



XunOPC 产品白皮书

版本 v0.9.3 | 编制: 产品部 | 编制日期: 2026 年 8 月 27 日

让一人公司拥有可运行、会学习、可治理的数字团队

聊天框是命令入口，经营结果才是首页；做成一次的方法，应该成为公司的能力。

目录

1. 产品定位.....	4
1.1 一句话定位.....	4
1.2 用户问题与用户价值.....	4
2. 整体架构.....	5
3. 产品能力详解.....	5
3.1 经营能力.....	5
3.2 模型与工作台.....	6
3.3 数字团队执行.....	8
3.4 Skills 能力复用.....	11
3.5 自动化.....	12
3.6 扩展与集成.....	13
3.7 治理与安全.....	14
4. 典型应用场景.....	17
4.1 信创研发工具链.....	17
4.2 技能沉淀与迭代.....	17
4.3 研发交付与版本管理.....	19
4.4 培训与新人带教.....	20
5. 交付标准.....	22
5.1 标准交付范围.....	22

5.2 项目化交付 22

6. 客户价值..... 22

6.1 时间不用耗在进度上 22

6.2 经验留在公司，换人不重来..... 22

6.3 用人门槛降下来..... 22

6.4 数据留在自己环境，才敢放权..... 23

6.5 每个动作都留痕，出了事可审计..... 23

6.6 越用越值钱，能力会复用..... 23

7. 附录..... 23

7.1 名词速查..... 23

1. 产品定位

1.1 一句话定位

XunOPC 是一款本地优先的 AI 智能体工作台，重点解决自动执行编码与电脑操作任务、并以经营台集中管理待决策事项，帮助个人和团队把重复性数字工作交给可信赖的 Agent 完成。

1.2 用户问题与用户价值

用户问题	XunOPC 提供的机制	用户的价值	可验证结果
写代码要在编辑器、命令行、搜索、测试工具之间来回切，换个工具上下文就断	读写文件、执行 shell、跨文件检索、跑测试，都收在同一个 Agent 会话里	一个会话从头写到尾，不用切工具	同一会话能查找改过哪些文件、跑过哪些命令
需求一复杂就不知从哪下手，自己拆步骤费时还容易漏	多步任务自动生成编号计划，子任务并行执行	拆解交给工具，人只确认方向	计划以清单落地，每个子任务执行状态都能查
AI 自己动手跑代码和命令，企业怕失控，不敢放权	命令先逐段做风险评估，敏感操作强制停下等人确认	关键动作由人拍板，不会自作主张	每条敏感命令都有审批记录，没确认不执行
需求没想清楚就动手，改完发现方向错了，白干	计划模式先只读调研、只出编号计划，不直接改代码	动手前先看清方案，少走回头路	执行前能看到完整计划，逐条确认后才动手
改动出错退不回去，越改越不敢动	每次改动前自动生成 git 影子引用快照	改坏了随时退回去，试错成本低	快照与当前状态可对比差异，一条命令回滚
代码、数据外流是实打实的风险，涉密和合规行业不敢用云端 AI	模型请求只发到自配置端点，日志不上传	数据不离开自己的网络，涉密合规行业也敢用	抓包可验证请求只指向自建端点，无外部上传
团队攒下的方法和配置，换个工具就废了	支持 SKILL.md 技能封装、MCP 接入，兼容 CLAUDE.md/AGENTS.md 已有配置	经验留下来反复用，旧配置带过来直接用	已有配置导入即生效，技能可在项目间复用

