新-代智能体产品家族 智能化办公平台 V1.0

用户操作手册

北京致远互联软件股份有限公司

2025年5月

目录

前言：AI时代的协同革命 3

一、 产品定位：人智协同 1

1.1品牌内涵：Collaborative Operating With Me 1

1.2产品架构：“入口-智能体-定制”三位一体 1

1.3产品蓝图：1+2+4+N 1

1.4与COP的协同：无缝嵌入企业现有系统 1

1.5五大核心特性 2

2.1运行环境要求 2

2.2 LLM大语言模型支持范围 3

2.3浏览器兼容 3

2.4数据库支持 3

二、 初始化和授权 3

3.1 系统管理员 3

3.2 集团管理员 4

3.3 单位管理员 4

三、 智能化办公平台 功能介绍 5

4.1超级入口 5

4.1.1智能门户 5

4.1.2智能助手 7

4.2智能体 10

4.2.1智能问答 10

4.i2.2 Exce分析 15

4.2.3 智能办公 17

4.2.4 辅助审批 21

4.2.5 总结阅读 24

4.2.6 智能创作 25

4.2.7 模型对话 27

4.2.8 安全助理 28

4.2.9 超级助理 31

4.3 智能化办公平台运行引擎 32

4.3.1大模型管理 32

4.3.2提示词管理 34

4.3.3智能体工具管理 35

4.3.4向量库 37

4.3.5Agent搭建器 38

4.3.6会话应用管理 40

4.3.7安全管理 41

4.3.8系统管理 43

4.3.9权限管理 43

# 前言：AI时代的协同革命

当AI从“工具辅助”进化为“自主决策”的智能体（Agent），企业协同办公正经历从“效率工具”到“数字员工”的范式跃迁。Gartner预测，2028年15%的日常工作决策将由代理型AI自主完成，智能体已成为企业数智化转型的核心抓手。

作为企业协同运营管理领域的领军者，致远互联基于20多年协同经验与AI技术深度融合，推出新一代智能体产品家族智能化办公平台（Collaborative Operating with me）。智能化办公平台以“人智协同”为核心理念，通过角色化智能体、多任务协作、灵活定制三大核心能力，重新定义组织工作方式，助力企业从“流程驱动”迈向“智能驱动”，开启人智协同的新纪元。

# 产品定位：人智协同

### 1.1品牌内涵：Collaborative Operating With Me

（1）技术层面：全面Agent化技术架构。

（2）交互层面：Call Me（交互方式），通过自然语言等新的交互提升效率。

（3）应用层面：角色化智能体（Me + “i”），为企业各角色提供专属数智分身。

### 1.2产品架构：“入口-智能体-定制”三位一体

智能化办公平台 是以智能体为形态的AI-COP数智运营产品家族，智能化办公平台 Agents实现组织从数字化到智能化 的跃迁，智能化办公平台 Agent Builder支持按需定制智能体。智能化办公平台可以在COP V5/V8 及协同运营领域模型上运行多个智能体构成人智协同的新范式。

### 1.3产品蓝图：1+2+4+N

（1）1个入口：一个超级入口。

（2）2个引擎: 智能化办公平台 Builder 设计引擎和运行引擎。

（3）4种类型：包含智能化办公平台智能套件、智能化办公平台智能应用、智能化办公平台设计套件、智能化办公平台协同套件。

（4）N个智能体： 结合企业自身业务场景打造专属的智能体应用。

### 1.4与COP的协同：无缝嵌入企业现有系统

智能化办公平台深度依托致远协同运营平台（COP，包括A6、A8、A9等产品线），不独立售卖，而是通过“智能体+COP”组合模式，将智能能力无缝嵌入企业现有协同、业务、运营场景，降低部署成本，加速价值落地。

1.5五大核心特性

运行环境及配置

### 2.1运行环境要求

智能化办公平台依赖如下组件服务，需要在服务器进行相关部署，再与协同系统进行配置互通使用：

|  |  |  |
| --- | --- | --- |
| 服务 | 说明 | 操作系统 |
| 智能化办公平台Builder-Engine | 智能化办公平台Builder-Agent引擎服务，提供Agent智能体的语义理解、调用执行处理 | CentOS或Ubuntu |
| 智能化办公平台Builder-Security | 智能化办公平台Builder安全服务，提供敏感词检测等安全策略的控制 | CentOS或Ubuntu |
| 智能化办公平台Builder-Manager | 智能化办公平台Builder管理服务，提供AI平台的维护管理及配置功能 | CentOS或Ubuntu |
| qdrant | 向量数据库，用于存储、检索高维向量数据，是RAG不可或缺的组件 | CentOS或Ubuntu |
| 数据库 | 关系型数据库，用于存储智能化办公平台Builder基础配置信息，可复用协同使用的数据库服务 | 无限制 |
| Nginx | 用于代理协同与智能化办公平台Builder各服务，确保服务间关联 | Linux或信创系统 |
| Embedding模型 | 将文本转换为高维向量的大模型服务，与qdrant搭配，是RAG不可或缺的组件 |  |
| LLM大语言模型 | 一种基于大量文本数据训练的深度学习模型，旨在理解和生成自然语言。DeepSeek、Gpt-4O、通义千问均属于此类。 |  |

说明：

1. 智能化办公平台 V1.0版本建议独立部署，需要至少一台服务器。详见智能化办公平台部署维护手册。
2. 智能化办公平台依赖协同主服务运行，需确保协同主服务已经包含智能化办公平台所需商务插件。
3. EmBedding模型可使用用户自采的向量化模型，也可部署安装包提供的开源模型组件。
4. LLM大语言模型涉及复杂的技术架构和高配置要求，需要客户自行采购，或使用公有云大语言模型。

### 2.2 LLM大语言模型支持范围

产品支持接入满足openai规范的大语言模型（公有或私有均支持），其他情况下有一定的适配工作量，支持的模型包含并不仅限于：

* DeepSeek（V3、R1）
* 通义千问（qwen2.5、qwen-plus）
* ChatGpt（4o）

### 2.3浏览器兼容

（1）Chrome 64+；

（2）Safari14+；

（3）Edge 79+；

### 2.4数据库支持

智能化办公平台依赖关系型数据库，用于存储智能化办公平台 Builder基础配置信息，可复用协同使用的数据库服务，智能化办公平台 V1.0支持的数据库为：mysql、oracle、sqlServer、达梦、人大金仓、postgre。详细见智能化办公平台部署维护手册。

# 初始化和授权

### 3.1 系统管理员

步骤1：购买智能化办公平台后，系统管理员在【后台管理】进入【智能化办公平台】点击【模型管理】在该模块新增和维护【大模型】。

步骤2：完成【大模型】接入后点击进入【系统管理】的【数据初始化】模块进行初始化配置。【向量库模型标识】仅支持选择模型类型为【Embedding】的模型，【模型标识】控制Agent、智能体使用的大模型，仅支持选择模型类型为【LLM】的模型。【协同Base Url】只需输入系统IP即可，如：http://118.112.188.178:6680。

