数字员工平台

产品说明书

V2.26

2026 年 11 月

目录

产品说明书.....11
日常工作.....11
员工与配置.....11
权限与治理.....12
连接与扩展.....12
使用边界.....13
术语表.....14
核心术语.....14
其他术语.....14
界面名称.....14
权限规则.....15
状态说明.....15
常见现象.....16
相关章节.....16
对话.....17
数字员工选择.....17
输入内容.....17
话题与历史.....18
执行反馈.....19
页面限制.....19
资料.....20
文件来源.....20
编辑器类型.....21
文件版本.....22
权限与限制.....23
定时任务.....24
任务看板.....24

定时任务.....26
运行状态与调度状态.....27
知识任务.....28
权限与异常.....28
知识中心.....29
产品边界.....29
页面组成.....29
知识库内容层级.....30
知识库范围与状态.....31
文档处理链路.....32
文件规格.....33
文档处理能力.....33
知识模型.....33
检索模式.....33
检索参数.....34
检索结果结构.....34
知识访问权限.....35
文档详情.....36
分段管理.....37
任务状态.....37
外部客户端接入.....37
使用情况与审计.....37
与数字员工的关系.....38
限制与异常状态.....39
界面与端差异.....40
主要区域.....40
平台差异.....41
状态提示.....41
品牌与命名.....42

项目协作.....43
内容与上下文.....43
对话与文件的可见范围.....43
工作台与项目事项.....44
进展跟踪.....44
自定义首页.....45
初始文件结构.....46
项目角色.....46
受保护内容.....47
版本与活动.....48
定稿与导出.....48
恢复与撤销.....49
会议与语音.....51
能力与配置范围.....51
会议字段.....52
状态与材料.....53
依赖与权限.....54
办公编辑.....55
格式与端能力.....55
会话与文件状态.....55
协作与冲突.....56
权限.....56
招募.....57
数字员工模板详情结构.....57
发布与发现.....58
创建与已有数字员工.....58
权限与依赖.....59
技能.....60
选用与安装.....60

技能内容与字段.....60
创建与发布校验.....60
安装状态.....62
MCP 服务.....63
插件与使用限制.....63
员工.....64
页面组成.....64
创建来源.....65
生命周期.....65
运行模式与容量.....65
权限边界.....65
依赖关系.....66
员工控制台.....67
概览指标.....67
当前菜单.....68
节点与执行审批.....68
Agent 与工作区.....69
快捷输入与梦境.....69
安全护栏.....70
通道与 IM 机器人.....70
任务与心跳.....70
运行实例与命令终端.....70
配置保存与同步.....71
模型与知识库.....71
MCP 服务.....71
知识库.....72
会议识别.....73
调试、日志与状态.....74
状态关系.....74

高风险能力.....75
管理后台.....76
后台分组.....76
大屏口径.....77
数字员工运行管理.....77
副本伸缩配置.....78
副本状态.....78
权限与部署差异.....79
异常状态.....79
模型与模板.....80
创建时的默认配置.....80
主动切换配置模板.....80
模型提供商与路由.....80
数字员工模板工作台.....81
MCP 与插件.....82
生效边界.....83
品牌与发布.....84
品牌字段.....84
外部语音.....85
客户端发布信息.....86
安全边界.....87
Agent 与工作区.....88
职责与调用.....88
常用文件.....88
配置与运行.....89
手动应用数字员工模板更新.....90
权限.....90
配置项.....91
配置位置与生效.....91

字段检查方法……92
典型数值参数……92
保存、应用与恢复……93
员工参数……94
参数分组……94
共享与独享……95
伸缩与回收……95
迁移与生效……96
运行实例……97
运行阶段……97
数据与实例……98
配置传播……98
维护动作……98
故障定位……98
业务插件……99
插件组成……99
对话选择与插件安装……99
安装范围……99
权限模型……100
版本与发布……100
配置与安全……101
知识服务……102
配置层次……102
模型引用……102
文档处理选项……104
检索设置……105
索引状态……105
权限与治理……105
诊断信息……106