2. 整体架构

基本架构：模型层入口 → 组织与调度 → 执行底座 → 学习闭环 → 经营层。



3. 产品能力详解

3.1 经营能力

痛点场景：任务一多，逐个会话追进度，重要决定容易漏。

解决路径：

经营台是默认首页。待决定、执行中、已完成、需要介入的任务都集中在这一屏：要拍板的批准、跑失败的任务、刚完成的结果，打开就能看到。

会话里的工具和电脑操作申请统一收进“决策收件箱”，跨会话集中处理。

失败和异常按认证、限流、模型、网络、超时分类并脱敏，给出直达设置或重新运行的补救路径。

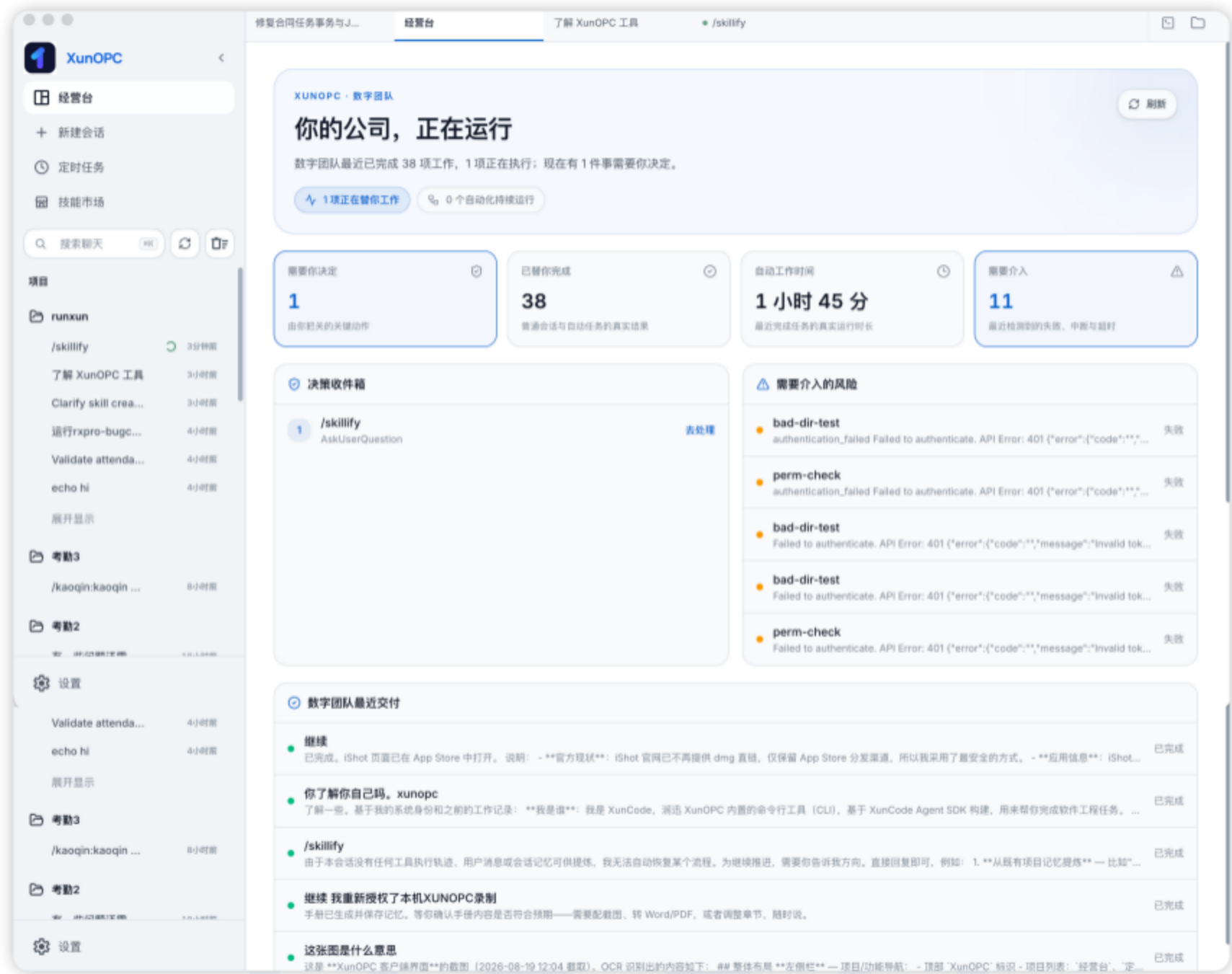


图 3-1 经营台（默认首页）：聚合待决定、执行中、已完成与需介入的真实活动

3.2 模型与工作台

痛点场景：模型接入、切换麻烦。

解决路径：

在 设置 → MaxModel 填一个 API Key，就能读取在线模型目录并选择模型。模型随时可换，项目状态、工作流和证据不受影响。对话窗口右下角可切换主模型、快速、高性能、均衡四类。

编辑 MaxModel

API 密钥

MaxModel

MaxModel

默认

.....

