

每次都要把文件逐个拖进聊天框？ 您的 AI 助手直接向档案库提问。

Claude、ChatGPT 或 Cursor 可以直接在 PaperOffice 中处理您的文档，遵循您的权限，无需将任何内容上传到聊天框。本指南介绍如何设置连接、将其限制在合适的 Workspaces 范围内以及如何安全使用。



30分钟内亲自体验

创建密钥，连接 Claude，向您的档案库提出第一个问题。想先试用的话，有一个演示 Workspace，无需账户。

为何编写本指南

AI 早已是团队的一员。 文档却还不是。

许多团队每天都向 Claude 或 ChatGPT 提问。但他们所询问的合同、发票和档案，仍然保存在文档管理系统中。



到目前为止，做法是：找到文档、下载、拖进聊天框、提问。之后每个副本都留在聊天记录里，而且之后也没有人知道哪个版本才是正确的。

借助 MCP，流程正好相反：由助手向 PaperOffice 提问。它在文档所在之处进行搜索和阅读，且仅限于其密钥允许的范围。本指南配有应用中的截图，逐步介绍设置方法，并说明事先应当决定哪些事项。

Daniel Schönland

PaperOffice 创始人兼首席执行官

适用对象

使用 Claude 或 ChatGPT 的团队

您希望直接在聊天中回答关于合同、发票和档案的问题。

IT 与数据保护

您创建密钥、限制访问权限，并在必要时将其封锁。

管理层

您决定哪些助手可以处理哪些数据。

之后您能做到什么

为您的 AI 助手创建密钥，将访问限制在特定 Workspace，连接 Claude、ChatGPT 或 Cursor，提出好的问题，对写入操作加以保护，并随时封锁访问权限。

概览

目录

01	一个问题，一份合同	04
02	为什么仅上传到聊天框还不够	05
03	流程一览	06
04	在应用中：创建密钥	07
05	将访问限制在特定 Workspace	08
06	连接 Claude	09
07	PaperOffice 连接页面	10
08	ChatGPT、Cursor 及其他	11
09	允许读取，审批写入	12
10	好的提问，可核实的回答	13
11	经审批后的写入	14
12	保护机密数据	15
13	团队启动时会问什么	16
14	30 分钟亲自测试	17
15	相关视频	18
16	五天内打造安全的助手	19
17	检查清单与开始	20

一览

- AI 助手通过 MCP 直接在 PaperOffice 中工作。它在那里搜索和阅读，而不是在聊天中收集副本。
- 它只能看到其密钥允许的内容。组令牌会将其限制在某个用户组的 Workspace 范围内。
- 每个工具都标明为读取、写入或删除。在助手中，您设定哪些操作无需询问即可执行。
- 机密数据留在档案库中：没有任何助手用户组可以访问包含人事档案或健康数据的 Workspace。
- 被封锁的密钥会立即断开助手的连接。

01 · 一个问题，一份合同

合同何时到期？ Claude 自行查询。

Northstar Industrial Systems 采购部的 Kevin Flynn 想在与 Kaltwerk 进行年度会谈之前，了解维护合同的费用以及到期时间。



到目前为止，他需要在 PaperOffice 中搜索合同、下载、拖进聊天框，并在那里提问。即使之后收到补充协议，聊天记录中仍保留着这份副本。

通过 MCP 连接，他直接向 Claude 提问。Claude 在 PaperOffice 中搜索 Kaltwerk，并在 Workspace “Contracts” 中找到维护合同 WV-2026-118。合同载明年度固定费用为 4,800 € 加增值税，合同到期日为 2028年10月31日。对于每条搜索结果，Claude 都会获得文档名称、编号和 Workspace，因此每个回答都可以在应用中核对。

