

(38) Miles Ma on X 万字长文 | WorkBuddy 从入门到精通

万字长文 | WorkBuddy 从入门到精通



在国内做 AI 交付，真正难的是把模型放进客户现有的工作里。到了政企项目，网络、数据、采购、账号和运维会先把方案筛一遍。国外工具再好，无法稳定访问、无法授权、无法进入采购，也只能停在演示阶段。

所以，WorkBuddy 一定要学。它把模型、本地工作空间、权限、技能、连接器和产物放在同一条任务里，让 AI 能够把文件做出来、把修改留下来，再交给人验收。它不能替代业务判断，也绕不开合规，但它离国内的真实工作比一个聊天框近得多。

下面从一份会议纪要开始，先跑通读取文件、生成产物和查看变更，再讲模型、技能、连接器、项目、助理与自动化。这套方法学会以后，换文件、换任务、换项目都能继续用。



WorkBuddy 解决的，是模型到交付之间那段路

普通聊天工具的典型动作是“你问一句，它回一段”。WorkBuddy 更接近一名坐在电脑前的执行者：先理解目标，再找材料，决定步骤，读取或修改获得授权的文件，必要时调用技能和外部服务，最后把结果交给你检查。

一个完整任务通常会经过这条路径：

选择工作空间 → 提供资料 → 说清输出要求 → WorkBuddy 规划并执行 → 生成产物 → 查看文件变更 → 人工验收和追问

因此，使用它时最重要的能力是给任务划清边界，花哨的“万能提示词”要排在后面。它要读什么，产物放在哪里，哪些文件不能动，最后怎样才算完成，这几件事越清楚，结果越稳定。对交付团队来说，**这些边界还决定了方案能否被复用和交接**。

从首页能看到，WorkBuddy 把入口分成“日常办公”“代码开发”“设计创意”，日常办公下面还有文档处理、金融服务、数据分析及可视化等快捷场景。分类本身没有那么重要，重要的是这些任务最后都回到同一套界面：工作空间负责限定材料，权限负责限制动作，模型负责理解，右侧面板负责展示产物和变更。



首页右侧有一个“概览/产物”区域。任务开始前它通常是空的；执行后，生成的文件会出现在这里。输入框下方则集中放着工作空间、权限、模式和模型。以后遇到结果不对，先看这几处，往往比反复改提示词更有效。**模型可以换，任务边界和验收位置不能跟着一起消失**。

要把它带进真实工作，先守住三个边界

建一个单独的练习文件夹

不要拿桌面、下载目录或一个正在交付的项目做第一次测试。新建一个空文件夹，例如：

```
WorkBuddy-练习/  
├── 会议纪要.txt  
└── 销售数据.csv
```

把文件副本放进去，保留原件。这样即使任务理解出现偏差，影响也被限制在练习区。等你熟悉“产物”和“变更”两个面板后，再把真实项目逐步迁进来。

默认权限起步

本机界面里，权限下拉菜单默认是“默认权限”。展开后还能看到“允许完全访问”的开关。小白阶段保持默认权限即可。它会在相对受控的范围里工作，遇到高风险操作再让你确认。



完全访问只会扩大操作范围，不会让模型突然变聪明。批量整理文件、跨目录搬运或运行某些本地工具时可能需要它；阅读资料、生成文档、分析表格等常见练习通常没有必要一开始就打开。

如果任务涉及删除、覆盖、上传、发信、付款、公开分享或改动大量文件，应当在指令中写出“执行前先列出计划并等待我确认”。当 WorkBuddy 弹出授权卡片时，也要看清对象和范围，不要习惯性地点确认。

先认清版本差异

本机 5.2.6 界面底部已经显示“新版本就绪”，并给出“更新日志”和“重启升级”。本次教程没有替用户重启升级，因为升级会打断正在进行的任务，也可能改变当前界面。

你可以先看更新日志，结束手头工作、保存重要文件后再升级。如果文章里的按钮和你的界面略有不同，优先按功能名称寻找，不必逐像素照抄。

把这些名词放回一条交付流程

刚开始最容易混淆的是一组听起来都像“帮我做事”的名词：任务、项目、技能、专家和连接器。可以先用下面这张表建立地图。

这些名词单独看很像产品菜单，放进交付过程就清楚了。任务承载一次工作，工作空间限定资料，权限限定动作，技能负责具体工具，连接器接入客户已有系统，项目负责把一套做法留给下一次。它们共同解决的是同一个问题：怎样把模型的一次回答变成可以反复执行、可以交接的工作。

名称	用大白话解释	什么时候用
任务	一次具体的工作过程	总结文件、做表、写报告、改代码
工作空间	这次任务被允许工作的本地文件夹	每个客户、课程或项目单独建目录
上下文	WorkBuddy 当前可参考的材料	文件、图片、对话、网页、项目资料
产物	任务交付出来的文件或可预览内容	Markdown、表格、PPT、网页、图片等
变更	WorkBuddy 对文件做过的新增、删除和修改	验收时逐项检查
模型	负责理解和生成内容的 AI 引擎	默认用 Auto，特殊任务再指定
模式	决定先问、先规划还是直接执行	问答、复杂项目、日常操作分别选择
技能	封装好的工具或固定动作	PDF 处理、图表、格式转换、特定流程
专家	带角色、方法和工具组合的单人配置	市场研究、产品经理、金融分析等
专家团	多个专家分工协作	复杂报告、跨专业方案，消耗通常更高
连接器	连接外部服务的桥	腾讯文档、邮箱、会议、TAPD、飞书等
项目	一组长期任务共享配置和资料的容器	团队知识库、产品需求、持续交付
助理	从微信、企业微信等入口远程叫起 WorkBuddy	离开电脑后提交和查看任务
自动化	按时间表重复运行的本地任务	日报、周报、资料巡检、定时汇总
记忆	从历史协作中保存的偏好和背景	长期保持称呼、格式、习惯和项目信息
灵感	可浏览、复用和分享的任务案例	不知道怎么下指令时找样例

先别急着把每个模块都配满。**第一个阶段只需要掌握任务、工作空间、权限、产物和变更**，已经足以完成大量日常工作。

先跑一件小事，看看文件能不能真正落地

下面用实际跑过的任务走一遍完整流程。练习文件 meeting-notes.txt 里有会议日期、三名角色、三项任务和各自的截止日期。目标是生成 action-list.md。

我特意没有从复杂报告或炫目的网页开始。**一个交付系统是否可靠，先看它能否读对文件、生成产物、保留原件，再把改动完整展示出来**。这个小任务足以检查整条链路。

第一步：选择工作空间

点击输入框左下角的文件夹位置，选择刚才建立的练习目录。选择成功后，界面会显示文件夹名称。本次实操使用的是 demo-workspace。



工作空间相当于给 WorkBuddy 画了一条工作边界。以后同时做多个客户项目时，不要在同一个大目录里混着跑。一个项目一个文件夹，任务历史、产物和变更才容易追踪，也能降低引用错文件的概率。

