CLI 接入

通过 CLI 让 AI Agent 使用 SAG 知识库能力，完成检索、阅读和文档管理。

场景：通过 CLI 将 SAG 知识库能力交给 AI Agent，由 Agent 按自然语言完成资料检索、文档阅读或知识库管理。

角色：已登录 SAG 且拥有目标知识库权限的成员；创建开放连接需要超级管理员或被授权的连接负责人。

路径：左侧【集成】→【开放接口】→打开知识库类型的开放连接。

CLI 接入是什么

CLI 接入让 AI Agent 可以通过命令行安装并使用 SAG 知识库能力。安装完成后，你可以在 ChatGPT、Codex 或其他支持执行命令的 Agent 中，直接用自然语言让 Agent 查询、阅读或管理 SAG 中的知识库内容。

它适合以下场景：

- 让 Agent 根据企业资料回答问题，并保留搜索结果中的引用信息；
- 让 Agent 阅读指定文档，整理或比较文档内容；
- 让 Agent 浏览多级文件夹，并把新文档上传到指定文件夹；
- 让 Agent 协助上传、重命名或移入回收站文档。

使用前准备

开始前请确认：

1. 你已经登录 SAG，并且拥有目标知识库的访问权限；
2. 你可以使用一个已配置好范围的知识库开放连接；

3. 你使用的 Agent 支持执行 `npx` 命令，并且能够读取安装结果。

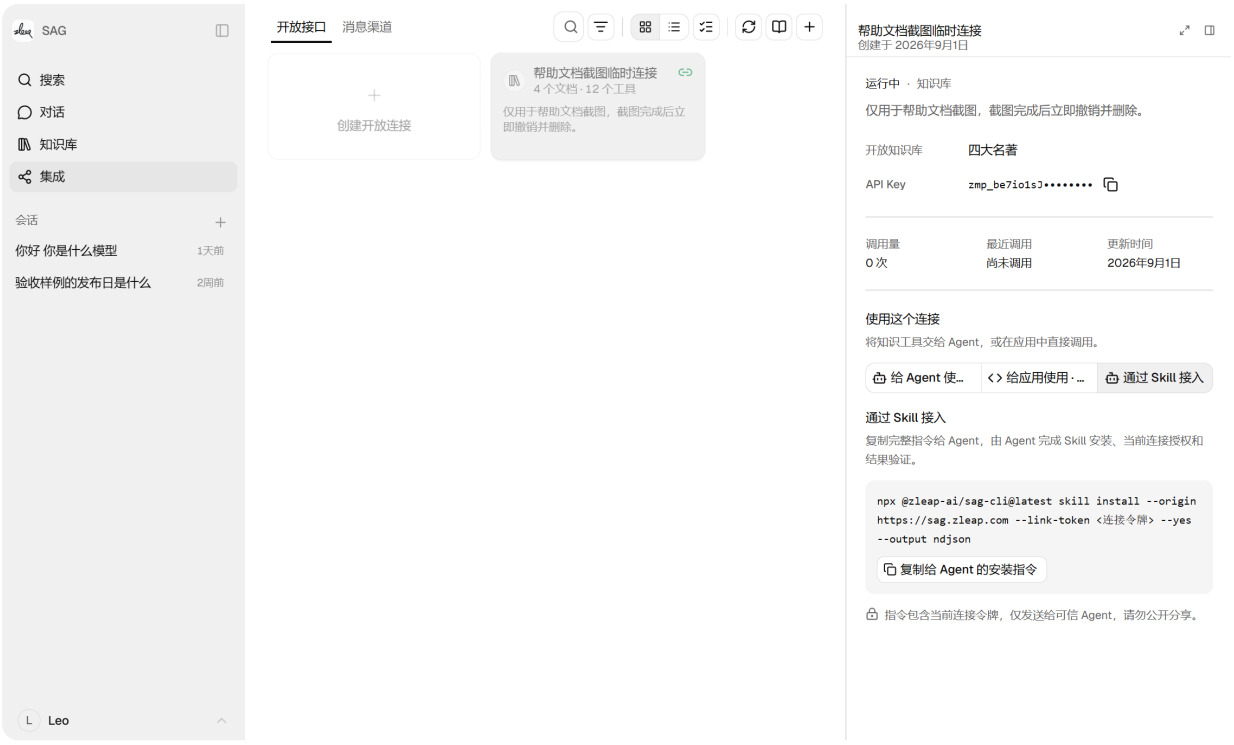
通过开放连接安装

开放连接适合需要限定知识库范围的 Agent。连接只能访问创建时授权的知识库，不会自动扩大范围。

1 打开 CLI 接入入口

进入【集成】→【开放接口】，打开知识库类型的开放连接，向下找到【使用这个连接】区域。

选择【通过 Skill 接入】，页面会显示完整安装指令。



2 复制安装指令

点击【复制给 Agent 的安装指令】，将完整指令交给可信的 Agent 执行。不要手动修改指令中的连接信息，也不要把指令公开发布。

Agent 会自动完成 CLI 安装、当前连接授权和结果验证。安装过程中请检查每条安装结果，确认没有失败项。

整个过程不需要另行打开浏览器授权；以连接页面生成的安装指令为准。

3 验证 CLI 是否可用

安装完成后，可以让 Agent 执行以下验证命令，查看当前连接可访问的知识库：

```
npx @zleap-ai/sag-cli@latest skill knowledge list --output ndjson
```

如果当前会话没有识别新安装的 CLI 能力，请刷新 Agent 或开启新会话后再试。

场景示例

以下为模拟对话，展示不同部门如何在自己的 Agent 中调用 SAG 知识库能力；实际可访问的知识库和执行结果取决于授权范围。