真正的难点

助手的能力取决于它被允许看到的内容。问题不在于它能否获得访问权限，而在于能访问什么、拥有何种权限，以及谁可以再将其收回。

02 · 为什么仅上传到聊天框还不够

关于副本的四个问题。 一个连接即可解决。

把文件拖进聊天框很快。但对于会不断变化、且并非所有人都可查看的文档，这会带来后果。

副本取代原件

每个上传的文件都是副本。出现补充协议时，聊天仍在使
用旧版本工作。

权限被留在身后

在 PaperOffice 中，用户组和 Workspace 决定谁能看到什
么。聊天框中的副本并不了解这些规则。

一个文件，一个问题

想讨论二十张发票的人，要上传二十个文件，并希望没有
遗漏。

缺乏总览

之后没有人知道哪些文件位于哪个聊天中。

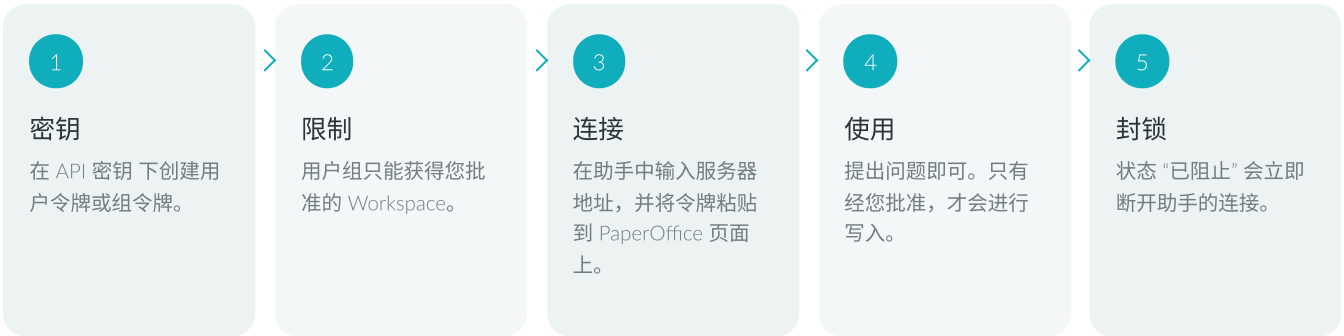
用两句话介绍 MCP

MCP (Model Context Protocol) 是一种开放标准，AI 助手借助它使用其他程序的工具。PaperOffice 提供一个 MCP
服务器：助手通过它进行搜索、阅读和工作，但仅限于其密钥的权限范围内。

助手能做什么	工具目录中的示例
搜索	全文、识别出的字段和语义，范围限于其有权查看的 Workspace
读取	内容、识别出的字段（如金额和期限）、摘要、审核结果
添加	在文档上创建备注和评论
整理	重命名或移动文档，处理任务

五个步骤。 其中之一是关闭开关。

设置只需几分钟。最重要的决定要先做：助手可以看到什么。



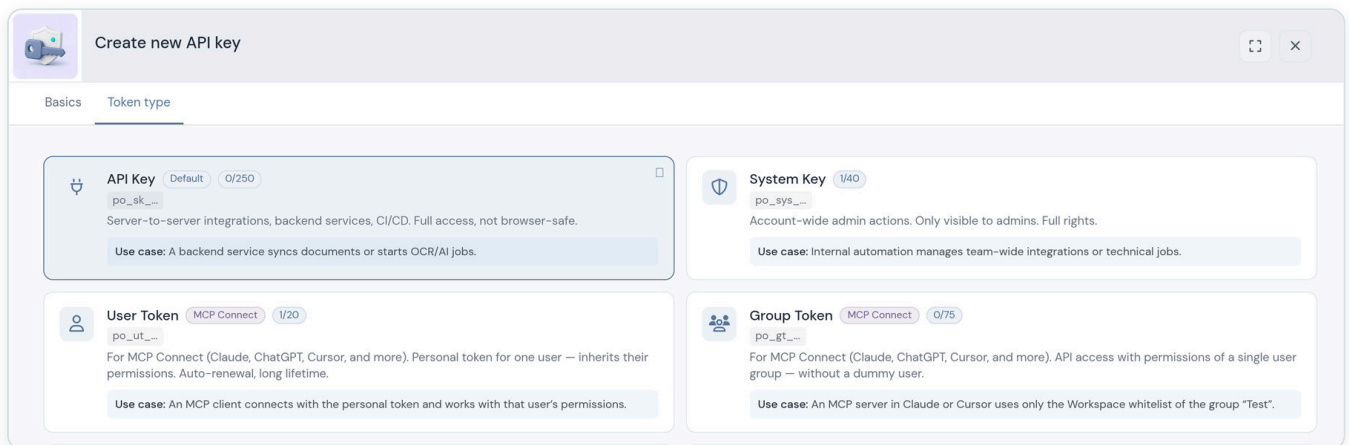
步骤	PAPEROFFICE 负责的部分	由您的团队决定的部分
密钥	生成令牌，可随时在列表中复制	谁获得密钥
限制	将用户组的权限应用于每次调用	哪些 Workspace 获得批准
连接	每次连接时检查令牌	哪些助手获得批准
使用	将每个工具标记为读取、写入或删除	哪些操作无需询问即可执行
封锁	在下次调用时拒绝被封锁的令牌	密钥何时过期