第二步：把要求写成四个部分

一个实用任务可以按“动作、输入、输出、约束”来写：

请读取工作空间中的《会议纪要.txt》，生成一份《行动清单.md》。

要求：用表格列出负责人、任务、截止日期和状态；

状态统一写“待开始”；

不要修改原文件；

完成后告诉我新建了哪个文件。

“读取会议纪要”是动作和输入，“行动清单.md”是输出，“表格字段、状态、不改原文件”是约束，“告诉我新建了哪个文件”是验收信号。

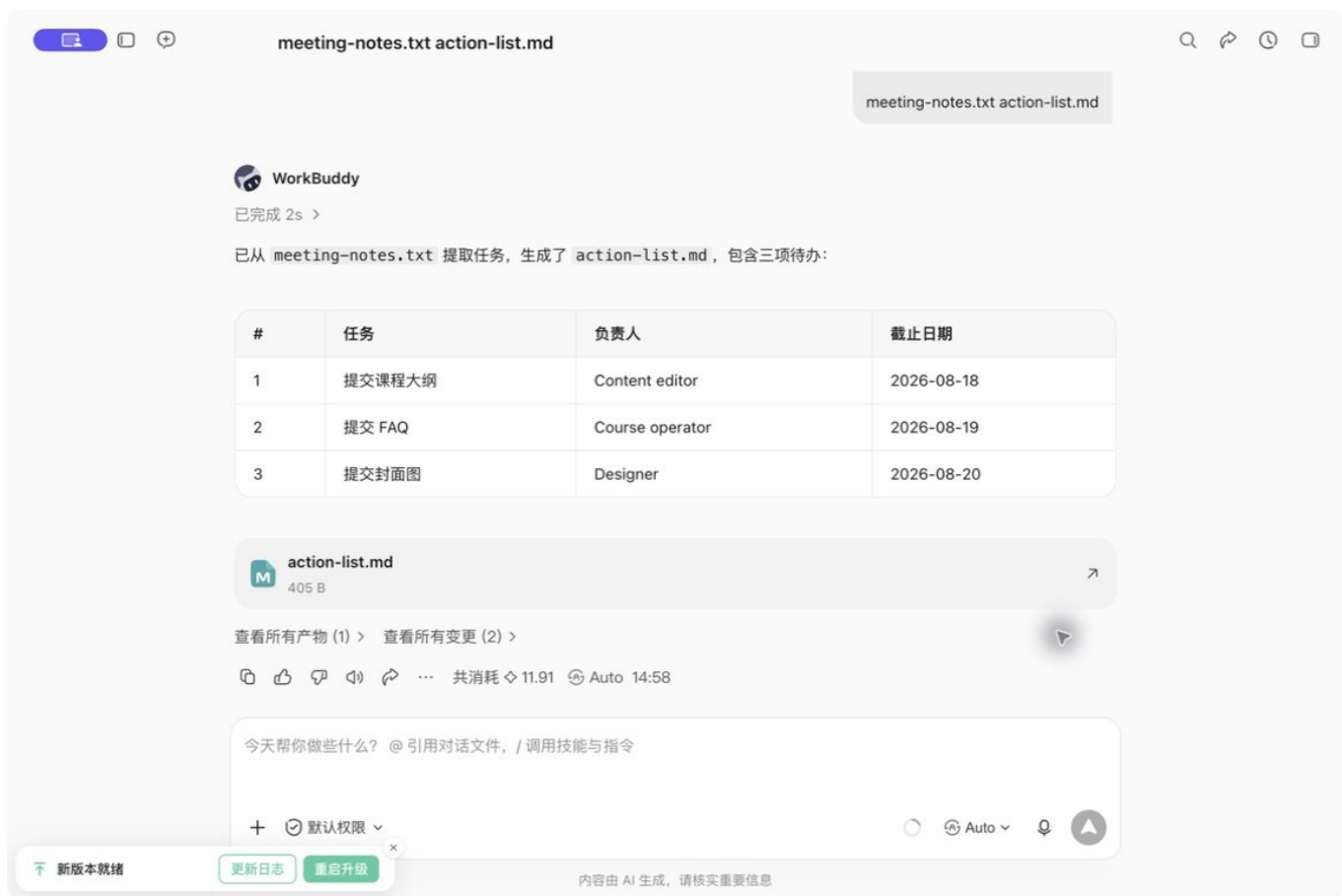


文件名最好写准确。材料很多时，可以点加号上传，也可以拖进输入框，或输入 @ 引用当前对话和工作空间中的文件。直接写“帮我处理一下这个”会迫使 WorkBuddy 猜测目标，猜对是运气，猜错却可能真的改文件。

第三步：发送并观察执行过程

点击发送后，任务会进入对话页。你会看到读取文件、创建产物、调用工具等过程信息，有些模型还会显示预计消耗、运行时间和阶段状态。任务执行时先别连续发送同一条指令，否则可能生成重复文件。

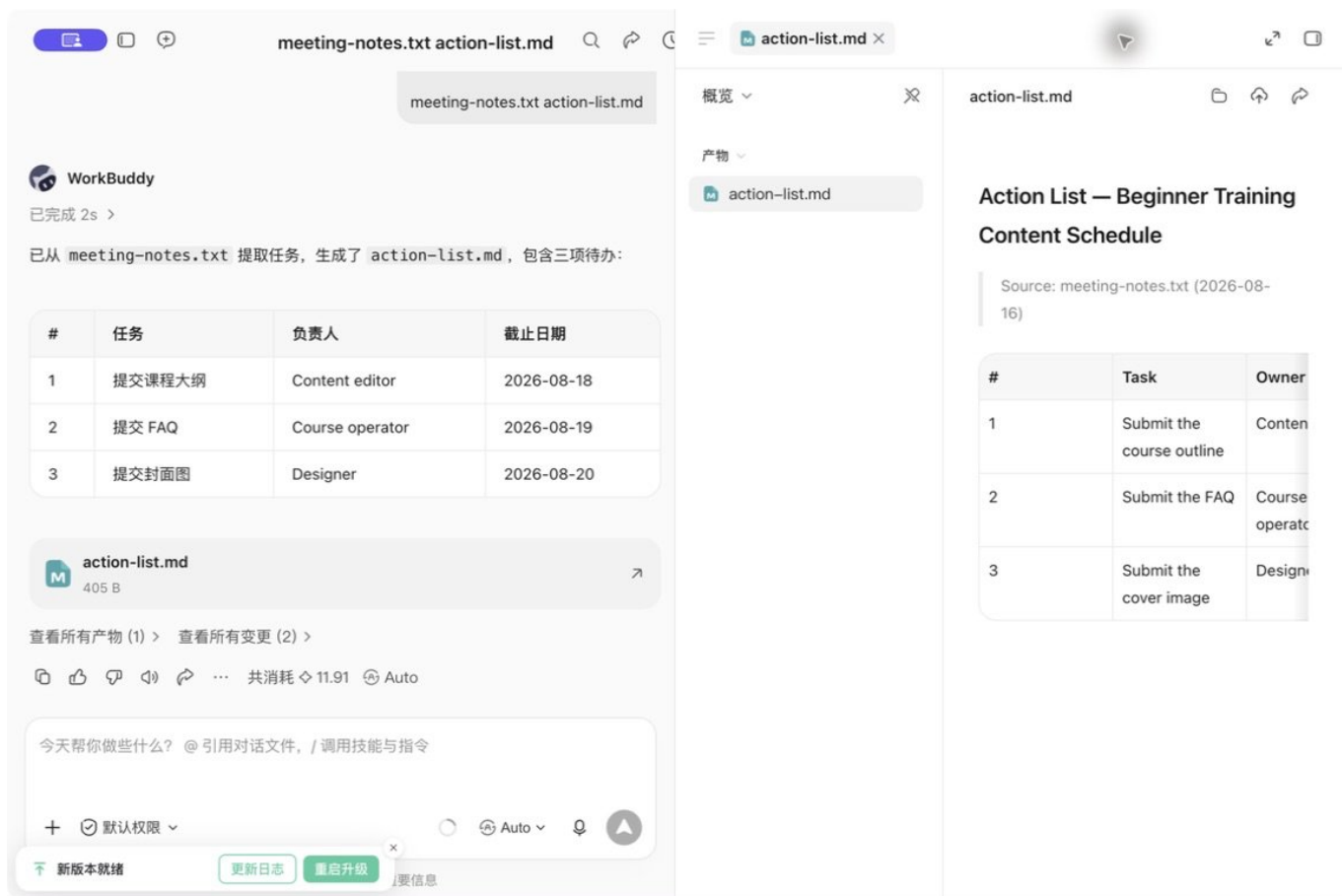
本次实操中，WorkBuddy 读取了 meeting-notes.txt，在两秒左右给出三项待办摘要，并生成 action-list.md。界面同时显示了本次使用的 Auto 模型和消耗信息。



如果它显示“正在准备”很久，先等一小会儿，再看网络状态和任务详情。新版更新日志一直在修复卡在准备阶段、弱网恢复和多任务切换的问题。不要在状态尚未明确时反复点击发送。

第四步：验收产物，不只看聊天回答

点击产物卡片，右侧会打开文件预览。这里能看到文件名、内容以及打开所在文件夹、上传到云端、分享等入口。**先检查标题、字段、行数、日期、格式和遗漏项，再决定是否导出或分享。**



本次产物包含三行任务，日期与原文件一致。英文角色名来自练习材料，说明 WorkBuddy 没有擅自替换负责人。状态列采用 Not started，与期望语义一致；如果交付必须是中文，就继续追问：“把状态列统一改成‘待开始’，负责人保留原文，其余不变。”

这类追问比重重新开一个任务更省上下文。修改后再预览一次，直到结果达到交付标准。

第五步：查看所有变更

点“查看所有变更”，右侧会列出新增和修改的文件。本次任务除了 action-list.md，还出现了 .workbuddy/memory/2026-08-16.md。验收不能只看产物卡片，代理在完成任务时可能记录本地记忆或产生辅助文件。

meeting-notes.txt action-list.md

meeting-notes.txt action-list.md

WorkBuddy

已完成 2s >

已从 meeting-notes.txt 提取任务，生成了 action-list.md，包含三项待办：

#	任务	负责人	截止日期
1	提交课程大纲	Content editor	2026-08-18
2	提交 FAQ	Course operator	2026-08-19
3	提交封面图	Designer	2026-08-20

action-list.md

405 B

查看所有产物 (1) > 查看所有变更 (2) >

共消耗 11.91 Auto

今天帮你做些什么? @ 引用对话文件, / 调用技能与指令

+ 默认权限

新版本就绪 更新日志 重启升级 内容由 AI 生成, 请核实重要信息

变更 >

文件变更 +12 -0

action-list.md +9

2026-08-16.md +3

看到额外文件先判断用途，再决定是否保留。不要因为文件以点开头就直接删除，也不要把.workbuddy 目录随手发给外部客户。交付前只打包真正需要的产物，是一个很值得养成的习惯。