财务部丨制度更新与资料检索



查找差旅报销标准，
并附上原文引用。



我整理了交通、住宿和餐补三类标准；
原文引用来自《差旅管理办法》第三章
“费用标准”。



把 D:\\部门资料\\财务制度\
2026 年报销管理办法.docx
上传到财务知识库。



文件已接收，正在上传到【财务知识库】；
当前状态为“处理中”，完成后我会
继续查询结果。



导入完成后告诉我处理结果。



导入已完成，文档状态为“已发布”；
现在可以在财务知识库中搜索并
查看引用。

人事部 | 员工政策问答

查找年假申请流程，并整理成员工可以执行的步骤。





申请流程是：先确认可用假期，再提交申请，等待直属负责人审批；所需材料和原文依据已一并列出。

新员工入职需要准备哪些材料？





我按办理顺序整理了身份证明、学历信息、银行卡资料和入职表单，报到前准备好即可。

这项员工政策的原文依据是什么？





依据是《员工假期管理办法》相关条款；我已标出文档名称和引用位置，方便你逐条核对。

产研部｜技术资料与故障处理



查找这个故障的历史处理记录。



我找到三条相关记录，并按故障现象、处理动作和最终结果整理成了时间线。



比较不同版本的解决方案有什么差异。



旧版侧重临时恢复，当前版本增加了根因修复和回滚步骤；差异已按适用条件标注。



找出最适合当前版本的处理建议，并附引用。



当前版本建议先执行配置校验，再按文档中的恢复步骤处理；引用位置已附在每条建议后。

销售部｜产品资料与客户准备

查找适合这个客户行业的产品能力。





结合客户行业和当前需求，
我筛出三项最匹配的产品能力，
并附上对应资料。

找几份相关行业案例，
并附原文引用。





我找到两份相关案例，
分别标注了客户背景、落地做法
和原文引用位置。

把这些资料整理成销售拜访提纲。





拜访提纲已按客户现状、
产品价值、案例证明和下一步行动
四部分整理完成。

安装完成后如何使用

安装完成后，直接用自然语言告诉 Agent 目标和范围即可。例如：

- “列出我可以访问的知识库，并说明每个知识库的用途。”
- “在指定知识库中搜索关于报销流程的资料，并给出引用。”
- “阅读这份文档，整理出适合新员工的操作步骤。”
- “列出财务制度知识库根目录中的文件夹，再进入报销制度文件夹查看它的子文件夹。”
- “在年度制度文件夹下新建一个 2026 年文件夹。”
- “把 `D:\部门资料\财务制度\2026 年报销管理办法.docx` 上传到指定知识库；导入完成后告诉我结果。”
- “把这份文档上传到财务制度知识库的年度制度 / 2026 年文件夹。”