04 · 在应用中：创建密钥

为助手创建密钥。 使用您本人或某个用户组的权限。

在右侧边栏中依次点击 [API和开发者](#) > [API 密钥](#) > [创建新密钥](#)，然后切换到 [令牌类型](#) 标签页。



- 1 选择 **令牌类型**。对于 Claude、ChatGPT 或 Cursor，请使用标有“MCP Connect”的两张卡片之一：用户令牌继承该人员的权限，组令牌继承某个用户组的权限。

用户令牌

供您个人使用的助手。它看到的正是您看到的内容。对于账户所有者来说，就是全部内容。

组令牌

适用于团队以及需要受限的情况。管理员可以创建，但该用户组必须事先存在。

如同密码

您可以随时在 **API 密钥** 列表中复制令牌。请像对待密码一样对待它。

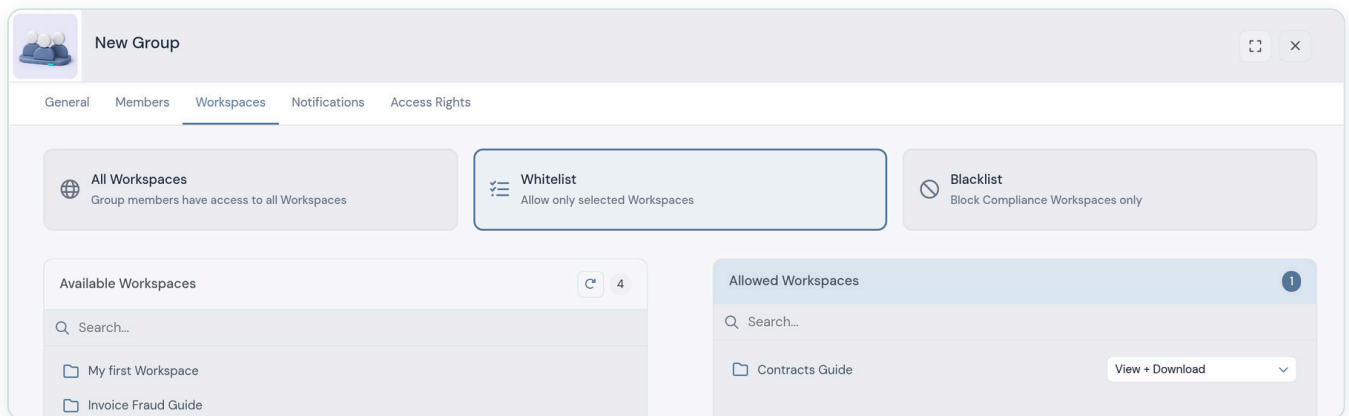
最快的方式

在 [帮助与学习](#) > [设置 PaperOffice](#) > [连接 AI 助手](#) 下，“创建令牌”会创建一个用户令牌。旁边是服务器地址，以及为您的助手准备的步骤（第 06 章）。