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

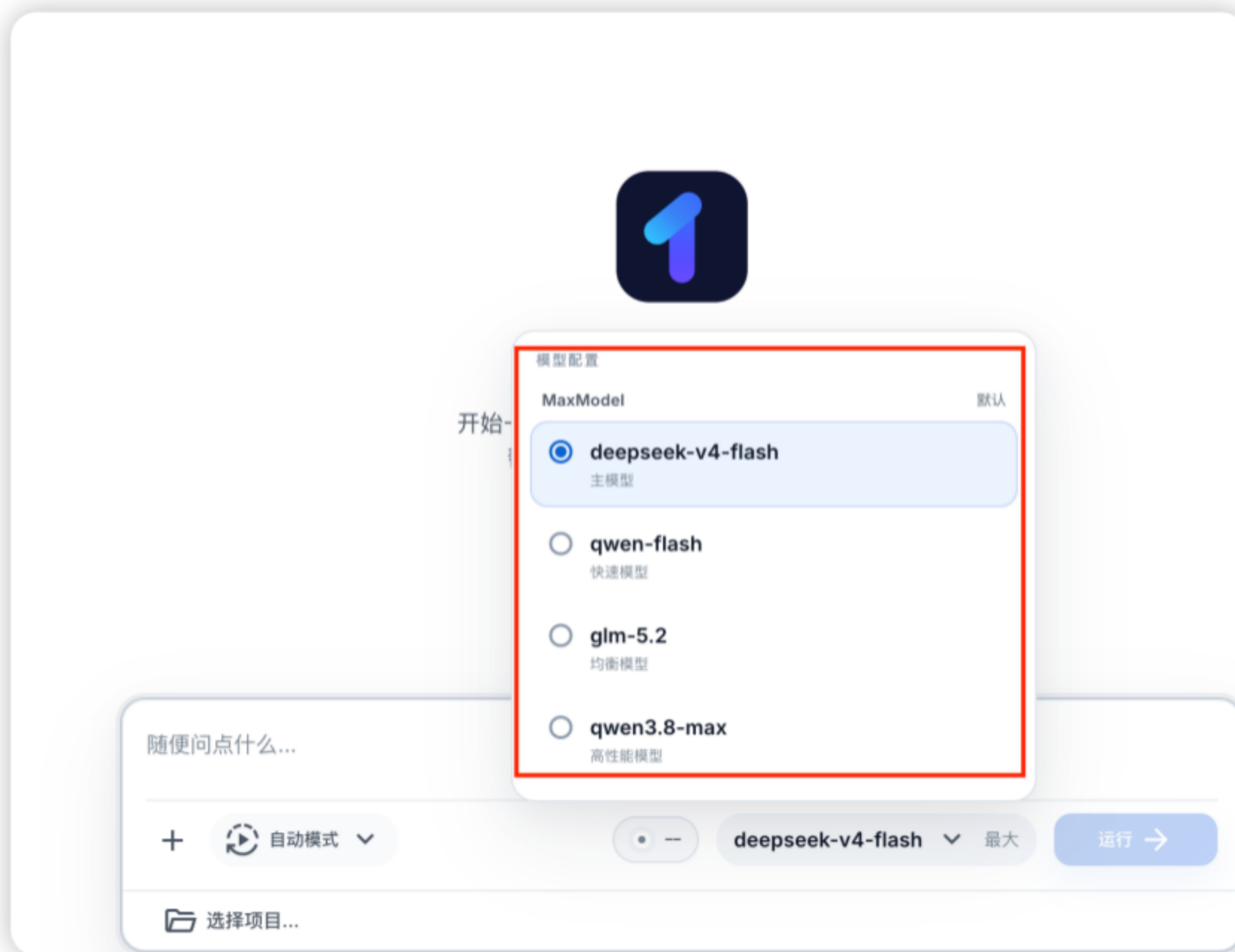


图 3-3 设置 → MaxModel：一个密钥接入在线模型目录

3.3 数字团队执行

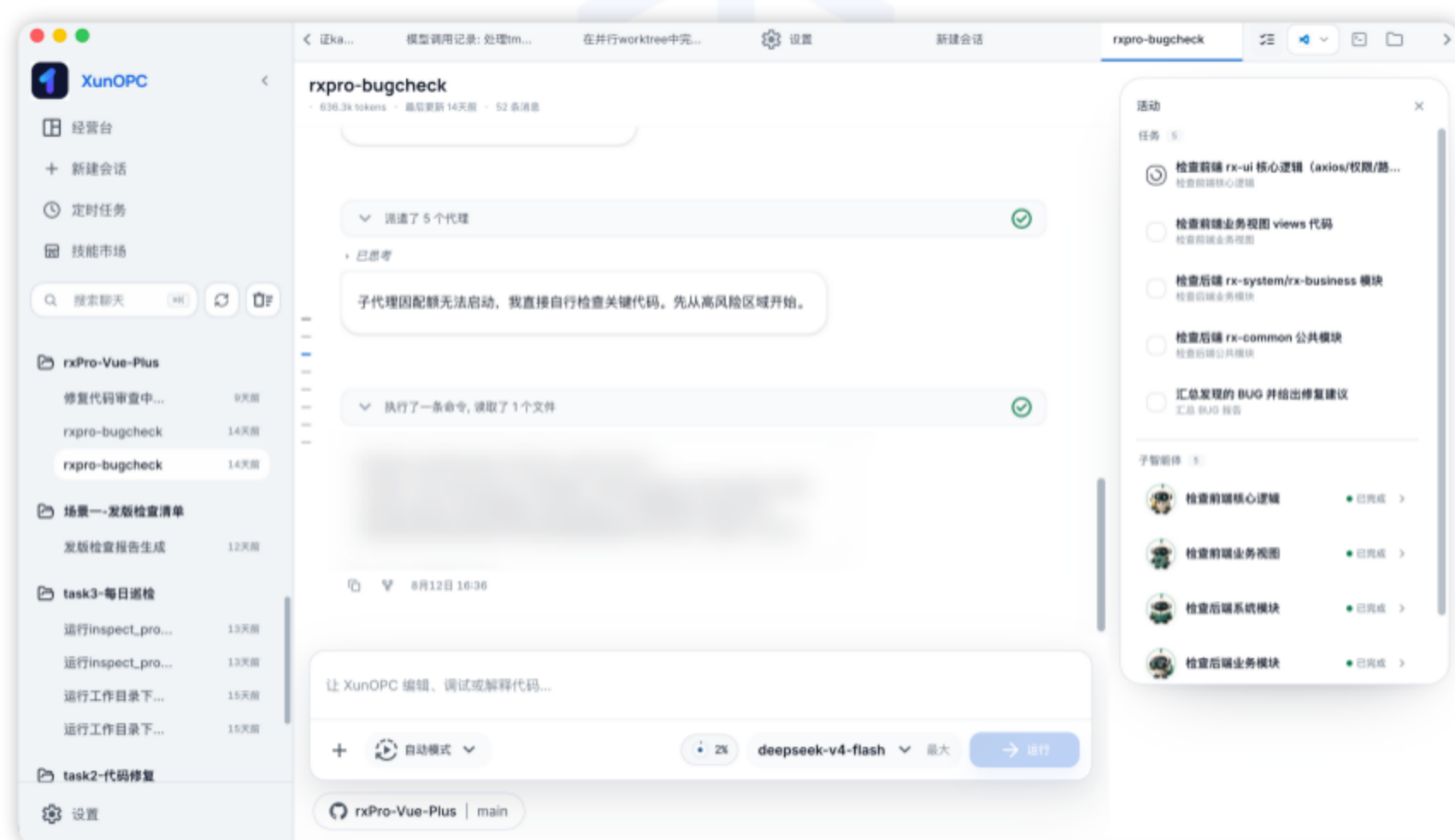
痛点场景：复杂任务的分工和交接靠人盯。

解决路径:

XunOPC 内置 6 个智能体, 负责通用执行、代码探索、方案规划、质量验证、产品指南等岗位。

复杂任务可以拆成子任务并行派发, 也可以多个智能体协同, 活动面板能看到任务计划、智能体状态和后台活动。长任务转成后台任务后, 关掉当前会话也能继续跑, 随时回来查看。

每项工作绑定一个真实项目: 新建会话时选择工作目录, 或为任务创建隔离的 Git 工作树, 多个任务并行不互相影响。终端也在同一个工作台里, 不用在工具间来回切。



