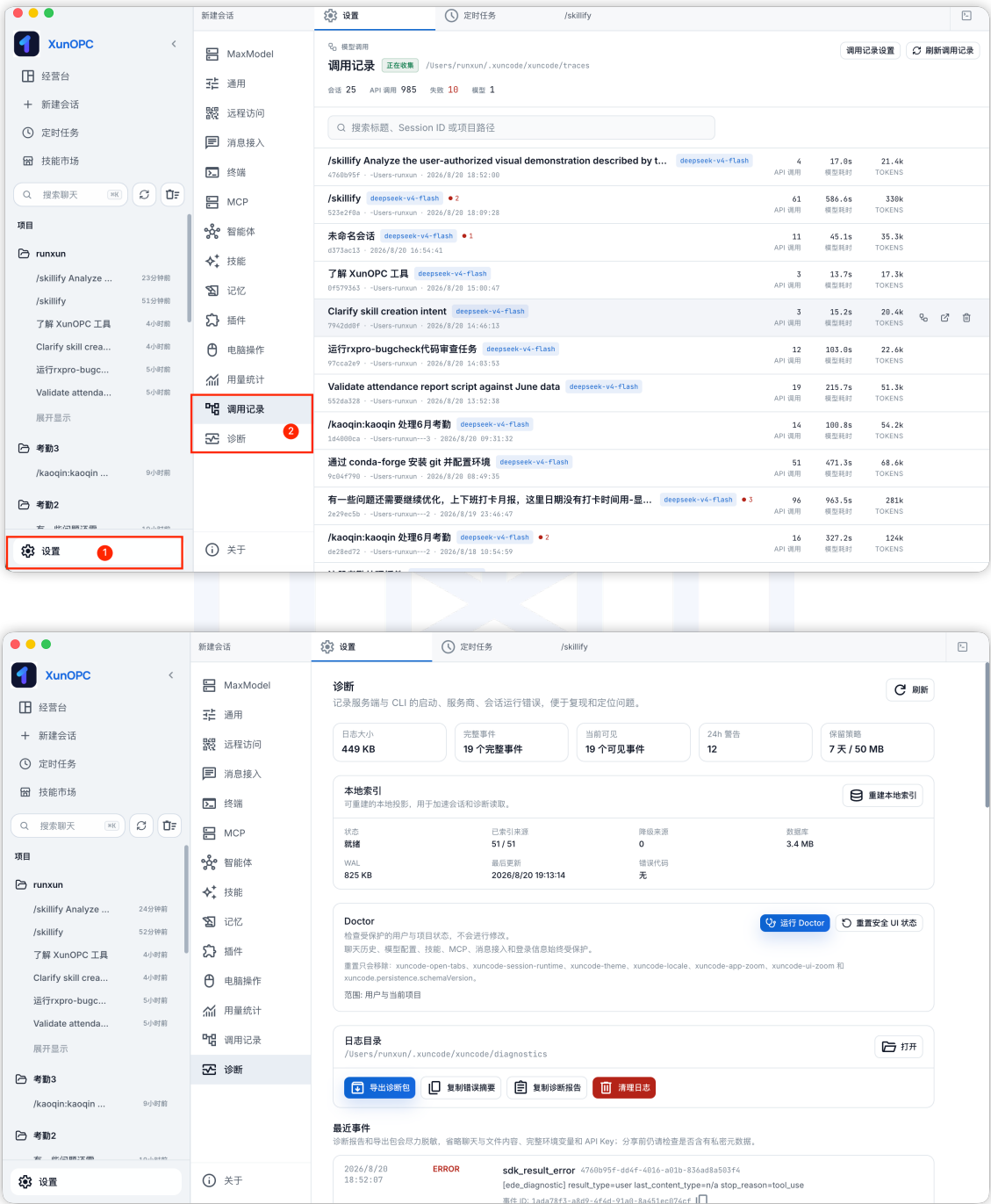
12.2 自动更新

正式版从润迅国内更新源检查版本。下载完成后按提示安装并重启；Apple 芯片和 Intel 各走独立通道。更新保留会话、项目、MaxModel、Skills、Memory、自定义数据目录、IM 和定时任务。