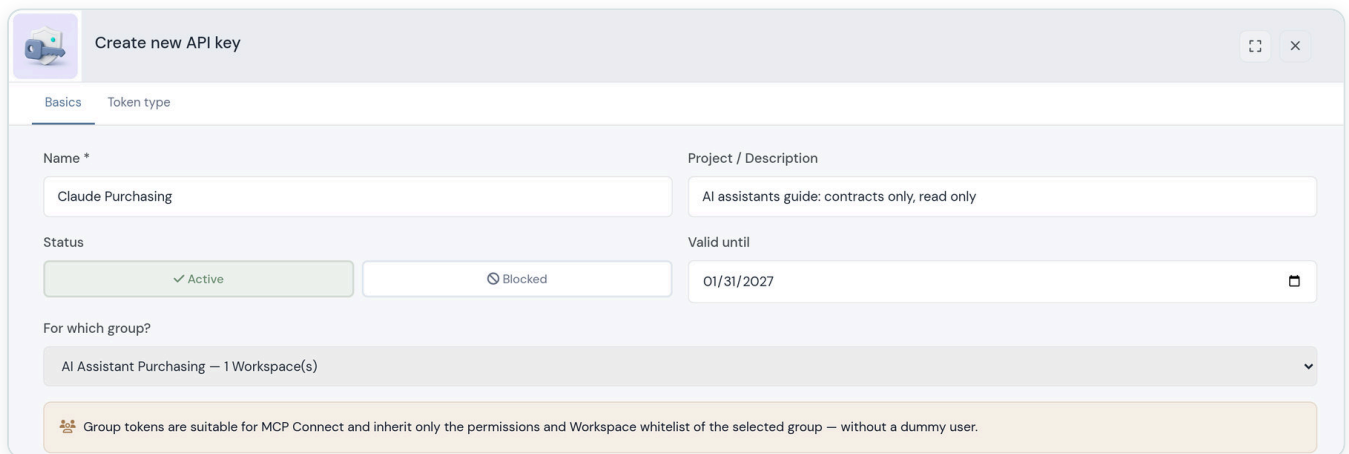
05 · 将访问限制在特定 WORKSPACE

助手能看到合同。 看不到人事档案。

您只需通过用户组分配一次权限。组令牌会完全继承该组的权限。



- 1 带白名单的用户组。在 **用户组** 下创建一个用户组，例如 "AI Assistant Purchasing"。在 "Workspaces" 标签页中选择 "白名单"，并仅允许助手应当看到的 Workspace。"查看 + 下载" 表示：仅读取。