### 3.2 集团管理员

购买智能化办公平台后，集团管理员在【后台管理】进入【智能应用设置】点击【智能化办公平台应用授权】可操作【授权单位】或【授权用户】。授权给单位只是该单位的单位管理员可针对单位下人员进行授权，只有授权到具体用户才可正常使用。可授权人员数量受购买插件时注册用户数量控制。

### 3.3 单位管理员

购买智能化办公平台后，单位管理员在【后台管理】进入【智能应用设置】点击【智能化办公平台应用授权】可操作【授权用户】。可授权人员数量受购买插件时注册用户数量控制。

# 智能化办公平台 功能介绍

## 4.1超级入口

### **4.1.1**智能门户

#### 4.1.1.1场景简介

智能化办公平台智能门户作为穿透OA场景的智能中枢枢纽，深度融合自然交互与智能决策能力，致力于提升企业级用户在复杂业务流程中的效率与体验。其核心场景聚焦于通过自然语言对话窗口实现"零门槛"业务处理，用户可随时唤醒超级助手完成待办穿透、待开会议查看操作；动态面板通过AI动态排序每日最高优先级待办事项，并智能提炼会议核心议程，形成决策焦点看板。同时集成的智能创作矩阵覆盖从文档生成到数据分析的一系列智能场景，支持Excel数据对话实现动态报表洞察，结合智能问卷与知识问答构建闭环式知识服务体系。通过将Agent智能体深度嵌入OA审批、项目管理等全流程节点，系统实现了业务流的自感知、自决策与自动化执行，形成覆盖事前预警、事中辅助、事后分析的智能化工作闭环。

#### 4.1.1.2使用配置

购买“智能化办公平台超级入口”插件后，即可在用户端页面右侧展示【智能门户】入口，无需其他配置。

#### 4.1.1.3操作流程

步骤1：登录进入协同首页，在【门户导航】中选择【智能门户】即可进入，如图：

步骤2：登录进入到智能门户首页，在用户没有待办事项和待开会议时，展示初始化首页。

步骤3：在用户待办事项和待开会议不均为空的情况下，展示动态看板首页。

步骤4：点击左侧快捷入口展开按钮，查看核心通用智能能力和常用智能体

步骤5：点击快捷入口智能体，发起交互。

步骤6：快捷入口下方，展示的是“历史会话”和“智能体广场”的快捷入口，点击进入详情。

步骤7：动态看板区域，点击待办内容，直接跳转审批详情，点击待开会议，直接跳转会议详情；点击工作指引，直接发起会话；

步骤8：对话框可直接发起会话，直接会话时调用智能化办公平台超级助手，会根据对话内容调用合适的应用进行回答；

步骤9：对话框上方，快捷操作区域，展示的是一些通用的快捷操作，比如点击“数据分析”，基于EXCEL做问数；

步骤10：对话框上方，在发起会话后，展示“发起新会话”按钮，点击发起新会话（同步回到首页）。

步骤11：对话框区域，除文本输入外，还支持“快捷指令”，点击可选择快捷指令进行对话，“快捷指令”一般是特定小场景中常用的指令，区别于“快捷操作”。

步骤12：对话框区域，除文本输入外，还支持文件上传，点击打开本地文件选择框。仅支持上传1个文件进行对话，支持.xlsx .xls .txt .docx .pdf .md （ .markdown ）.csv格式文档。

### **4.1.2智能助手**

#### 4.1.2.1场景简介

深度融合协同各类业务场景，通过AI能力实现业务处理的自动化、智能化与个性化。可根据当前业务场景自动识别并唤起对应的智能体，支持参数传递、数据回填、状态同步等功能。用户只需一句话即可触发关键业务流程，确保业务系统与智能体之间的信息高效流转。

#### 4.1.2.2使用配置

购买“智能化办公平台超级入口”插件后，即可在用户端页面右侧展示【智能助手】入口，无需其他配置。

#### 4.1.2.3操作流程

步骤1：进入协同办公首页，点击右侧【智能助手】图标即可进入智能助手侧滑框。

步骤2：进入【智能助手】，默认最小化展示侧边栏，可点击【放大】或【展开】按钮进入智能助手【全屏页面】。侧边栏货全屏状态下，可点击【收起】按钮隐藏【智能助手】。

步骤3：【智能助手】包含以下模块：

1. 导航区：【超级助理】【智能体】【历史会话】【常用助手】【使用指南】；
2. 开场白引导区：【智能体介绍】【开场白预置问题】；
3. 输入对话区：【发起新对话】【输入框】【快捷指令】【上传附件】【发送及停止】；
4. 窗口操作区：【收起】【放大/缩小】；

进入【智能助手】，默认选中【超级助理】，在智能化办公平台运行引擎中【超级助理】中可配置多个【Agent】。通过和【超级助理】对话，可自动根据用户语义调用对应【Agent】执行业务。

步骤4：点击【智能体】进入智能体广场，可以查看所有有权限使用的智能体，智能体会根据智能化办公平台运行引擎创建的标签进行分类。支持通过名称对智能体进行【搜索】，点击智能体可进入对应【智能体】专属页面。

步骤5：点击进入【历史会话】，可以查看所有对话历史会话记录。可【搜索】【删除】【编辑】历史会话。

步骤6：点击进入【历史会话记录】，可以查看对话详细内容，支持继续进行对话。

步骤7：根据对话【智能助手】会记录7个【常用助手】，可快速点击进入智能体专属页面。

步骤8：可以使用【助手引导问题】和【快捷指令】快速发起对话。

步骤9：对话中智能体正在进行回答时不支持【发起新对话】和输入内容发送问题。如需进行新的对话需点击对话输入框中【停止】按钮，中断本次对话后，才可输入问题发起新的对话。

步骤10：支持【上传附件】进行对话。仅支持上传1个文件进行对话，支持.xlsx .xls .txt .docx .pdf .md （ .markdown ）.csv格式文档。

## 4.2智能体

### **4.2.1智能问答**

#### 4.2.1.1场景简介

智能问答在企业内部的提升员工效率、降低培训成本和增强知识管理方面发挥重要作用。分别包含以下核心场景能力：

1）新员工入职时需要了解公司文化、组织架构、岗位职责、IT系统使用等信息。

2）企业在日常运营中积累了大量的业务知识、技术文档、客户案例等，员工在工作中常需快速查找这些信息。

3）员工经常需要查询公司的规章制度，如考勤制度、薪酬福利、信息安全政策、差旅标准等。

#### 4.2.1.2使用配置

步骤1：进入【后台管理】选择【集团管理员】或者【单位管理员】可接入或维护大模型。

步骤2：进入【应用】找到【智能问答】智能体。

步骤3：点击进入【智能问答】。可对图标、名称、描述、Agent、开场白、开场白预置问题、问题建议、兜底方式、模型标识进行维护。智能问答由【智能问答Agent】组成。

步骤4：选择【智能问答Agent】，可查看Agent详情，设置Agent描述或删除Agent。点击【设置】，可设置Agent描述，准确描述Agent包含的内容范围，可改善Agent使用准确率。