问、想、做：执行权限要一层层放开

输入框的“更多操作”里可以切换模式。本机界面显示默认模式，并提供“计划 Plan”和“仅问答 Ask”两个开关。旧版官方教程中还能看到“做一做、想一想、问一问”的说法，含义基本对应。

这三种模式可以看成三档操作权限。**还在了解材料时只读，任务复杂时先看计划，输入输出明确后再直接执行**。把所有事情都交给默认模式，省下的是一次确认，增加的可能是整批文件返工。



仅问答 Ask：先了解，不改文件

适合“这个文件讲了什么”“这个项目有哪些风险”“给我解释这段代码”等问题。**还在摸清材料时，用仅问答最安心。**

示例：

只阅读工作空间，不修改任何文件。列出这里有哪些文件，每个文件大概做什么，并指出你不确定的地方。

计划 Plan：复杂任务先把路线摆出来

适合涉及多个文件、多个阶段或多种工具的任务。**WorkBuddy 先给出计划，你确认后再执行**。做竞品研究、课程生产、网站改版、数据报告时，这个模式能提前暴露理解偏差。

示例：

请先读取工作空间，拟定一个“销售月报”的制作计划。
计划里列出要读取的文件、清洗步骤、图表、最终产物和验收标准。

先不要修改文件，等我确认后再执行。

默认模式：目标明确时直接做

适合边界清晰、风险较低的日常动作，例如从会议纪要生成清单、把 CSV 变成图表、按现有模板补齐一份文档。**目标明确、风险较低，才适合直接执行。**

一个简单判断方法是：你能否在十秒内说清输入、输出和不能做什么？可以，就用默认模式；还说不清，就先 Ask；步骤多、代价高，就先 Plan。

它能看到什么，常常比模型有多强更重要

WorkBuddy 支持上传或引用 PDF、Word、文本、Markdown、Excel、CSV、PPT、图片、压缩包和常见代码文件。不同版本、模型和账户方案的支持范围可能不同，超大文件也可能需要拆分。

在客户现场，模型质量只是结果的一部分。它读到旧制度、错版本或另一个项目的文件，再强的推理也会沿着错误材料继续走。**很多看起来像模型能力的问题，根源在工作空间、文件版本和上下文。**

提供材料有四种常见方式：

选定工作空间，让它读取授权目录中的文件。

点击加号上传文件或文件夹。

把文件、图片直接拖进输入框。

使用 @ 引用对话文件或项目材料。

资料少时可以直接上传。资料长期使用或文件之间有关联时，选择工作空间更合适。团队共享的规章、产品资料、FAQ 则适合放进项目资产或已连接的知识库。

每次任务都要确认它读到的是哪个版本。文件名里带日期或版本号，能减少“新旧稿混用”。如果同名文件很多，可以写出相对路径，并要求它先列出准备读取的文件。

交付里的第一条纪律：给够用的最小权限

权限设置的目标是让任务顺利完成，同时把意外操作的影响控制住。**默认权限适合多数办公任务，完全访问只留给确实需要的场景**，开启前应先备份。

官方文档说明，WorkBuddy 默认以本地处理为主，服务器侧处理必要片段，并限制未授权目录和敏感路径；高风险动作会要求二次确认。实际使用时仍要**把授权、云端模型处理和文件分享视为三件不同的事**。文件能被本地应用读取，不等于适合交给外部模型，也不等于可以公开分享。

含有身份证、合同金额、未发布财报、客户名单、密钥或内部代码时，先做脱敏。连接第三方技能和连接器前阅读权限说明。涉及公司合规的内容，以组织自己的安全规则为准。

国内项目选模型，稳定可用排在前面

模型下拉菜单里会列出当前账户可用的模型和思考档位。本次实机界面能看到 Auto，以及混元、GLM、MiniMax、Kimi、DeepSeek 等不同模型选项，还提供 Max 模式和自定义模型入口。名单会随版本、套餐、地区和服务状态变化。

国内项目很难只按单次测评成绩选模型。组织允许使用哪些服务，数据能否送出当前环境，额度是否稳定，发票和支持能不能跟上，都会影响最终选择。WorkBuddy 把多种国内模型放在一个任务入口里，价值主要来自替换和管理更方便，并不代表每个模型适合所有任务。



刚开始建议用 Auto。它省去了逐个比较模型的负担，常见办公任务通常够用。遇到以下情况再手动选择：

- 需要看图片或截图时，选择明确支持视觉输入的模型。
- 大段代码、复杂表格或长文档，需要更强的上下文和推理能力。
- 任务成本敏感时，避免不必要地开启高消耗档位。
- 组织接入了指定模型时，按数据合规和团队规范选择。

Max、深度思考或强模型通常意味着更长等待和更多积分消耗。用强模型重做一个模糊任务，往往仍然会得到模糊结果。 **先把资料和验收标准说清，再升级模型**。

如果输出中断或质量突然下降，查看任务详情里的模型、消耗和运行时间。有些故障来自额度、网络或服务状态，并非提示词本身。

交付要留下记录，不能只留一段聊天

任务发送后会保留在历史列表里。你可以修改标题，让它从一串自动摘要变成容易识别的名字，例如“8 月销售分析：待复核”。任务多起来后，标题里加项目名、日期和状态，比依赖默认名称更容易找到。

对话页顶部提供任务内搜索、分享和详情入口。任务内搜索适合定位一个文件名、数字或错误信息；详情里可以核对模型、运行阶段、耗时和消耗；分享前则要检查对话中是否出现本地路径、客户名称、内部资料和个人信息。

新版已经增加批量删除和归档任务。归档适合暂时不用、以后仍可能复查的任务；删除前要确认重要产物已经单独保存。 **对话历史不能充当唯一文件仓库**，产物仍应进入清楚的项目目录或云端交付位置。

一个持续任务最好留在原对话里追问，因为已有材料和修改记录都在。目标已经更换、工作空间不同或需要隔离权限时，再新建任务。把无关工作硬塞进同一条对话，会让上下文越来越混乱。

能打开的产物，才有机会成为交付物

WorkBuddy 的右侧区域是验收工作台。根据任务不同，你可能看到以下内容：

聊天框里的答案很容易让人产生完成感，客户最后接收的却通常是 Word、Excel、PPT、网页、图片或代码。 **文件在哪里、能不能打开、内容有没有缺、过程改了什么**，这些才是右侧面板要回答的问题。

- 产物：文档、表格、PPT、报告、网页等可交付文件。
- 工作空间文件：文件树和文件预览。
- 浏览器：调研过程中打开的网页和结果。
- 变更：新增、删除、修改了哪些文件，以及行数变化。

交付前至少检查文件能否打开、内容是否完整、数字能否回到来源、有没有意外变更。网页预览正常也不代表导出的文件一定正常，PPT、Excel、PDF 最好再用对应软件打开一遍。

如果结果不满意，不用立刻重新开任务。围绕当前产物提出局部修改，例如“只改第二张表，不动正文”“保留版式，把所有日期改成 YYYY-MM-DD”“先列出准备删除的文件，不要执行”。这样的指令能利用已有上下文，也更容易控制改动范围。

放回真实工作，它能承担哪些部分

文档整理

适合会议纪要、制度摘要、方案改写、合同要点、FAQ 和周报。

读取 @会议纪要.docx，生成《项目周报.md》。
结构为：本周完成、当前风险、下周计划、待确认事项。
所有结论都要标注来自纪要的哪一段；没有依据的内容写“待确认”。
不要修改原文件。

验收时看有没有把“讨论”写成“已经决定”，有没有捏造负责人和日期。 **摘要任务最常见的错误，是把不确定内容说得太确定**，语言反倒经常很流畅。

表格分析与可视化

读取 @销售数据.csv，检查缺失值、重复行和日期格式。
先汇报数据质量问题，再按月份计算销售额、订单量和退款率。
生成《销售分析.xlsx》和《销售趋势.png》，不要覆盖原始 CSV。

要求先做数据体检很重要。图表画得漂亮，原始数据若有重复或口径混乱，结论仍然不可靠。验收时抽查两个月份，用计算器或 Excel 复算一遍。

演示文稿和汇报材料

根据工作空间中的调研报告和品牌素材，制作 10 页汇报 PPT。
听众是不了解技术的业务负责人，每页只讲一个结论。
先输出页纲让我确认，再生成 PPTX。
所有数字在备注区写明来源文件和页码。