12.3 诊断与调用记录

诊断页用于检查本地服务、Provider、会话、索引、MCP、适配器和数据状态。索引异常时可确认后重建；分享诊断前删除客户数据并确认凭证已经脱敏。



13. 故障排查

现象	优先处理
新会话断开 / ECONNRESET	在 MaxModel 测试连接，确认 Key、模型和网络；重启会话，再看诊断

现象	优先处理
模型目录加载失败	刷新；确认 Base URL 没有 /v1；可临时手动输入模型 ID
400 参数或输出上限	升级最新版，重新选择模型，降低输出/推理强度，检查网关 Beta 头
Skill 不能启用	进入 Skill Gym 完成所有必需场景；检查内容是否在验证后被修改
Skill 显示不兼容	检查目录名、name、description；中文标题放 metadata.xunopc-title
电脑操作组件未安装	确认 Python 3，执行环境安装，授予辅助功能和屏幕录制并重启
定时任务没运行	确认任务启用、电脑未休眠、XunOPC 一直打开
IM 已扫码但不能聊天	让用户发送配对码或加入允许列表；检查 Adapter 状态
H5 手机连不上	确认手机可达本机 IP、允许来源、Token、反代 WebSocket 与代理头
更新重启异常	停止会话和终端，完全退出后重开；必要时覆盖安装同架构版本

14. 安全检查清单

1. ☐ API Key 只保存在设置中，没有进入仓库、截图或会话。
2. ☐ 重要项目使用“询问权限”，未在真实环境打开“跳过全部”。
3. ☐ 外部发送、发布、付款、合同、删除和访问控制保留人工批准。
4. ☐ 第三方 Skill/MCP/插件已核对作者、来源、权限、目标目录和外联。
5. ☐ H5 默认关闭；启用时使用可信网络和 HTTPS，Token 按密码管理。
6. ☐ IM allowedUsers/pairedUsers 非空，离职或不再需要的用户及时移除。
7. ☐ Computer Use 只预批必要应用，屏幕不暴露敏感内容。
8. ☐ 升级和数据目录迁移前，重要任务结束且已有备份。



附录：可直接复制的任务模板

代码修复

复制使用 先复现并确认问题真实性；定位根因后做完整修复，并检查同类路径。不要覆盖现有用户修改，不新增依赖。验收：回归测试、相关完整测试、修改文件与剩余风险。

代码审查

复制使用 只做审查，不修改代码。重点检查正确性、权限、安全、并发、持久化、错误恢复和测试盲区；按严重程度列出文件与行号，并区分已证实、疑似和已排除。

产品需求

复制使用 把这个想法转成可开发方案：目标用户、真实问题、最小闭环、数据对象、权限边界、失败恢复、验收标准和不做什么。先给方案，我批准后再开发。

自动化

复制使用 把这项重复工作设计成定时任务。先手动跑通一次，明确输入、输出、幂等、重试、超时、审批和失败进入经营台的处理方式，再启用计划。

沉淀 Skill

复制使用 把本次成功过程用 /skillify 沉淀为项目 Skill。移除失败尝试、凭证、客户数据和机器专属值，补全输入、输出、验证规则和安全审批点；保存后运行完整 Skill Gym。

竞品对照

复制使用 在同一提交、同一模型、同一任务和同一环境下执行。保留原始会话、工具记录、Diff、构建/测试结果与时间；至少重复三次，盲评结果，不把未验证步骤计为完成。

官方入口 产品：<https://www.runxun.com/ai/xunopc> 下载：
<https://www.runxun.com/ai/xunopc/download> 在线文档：
<https://www.runxun.com/ai/xunopc/docs>