步骤5：点击【详情】可查看、修改该Agent的角色设定、推理模式（ReAct模式、按顺序执行）、工具、向量库、对话轮数、模型标识、模型标识（随机性、单词回复随机性）。Agent定义完成之后，点击【确定】即可在右侧【预览&调试】中进行对话，实时检查效果是否符合业务预期。

步骤6：【智能问答】依赖企业知识或制度文档，在【智能问答Agent】中，可查看向量库详情，设置向量库描述或删除向量库。点击【设置】，可设置向量库描述，准确描述向量库包含的内容范围，可改善模型使用向量库的准确率。

步骤7：点击【详情】进入【向量库】可维护向量库中知识文档，支持TXT、PDF、MARKDOWN、DOC、DOCX格式的本地文件，每个文件不超过50MB，最多可上传100个文件。点击【查看】进入对应文档可手动维护切片。需要注意的是添加制度文档时需检查向量切片词、句、段落的完整性，以保障合规审查结果的准确性。

步骤8：智能体配置完成后，进入【后台管理】选择【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.1.3操作流程

步骤1：进入协同办公首页，在【导航】中，光标移入【本门户空间】选择并点击【智能门户】进入【超级入口】。也可在页面右侧点击章鱼悬浮图标进入【智能门户】。

步骤2：进入【超级入口】或【智能门户】默认选中【超级助理】，可直接在【超级助理】下发出指令，超级助理可自动根据用户语义直接调用智能办公智能体执行任务。

步骤3：【智能门户】可通过点击【放大】进入全屏模式，也可点击【收起】或【缩小】可回到侧边栏模式。

步骤4：在【超级入口】或【智能门户】可以通过@符号，选择并指定【智能问答】根据用户指令执行任务。

步骤5：在【超级入口】或【智能门户】可以通过直接选择【智能问答】进入智能问答智能体页面。也可点击进入【智能体广场】通过【搜索】或【翻页】查找到【智能问答】。

步骤6：在【智能问答】智能体页面，可通过点击【引导问题】快速发出指令，也可通过点击对话输入框中的【快捷指令】快速发出指令。

步骤7：在问答过程中【智能问答】会展示回答过程中【参考知识源】，可展开查看知识源，支持点击【下载】至本地。

步骤8：【智能问答】结果可点击【复制】快速将回答使用在其他业务场景中。如果回答的结果不满意，可通过点击【重新生成】重新发送同一个问题重新生成回答结果。

步骤9：针对【智能问答】回答的每一个问题的答案，可通过点击【意见反馈】选择或填写意见，帮助【智能问答】提供更精准的回答。

步骤10：【智能问答】在回答过程中会根据上一个问题、参考知识源生成3个用户可能会关心的【推荐问题】，可通过点击推荐问题快捷提问。

步骤11：【智能问答】在回答过程中可在底部【对话输入框】中点击【停止】停止本次回答。需要注意的是本次回答未完成输入信息之后无法发送问题。

步骤12：【智能问答】支持多轮问答，可通过不断的追问更深入的了解相关知识、制度。

### **4.i2.2 Exce分析**

#### 4.2.2.1场景简介

上传Excel文件进行数据分析，生成可视化图表和总结建议。

•**文件上传：**支持xlsx、xls、csv格式的文件上传；

•**数据分析：**自动识别并处理分析不同类型的数据（数值型、文本型等）；

•**可视化展示：**支持生成占比图、趋势图、柱状图等图表；

•**数据洞察分析：**自动生成基于数据分析和洞察生成文字总结、业务建议；

#### 4.2.2.2使用配置

步骤1：以集团管理员或单位管理员身份进入智能化办公平台 Builder后台，切换至应用菜单，通过搜索Excel分析，找到对应应用。

步骤2：进入Excel分析应用，可以修改描述、开场白、问题建议、兜底方式以及切换选择模型标识。

步骤3：配置完成后，进入【后台管理】切换【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.2.3操作流程

步骤1：进入智能门户或智能助手后，可通过常用菜单区找到Excel分析。

步骤2：接下来你可以上传Excel文件，提出你的问题和要求进行分析了。

•**注意1：**仅支持上传一个文件，且文件大小限制在10M以内；

•**注意2：**仅支持单一sheet页数据解析(如果上传多sheet页文件，仅对当前激活的sheet页进行解析)；

•**注意3：**对于xlsx、xls、csv中结构化数据，可按维度（下拉框、文本、日期类型）和指标（数值、货币类型）解析出结构化数据的结果；

•**注意4：**对于xlsx、xls、csv中没有结构化数据，无法解析出按维度、指标统计的数据结果，不支持这类上传文件的解析问数；

### **4.2.3 智能办公**

#### 4.2.3.1场景介绍

智能办公包含流程发起及查询、菜单导航查询、新闻公告及通讯录查询三大模块能力，覆盖场景丰富，分别包含以下核心场景能力：

1）只需通过对话告诉智能办公你想发起的流程表单，或者上传一份相关的文档（如Word、PDF等），智能办公就能自动识别并提取关键信息，匹配到对应的表单字段，帮您一键快速发起流程。

2）根据待办事项的优先级和是否即将超期，自动筛选出当前最需要你处理的6条待办事项，让你第一时间聚焦重点任务，避免遗漏和延误。

3）对所有已处理的流程事项进行多维度的数据分析，包括处理效率、类型分布等，输出详尽的总结报告，帮助你轻松向上汇报工作成果。

4）根据多个条件自由组合查询，比如输入发起人、部门、流程模板名称、发起或接收时间范围等，智能办公就能精准地帮您找到你要的待办或已办流程信息。

5）只需通过对话告诉智能办公你需要打开的菜单，即可快速查找到对应的菜单入口，你只需点击即可前往对应业务模块。还可通过姓名、联系方式快速帮您查询组织内在职人员。

#### 4.2.3.2使用配置

步骤1：进入【后台管理】选择【集团管理员】或者【单位管理员】可接入或维护大模型。

步骤2：进入【应用】找到【智能办公】智能体。

步骤3：点击进入【智能办公】。可对图标、名称、描述、Agent、开场白、开场白预置问题、问题建议、兜底方式、模型标识进行维护。智能办公由【文化建设查询】、【效能分析】、【协同处理】、【通讯录查询】、【流程发起】、【应用导航】、【会议查询】7个Agent组成。

步骤4：选择对应【Agent】，可查看Agent详情，设置Agent描述或删除Agent。点击【设置】，可设置Agent描述，准确描述Agent包含的内容范围，可改善Agent使用准确率。

步骤5：点击【详情】可查看、修改该Agent的角色设定、推理模式（ReAct模式、按顺序执行）、工具、向量库、对话轮数、模型标识、模型标识（随机性、单词回复随机性）。Agent定义完成之后，点击【确定】即可在右侧【预览&调试】中进行对话，实时检查效果是否符合业务预期。

步骤6：智能体配置完成后，进入【后台管理】选择【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.3.3操作流程

步骤1：进入协同办公首页，在【导航】中，光标移入【本门户空间】选择并点击进入【智能门户】（系统管理员可自定义名称）。也可在页面右侧点击章鱼悬浮图标进入【智能助手】。