PPT 任务适合 Plan 模式。 **先看页纲，再生成 PPT**，能避免做到十页之后才发现叙事方向错了。生成后检查字体、图片版权、图表刻度、备注和投影比例。

深度调研

调研 2026 年国内企业 AI 办公代理的主要产品。
先提出检索计划，优先使用官网、帮助中心、更新日志和原始公告。
把事实、厂商自述和你的推断分开。
最终生成《调研报告.md》和《来源清单.csv》，记录标题、网址、日期和引用用途。

调研的关键在于留住证据，页面数量不能替代证据质量。要求来源清单和日期，后续才能复核。搜索结果摘要只能帮助定位，重要结论要回到原页面。

批量文件整理

扫描工作空间中的文件，只生成整理方案，不执行移动。
按“文档、表格、图片、压缩包、其他”分类，列出拟移动路径和重名冲突。

等我确认后再移动；不删除任何文件。

批量操作先计划，再小范围试跑，确认后才扩大。 目录根部、桌面、云盘同步目录不要作为第一次实验对象。

代码开发

先阅读项目 **README** 和测试说明，解释这个项目如何启动。
再定位“导出按钮无响应”的可能原因，只做诊断，不修改代码。
输出相关文件、证据和最小修复方案，等我确认后再改。

代码开发场景适合把诊断和修改分成两次任务。修改后要求运行相关测试、展示差异，并说明还有哪些没有验证。**代码写完不等于功能已经可用。**

设计、图片和视频

根据 @品牌说明.pdf 和 @产品截图.png，先给出三种封面方向。
尺寸 **1600×900**，保留右上角标题安全区，不使用无授权人物照片。
我选择方向后再生成最终图片，并保留可修改的源文件。

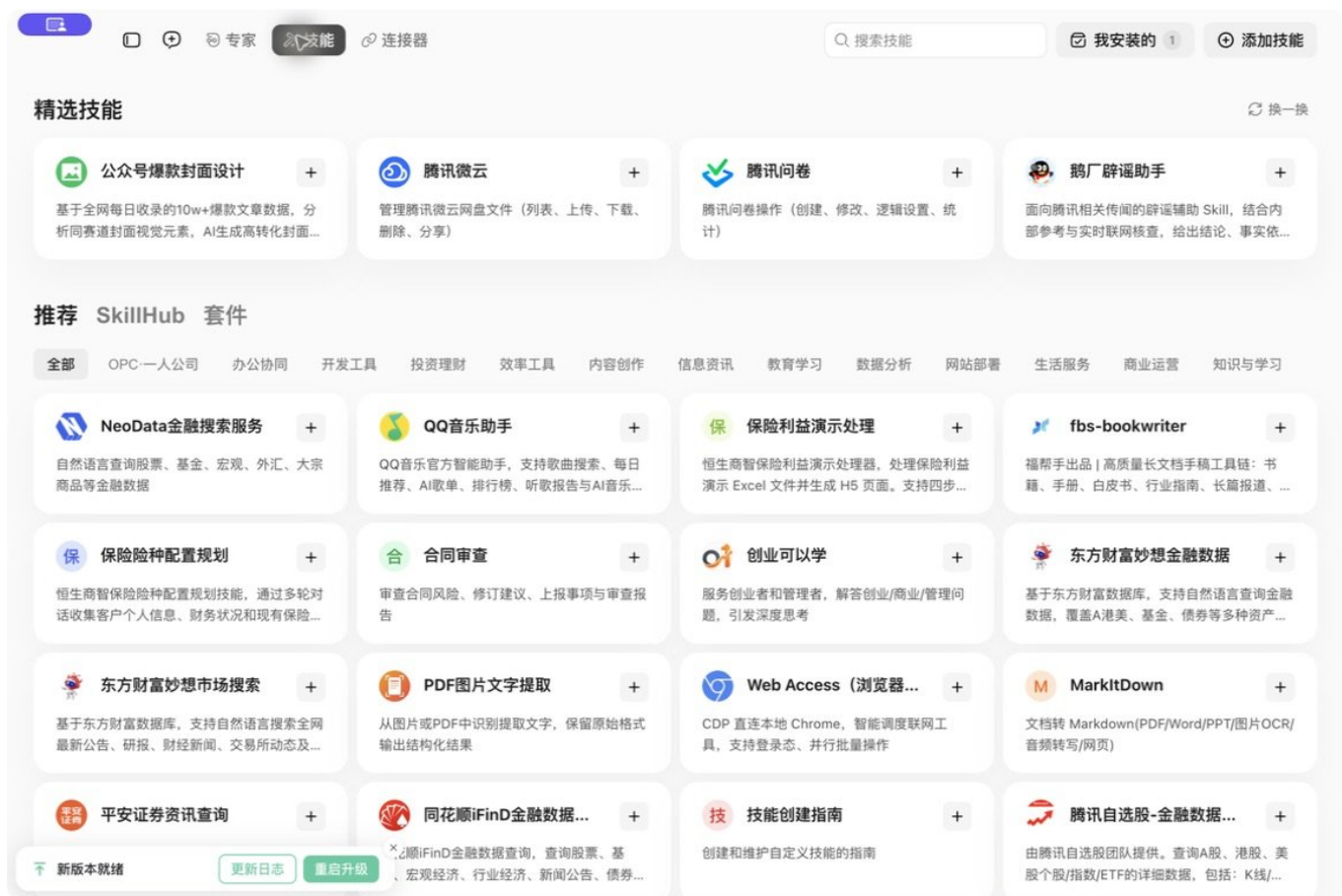
设计任务需要给尺寸、品牌色、文字、参考图和禁止项。**生成式图片里的小字、Logo、手指和数据图表要逐项检查。** 视频任务还要写清时长、比例、字幕、配音和导出格式。

技能：把零散动作做得更稳定

技能可以理解成封装好的工具和操作流程。它可能包含说明、脚本、依赖和参数，让 WorkBuddy 在特定任务上更稳定。例如文档格式转换、图表生成、图片处理、特定网站操作等。

一次交付靠人盯着提示词也许能跑通，**连续交付需要把稳定动作固化下来。** 技能的意义在于减少“这次记得做、下次忘了做”的波动。不过它仍然是代码和外部能力的载体，来源、权限和数据去向都要检查。

技能市场分为推荐与分类列表，已安装技能可以在管理页启用、停用或卸载。本机界面中还能从市场搜索和查看技能详情。



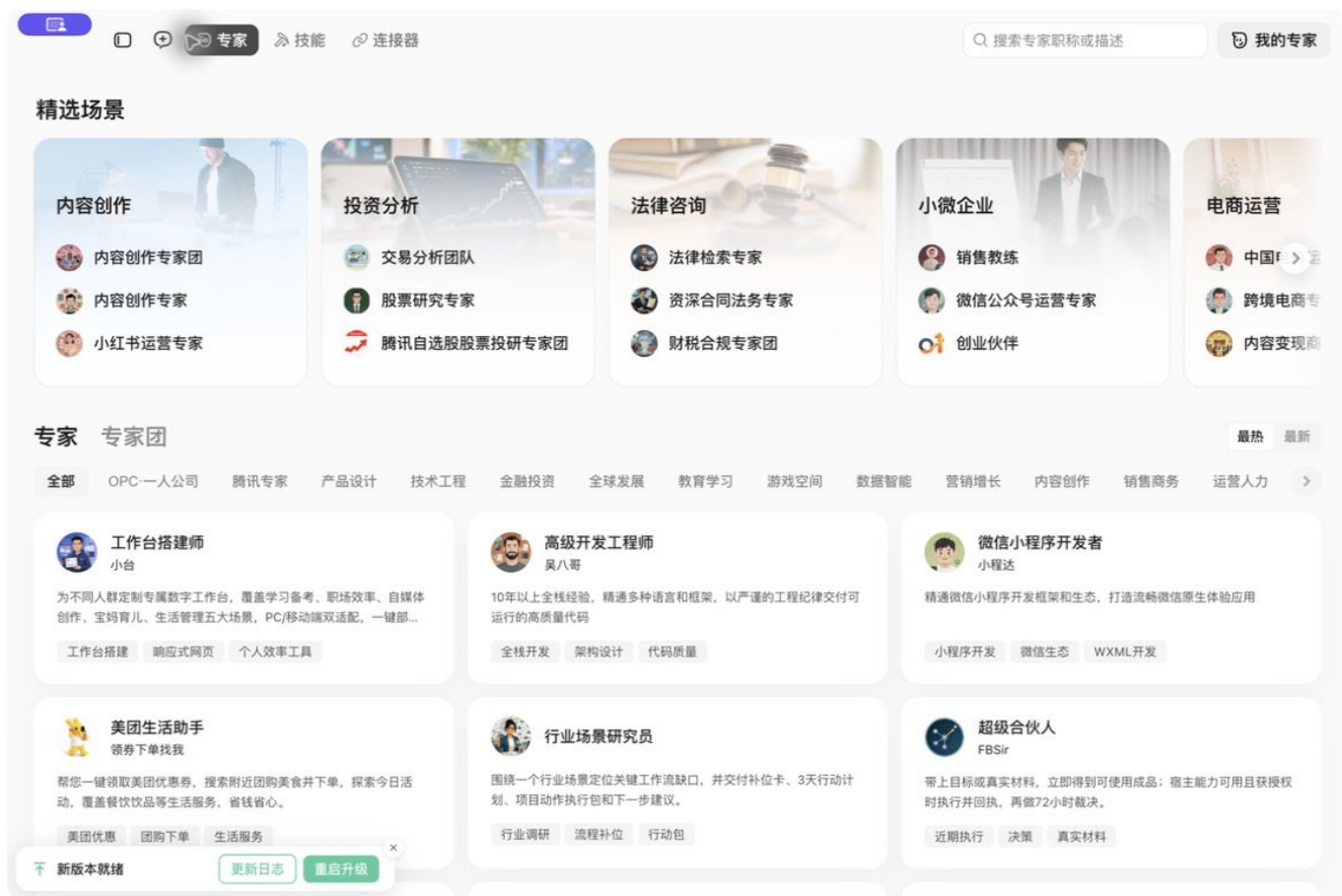
安装前要看三件事：**它会读取什么，会运行什么，会把数据发到哪里**。第三方技能可能访问输入内容、文件或凭据，也可能调用外部服务。只安装来源可信、当前任务确实需要的技能；暂时不用时关闭。遇到需要安装依赖、登录账号或赋予高权限的技能，先在测试工作空间里验证。