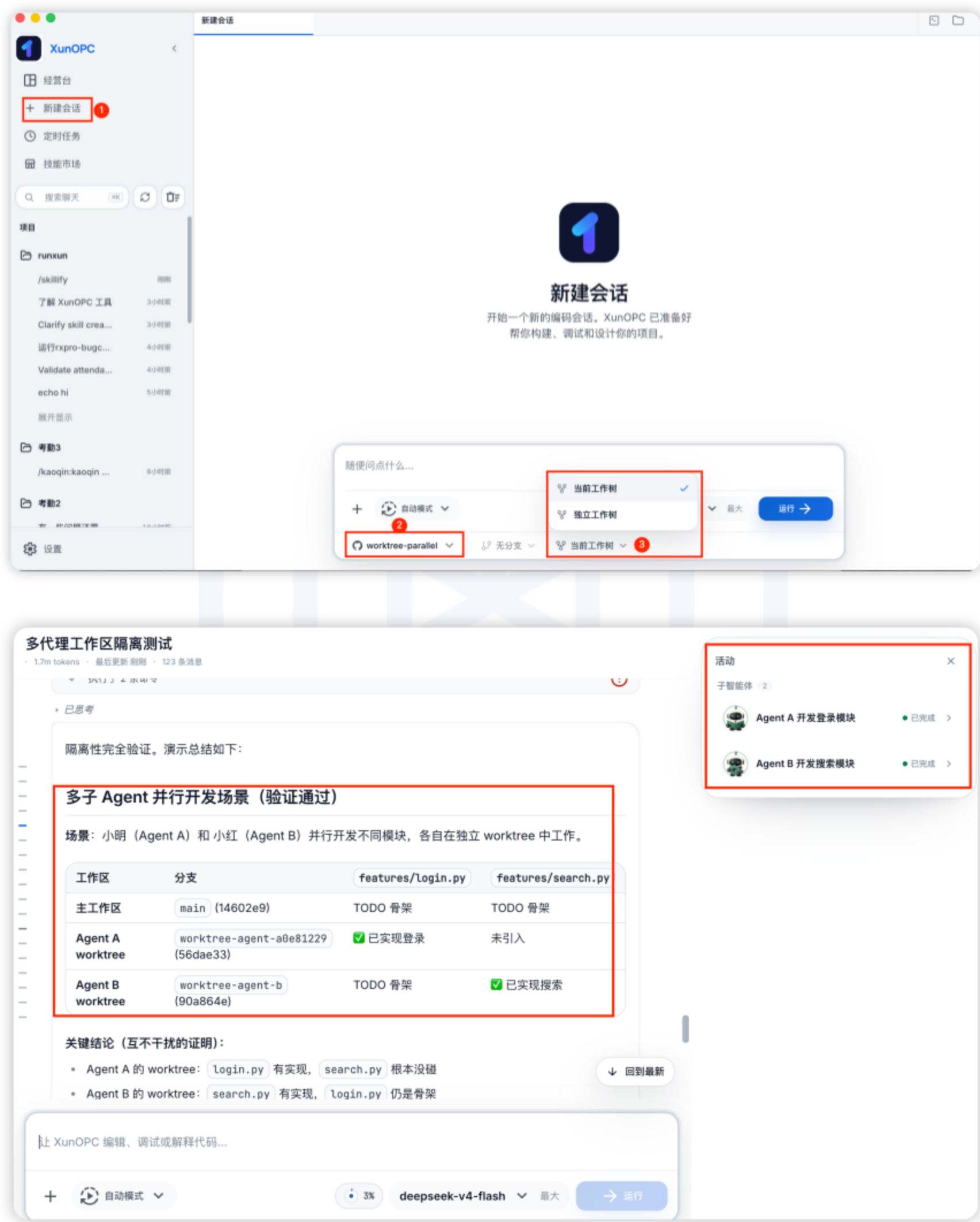


图 3-2 活动面板：任务计划、与后台活动，工作目录以及独立工作树

3.4 Skills 能力复用

痛点场景：成功方法留在每个人记忆里，换人换场景就从头试错，人的知识没有沉淀为公司资产。

解决路径：

一次成功的任务，完成后 XunOPC 会建议沉淀，也可以手动 /skillify，把这次流程写成可复用的 Skill。自然语言识别到创建意图会先进入审阅，通过后保存到受控目录。

Skill 保存的是步骤、输入、输出和验证规则，不只是提示词。Skill Gym 用正常路径、失败恢复、无 Skill 基线、输入边界、安全边界几类场景验证，全部通过才启用。验证结果和版本、内容摘要绑定，改过、回滚或篡改都会失效；运行中真实失败自动暂停；历史版本保留，可追溯、可回滚。