步骤2：进入【智能门户】或【智能助手】默认选中【超级助理】，可直接在【超级助理】下发出指令，超级助理可自动根据用户语义直接调用智能办公智能体执行任务。

步骤3：【智能助手】可通过点击【放大】进入全屏模式，也可点击【收起】或【缩小】可回到侧边栏模式。

步骤4：在【智能门户】或【智能助手】可以通过@符号，选择并指定【智能办公】根据用户指令执行任务。

步骤5：在【智能门户】或【智能助手】可以通过直接选择【智能办公】进入智能办公智能体页面。也可点击进入【智能体广场】通过【搜索】或【翻页】查找到【智能问答】。

步骤6：在【智能办公】智能体页面，可通过点击【引导问题】快速发出指令，也可通过点击对话输入框中的【快捷指令】快速发出指令。

步骤7：在【智能办公】上传文件发起流程表单时，需先【提取关键信息】，然后明确指令智能办公发起流程的【模板名称】，如存在重复或类似的表单，需在通过发送对话中智能办公返回的【表单序号】或【模板名称】选择需要发起流程表单模板。确定并选择模板之后，智能办公会自动提取【表单字段】，根据提示确认执行填单，即可将文件中信息提取并回填至制定的【表单模板】，用户可点击快捷入口，前往表单页面完善字段信息，并发送即可。

### **4.2.**4 **辅助审批**

#### 4.2.4.1场景简介

用户处理待审批的流程表单时。辅助审批自动监测到打开的流程表单，并立即唤起了审批辅助工具。

根据当前流程处理人所属的业务领域以及其岗位职责，自动识别、提取并梳理出此次审批所需的关键要素，同时，辅助审批依据预先构建的向量库中的制度文档，对提交的流程表单进行自动合规检查，可以快速发现可能存在的风险点或不合规之处，如资金使用是否符合规定、项目实施计划是否合理等，确保所有审批事项都符合公司的政策和法律法规要求。

最后，基于前面两个步骤梳理出的审批关键要素和合规审查结果，审批建议功能为当前流程处理人提供综合的审批建议。

#### 4.2.4.2使用配置

步骤1：进入【后台管理】选择【集团管理员】或者【单位管理员】可接入或维护大模型。

步骤2：进入【应用】找到【辅助审批】智能体。

步骤3：点击进入【辅助审批】。可对图表、名称、描述、Agent、开场白、开场白预置问题、问题建议、兜底方式、模型标识进行维护。辅助审批由【辅助审批Agent】组成。

步骤4：选择【辅助审批Agent】，可查看Agent详情，设置Agent描述或删除Agent。点击【设置】，可设置Agent描述，准确描述Agent包含的内容范围，可改善Agent使用准确率。

步骤5：点击【详情】可查看、修改该Agent的角色设定、推理模式（ReAct模式、按顺序执行）、工具、向量库、对话轮数、模型标识、模型标识（随机性、单词回复随机性）。辅助审批需要依据预先构建的向量库中的制度文档，对提交的流程表单进行自动合规检查，因此需添加【辅助审批】所需制度文档构建的【向量库】。Agent定义完成之后，点击【确定】即可在右侧【预览&调试】中进行对话，实时检查效果是否符合业务预期。

步骤6：【辅助审批】依赖制度文档，在【辅助审批Agent】中，可查看向量库【内部管理制度】详情，设置向量库描述或删除向量库。点击【设置】，可设置向量库描述，准确描述向量库包含的内容范围，可改善模型使用向量库的准确率。

步骤7：点击【详情】进入【向量库】可维护向量库中知识文档，支持TXT、PDF、MARKDOWN、DOC、DOCX格式的本地文件，每个文件不超过50MB，最多可上传100个文件。点击【查看】进入对应文档可手动维护切片。需要注意的是添加制度文档时需检查向量切片词、句、段落的完整性，以保障合规审查结果的准确性。

步骤8：智能体配置完成后，进入【后台管理】选择【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.4.3操作流程

步骤1：进入【智能门户】或协同办公【首页】点击需要处理的待办，跳转至流程详情同时会自动唤起【辅助审批】。

步骤2：【辅助审批】会自动根据所属业务及当前处理人角色提取和梳理【审批关键要素】，并根据关联的向量库制度文档进行【合规审查】，结合梳理的审批关键要素、合规审查结果综合给出【审批建议】。

步骤3：【辅助审批】会根据关联的向量库制度文档进行【合规审查】，审查完成会列举【参考知识源】可点击展开查看详细的知识源文件。点击参考知识源文件名称，可将知识源下载至本地。

步骤4：【辅助审批】可在对话中设置是否弹出，在打开流程详情自动进行辅助审批的对话页面，可点击【不再自动弹出】关闭自动进行辅助审批，页面出现【操作成功】即设置成功。需要注意的是，暂时无配置页面、也不支持对话进行配置，操作【不再自动弹出】之后，系统会将该操作记录存在本地，清空浏览器缓存后【辅助审批】依然可自动弹出。

### **4.2.5 总结阅读**

#### 4.2.5.1场景简介

上传文档进行解析，快速扫描并理解文档内容，自动精确提取摘要。

•**文件上传：**支持txt、pdf、docx、markdown等文件类型的上传识别；

•**文档摘要生成：**利用自然语言处理技术，自动生成输入文档的简洁摘要；

#### 4.2.5.2使用配置

步骤1：以集团管理员或单位管理员身份进入智能化办公平台 Builder后台，切换至应用菜单，通过搜索总结阅读，找到对应应用。

步骤2：进入总结阅读应用，可以修改描述、开场白、问题建议、兜底方式以及切换选择模型标识。

步骤3：配置完成后，进入【后台管理】切换【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.5.3操作流程

步骤1：进入智能门户或智能助手后，可通过常用菜单区找到总结阅读。

步骤2：接下来你可以上传文件，提出你的问题和要求进行分析了。

**•注意1：仅支持上传一个文件，且文件大小限制在10M以内；**

**•注意2：仅支持txt、pdf、docx、markdown类型的文件；**

### **4.2.**6 **智能创作**

#### 4.2.6.1场景简介

预置19个智能创作应用，围绕办公工具、商业营销、行政人事、产品研发、国际化5个分类展开，辅助企业内各角色人员进行日常工作。

#### 4.2.6.2使用配置

步骤1：以集团管理员或单位管理员身份进入智能化办公平台 Builder后台，切换至应用菜单，智能创作标签下可查找所有创作类智能体应用。

步骤2：进入智能创作-文案策划应用，可以修改描述、开场白、问题建议、兜底方式以及切换选择模型标识。

步骤3：文案策划应用引用办公创作agent，可进入办公创作agent配置页。

步骤4：办公创作agent默认为正式状态，可查看办公创作agent相关配置。

步骤5：注意，办公创作agent处于“正式”且“已发布”状态时，是不可编辑的。首先需要进入服务管理-Agent页签-找到办公创作agent进行取消发布操作，再到Agent管理页面找到办公创作agent进行停用，此时办公创作agent处于“测试”状态，可进行编辑。

步骤6：配置完成后，进入【后台管理】切换【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.6.3操作流程