登录.....107
页面区域.....107
身份状态.....108
登录态与退出.....108
认证方式与密码.....108
异常边界.....108
个人设置.....109
账号菜单.....109
个人资料字段.....109
偏好与语言.....109
环境变量.....110
应用更新与下载.....110
安全限制.....111
发布审核.....112
审核中心结构.....112
审核范围与状态.....113
审核规则.....113
安全审计.....113
权限与完整性.....114
组织与权限.....115
用户账号.....115
组织与团队.....115
角色与菜单权限.....116
资源授权.....117
LDAP.....117
API Token.....117
权限判定边界.....118
消息通道与集成.....119
通道配置字段.....119

通道实例、保存与测试.....119
私聊与群聊策略.....120
微信通道.....120
钉钉通道.....121
飞书通道.....122
企业微信通道.....123
QQ 通道.....124
身份与资源.....125
对外发送.....125
集成治理.....125
字段与状态.....126
数字员工与运行.....126
任务与日程.....127
知识处理.....128
审核与发布.....128
通用字段.....129
安全与审计.....130
资源授权.....130
高影响操作.....130
数据范围.....131
凭据.....131
审计与职责.....132
结论边界.....132
浏览器扩展.....133
连接链路.....133
标签页与网站权限.....134
扩展版本与分发.....134
执行边界.....134
个人连接.....135

令牌字段……135
权限……136
个人连接与变量……137
状态影响……137
消息与用量……138
通知状态……138
使用量口径……139
部署与权限……139
审计中心……140
角色与能力……140
页面与记录……140
任务与过程……142
状态与风险……143
记录范围与正文……144
完整性与留存……144
外部交付与密钥……145
技能治理……146
组织策略……146
提案与审核……147
范围与安装……147
统计解释……148
版本与历史……148

产品说明书

术语表：数字员工模板、数字员工、Agent、技能与工作区等概念。

完整步骤见操作手册。

日常工作

- 对话
- 资料
- 定时任务
- 知识中心
- 界面与端差异
- 项目协作
- 会议与语音
- 办公编辑

员工与配置

- 招募
- 技能
- 员工
- 员工控制台
- 管理后台
- 模型与模板
- 品牌与发布
- Agent 与工作区

- 配置项
- 员工参数
- 运行实例
- 知识服务

权限与治理

- 登录
- 个人设置
- 发布审核
- 组织与权限
- 字段与状态
- 安全与审计
- 消息与用量
- 审计中心
- 技能治理

连接与扩展

- 消息通道与集成
- 个人连接
- 浏览器扩展
- 业务插件

使用边界

状态	含义
只读	当前内容不允许修改。
暂不可用	状态未知或尚未获取。
未配置	依赖尚未建立。

各功能的权限与客户端限制见对应章节。

术语表

核心术语

术语	定义
数字员工模板	用于复用、分发的静态预制方案资产，不是运行中的数字员工。
数字员工	由数字员工模板招募创建、独立运行的 Agent 业务实例。
Agent	数字员工的内核智能执行主体，不等于数字员工模板或数字员工。
技能	可供 Agent 调用的最小能力单元，可以包含方法、指令、脚本和资源。
工作区	数字员工的隔离运行环境，保存文件、配置和会话上下文，不包含全部本机文件。

其他术语

术语	定义
用户	发起请求的登录身份。
运行实例	承接数字员工任务的执行单元，在线状态与数字员工记录分别维护。
话题	保存连续工作中的消息和处理过程。
资料	文件及其版本的使用入口。
项目	由目标、共享材料、成员、活动和对话组成的协作范围。
知识	经过解析、分段及索引后，可以按权限检索的原文内容。
MCP	连接客户端与工具服务的协议，服务和访问令牌分别具有身份与授权范围。
插件	提供页面、业务服务或数字员工工具的扩展，具有自身权限。