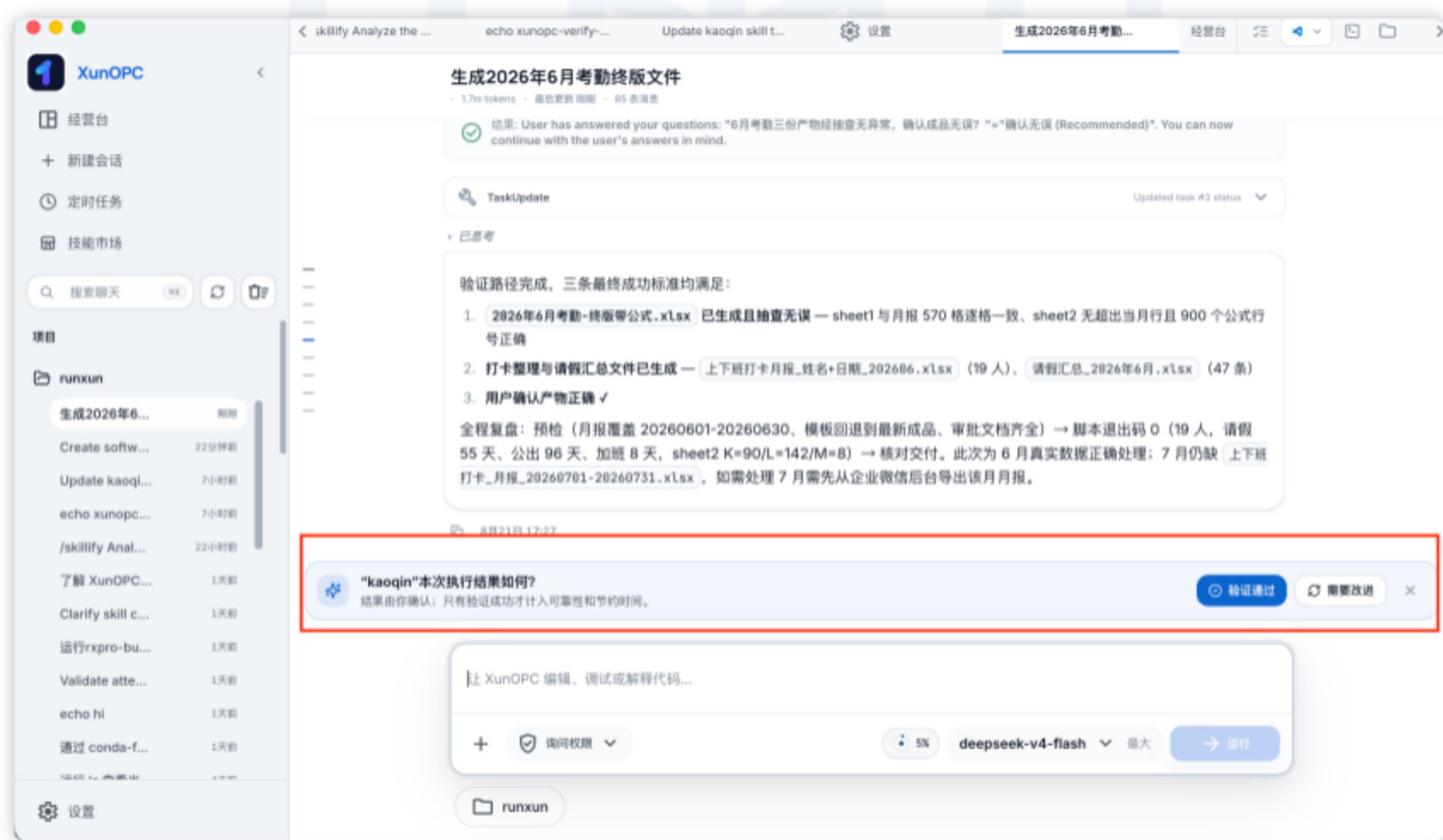




图 3-4 Skill：提炼 → 审阅 → Skill Gym 验证 → 启用

3.5 自动化

痛点场景：重复工作靠人盯着跑，做完才能看到结果。

解决路径：

定时任务在 侧栏 → 定时任务 里按计划在本机运行，完成后通过桌面通知。

新建定时任务

×

描述*

任意会话中输入 /schedule 即可创建。

审查昨天的提交并标记可疑之处

查看过去 24 小时的提交。总结变更内容，标记有风险的模式或缺失的测试，并记录值得跟进的事项。

0 活跃

所有权限

deepseek-v4... MaxModel

runxun

⚠

跳过模式将授予完整系统访问权限 范围 /Users/runxun.

频率

每天

09:00

☒ 完成后推送通知
任务完成后发送原生桌面通知或 IM 消息。

☒ 桌面

☐ 飞书 未配置

取消

创建任务

3.6 扩展与集成

MCP 连接外部工具和数据源，支持 STDIO、HTTP、SSE 三种传输。

版权所有 © 深圳润迅数据通信有限公司。保留一切权利

地址: 广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话: 400-854-5566

官网: www.runxun.com

13



图 3-5 设置 → MCP：连接 STDIO / HTTP / SSE 工具

3.7 治理与安全

痛点场景：权限、凭证、不可逆操作自动化后，风险点变多。

解决路径：

五个权限控制自动化程度：询问权限是默认，每次执行前逐项确认；自动接受编辑放行文件修改，其他动作仍需确认；自动模式审查工具调用后执行安全操作；计划模式只分析不执行；跳过全部只用于可恢复、隔离、无敏感数据的受控环境。高风险操作（比如删除目录）即使已授权也会拦截确认，防止误删。