步骤1：进入智能门户或智能助手后，可通过智能体广场进入智能创作标签

步骤2：接下来你可以提出要求进行智能创作。

### **4.2.7 模型对话**

#### 4.2.7.1场景简介

模型对话智能体是企业数智化转型中的敏捷型AI中枢，专为已部署自研大模型（公有云/私有化）的客户设计，致力于降低大模型规模化应用门槛。针对企业存在的大模型能力调用复杂、多模型协同落地难、AI服务与办公场景割裂等挑战，该智能体打造了"开箱即用式"接入方案——通过可视化界面快速对接企业现有大模型（支持同时接入多个引擎），无需重建底层架构即可将智能问答能力嵌入OA、IM等协同系统，实现全员无感知的AI服务触达。员工在日常办公中可切换不同厂商或自研的大模型进行提问。管理者通过统一配置中心完成模型策略调整、权限管理及服务发布，保障企业既充分释放多模型技术红利，又实现知识资产与交互体验的集中治理，让大模型真正成为渗透于每项业务流程的智能生产力。

#### 4.2.7.2使用配置

步骤1：进入智能化办公平台 Builder后台，切换至应用菜单，通过搜索模型对话，找到模型对话应用。

步骤2：进入模型对话应用，可以看到模型对话应用通过引用Agent模型对话实现。

步骤3：进入模型对话Agent。

步骤4：找到模型对话Agent模型标识，切换为希望对话的大模型后保存即可。

步骤5：注意，当模型对话Agent处于“正式”运行状态时，是不可编辑的。需要通过Agent菜单找到模型对话Agent，点击更多操作找到“停用”按钮，停用后才可编辑修改模型标识。

步骤6：还有一种取巧的配置办法，在模型对话应用中删除模型对话Agent，直接通过模型对话的大模型兜底回复设置希望对话的大模型，也能实现模型对话的效果。

步骤7：智能体配置完成后，进入【后台管理】选择【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.7.3操作流程

步骤1：进入智能门户或智能助手后，可通过常用菜单区找到模型对话

步骤2：接下来你可以向模型对话进行任意提问了。

### **4.2.8 安全助理**

#### 4.2.8.1场景简介

安全助理是为企业安全管理人员打造的智能化安全护航平台，深度聚焦日常安全管理中的高频痛点场景，提供全流程解决方案。当企业面临外部威胁情报滞后、漏洞修复响应迟滞、防护日志分散难溯源、安全报告依赖人工耗时低效等问题时，安全助理通过七大核心能力重构管理流程：它通过自动化爬取全球热门威胁情报并匹配企业资产关联性，实现风险精准感知；实时推送漏洞补丁提醒并支持一键修复，规避遗漏风险；集中聚合多源防护日志的拦截攻击数据，提供多维度可视化分析与上下文穿透式追溯能力；更依托AI自动生成动态安全态势分析报告，7×24小时呈现防护效果与风险趋势，大幅降低人效成本。通过"感知-分析-处置-验证"的闭环赋能，帮助安全团队实时掌控全局安全水位，将被动响应转化为主动防御，显著提升安全管理质效。

注意：安全助理会定期采集外部热门威胁情报，对应安全助理的新增供应链预警和安全态势报告中的部分内容会受到影响，如果遇到请排查该问题，确保不会被认为是bug；当系统处于内网环境时，可通过配置白名单解决该问题。

#### 4.2.8.2使用配置

注意：

1. 安全助理是开箱即用的智能体应用，仅需进行应用授权即可受用。
2. 安全助理内置多个复杂的安全Agent，非必要不建议修改调整，随意修改调整后或产生报错等异常情况。
3. 部分数据需要安装主动防御产品，详见《[智能化办公平台 v1.0安装部署手册主动防御安装部署手册--智能安全助理插件版](https://docs.qq.com/doc/DQUNiV2hPcG1NZ0Ny)》手册地址：<https://docs.qq.com/doc/DQUNiV2hPcG1NZ0Ny>
4. 需要添加网络白名单的地址：（不配置会导致供应链预警、安全态势报告的部分内容无法完整输出）
	1. 致远官方漏洞库查询接口：https://service.seeyon.com
	2. 国际漏洞库CVE查询工具 ：https://www.cve.org；https://cveawg.mitre.org

应用授权：安全助理通过智能化办公平台应用授权即可使用，进入【后台管理】选择【集团管理员】或【单位管理员】，点击【智能应用设置】选择【智能化办公平台应用授权】通过【操作】点击并选择【授权用户】可完成该智能体的授权配置，未授权用户无法使用该智能体。同时，授权用户数超出注册用户数，将无法授权成功，需联系管理员购买注册用户数。

#### 4.2.8.3操作流程

步骤1：进入智能门户或智能助手后，可通过常用菜单区找到安全助理

步骤2：查询新增产品最新漏洞预警，通过快捷指令按钮唤起，在指令中选择“新增产品漏洞预警”，安全助理根据客户购买产品情况回答最新相关漏洞情况并提供补丁下载地址。点击下载地址，浏览器自动下载补丁包。

步骤3：查询最新增供应链风险预警，通过快捷指令按钮唤起，在指令中选择“新增供应链风险预警”

步骤4：安全助理抓取外部热门威胁情报，并结合自身产品涉及到的组件等供应链内容，进行相关性分析并提供处置建议

步骤5：查询系统监控日志分析，通过快捷指令按钮唤起，在指令中选择“系统监控日志分析”

步骤6：：安全助理统计三类安全防护日志进行整理归类，针对系统账号攻击情况、历史漏洞攻击数据、未知漏洞攻击情况进行展示。

步骤7：安全助理可对系统监控日志分析情况进行进一步的穿透分析，例如查询系统账号攻击分析，安全助理会根据日志底表，穿透分析系统账号攻击明细情况，并提供分析建议。

步骤8：安全助理定期生成多维度、全方面的深度安全报告，通过快捷指令“安全态势报告”发送指令。

### **4.2.**9 **超级助理**

#### 4.2.9.1场景简介

•**ALL in One人机协同新范式：**智能化办公平台超级助理可通过配置具备大多数智能体的能力，能完成绝大多数高频协同场景的任务；

•**智能体调度：**智能化办公平台超级助理具备多智能体调度的能力，基于用户意图的理解，自动分配对应的智能体执行任务；

•**“@”智能体应用：**智能化办公平台超级助理支持@功能， 可以通过输入“@”选择想要对话的智能体，实现快捷切换。

#### 4.2.9.2使用配置

步骤1：以集团管理员或单位管理员身份进入智能化办公平台 Builder后台，切换至应用菜单，通过搜索智能化办公平台，找到对应应用，智能化办公平台为系统预置的超级助理。