涉及上传、重命名或移入回收站等管理操作时，应明确指定目标知识库和文档，并在 Agent 执行前确认操作意图。

在子文件夹中管理资料

CLI 支持浏览多级文件夹、创建子文件夹、重命名或删除文件夹，以及把新文档上传到指定文件夹。安装完成后不需要自己查找文件夹 ID，也不需要输入 CLI 命令，直接把目标知识库、文件夹路径和操作告诉 Agent 即可。

直接这样告诉 Agent

想完成的操作	自然语言示例
查看根目录	“列出「财务制度」知识库根目录下的文件夹。”
进入子文件夹	“进入「财务制度」知识库的「年度制度」文件夹，继续列出里面的子文件夹。”
核对同名文件夹	“显示所有名为「2026 年」的文件夹及其完整路径，让我选择。”
创建子文件夹	“在「财务制度」知识库的「年度制度」文件夹下创建「2026 年」文件夹。”
上传到文件夹	“把 `D:\资料\2026 年报销管理办法.docx` 上传到「财务制度」知识库的「年度制度 / 2026 年」文件夹，完成后告诉我导入结果。”
上传到根目录	“把这份文档上传到「财务制度」知识库根目录。”
重命名文件夹	“把「财务制度 / 年度制度 / 2026 年」重命名为「2026 年制度」。”
删除文件夹	“删除「财务制度 / 历史制度 / 2023 年」文件夹；先告诉我会影响哪些子文件夹、文档和同步计划，我确认后再执行。”

Agent 会根据完整路径逐层定位目标文件夹。如果存在同名文件夹或目标不明确，Agent 会先展示完整路径，请你选择后再继续；涉及删除时，会先展示影响范围并等待确认。

> ⚠️ 文件夹操作须知
>
> 1. 删除文件夹会递归删除其子文件夹，并将其中的文档移入回收站；如涉及持续同步计划，预览中会同时显示影响范围。
> 2. 文件夹只用于整理知识库内容，不会改变文档的检索范围或访问权限。
> 3. CLI 暂不支持移动已有文件夹或文档；需要调整已有内容的位置时，请在 SAG 知识库页面中操作。

当前支持的知识库能力

当前 CLI 接入支持以下用户可见能力：

能力	说明
查看知识库	查看当前授权范围内的知识库及简介。
查看文档目录	浏览知识库中已经发布的文档。
浏览多级文件夹	从根目录逐层查看子文件夹，并核对文件夹完整路径。
管理文件夹	创建、重命名或删除知识库文件夹。
搜索知识库并进行问答	检索知识库内容，回答问题并读取搜索结果中的引用信息。
阅读文档	查看已发布文档的正文和结构。
上传单个文档	向指定知识库的根目录或指定文件夹上传一个文档。
查看文档导入进度	查看上传文档的处理进度和结果。
查看上传大小限制	查看当前允许的文档上传大小。
重命名文档	修改知识库中文档的名称。
将文档移入回收站	将指定文档移入回收站。

权限范围与限制

- 通过开放连接安装时，只能访问连接创建时授权的知识库范围；
- 文档上传、重命名和移入回收站属于管理操作，请在执行前确认目标和结果；
- 文档仍在导入时，搜索结果可能尚未包含最新内容。

> ⚠ 安全提示
>
> 1. 安装指令包含连接令牌，只发送给可信 Agent，请勿公开分享。
> 2. 如果原令牌无法再次读取或怀疑泄露，请先轮换 API Key，使旧令牌立即失效。

3. 如果安装结果出现失败项，请先处理失败项，再开始使用该 CLI 能力。