- 2 创建组令牌。在 "适用于哪个组？" 下选择新建的用户组。设定 "有效期至" 后，密钥会自动过期。

受保护的 Workspace

受保护 Workspace 的密码和短信验证码绝不应出现在聊天中：通过 Claude 和 ChatGPT，连接根本不接受它们。解锁请在应用中进行。

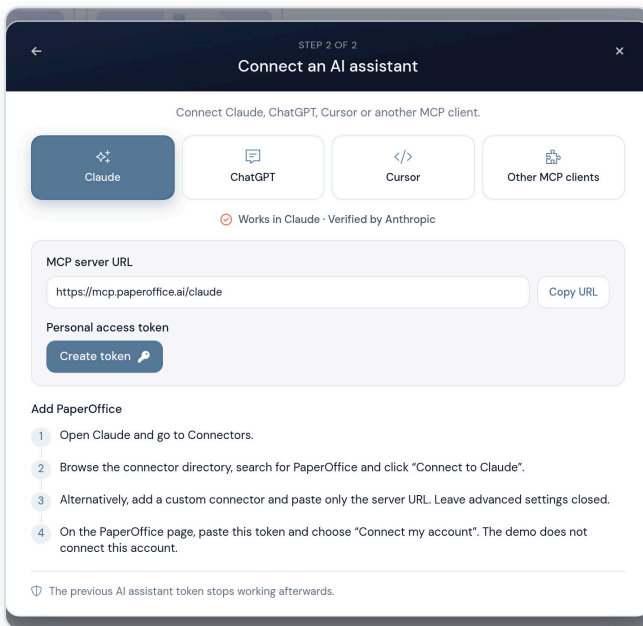
每个用途一个密钥

采购、会计和销售各自拥有独立的用户组和独立的令牌。这样，每一个都可以单独封锁。

06 · 连接 CLAUDE

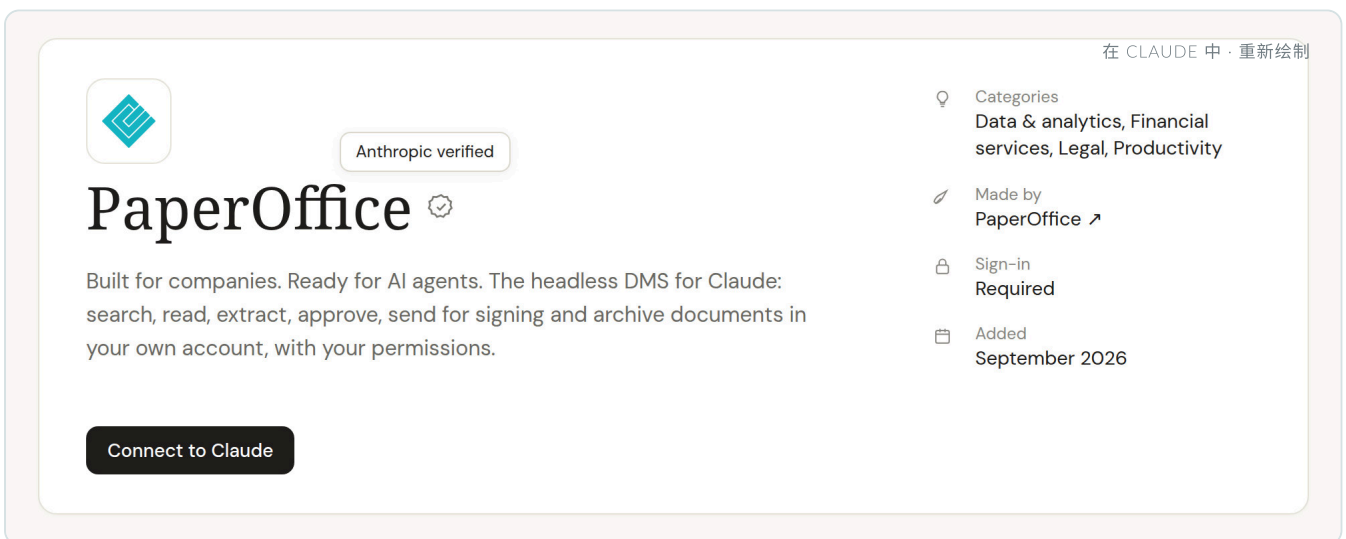
服务器地址、令牌，完成。 应用会显示每一步。

在 [帮助与学习](#) > [设置 PaperOffice](#) > [连接 AI 助手](#) 下选择您的助手。应用会显示对应的服务器地址和步骤。



- 1 服务器地址： <https://mcp.paperooffice.ai/claude>
- 2 令牌：“创建令牌”会创建一个用户令牌。之前以此方式创建的令牌将不再有效。
- 3 在 Claude 中：在“自定义”>“连接器”下，从目录中选择 PaperOffice，或使用服务器地址添加自定义连接器。
- 4 登录：在 PaperOffice 页面上粘贴令牌，然后选择“Connect my account”（第 07 章）。

- 1 在 PaperOffice 中。“Claude”标签页：复制服务器地址，然后点击“创建令牌”。



- 2 在 Claude 中。在目录中找到带有“经 Anthropic 验证”标识的 PaperOffice。点击“连接到 Claude”会打开 PaperOffice 的连接页面。

您自己的账户或演示。 您在一个页面上做决定。

连接时，您的助手会打开页面“Connect ... to PaperOffice AI”，该页面提供两种方式。

使用您自己的 PaperOffice 账户

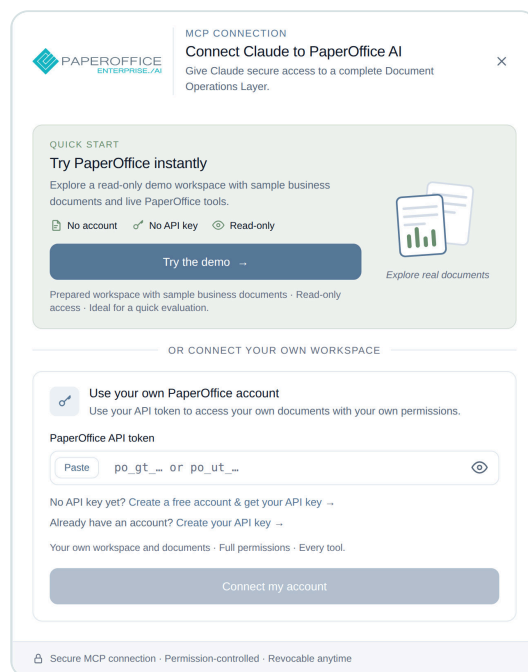
粘贴用户令牌或组令牌，然后点击“Connect my account”。之后助手将以该密钥的权限工作。

试用演示

一个带有示例文档的演示 Workspace，无需账户和密钥，仅供读取。适合初步了解。

“Full permissions · Every tool”