步骤2：进入智能化办公平台应用，可以修改描述、开场白、问题建议、兜底方式以及切换选择模型标识。

可以修改智能化办公平台超级助理引用的Agent配置，根据需要添加或者删除Agent。

步骤3：为了达到更优的智能体调度效果，可以通过优化引用Agent的描述进行。

**•注意1：智能化办公平台超级助理的调度能力是通过对用户的意图识别，当智能化办公平台添加了名字能力相似的agents时，容易产生幻觉出现调度错误的智能体执行任务的情况；因此不建议添加过多或相似的agent能力。**

**•注意2：智能化办公平台超级助理无需进行应用授权；**

#### 4.2.9.3操作流程

步骤1：进入智能门户或智能助手后，默认定位到超级助理。

## 4.3 智能化办公平台运行引擎

### **4.3.1大模型管理**

#### 4.3.1.1场景简介

本模块负责模型接入与管理，支持LLM和Embedding类型模型，已接入并适配DeepSeek、GPT、通义千问等多种大模型。

模型类型：LLM模型、Embedding模型；

LLM模型：规模庞大的机器学习模型，它们通常拥有数亿甚至数千亿个参数，能够处理海量的数据，从而在各种任务中表现出惊人的能力。LLM模型用于提示词、Agent、应用进行保存和调试时必须选择。

Embedding模型：一种将离散的符号数据（如单词、句子、图像等）映射到连续的向量空间中的技术。这种映射能够捕捉数据之间的语义、结构等关系，使得原本难以直接处理的符号数据转换为计算机更容易理解和操作的数值向量形式‌。Embedding模型用于向量库保存时必须选择。

接入模型维护：对接模型厂商和不同厂商对应的模型；

模型管理：配置企业购买的公有模型或私有化部署的模型；

模型状态：完成模型配置并启用后，所有提示词模板、Agent、应用等均可调用该模型。

#### 4.3.1.2使用配置

步骤1：在菜单中点击【模型】菜单，即可进入模型列表页面，查看系统中维护的所有模型标识。

**注： 至少配置1个LLM类型的模型、1个Embedding类型的模型，且状态为启用，连接状态为通过。**

#### 4.3.1.3操作流程

步骤1：点击【接入模型维护】按钮，即可进入[接入模型维护]页面，在此页面中可查看并维护模型编码以及分类相关信息。

步骤2：页面左侧分类筛选模块，可显示分类列表，同时支持添加、编辑、删除分类。

步骤3：右侧模型编码列表支持查看所有模型编码列表，并支持对模型编码进行新增、编辑、删除操作；点击【新增】按钮即可打开“新增模型”弹框，在弹框中输入或选择模型名称、模型类型、模型分类信息后即可新建模型；点击列表中的【编辑】按钮即可在弹框中编辑模型信息，点击列表中的【删除】按钮可在二次确认后删除对应的模型编码。

步骤4：维护好模型编码后，即可返回模型标识页面在模型编码中添加模型标识，模型标识即可在提示词、Agent、向量库、应用中调用，在模型标识列表页面中，可以进行新增、修改、测试、启用/停用、删除相关操作。

### **4.3.2提示词管理**

#### 4.3.2.1场景简介

提示词模板维护，可修改提示词变量和内容，配置模型，对提示词进行预览调试。已预置20+智能创作类提示词模板。

提示词维护：提供提示词模板维护以及预览调试，支持新增/编辑含动态变量的模板内容，可调用指定AI模型并实时预览调试，确保提示词在不同模型场景下的精准性和有效性；

提示词预置数据：系统预置20+创作类提示词，包括新闻稿生成、文本内容扩写、文案润色等，可对此进行提示词维护、调试等；

效果评价：针对提示词模板的效果进行评价，可依据评价记录帮助用户快速定位最优版本并可应用此版本为最新版本；

提示词发布：支持将验证通过的提示词模板一键发布为标准化 API 服务，可供内部Agent作为工具引用。

#### 4.3.2.2使用配置

步骤1：在菜单中点击【提示词】菜单，即可进入提示词列表页面，查看系统中维护的所有提示词。

#### 4.3.2.3操作流程

步骤1：点击右上角【新增】按钮即可打开[新增提示词]页面，在新增提示词页面需要输入模版编码、模版名称、说明并选择添加好的模型标识；随后用户需要在下方填写提示词，并可以根据需要为提示词添加变量，变量需要输入变量key、变量名称、数据类型、是否必填属性，需要注意添加的变量可在提示词中通过输入“{”来选择引用；最后用户可对大模型的随机性（从0-1）、单次回复限制及返回格式等参数进行配置；最后通过【确认】和【取消】按钮来保存或放弃本次修改；

配置完成后用户即可在右侧的调试&预览区域输入配置好的变量以及用户问题对本提示进行预览及调试，支持对回答的结果评分。

步骤2：提示词支持多版本管理，用户完成提示词的新增后，可在列表中点击【运行记录】进入提示词版本管理页面，在此页面可查看提示词历史版本的名称、说明、效果等信息，支持分版本查看运行记录，并切换使用的提示词版本。

步骤3：完成提示词添加后，即可在提示词列表中对提示词进行管理，支持提示词的编辑、复制、启用/停用、删除、导出等功能；需要注意启用状态的提示词可以发布，但无法进行编辑等操作，测试状态的提示词允许编辑、删除等操作，但不允许发布。

步骤4：如需要在不同环境之间迁移提示词，可通过提示词的导入、导出功能实现，如需导出单个提示词，可点击列表操作中的【导出】按钮，如需批量导出提示词，可通过列表左侧的复选框选中多个提示词，然后点击页面右上角的【导出】按钮进行批量导出，导出的工具为JSON格式文件；导出后可通过页面右上角的【导入】按钮，上传JSON格式文件后即可导入提示词。

### **4.3.**3智能体**工具管理**

#### 4.3.3.1场景简介

区分预置工具和自定义工具,支持自定义工具维护和工具内接口的维护，接口支持http、openapi Schema两种。

工具维护：提供自定义工具维护，支持通过可视化界面新增/编辑 / 删除工具；

工具状态：通过启用/停用操作更新工具状态，启用状态的工具不可修改工具基本信息，内部Agent可引用启用状态工具内的接口

接口维护：提供灵活接口配置方案，可视化界面新增/编辑/删除接口；

接口调试：提供接口全链路调试能力，对接口进行调试，更新接口测试状态，测试通过的接口可供内部Agent引用。

#### 4.3.3.2使用配置

步骤1：在菜单中点击【工具】菜单，即可进入工具列表页面，查看系统中存在的所有工具；系统中的工具存在预制工具和自定义工具两大类，其中预制工具是系统出厂自带工具，用户简单配置后可直接使用，自定义工具为用户自己开发的工具；两种工具可通过左上角页签进行切换。

#### 4.3.3.3操作流程

步骤1：点击右上角【创建工具】按钮即可打开创建工具弹框，填写名称、编码、描述必填信息后即可创建自定义工具。

步骤2：点击一个已创建的工具，即可进入工具编辑页面，在工具编辑页面中可以进行工具信息修改、添加工具接口、修改工具接口、编辑请求参数&返回参数、删除接口、复制接口、导出接口等；添加工具接口支持“新增Http接口”、“导入OpenAPI”、“导入”三种方式，使用Http接口导入需要用户编辑完善请求参数及返回参数，使用OpenAPI导入和文件导入都可以自动填充相关结构，无需用户手动输入，但需要注意导入的文件必须是智能化办公平台中导出的接口文件；参数中请求参数分为Body、Header、Query支持分别填写，所有参数结构需要为标准的JSON Schema结构，允许配置是否必填及默认参数值。