调用记录能定位模型、工具和会话的问题；诊断和索引重建为本地数据和连接提供补救，索引损坏可以安全重建。

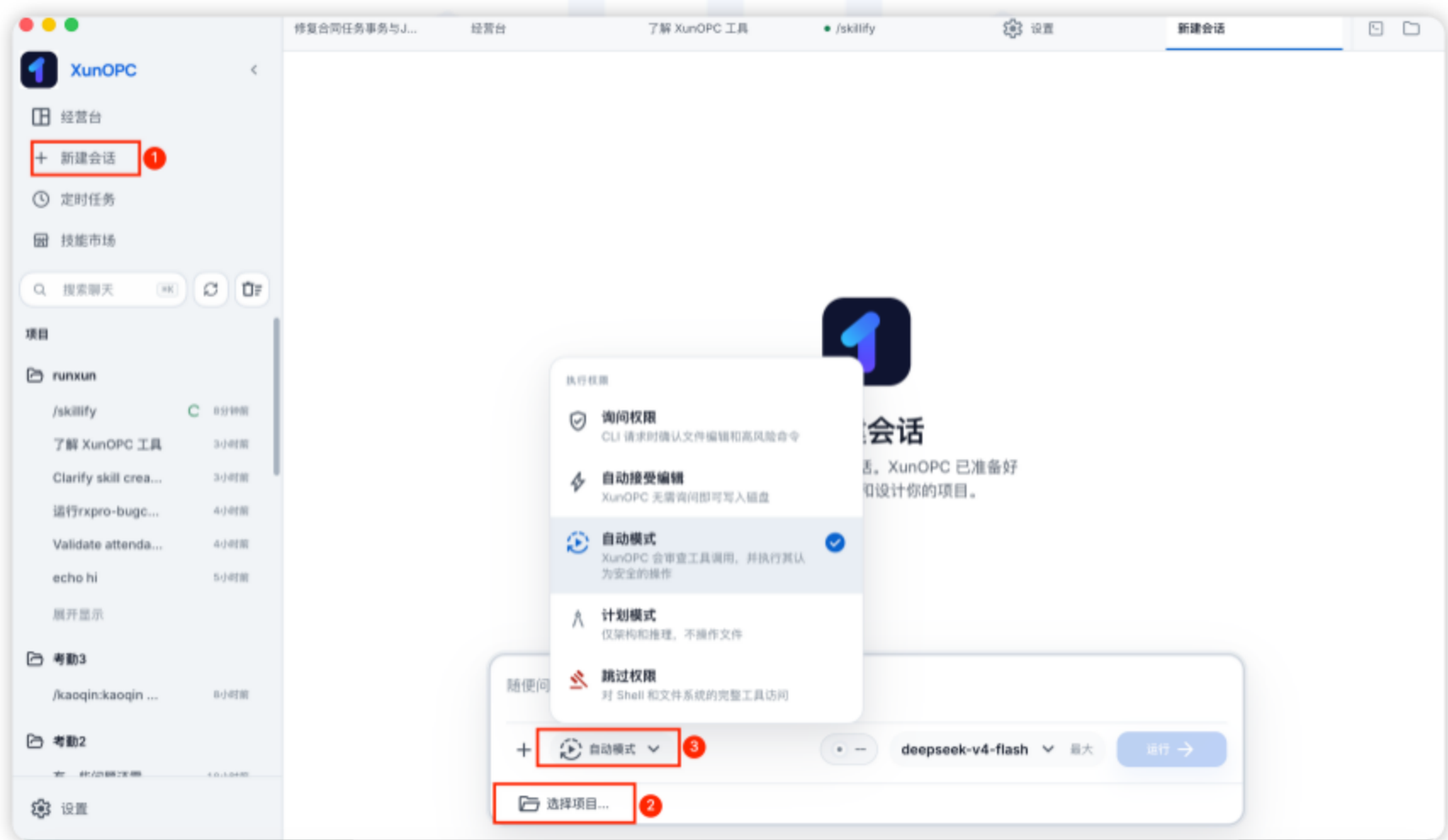






图 3-6 设置 → 调用记录：定位模型与工具问题

4. 典型应用场景

4.1 信创研发工具链

需求背景：信创环境下，开发工具需要与私有化部署配套，代码、终端与 Git 操作必须在可控边界内完成，数据不出域。对于央国企等客户，这是采购的前提条件。

XunOPC 把代码、任务上下文、执行记录、审计日志都留在客户自己的环境里，整个工具链在信创内部运转。

解决方案：

XunOPC 本地优先：会话、设置、Skills、任务、索引默认存在本机；凭证在设置和诊断里脱敏展示；调用记录能定位模型、工具和会话的问题。研发团队在信创内网里就能完成代码理解、缺陷修复、客户定制、测试、发版和复盘。

4.2 技能沉淀与迭代

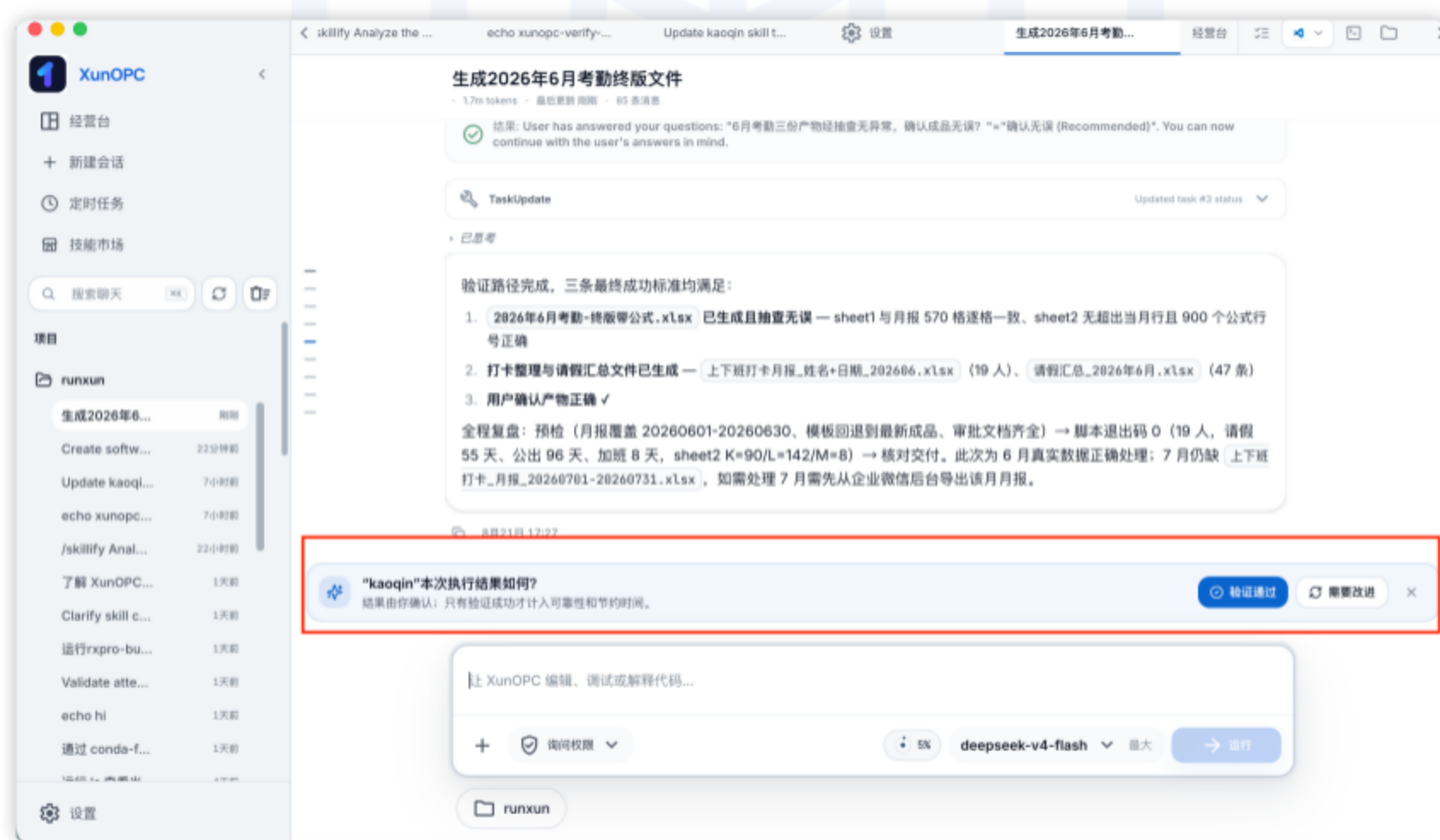
需求背景：核心员工离职或调岗，攒下的经验、踩过的坑、理顺的流程，全被带走。接手的人从头摸索、重复踩坑，成本越来越高，交付越来越慢。

解决方案:

用户和 XunOPC 的一轮对话，围绕一个真实目标走完规划、执行、工具调用、验证和交付。任务完成后，XunOPC 会建议把这段流程沉淀成可复用的 Skill，也可以手动 /skillify；提炼并审阅后保存到受控目录，团队共享。