调用技能时可以在输入框输入 /，也可以在任务里明确说“使用某某技能”。如果 WorkBuddy 没有调用你预期的技能，检查它是否已经安装并启用，名称是否一致，当前模型和权限是否满足要求。

专家与专家团：把方法和分工带进任务

专家中心提供不同岗位和领域的角色。专家通常带着一套更固定的任务理解方式、流程和工具配置。你不需要每次从头解释“请站在产品经理角度”，可以直接切换到对应专家。

这种角色配置适合把团队已经认可的方法带进任务，**却不能凭空补出行业经验**。客户口径、业务例外和真实决策仍要由项目成员提供。专家团人数更多，也不代表结论自然更可靠，最后仍要回到证据和产物上验收。



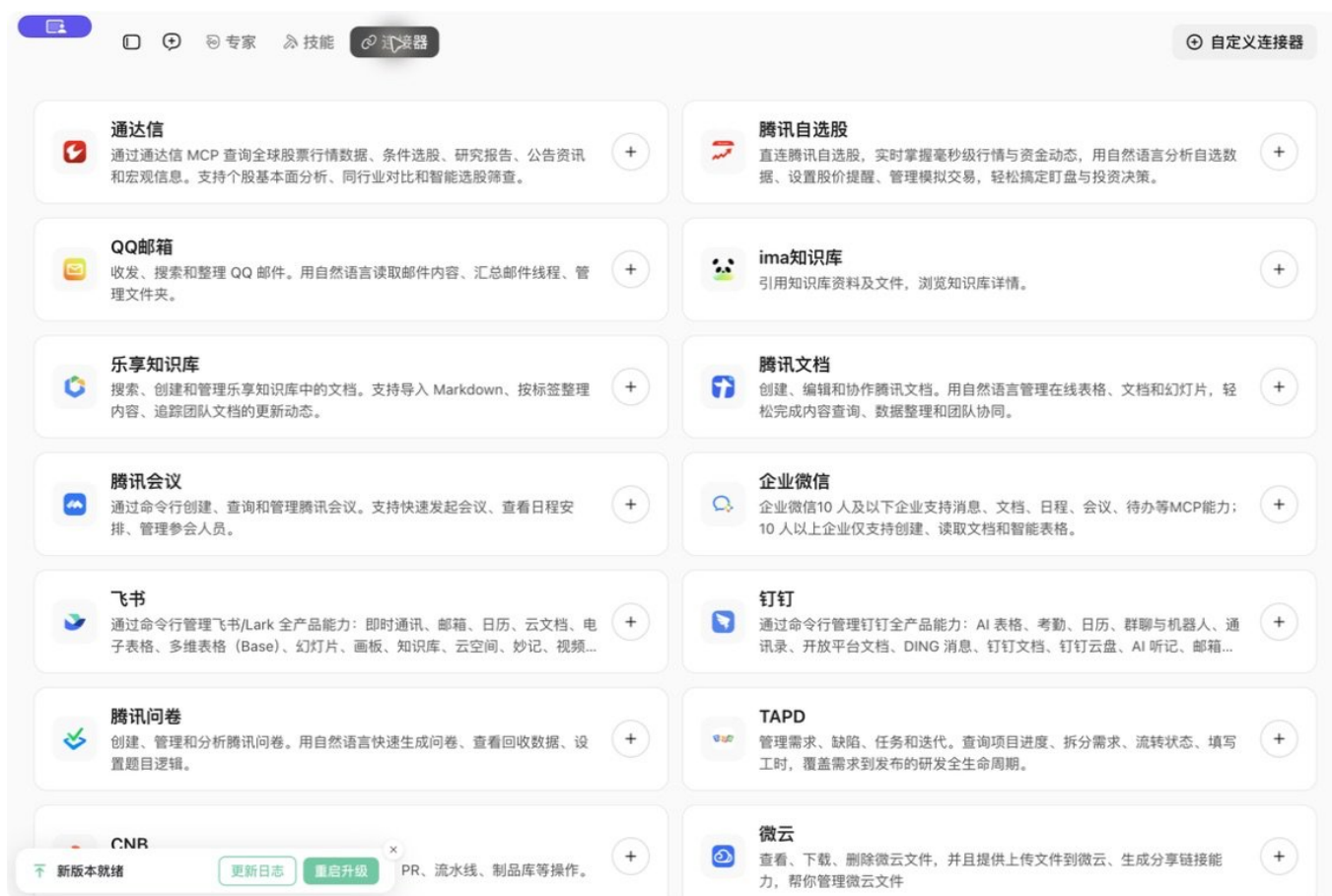
专家适合单一专业主导的任务，例如市场研究、产品需求、财务分析。专家团会让多个角色分工，适合需要研究、分析、写作和审阅共同参与的复杂交付。官方教程提醒，专家团通常会带来数倍积分消耗，所以别用它处理一段简单改写。

可以这样理解三者的差别：技能解决“会不会使用某个工具”，专家解决“以什么专业方法做”，专家团解决“多个角色怎样协作”。先用普通任务做通，再判断缺的是工具、方法还是人手。

连接器：国内生态为什么重要

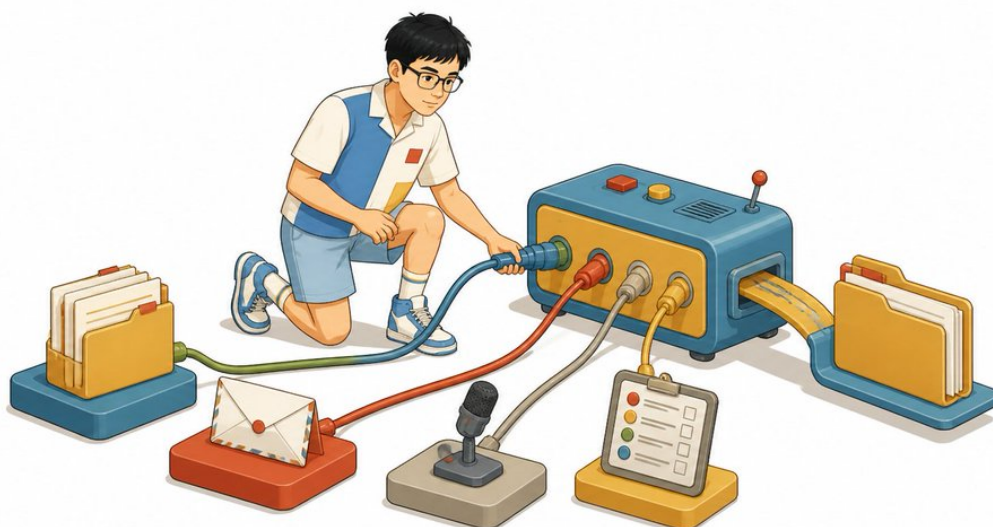
连接器让 WorkBuddy 读取或操作外部服务。本机连接器页面能看到腾讯文档、QQ 邮箱、腾讯会议、企业微信、飞书、钉钉、TAPD、腾讯问卷、乐享、ima 等入口，也有金融和其他业务服务。可用列表会随版本和账号变化。

这部分最能解释 WorkBuddy 在国内交付里的位置。客户资料本来就在这些系统中，团队每天也在这些入口里沟通。**工具能够接入现有环境，项目才有机会少做一层人工搬运**。连接器数量多本身没有意义，关键是你需要的系统能否稳定授权、检索和写回。