步骤3：编辑完成接口信息后，即可点击调试按钮对接口进行调试，点击后系统会根据请求参数自动生成请求JSON结构，用户补充请求体后即可点击执行以运行接口，执行后即可查看运行结果以及完整的输出JSON结构。

步骤4：工具配置完成后可在工具列表页面对工具进行管理，可进行添加标签、编辑工具信息、删除工具、复制工具、启用/停用工具等操作。

步骤5：如需要在不同环境之间迁移工具，可通过工具的导入、导出功能实现，如需导出单个工具，可点击卡片选项中的【导出】按钮，如需批量导出工具，可通过卡片右上角的复选框选中多个工具，然后点击页面右上角的【导出】按钮进行批量导出，导出的工具为JSON格式文件；导出后可通过页面右上角的【导入】按钮，上传JSON格式文件后即可导入工具。

### **4.3.**4向量库

#### 4.3.4.1场景简介

支持上传本地文档，存储企业私域向量化数据。Agent可引用向量库，通过知识库检索匹配相关的知识，一般用来支持问答场景。

向量库维护：支持创建 / 修改 / 删除向量库,操作时必须绑定指定 Embedding 模型以确保向量生成一致性；

文件管理：支持多种文件类型（PDF/Word/MARKDOWN/TXT ）上传，提供智能文本分段引擎;

分段维护：提供分段切片可视化交互管理，支持手动修改 / 新增 / 删除切片，实时切片效果预览。

#### 4.3.4.2使用配置

步骤1：在菜单中点击【向量库】菜单，即可进入向量库列表页面，查看系统中存在的所有向量库。

#### 4.3.4.3操作流程

步骤1：点击右上角【新增】按钮即可打开“新增向量库”弹框，填写名称、说明、模型标识等必填信息后即可新建向量库。

步骤2：新建向量库后，即可点击【查看】进入向量库管理页面，在向量库管理页面中可以通过点击【上传文件】打开文件上传页面，点击【测试】按钮即可打开向量库测试页面，点击【导出】即可将当前向量库以JSON格式文件导出，点击【导出记录】即可查看该向量库的导出记录，点击列表中的【查看】即可进入文件查看页面，点击列表中的【设置】即可重新配置该文件的分段设置，点击【删除】即可删除对应文件。

步骤3：点击【上传文件】即可在新页面中上传文件，文件选择完成后，点击下一步对文件分段进行设置，可选择“自动分段”及“自定义分段”两种分段方式，选择自动分段后无需配置，系统会自动计算分段，选择自定义分段后需配置分段标识符、分段最大长度、分段重叠比例及文本预处理规则；配置完成后点击保存并处理系统即开始对文件进行分段处理，处理好的文件会在文件列表中展示出来。

步骤4：在文件列表点击【测试】按钮即可进入命中测试页面，用户可在此处输入测试问题并点击测试按钮进行命中测试，下方TOP代表命中的切片数量。

步骤5：点击向量库列表页面右上角的【导入】按钮，即可将此前导出的向量库直接导入，点击按钮后可在弹框中选择文件、模型标识以及重复数据导入处理方式。

### **4.3.5Agent搭建器**

#### 4.3.5.1场景简介

中文常译为“智能体”，是指在特定环境中能够自主行动、感知和决策的实体。它可以是一个软件程序，也可以是一个机器人。Agent的核心能力在于能够根据环境变化做出适应性反应。简单来说，Agent 就是一个能自己“动脑子”干活的智能帮手。

Agent核心公式：Agent（智能体）=LLM（大模型）+ Planning（规划）+Memory（记忆）+ 检索 + Tools（工具）。

Agent的作用：通过角色设定（希望agent完成的任务、具备的能力、输入及输出的要求等）、推理模式（ReAct模式、按顺序执行）、模型标识设置，引用提示词、工具和向量库，完成Agent的理解与推理、任务规划与执行，同时根据执行结果进行调整优化；

Agent维护： Agent的增删改查，设置Agent角色设定、推理模式、模型标识，引用工具和向量库;

Agent调试：针对Agent进行预览调试，可查看Agent历史会话记录，Agent执行的日志详情查看;

Agent发布：提供标准化 API 发布流程，可在服务管理中查看以及取消发布。

#### 4.3.5.2使用配置

步骤1：在菜单中点击【Agent】菜单，即可进入Agent列表页面，查看系统中存在的所有Agent。

#### 4.3.5.3操作流程

步骤1：点击右上角【创建Agent】按钮即可打开“创建Agent”弹框，填写名称、编码、描述等必填信息后即可新建Agent。

步骤2：在创建Agent弹框中填写完成相关信息并点击保存后，即可打开[Agent编辑]页面，在Agent编辑页面首先需要填写角色设定，并可以根据需要选择推理模式，推理模型可选择“ReAct模式”和“按顺序执行”两种模式，其中ReAct模式由大模型自主选择调用哪些工具及向量库，按顺序执行则默认按照从上到下的顺序执行所有工具和向量库；

随后可在工具模块点击【添加】按钮，即可在弹框中选择需要的工具添加至Agent中，添加后可在Agent中查看工具的输入JSON结构、配置输入默认值、进行删除等操作；

添加完成工具后可继续添加向量库，可在向量库模块点击【添加】按钮，即可在弹框中选择需要的向量库添加至Agent中，添加后可在Agent中跳转查看向量库详情、设置向量库描述以及删除已添加的向量库，需注意此处修改的向量库描述作用范围仅为本Agent内，修改的描述不会影响被其他Agent调用的向量库；

完成向量库配置后可继续配置Agent的对话轮数以及模型标识；

最后用户可对大模型的随机性（从0-1）、单次回复限制及返回格式等参数进行配置；最后通过【确认】和【取消】按钮来保存或放弃本次修改；

配置完成后用户即可在右侧的调试&预览区域输入配置好的变量以及用户问题对本提示进行预览及调试，支持查看大模型回复的日志记录。

步骤3：完成Agent配置后即可在Agent卡片列表页面对Agent进行管理，提供搜索、标签分类、基本信息编辑、删除、复制、启用/停用等操作，需注意仅用已启用（正式状态）的Agent才允许调用时被查看及发布，停用（测试状态）的Agent无法在引用时被搜索到或发布。

步骤4：如需要在不同环境之间迁移Agent，可通过Agent的导入、导出功能实现，如需导出Agent，可点击卡片操作中的【导出】按钮，在弹框中配置导出范围后，即可成功导出Agent文件，导出的Agent为JSON格式文件；导出后可通过页面右上角的【导入】按钮，上传JSON格式文件并配置模型标识、重复数据处理方式、导入范围等基本信息后，即可完成Agent的导入操作。

步骤5：已完成导入/导出后，可点击右上角【导入导出记录】按钮进入Agent导入导出记录页面，该页面可通过点击左上角“导入记录/导出记录”切换页签查看对应记录列表，列表中可显示文件相关信息、任务状态、创建时间、创建人等信息，并可重新下载导出文件、查看失败日志及删除相关记录。