这指的是粘贴的密钥拥有的全部权限。请通过组令牌进行限制（第 05 章）。



Claude 的连接页面

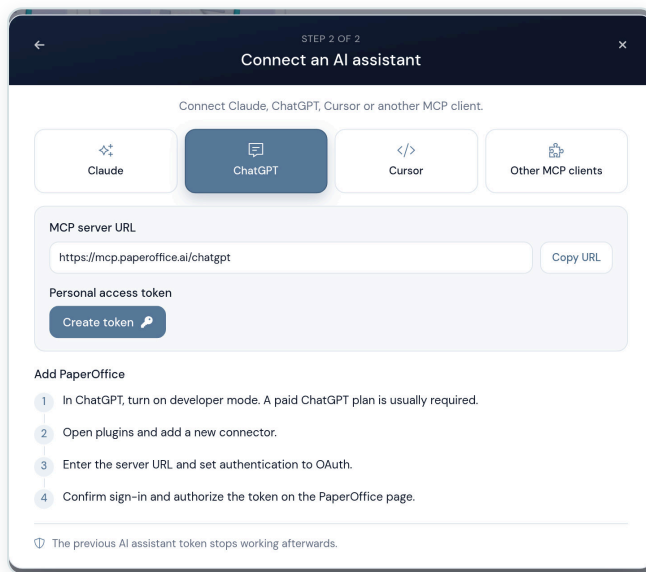
值得了解

Claude 获得的并不是您的令牌本身，而是它自己的连接密钥。如果您在 PaperOffice 中封锁了该令牌，连接也随之结束。

08 · CHATGPT、CURSOR 及其他

每个助手都有自己的地址。 密钥保持不变。

同一对话框中有“ChatGPT”、“Cursor”和“其他 MCP 客户端”标签页，每个标签页都有各自的服务器地址和步骤。



- 1 开发者模式：在 ChatGPT 中开启开发者模式。这通常需要付费的 ChatGPT 套餐。
- 2 连接器：新建一个连接器，输入服务器地址，身份验证选择“OAuth”。
- 3 登录：在 PaperOffice 页面上粘贴令牌并完成连接。

- 1 ChatGPT。服务器地址 <https://mcp.paperoffice.ai/chatgpt>。

助手	服务器地址	工具
Claude	mcp.paperoffice.ai/claude	完整目录，约 350 个工具
ChatGPT	mcp.paperoffice.ai/chatgpt	为 ChatGPT 组合的 56 个工具
Cursor	mcp.paperoffice.ai/cursor	mcp.json 中的一条记录；应用会显示该代码块
其他 MCP 客户端	mcp.paperoffice.ai/dms	将令牌作为 Bearer 令牌输入

CHATGPT 的其他保护规则

ChatGPT 适用额外的保护规则：电子邮件地址、电话号码、IBAN 和证件号码等个人信息会自动打码；人事、证件、健康和保险文件保持封锁。

09 · 允许读取，审批写入

读取可以立即进行。 更改需等待您点击确认。

PaperOffice 会标注每个工具。哪些操作无需询问即可执行，在助手中设定。

Tool permissions

Choose when Claude is allowed to use these tools.

在 CLAUDE 中 · 重新绘制

Read-only tools	Always allow
Search documents in DMS	☒ ☐ ☐
List accessible workspaces	☒ ☐ ☐
Get document details and metadata	☒ ☐ ☐

Write/delete tools	Needs approval
Add document note	☐ ☒ ☐
Move document to workspace	☐ ☒ ☐
Documents Notes Delete	☐ ☒ ☐

1 在 Claude 中。在“自定义”>“连接器”>PaperOffice 下：只读工具设为“Always allow”，写入/删除工具设为“需要审批”。这是我们的建议。

标志	含义	示例
只读	只读取，不做任何更改	搜索文档、查看详情、列出 Workspace
写入数据	创建或更改某些内容	创建备注、移动文档
破坏性	更改或删除某些内容，或触达外部人员	重命名、删除备注、完成任务

仅经审批才可删除

在客户端中将写入和删除工具设为“需要审批”。之后，助手会在每次更改和每次删除前进行询问。

只在够用的地方授予读取权限

对于纯粹的信息查询，“查看 + 下载”权限就已足够。此时助手不会更改或删除任何内容，即使经过批准也不会。

10 · 好的提问，可核实的回答

提问要具体。 答案连同来源一并给出。

问题越精确，助手需要猜测的就越少。请始终要求它指明文档。

K

When does the maintenance contract with Kaltwerk end, and what does it cost per year?
Name the document.

在 CLAUDE 中 · 重新绘制

◆ Search documents in DMS >

◆ Get document details and metadata >

Maintenance contract WV-2026-118 with Kaltwerk Kältetechnik ends on October 31, 2028. The annual flat fee is EUR 4,800 plus VAT.

The last day to cancel is July 31, 2028, three months before the contract ends.