连接过程通常包含添加、登录或授权、选择权限范围、测试连接。连接成功后，可以在任务中引用云端资料或调用服务。例如从腾讯文档检索制度、整理腾讯会议记录、从邮箱提取待办，再把产物保存回云端。

授权时不要只看“连接成功”。还要确认账号归属、可读空间、写入权限和撤销方式。涉及邮件发送、创建工单、改动云文档时，最好先要求生成草稿或预览，确认后再执行。

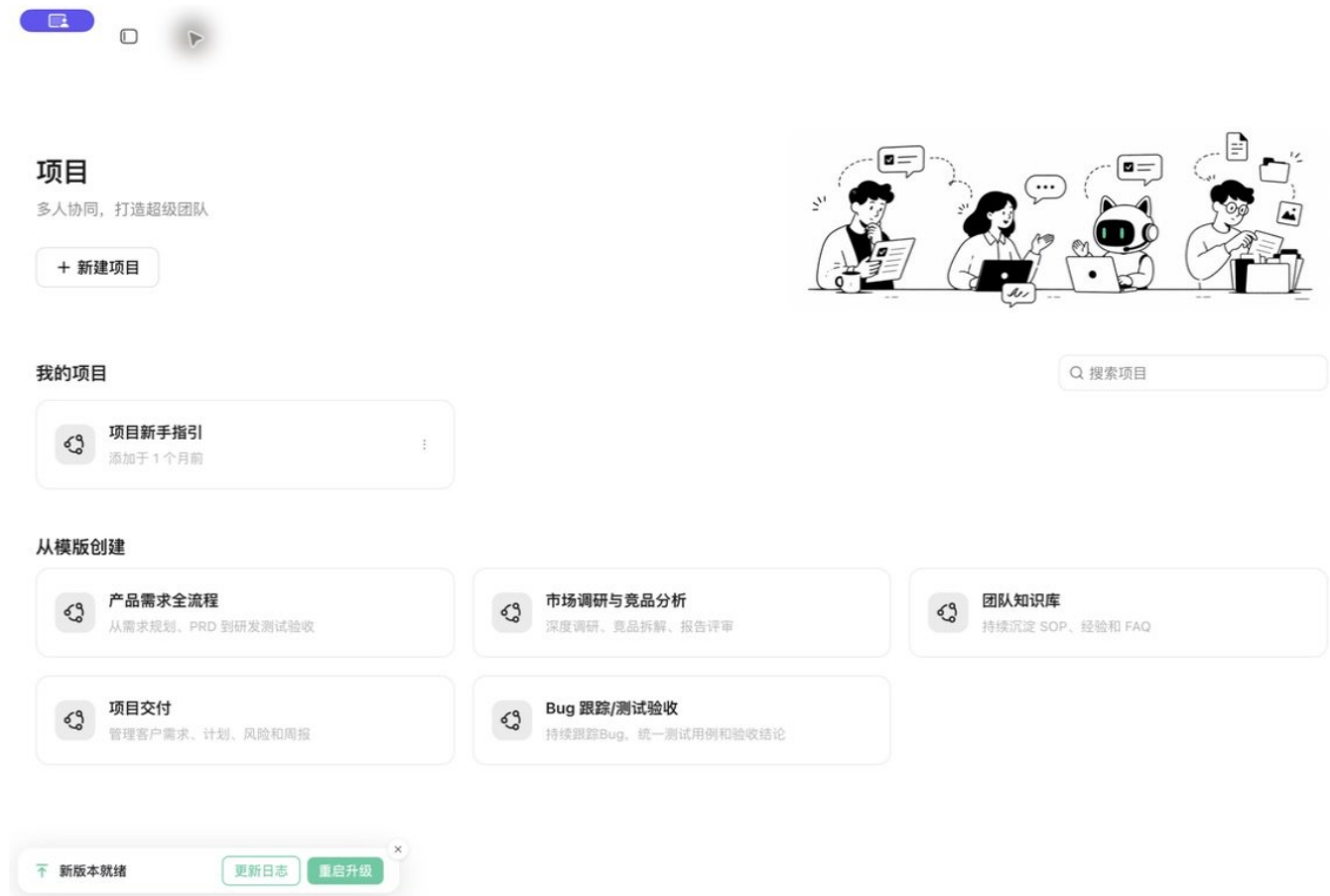


项目：把一次成功变成可重复交付

当一个主题会持续数周或数月，单独的任务会逐渐散乱。项目提供了更高一层的容器，让任务共享指令、资料、连接器、专家和技能。

交付团队最怕“只有当时操作的人会用”。提示词存在某个人的聊天记录里，文件散在不同目录，换一个同事就要重新摸索。**项目把固定说明、资料 and 工具放在一起，让验证过的做法能够被接手。**它不能代替项目管理，却能减少方法随着人员变化而丢失。

项目页提供产品需求全流程、市场调研与竞品分析、团队知识库、项目交付、Bug 跟踪与测试验收等模板。小白可以从模板观察一个完整项目需要哪些要素，再创建自己的项目。



一个项目至少可以准备这些内容：

- 项目目标和不做什么。
- 常用输出格式和命名规则。
- 团队资料、模板和术语表。
- 需要的技能、专家与连接器。
- 每次任务的验收标准。

任务进入项目后会继承相关配置，减少重复说明。项目资产适合保存长期参考材料，但别把所有硬盘文件一股脑上传。**资料越多，上下文越需要维护：过期文件要标记，重复版本要清理，敏感材料要分级。**

官方教程还介绍了项目动态、任务、产物、分享、项目资产和自动化等能力。团队使用时要明确谁能编辑项目指令、谁能添加公共连接器、谁负责最终审核。共享配置改错一次，可能影响后续多次任务。

助理：远程入口的价值和边界

助理功能把 WorkBuddy 接到微信、企业微信、QQ、钉钉、飞书等移动入口。你可以离开电脑后发起任务、查看进展或收到结果。本机已经连接微信小程序，因此页面显示“已连接”。

国内团队大量临时沟通发生在手机上，远程入口确实能缩短任务发起和结果查看的距离。但手机端更容易出现一句话说不清目标、在公共聊天里暴露信息的问题。**助理适合提交边界清楚的任务，复杂交付仍要回到电脑上验收。**



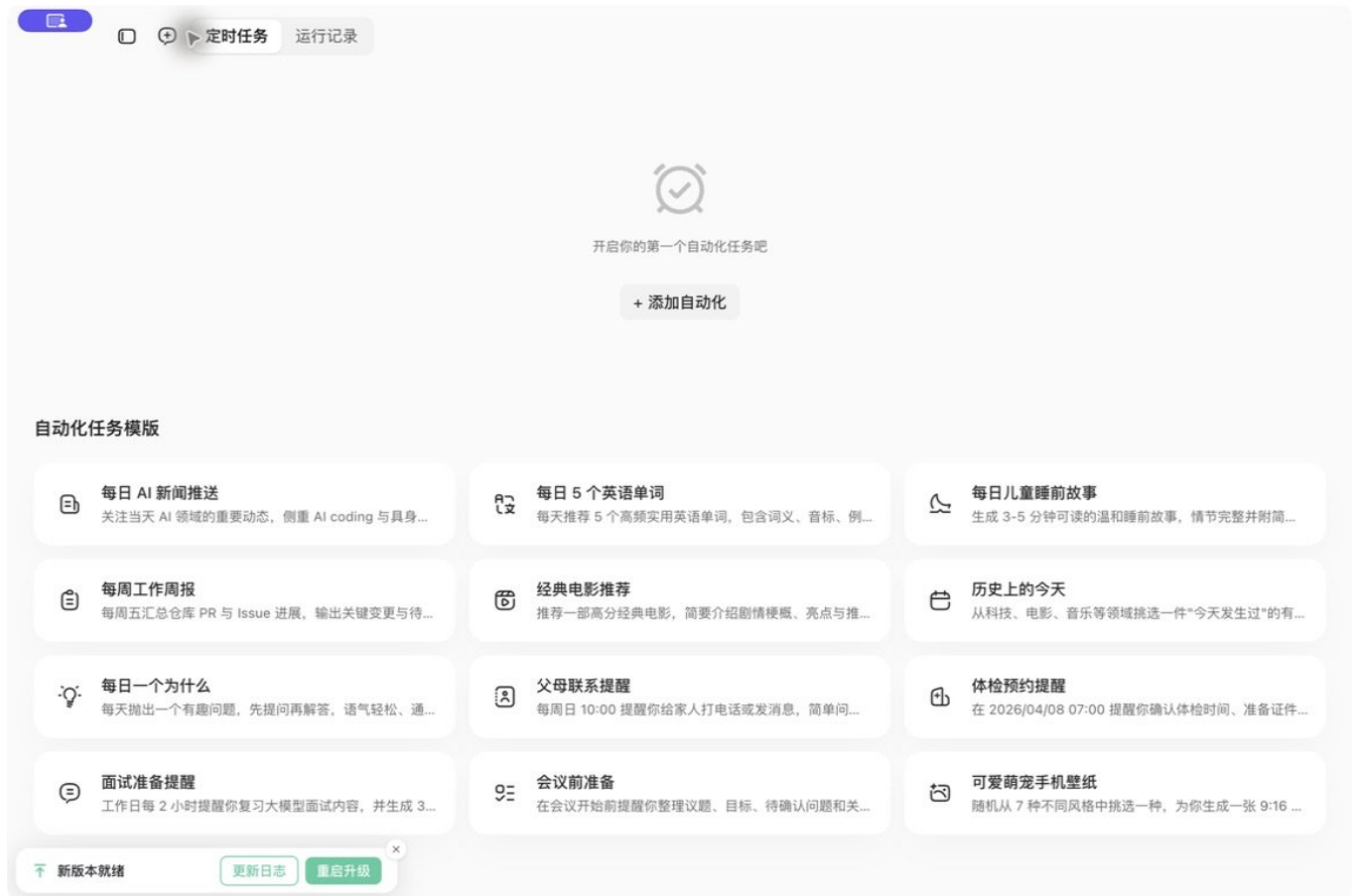
远程不等于云端替你接管电脑。按照官方教程，电脑需要保持开机，WorkBuddy 需要运行；网络、睡眠和登录状态都会影响任务。普通工作区可以并行多个任务，助理更像固定目录中的一条持续线程，具体行为以当前版本为准。