### **4.3.**6会话应用管理

#### 4.3.6.1场景简介

一个完整智能场景的闭环，可承载多个Agent，通过会话与用户直接产生交互，通过意图识别和多个Agent的编排完成智能场景实现。例如智能办公应用，包含多个办公智能体，可以发起流程、查询待办事项、打开协同协同菜单等。

应用维护：应用的增删改查，可引用单个/多个Agent，设置开场白、问题建议和兜底方式;

应用调试：针对应用进行预览调试，可查看应用历史会话记录，应用执行的运行过程查看；

应用标签管理：对应用进行标签设置，按标签进行应用的搜索;在智能化办公平台入口-侧边栏广场中按标签展现。

#### 4.3.6.2使用配置

步骤1：在菜单中点击【应用】菜单，即可进入应用列表页面，查看系统中存在的所有应用。

#### 4.3.6.3操作流程

步骤1：点击右上角【创建应用】按钮即可打开[应用定义]页面，在应用定义页面需要上传图标，输入名称、描述等必填信息；

随后用户可以在下方Agent模块点击【添加】按钮，即可在弹框中选择需要的Agent添加至应用中，添加后可在应用中跳转查看Agent的详情、配置Agent描述、进行删除等操作，需注意此处修改的Agent描述作用范围仅为本应用内，修改的描述不会影响被其他应用调用的Agent；

添加完成Agent后，用户可在下方设置应用的开场白、开场白预制问题（做多可设置10个）、问题建议以及应用兜底方式，需注意选择大模型兜底是需要选择模型标识；

最后通过【确认】和【取消】按钮来保存或放弃本次修改；

配置完成后用户即可在右侧的调试&预览区域输入配置好的变量以及用户问题对本提示进行预览及调试。

步骤2：完成应用配置后即可在应用卡片列表页面对应用进行管理，提供搜索、标签分类、删除、复制、设置通用应用等操作。

### **4.3.**7安全管理

#### 4.3.7.1场景简介

1. 敏感词管理：提供敏感词设置、敏感词检测和敏感词日志查看。设置的敏感词为全局敏感词，面向智能化办公平台 Builder中预览调试和智能化办公平台的入口全部生效。
2. 日志管理：记录用户在系统中操作的历史记录，便于进行系统追溯、安全审计。

#### 4.3.7.2使用配置

1. 进入安全-敏感词，提供敏感词管理页面；
2. 进入安全-日志，提供操作日志的查看和查询页面；

#### 4.3.7.3操作流程

1、敏感词管理

步骤1：敏感词设置

新建分类：可设置分类名称、处理方式；

新建敏感词：可选择左侧分类后在分类下新建敏感词，默认携带所属分类和分类的处理方式。可维护敏感词、所属分类、处理方式；

步骤2：敏感词检测

启用用户输入敏感词检测：默认不勾选，勾选后点击确认保存；

步骤3：敏感词检测执行效果

检测执行作用范围：提示词预览&调试、Agent预览&调试、应用预览&调试； 智能化办公平台超级入口对话用户录入；

1. 敏感词处理方式=阻断，记录敏感词检测日志，检测到信息包含敏感词，直接按系统提供固定的话术回复输出；

b、敏感词处理方式=不处理，记录敏感词检测日志，检测到信息包含敏感词，可包含敏感词正常回复输出；

步骤4：敏感词日志

•可查看敏感词检测日志，包括操作时间、操作人、业务来源、消息内容等；

2、日志管理

步骤1：日志查看-提供智能化办公平台操作日志的查看，包括操作时间、操作人员、访问地址、访问方式、操作模块、操作类型、业务名称、业务编码信息；

步骤2：日志查询-支持按访问方式、操作模块、操作人员、操作时间进行过滤查询；

步骤3：日志导出-操作导出，直接将日志结果导出为excel格式文件下载到本地；

### **4.3.**8系统管理

#### 4.3.8.1场景简介

数据初始化：对于初始安装智能化办公平台的企业，需要对预置的应用进行初始化操作，设置企业已配置的模型和协同系统地址，以达到开箱即用的目的。

#### 4.3.8.2使用配置

#### 4.3.8.3操作流程

步骤1：首次进入数据初始化页面，所有应用的初始化状态=未进行；

步骤2：进行初始化数据配置：

 模型标识：选择模型管理中状态=启用，模型类型=LLM模型；

 协同baseurl：输入协同系统地址；

 向量模型标识：选择模型管理中状态=启用，模型类型=embedding模型；

步骤3：选择需要初始化的应用，点击确认进行数据初始化；

**注：已完成初始化的应用不支持重新初始化；**

**当所有应用的初始化状态=已完成，确认按钮置灰不可点击；**

### **4.3.**9**权限**管理

#### 4.3.9.1场景简介

1. 用于控制协同系统的不同角色用户进入智能化办公平台 Builder能够操作的功能和数据范围；
2. 智能化办公平台 Builder中搭建的应用，在协同系统中授权用户，用于控制哪些用户能够在智能化办公平台入口中可以使用哪些应用；

#### 4.3.9.2使用配置

智能化办公平台应用授权： A8\A6-后台管理-智能应用设置-智能化办公平台应用授权

**注：授权用户操作保存时，进行智能化办公平台注册用户判断及控制，如果授权用户数大于智能化办公平台注册用户数，则无法保存。**

#### 4.3.9.3操作流程

1. 智能化办公平台 Builder功能权限控制规则：针对A82\A81\A6产品系列，提供固定的菜单资源映射进行控制。

|  |  |  |
| --- | --- | --- |
| 协同系统产品序列 | 固定角色 | 智能化办公平台 Builder可见菜单 |
| A82 | 系统管理员 | 模型、工具、向量库、服务、安全、系统管理 |
| 集团管理员 | 模型、提示词、工具、向量库、Agent、服务、应用 |
| 单位管理员 | 模型、提示词、工具、向量库、Agent、服务、应用 |
| A81 | 系统管理员 | 模型、工具、向量库、服务、安全、系统管理 |
| 单位管理员 | 模型、提示词、工具、向量库、Agent、服务、应用 |
| A6 | 单位管理员 | 模型、提示词、工具、向量库、Agent、服务、应用、安全、系统管理 |

**注：不支持使用三员分离模式下应用智能化办公平台；**

1. 智能化办公平台应用授权规则：

2.1集团管理员可授权智能化办公平台应用范围：系统预制的应用+集团管理员角色创建的应用；

 授权单位：

a、应用授权给多个/单个单位，单位管理员进入应用授权，可以对该应用在单位内用户授权；

b、逆向取消单位授权，会将原有的授权单位记录、单位授权用户记录清除；

 授权用户：

a、集团管理员可直接将应用授权给多个单位的用户；

b、逆向取消授权，会将已授权的用户记录清除；

c、用户选择页签：单位、部门、组、岗位、职务级别；

2.2单位管理员可授权智能化办公平台应用范围：系统预制授权给单位+集团创建授权给单位+本单位创建的应用；

授权用户：

a、单位管理员可以将应用给单位内用户授权，不支持跨单位授权；

b、逆向取消授权，会将已授权的用户记录清除；

c、用户选择页签：部门、组、岗位、职务级别；