界面名称

导航入口、品牌称谓及后台“专家市场”的含义见界面与端差异。

权限规则

范围	说明
访问条件	身份、入口、资源授权、动作权限及状态依赖共同决定访问。见组织与权限。
数字员工	发现范围不授予对话、设备连接或管理权限。见员工权限。
授权来源	多个来源可以共同授权，撤销一项不撤销其余来源。四类授权等级见资源授权。
知识	成员身份、目录继承与历史文件独立限制共同决定访问，管理浏览不授予正文读取。见知识中心。
项目	项目角色控制项目内动作。见项目角色。
插件	插件按自身业务角色和数据范围授权，不套用数字员工授权等级。见插件权限。

状态说明

范围	说明
数字员工	配置生命周期与运行就绪分别判断。见生命周期。
运行实例	运行阶段记录执行环境状态。见运行阶段。
知识	处理阶段与最终结果分别记录；归档内容只读，不参与检索或写入。见知识库状态及任务状态。
技能与插件	草稿、审核、发布、安装和同步分别记录；安装范围与业务授权另行判断。见技能安装及插件发布。

常见现象

现象	说明
数字员工可见但不能对话	可见不表示具有使用权限或运行就绪。见员工权限。
技能已安装但未调用	Agent 按任务需要调用技能。见选用与安装。
切换数字员工后插件入口消失	入口受安装范围与访问条件限制。见安装范围。
知识库可见但正文拒绝	知识库可见性不等于正文读取权。见知识权限。
文件有名称但无法打开	文件名不表示内容已保存或下载。见资料版本。

相关章节

员工、知识、项目、业务插件、组织与认证分别说明对应的功能与权限规则。具体任务见操作手册。

对话

对话使用当前身份、所选数字员工、话题历史和本次材料处理请求。

数字员工选择

所选数字员工决定本次请求的运行上下文。用户尚未选择数字员工时，输入区、附件和语音提示先完成选择。

启用状态、发现范围与使用授权共同决定可选范围。数字员工管理页的访问权限不授予全部数字员工的对话权限。

数字员工切换改变后续请求使用的能力和资源，历史消息保持原有内容。数字员工未就绪、设备离线、模型错误或等待确认均会影响请求执行。

输入内容

输入	作用	边界
文字请求	说明目标、材料、约束和输出	不凭空获得文件或外部账号权限。
附件	提供本轮使用的文件	上传、读取和内容理解是不同阶段。
知识范围	指定本次任务使用的知识库	数字员工须已接入知识 MCP；选择不安装服务或授予权限，见知识接入。
技能选择	为本次请求指定工作方法，无须先安装	选择不加入“已具备”，不替代长期安装；两种范围见技能。选择不代表执行成功。
插件选择	为本次请求选择数字员工提供的内置插件	不安装业务插件或运行时插件，见插件入口的区别。
“工具”菜单	切换推理过程与工具调用的显示	显示开关不改变 MCP 接入、工具权限或实际调用。
本地文件夹	指向设备上的授权目录	需要对应客户端、设备连接与访问授权。
计划模式	先生成步骤并确认范围	不代替外部系统审批。