第一次使用助理，可以从只读任务开始，例如“列出今天工作空间里新增的文件”“总结这份周报”。确认链路可靠后，再尝试生成文件。删除、外发、上传等动作仍应保留人工确认。公共聊天或群聊里也不要发送敏感文件名、密钥和客户资料。

自动化：重复工作可以交给时间表

自动化页可以添加定时任务，也提供 AI 早报、每日英语、睡前故事、周工作汇报等模板。它适合重复、规则清楚、即使无人盯着也能安全执行的工作。

自动化是交付成熟之后的结果，不能用来掩盖一条还不稳定的流程。**手动运行时会漏字段、找错目录的任务，改成定时只会更稳定地制造错误**。先把输入、路径、输出和验收跑顺，再交给时间表。



一条自动化通常包含名称、工作空间、任务指令、模型或技能、运行时间和通知方式。建议从低频、只读、可核验的任务开始：

每周五 17:30 读取本周工作日志，只生成《本周汇总草稿.md》。
按“完成、风险、下周计划、待确认”整理。
不要发送邮件，不覆盖历史文件；文件名带当天日期。
完成后把产物链接推送给我。

创建后先手动运行一次，检查路径、权限、产物命名和通知。确认无误再启用时间表。提示词里包含删除、付款、批量发送或覆盖的自动化风险很高，不适合作为无人值守任务。

自动化长期运行后还要维护。文件结构变化、连接器授权过期、模型下线、额度不足，都可能让原本正常的任务失败。至少每月检查一次最近运行记录和失败原因。



本地、项目资产与云端不要混在一起

“我的文件”提供云端文件空间，本机页面显示已用容量和文件夹列表。生成的产物可以上传到云端，便于跨设备查看或分享。

国内客户常常会追问资料到底留在哪里。**这个问题不能只用“本地优先”四个字回答**。原始文件、项目资产、模型处理片段和最终产物可能处在不同位置，团队需要逐项弄清并记录。WorkBuddy 提供了这些入口，具体项目仍要按客户制度决定哪些可以上传、哪些只能留在指定设备。



我的文件

快捷查看任务成果，上传到云端网盘开启跨端同步。

任务成果 云端网盘

新建文件夹 上传文件 存储空间已用 880.08 KB / 5.00 GB

全部类型

搜索文件或文件夹...

☐ 名称	类型	更新人	更新时间	大小
 配置文件	文件夹	Miles	2026/6/27	-

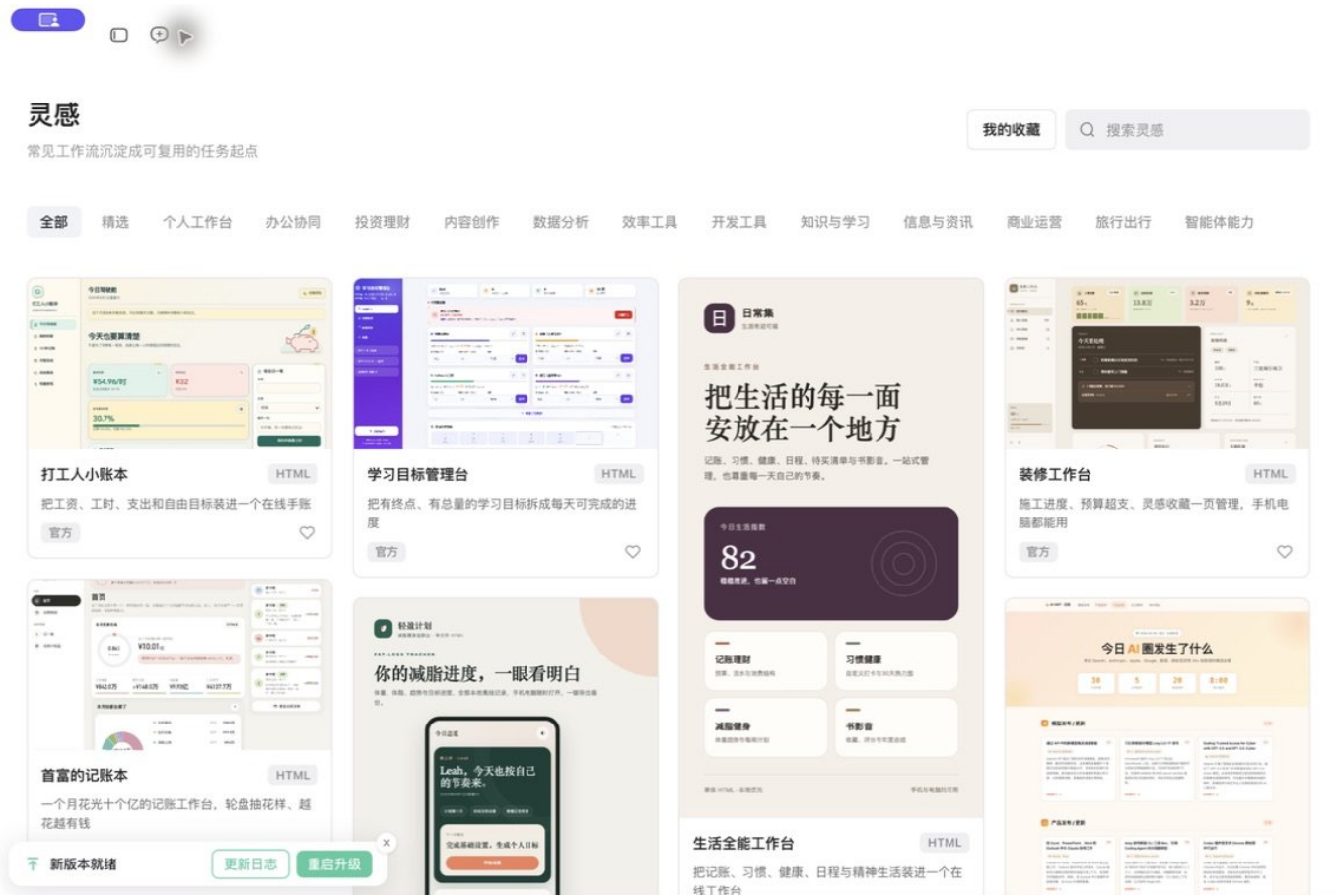
新版本就绪 更新日志 重启升级

云端文件、项目资产和本地工作空间用途不同。工作空间适合当前电脑上的执行；项目资产适合一个长期主题的共享背景；云端网盘适合保存和流转产物。**不要把三者当成同一个备份系统，重要原件仍要有独立备份。**

连接腾讯文档后，WorkBuddy 可以搜索文档、把资料加入任务，并把产物保存回云端。乐享、ima 等知识来源也能通过连接器进入任务。检索命中后仍要打开原文确认日期、作者和适用范围，尤其是制度、价格和产品功能等会变化的信息。

灵感：可以复用案例，不能照搬环境

不知道怎样开口时，可以进入灵感页。这里展示可复用的任务案例，适合观察别人给了哪些输入、要求了什么产物、用了什么 workflow。



新版加入了灵感分享口令和“一键做同款”等能力，可以更快复刻任务或网页样式。**复用前仍要替换资料、权限、品牌和输出路径。**案例里的提示词只是起点，别让它在你的真实工作空间里照搬别人的文件名和外部服务。