下次遇到类似任务，本地会自动注入这个 Skill，不用从头讲背景、重复操作，新人直接复用老手的成功路径。业务或环境变了，可以修订 workflow 并重新验证——Skill Gym 用正常路径、失败恢复、无 Skill 基线、输入边界、安全边界几类场景验证，全部通过才启用新版本；验证结果和版本、内容摘要绑定，改过、回滚或篡改都会失效。

每次真实运行的成功或失败都会回到 Skill 里：真实失败自动暂停，不继续扩散；用户确认成功才累计成功率。Skill 在一次一次使用中迭代，越用越准。

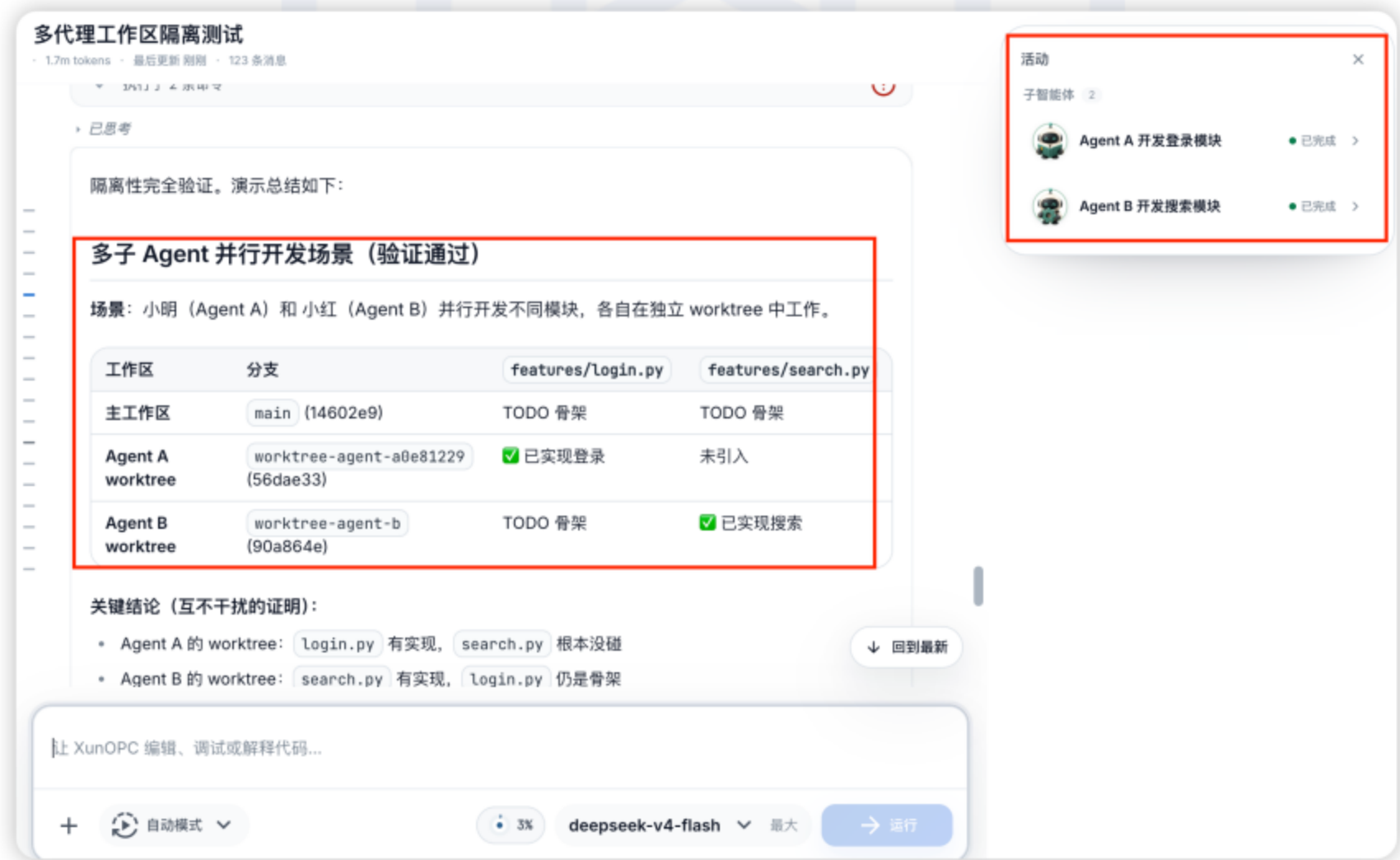




4.3 研发交付与版本管理

需求背景：软件与 AI 服务团队的高频工作是代码理解、缺陷修复、客户定制、测试、发版与复盘。多个子 Agent 并行改同一个项目，版本容易乱，交付口径难统一。

解决方案：用项目工作树隔离并行任务，每个子 Agent 在独立的工作树里改，互不干扰；同一会话内完成代码修改和验证，改动差异实时可见，做错了可以撤销。发版步骤沉淀成 Skill，团队按同一套流程交付，测试记录和复盘留在 workflow 里，版本有据可查。