◆ Source: Maintenance Contract WV-2026-118 - KALTWERK.pdf · Workspace "Contracts Guide"

1 在 Claude 中。Claude 进行搜索，阅读合同并指明来源。更多示例：“Invoice Fraud Guide Workspace 中哪些发票在隔离区，原因是什么？”以及“请总结 3 号厅的租赁合同：期限、解约期限、出租人。”

如何提问更好	原因
指明 Workspace	助手随后会有针对性地搜索，而不是遍历所有 Workspace。
要求指明文档	对于每条结果，它都会获得名称、编号和 Workspace。这样您就能在应用中核对答案。
要求提供字段	PaperOffice 在阅读时已识别出金额、日期和期限。助手会直接采用它们，而不是估算。
让它计算，再核对	日期减去解约期限，由助手自行计算。请对照合同核对结果。

11 · 经审批后的写入

关于合同的一条备注。 仅经您批准之后。

如果助手被允许写入，它会直接在文档中工作：添加备注、评论或新名称。设为“需要审批”时，它会先行询问。

K Add a note to maintenance contract WV-2026-118: Check cancellation by July 31, 2028.

在 CLAUDE 中 · 重新绘制

I'll add the note to the contract. The tool writes data, so it needs approval.

Claude wants to use a tool from PaperOffice

Tool	Add document note
Document	Maintenance Contract WV-2026-118 - KALTWERK.pdf
Note	Check cancellation by July 31, 2028.

Deny

Allow

1 在 Claude 中。由于该工具会写入数据，Claude 会先询问。只有在您批准后，备注才会添加到文档上，并可在“活动”下看到。

添加

创建和编辑备注及评论。

整理

重命名文档，或将其移到另一个 Workspace。

任务

接手、升级或完成任务。

事先决定

哪些 Workspace 可由助手更改，在用户组中设定。对于纯粹的信息查询，“查看 + 下载”就已足够；此时它不会写入任何内容，即使经过批准也不会。

12 · 保护机密数据

由您决定助手能看到什么。 机密数据留在档案库中。

PaperOffice 只向助手提供其密钥允许的内容。它获取的内容会由其提供商在对话中进行处理。因此，首先就不要向其开放机密数据。



将机密数据留在档案库中

人事档案、健康记录和证件存放在没有任何助手用户组可以访问的 Workspace 中。

卡号已打码

信用卡号在结果中已打码，对每个助手都一样。

为 ChatGPT 提供更多保护

个人信息会自动打码；人事、证件、健康和保险文件保持封锁。

您的约定

哪个助手可以处理哪些数据，是您与 AI 提供商约定的事项，并应记录在您的数据保护文档中。

可追溯	位置
已连接的密钥	API 密钥 列表，标签“Claude · MCP”
调用了哪些工具	工具调用日志，您的 IT 部门可通过 API 调取
助手添加了什么	文档上的备注和评论；对防篡改文档的更改记录在审计历史中

13 · 团队启动时会问什么

七个问题 开始之前。



助手能看到所有文档吗？

只能看到其密钥允许看到的文档。使用组令牌时，即为该用户组的 Workspace。

它能删除任何东西吗？

仅当其权限允许时才可以。在客户端中将写入和删除工具设为“需要审批”，之后它会在每次删除前询问。

如何封锁访问？

在 API 密钥 列表中打开该密钥并选择“已阻止”。下一次调用会被拒绝。在您创建第二个令牌之后，才能封锁自己最后一个用户令牌。

哪些助手可以使用？

Claude、ChatGPT、Cursor 以及其他支持 MCP 的客户端，各自有独立的服务器地址。

需要付费的 ChatGPT 吗？

开发者模式通常需要。Claude 通过其连接器目录连接 PaperOffice。

无需账户也能试用吗？

可以。在连接页面上选择“Try the demo”：一个带有示例文档的演示 Workspace，仅供读取。

费用是多少？

每次调用都消耗 Credits，与 API 相同。具体内容请参见价格页面：paperoffice.ai/en/pricing。

14 · 30 分钟亲自测试

先试演示。 然后用您自己的档案库。

两种试用方式：无需账户的演示，以及使用我们指南中的测试包、通过您自己的账户进行试用。

CLAUDE 与 PAPEROFFICE

设置、视频和演示，尽在一页

Claude 的服务器地址 <https://mcp.paperoffice.ai/claude>

无需账户的演示 在连接页面上选择 "Try the demo"

paperoffice.ai/l/claude



- 1 演示：在 Claude 中连接 PaperOffice，在连接页面上选择 "Try the demo"，然后提出一个问题。
- 2 您自己的账户：在 app.paperoffice.ai 上创建一个 Workspace，并上传一个测试包，例如指南《Detecting Invoice Fraud》中的测试包。
- 3 限制：创建一个只包含此 Workspace 的用户组，权限设为 "查看 + 下载"，再加一个组令牌。
- 4 连接：在连接页面上粘贴组令牌，点击 "Connect my account"。
- 5 提问："此 Workspace 中哪些文档在隔离区，原因是什么？"
- 6 封锁：将组令牌设为 "已阻止"，然后再次提出同一个问题。