适合沉淀为灵感的任务，通常已经稳定跑过几次，输入结构明确，产物有验收标准。一次偶然成功的复杂提示词还不算模板。

记忆：长期协作少重复，过期信息也要清理

长期记忆会从历史对话中提取偏好和背景，例如常用称呼、写作格式、项目术语。官方教程说明，用户可以查看、编辑、删除、停用和导入记忆。

记忆的价值在于少重复说明，风险也来自这里：**过期信息可能继续影响新任务**。本次实操的变更面板里就出现了本地workbuddy/memory 文件。使用一段时间后，应定期检查记忆，删除已经失效的角色、路径、口径和临时要求。

不要把密码、密钥、验证码或客户隐私写成“以后记住”。这类信息应该放在专门的凭据管理工具里，并按连接器授权流程使用。

设置：稳定运行比方便更重要

系统设置里可以调整语言、字体、简洁模式、启动行为、防止电脑休眠等选项，不同版本还会增加模型、数据管理和快捷方式相关配置。

如果经常运行长任务，可以考虑开启防止休眠，但要留意耗电和电脑散热。简洁模式适合熟练后减少界面提示。自动安装非高风险依赖虽然方便，第一次使用时仍建议保守一些，让每次新增能力更容易追踪。

自定义模型涉及接口地址、密钥、费用和数据去向。除非你已经理解服务商、账单和合规边界，否则先使用内置 Auto。 **密钥不要写进普通任务或工作空间文件**。

最新功能只能作参考，交付以已安装版本为准

截至 2026 年 8 月 16 日，官方更新日志的最新版本是 5.3.13，发布于 8 月 13 日。最醒目的新能力是灵感“一键做同款”，用于快速套版复刻网页；同时优化了多任务切换和知识库上传，并修复了子任务卡在准备中、图表展示、代码块重叠、网页搜索链接为空等问题。

更新日志适合判断产品有没有持续维护，不适合直接写进交付承诺。客户电脑上安装的版本、账号实际拥有的功能、模型和连接器状态都要现场确认。 **当前环境打不开的功能，不能算已经交付**。

前几个版本也带来不少实用变化：

- 5.3.12 增加灵感分享口令，改善移动端、弱网和电脑休眠后的连接恢复。
- 5.3.11 增加网络检查快捷入口、批量删除或归档任务、本地搜索已安装技能、开机启动设置、文件变更详情开关，并加强微信和企业微信中的流式反馈。
- 5.3.3 重做项目计划，增加企业智能体身份和欢迎语，增强腾讯文档、PPT 插件预览、本地长期记忆展示与编辑，以及技能、插件、连接器的推荐入口。

本机仍是 5.2.6，因此文中能看到“新版本就绪”。这类差异必须写清：最新版更新日志说明产品已经具备什么，不代表读者当前安装的版本立即就有。升级后最好用练习工作空间重跑一次小任务，再恢复重要项目。

到了现场出问题，按这个顺序排查

点击发送没有反应

先确认输入框里是否真的有文字，工作空间是否有效，模型是否可用，当前是否有登录或额度提示。尝试删除多余空行，重新输入一小段纯文本。仍无反应时查看网络检查和更新日志，不要连续快速点击。

长时间停在“准备中”

等待一两分钟，查看任务详情和网络状态。暂停其他大任务，避免同时跑太多工作流。新版多次修复准备阶段和多任务切换问题，版本较旧时可以在保存现场后升级。

找不到文件

检查工作空间名称、文件是否在子目录、文件名和扩展名是否准确。用 @ 显式引用，或先让 WorkBuddy “列出准备读取的文件，不执行其他动作”。云端文件还要确认连接器授权没有过期。

产物生成了，但内容不完整

回到验收标准，告诉它缺哪一列、哪一节、哪几页。长资料可以分阶段处理：先建立目录和来源索引，再逐节生成，最后合并。不要只说“再详细一点”，那会让修改方向继续模糊。

修改了不该动的文件

立即停止继续任务，打开“查看所有变更”，记录文件和行数。先从备份或版本控制恢复，再修改提示词和权限。下一次明确写“只新增文件，不修改或删除现有文件；如必须修改，先征得确认”。

图片、PPT 或网页预览异常

确认所选模型支持图片，素材格式没有损坏。生成 PPT 后用 PowerPoint 或 WPS 实际打开；网页要检查不同窗口宽度；图片中的文字要放大查看。预览是验收入口，不能替代最终格式检查。

技能或连接器调用失败

检查是否安装并启用，账号是否登录，授权范围和有效期是否正常，依赖是否缺失。先运行一个最小测试，例如只搜索一份云文档，不要直接发起跨多个系统的长流程。

消耗比预期高

查看任务使用的模型、专家团、深度思考和重试次数。简单任务使用 Auto 或普通模式，复杂任务先 Plan。避免把同一份长资料反复上传，也不要让多个专家处理可以由一个专家完成的工作。

从会操作到能交付，可以按七天练

第一天只做只读问答。准备三个普通文件，让 WorkBuddy 说明目录结构、总结文档、解释表格字段，全程不修改文件。

第二天完成本文的行动清单练习，学会选择工作空间、生成产物、查看变更和继续追问。

第三天用一份 CSV 做数据体检、汇总和图表。抽查计算结果，认识“图表正确”和“数据可靠”之间的差别。

第四天尝试 Plan 模式，先做一个十页 PPT 的页纲，确认后再生成文件。重点练习验收标准。

第五天安装一个来源可信的技能，连接一个你确实需要的云端服务。记录授权范围，并完成最小测试。

第六天创建一个项目，把固定说明、资料和模板放进去，连续跑两个任务，观察共享配置有没有减少重复说明。

第七天创建一条低风险自动化，先手动运行，再设置低频时间表。最后回看一周的任务历史、产物、变更和积分消耗，整理出自己的模板。

七天之后，判断自己是否熟练，就看能否稳定做到五件事：**给任务划边界，选对模式和模型，提供可追踪材料，验收产物与变更，遇到失败知道从哪里排查**。

五个可以直接改的交付任务模板

只读摸底

只读取当前工作空间，不修改、不创建、不删除任何文件。
请列出目录结构，说明每个文件可能的用途、更新时间和相互关系。
不确定的地方明确标记，不要猜测。

先计划后执行

目标是完成【产物名称】。
输入材料在【路径或 @文件】。
请先列出步骤、会读取的文件、会调用的工具、预计新增或修改的文件、风险点和验收标准。
我确认前不要执行。

安全生成新文件

读取【输入文件】，新建【输出文件】。
保留原文件，禁止覆盖、删除和移动现有内容。
输出必须包含【字段或章节】。
完成后汇报新建文件路径，并列出所有文件变更。

局部修改

只修改【文件】中的【具体区域】。
其他段落、格式、文件名和目录结构保持不变。

修改前先复述你准备改的内容，修改后展示差异。

交付前检查

请作为审阅者检查当前产物，不要直接修改。

核对事实、数字、日期、来源、缺失项、格式和文件可打开性。

把问题分为“必须修复、建议修复、需要我确认”，并给出证据位置。

WorkBuddy 真正重要的地方

WorkBuddy 的重要性可以用一句话概括：**它把模型从聊天框带进了真实工作**。材料在本地目录或国内业务系统里，任务要经过权限控制，结果需要落成文件，改动还要能够检查。这几件事连起来，模型才有机会参与一次完整交付。

在国内做项目，这层工作台尤其现实。国外模型和工具仍然可以用于研究、原型和部分开放场景，进入政企客户环境后却要面对网络、账号、采购、数据和运维要求。**团队最后选择的方案，必须兼顾能力、可用性和合规边界**。WorkBuddy 接入国内模型和常见服务，至少让这条路短了一些。

它也只是一张工作台。客户业务怎么理解，敏感数据怎样处理，产物能不能被采纳，出了问题由谁负责，这些判断仍然在人手里。模型会出错，连接器会失效，自动化会把小问题放大。本文反复强调独立工作空间、最小权限、查看全部变更，正是因为执行能力越强，边界越需要提前画清。

如果目标只是做一次好看的技术演示，可选工具很多。要在国内客户环境里尽快交出一份能打开、能核对、能继续修改的文件，选择会明显收窄。**WorkBuddy 的优势是把模型、文件、国内服务和交付结果放在了一起**。

下一次打开首页，不用先研究完所有按钮。建一个练习文件夹，放进一份无敏感信息的会议纪要，用本文的模板生成行动清单，再认真打开“产物”和“查看所有变更”。这一步跑通以后，你会同时掌握 WorkBuddy 的基本操作，以及把 AI 安全带进真实工。

一起成长，一起赚钱。我是 Miles，一名从大厂转型 FDE 的 AI 算法专家，做过算法研发、优化部署，也做过企业培训。关注我 [@miles_mazy](#)



Miles

AI 算法专家 × FDE
企业 AI 培训 · 落地 · 部署

关注我