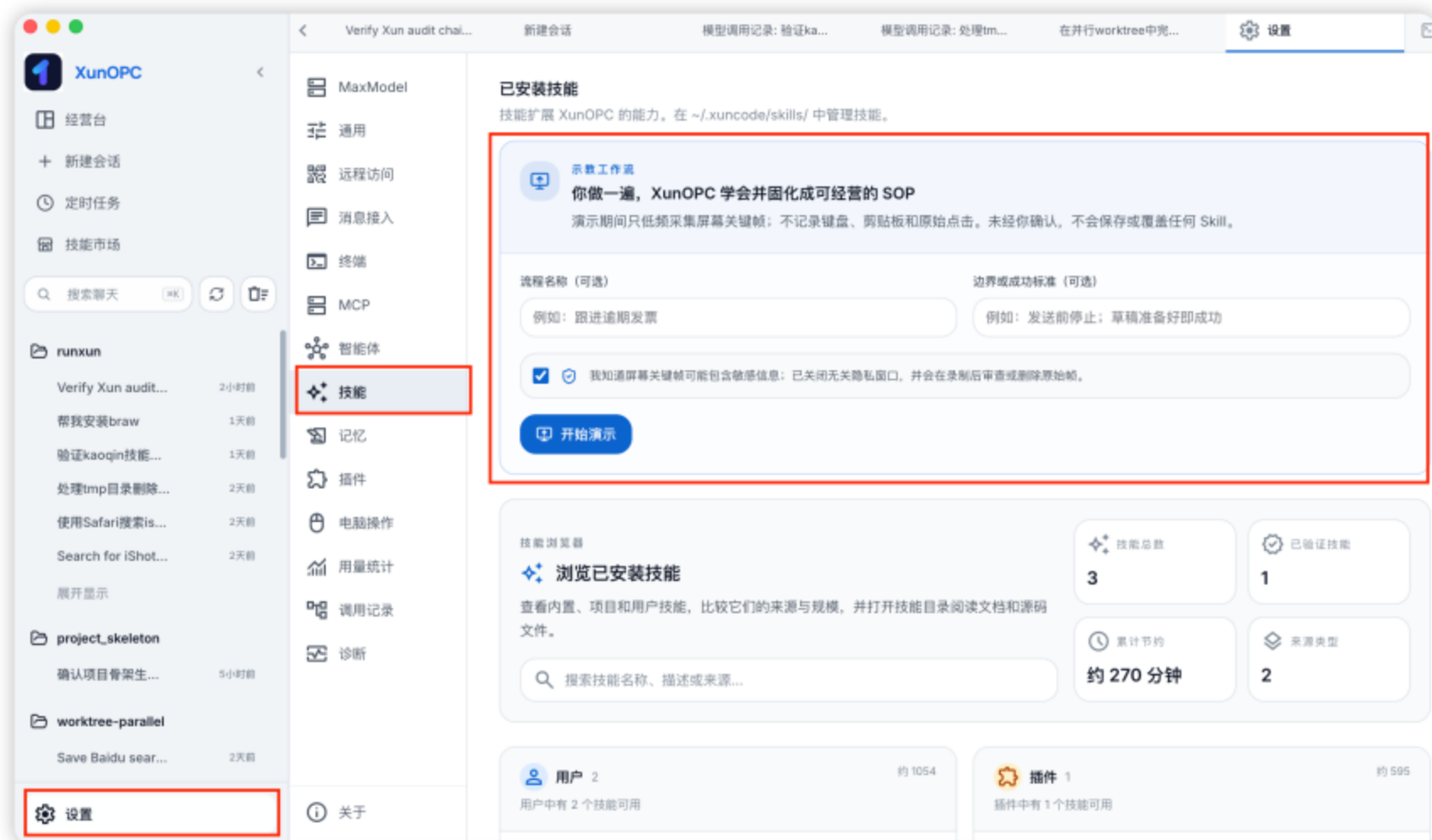
4.4 培训与新人带教

需求背景：老师傅的经验只在脑子里，新人上手要有人带、要讲很多遍；培训材料散落各处，带教质量因人而异。

解决方案:

用 Record & Replay 把老师傅的操作过程录下来，转成带教 Skill，新人按步骤学，卡住的地方看回放，不用等人在旁边。

操作手册和培训材料沉淀成结构化文档，团队共享；带教流程有版本，业务变了就修订重新验证，越用越顺。



5. 交付标准

5.1 标准交付范围

独立安装包与独立更新通道。

官方下载、产品说明、使用文档和更新日志统一托管于润迅官网。

5.2 项目化交付

面向需要把 XunOPC 接入现有工具与流程的团队，以下扩展项依据客户环境单独确认：

安装与部署：提供独立安装包，支持远程安装与远程协助，按客户环境确认。

Model：需要用户自行购买模型密钥 Key

MCP：连接外部工具与数据源。

插件：打包 Skills、智能体、MCP 与语言服务。

IM 与 H5：把入口延伸到手机和常用消息工具。

6. 客户价值

6.1 时间不用耗在进度上

任务自己跑，不用你盯着。该你拍板的、失败了的、做完的，都摆在经营台一屏上，什么时候打开都不会漏。你的时间花在决定上，不花在盯进度上。

6.2 经验留在公司，换人不重来

成功任务沉淀成 Skill。不用你专门花时间教它、训练它，省掉人训练 skill 所需要的技能门槛，时间成本还有便捷性。人走了，经验还在；换人、换项目，不用从头开始。

6.3 用人门槛降下来

招人不用非找熟手。依托于系统内置专家技能库，让新人能快速了解工作，AI 就直接能赋能。老师傅的做法沉淀成带教 Skill，新人照着学就能上手；同样的新人，别人带三个月，你三天能上手。换人、扩招，经验都不会断档。

6.4 数据留在自己环境，才敢放权

你的每一次对话、都只留在你自己的电脑上。这意味着你可以放心把敏感的工作交给它去做——不管是内部文档、客户资料还是商业机密，不用担心被第三方看到。高风险操作（比如删除目录）即使自动模式权限也会先拦截确认。

6.5 每个动作都留痕，出了事可审计

工具调用、审批、文件改动都有记录，同样出个差错，别人靠回忆、靠对质，半天说不清；你打开记录，出了差错能查到是哪一步、哪个模型、哪个工具的问题。满足涉密、审计这类要求严格的客户。

6.6 越用越值钱，能力会复用

普通软件买来就是固定功能，XunOPC 用着用着会积累：每一轮成功任务、每一个验证通过的 Skill，都在往公司里存资产。Skill 在一次一次使用中迭代，越用越准；团队积累越多，后面的人越省力。

7. 附录

7.1 名词速查

名词	解释
XunOPC	面向一人公司与小型数字组织的 AI 原生经营操作系统
MaxModel	统一模型中转服务，一个 API Key 接入可用模型目录
Skill	可发现、可审阅、可验证、可版本化的复用能力
Skill Gym	以正常、恢复、基线和边界场景对当前 Skill 版本进行证伪的验证套件
Record & Replay	用户主动示教并采集关键帧、标记和说明，再提炼成结构化 workflow
MCP 经营台	连接外部工具、数据源和服务的开放协议 聚合真实待决策、进行中、异常和完成结果的默认首页