MCP 与 HTTP API

为 AI Agent 或企业应用配置 MCP 和 HTTP API 接入。

接入方式一：为 AI Agent 安装 MCP

MCP（Model Context Protocol）是让 AI Agent 调用外部能力的标准协议。SAG 企业版知识库通过 MCP 接入后，Agent 可以按照连接授权的范围检索和阅读企业文档。

1 获取 MCP 安装配置

打开连接详情，进入【给 Agent 使用 · MCP】标签，展开【完整客户端配置】，复制 JSON 配置。配置示例如下：

```
{
  "mcpServers": {
    "sag-knowledge": {
      "type": "streamable-http",
      "url": "https://your-sag-domain/api/v1/integrations/open-connections/{
      "headers": {
        "Authorization": "Bearer YOUR_API_KEY"
      }
    }
  }
}
```

2 在 Agent 中安装 MCP（以 CodeBuddy 为例）

以 CodeBuddy 为例：

1. 打开 CodeBuddy 侧边栏，点击右上角【设置】图标。
2. 切换到【MCP】标签。
3. 点击【添加 MCP】，将上一步复制的 JSON 配置粘贴到配置文件中。
4. 保存后，MCP 服务器状态变为绿色即表示连接成功。

其他支持 MCP 的 Agent（如 Cursor、Claude Desktop、Cline 等）操作类似，均在其 MCP 配置文件中添加相同格式的服务器配置。

3 验证开放能力

安装完成后，Agent 的能力列表中会出现该连接已经开放的知识库能力。向 Agent 提问或发出检索请求时，它只能使用连接授权范围内的文档。

接入方式二：应用通过 HTTP API 接入

1 获取接口地址和示例

打开连接详情，进入【给应用使用 · HTTP API】标签，复制接口地址和调用示例。所有请求使用同一个 API Key，通过 `Authorization: Bearer <API_KEY>` 认证发送。

使用 CLI 接入

如果希望通过命令行让 Agent 直接使用 SAG 知识库能力，而不是在 Agent 中手动配置 MCP，请查看 CLI 接入 页面，了解安装和使用方式。

> ⚠ 注意
>
> 1. 普通成员只能使用已有的开放连接，无法自行创建或管理；如需新建连接，请联系超级管理员。
> 2. API Key 是敏感凭证，不要在代码或日志中明文记录，也不要分享给他人；创建后请立即保存。
> 3. 开放连接只能访问创建时授权的知识库范围，不会自动扩展到其他知识库。