如何判断它生效了

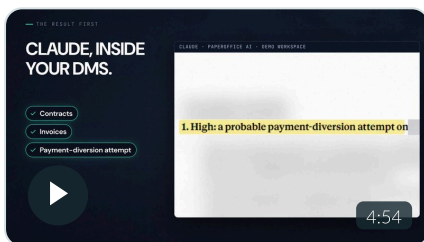
助手只会指出来自允许的 Workspace 的文档。封锁之后，它将无法再从 PaperOffice 获得任何回答。

测试费用 请参见我们的价格页面：paperoffice.ai/en/pricing

15 · 相关视频

更喜欢看视频？ 关于 Claude、ChatGPT 和 MCP 的短片。

paperoffice.ai 上的短片。用手机相机扫描二维码，或打开链接。



Claude 演示

从设置到结果。

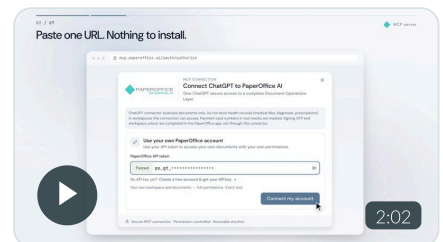
paperoffice.ai/l/claude



连接 ChatGPT

在 ChatGPT 中设置 PaperOffice。

paperoffice.ai/l/chatgpt-setup



面向开发者的 MCP

粘贴服务器地址，无需安装。

paperoffice.ai/l/developer-mcp



更多内容见 [ACADEMY](#)

所有课程和网络研讨会都可在 paperoffice.ai/l/academy 查看，按主题从第一个 Workspace 一直排列到系统集成。

16 · 五天内打造安全的助手

先从一个团队开始。 然后逐个用户组推进。

入门只需一个团队、一个 Workspace、一个用户组和一个组令牌。



1

第 1 天 · 目的

确定哪个团队想提出哪些问题，以及为此需要哪些 Workspace。

2

第 2 天 · 用户组与密钥

创建带白名单的用户组，权限设为“查看 + 下载”，并创建带有效期的组令牌。

3

第 3 天 · 连接

连接 Claude 或 ChatGPT，允许读取类工具，并将写入类工具设为需要审批。

4

第 4 天 · 提问

提出十个日常工作中的真实问题，并对照文档核实每一个答案。

5

第 5 天 · 规则

以书面形式明确：谁创建密钥、谁封锁密钥，以及助手可以写入什么。

衡量这四项指标

无需下载

无需下载即可回答的问题所占比例

正确

对照文档核查后经得起检验的答案所占比例

每个问题的耗时

从提问到经核实的答案

带有效期的密钥

设置了“有效期至”的密钥所占比例

事先用人工方式测量相同的指标一次；只有对比才能显示效果。

17 · 检查清单与开始

在扩展之前。

- ☐ 已确定哪些团队使用哪个助手。
- ☐ 每个团队都有一个带白名单的用户组和各自的组令牌。
- ☐ 没有任何助手用户组能看到敏感 Workspace。
- ☐ 每个密钥都有有效期。
- ☐ 只读工具可自由运行；写入和删除工具仅经审批后才可执行。
- ☐ 对于纯粹的信息查询，助手用户组拥有“查看 + 下载”权限。
- ☐ 已确定当某人离开团队时由谁封锁密钥。
- ☐ 已提出十个真实问题，并已对照文档核实。

立即开始

创建账户，创建密钥，连接 Claude 或 ChatGPT。从免费套餐（Free）开始，无需信用卡。

app.paperoffice.ai

继续阅读

解决方案

PaperOffice 在 Claude 中

设置

PaperOffice 在 ChatGPT 中

开发者

PaperOffice 的 MCP 服务器

对本指南有疑问？

如果您对设置、权限或密钥有疑问，请与我们联系。

paperoffice.ai/contact

截至 2026 年 10 月。应用中的图片来自测试账户。Claude 的界面按真实的标签、工具名称和测试文档重新绘制。Claude 是 Anthropic 的产品，ChatGPT 是 OpenAI 的产品，Cursor 是 Anysphere 的产品。本指南中的所有示例、公司、姓名和数值均为虚构。PaperOffice，paperoffice.ai。