对话输入区的添加菜单与本次知识范围

附件上传或转换期间，输入区阻止发送。文件名出现不表示附件已就绪；失败附件提供“重试”与“移除”，正文引用的本机路径也不等于已上传文件。

话题与历史

话题保存连续消息及相关工作过程。继续同一话题可保留上下文，新话题用于新的工作目标。话题列表的搜索、类型和未读状态帮助定位记录。

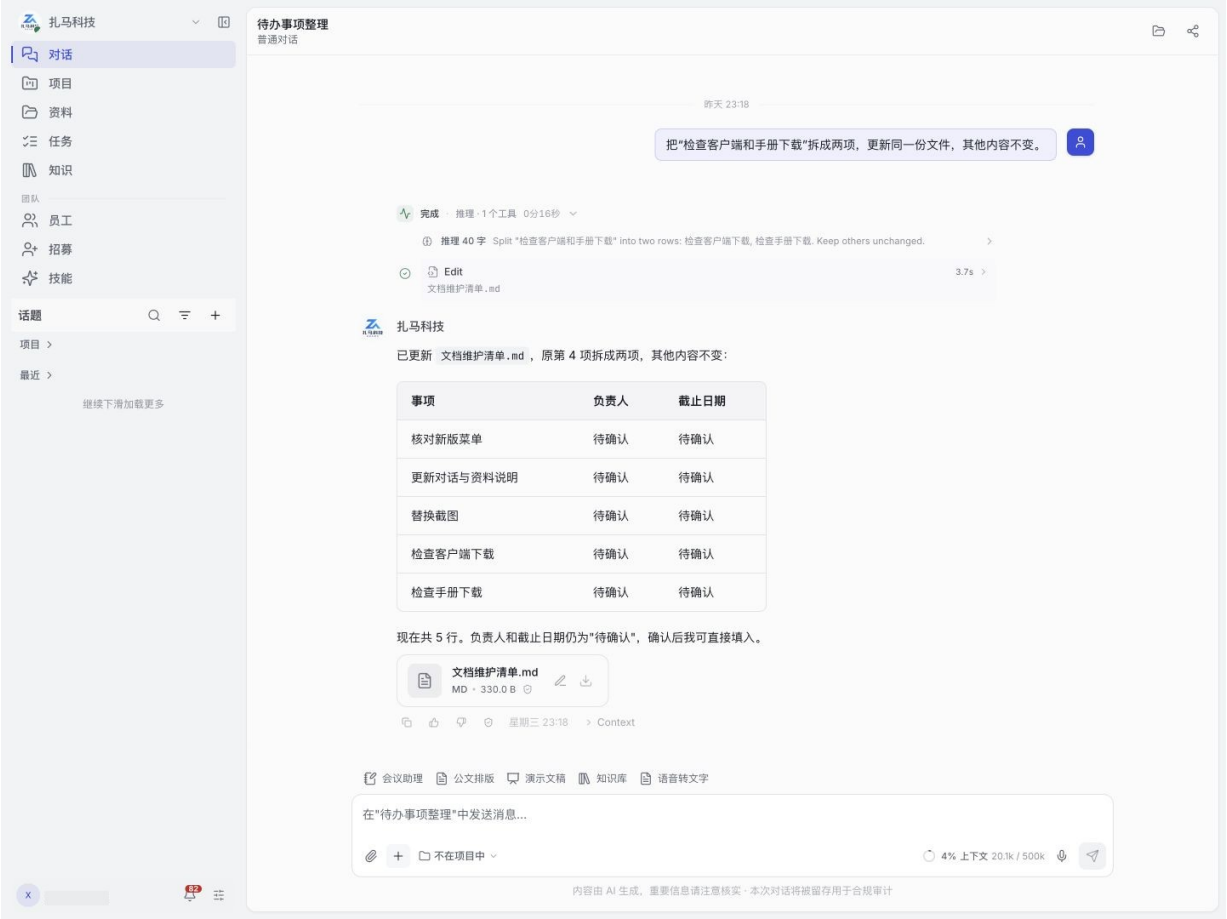
定时结果接收话题具有独立发送限制。该类话题的只读状态不表示普通对话发生故障。

项目对话涉及共享材料、成员访问与交接，见项目协作。话题历史与数字员工长期记忆分别保存；话题附件也不自动发布为共享知识。

执行反馈

活动呈现工具调用、处理中、等待确认、失败和完成等过程信息；工具成功表示该次调用返回成功，最终答复与交付文件仍可能需要内容核对。

中止用于请求停止当前处理，不会撤销已经提交到外部系统的动作。用户在重发或重试前核对已有活动和产物，避免重复发送、写入和创建任务。



回复活动中的实际工具调用、文件修改与交付文件

页面限制

数字员工配置、身份权限、客户端能力和部署条件决定工具、技能、语音、附件来源、项目及并排编辑的可用范围。

未经当前菜单开放的路由不能作为功能入口。操作见对话，界面区域见界面与端差异。

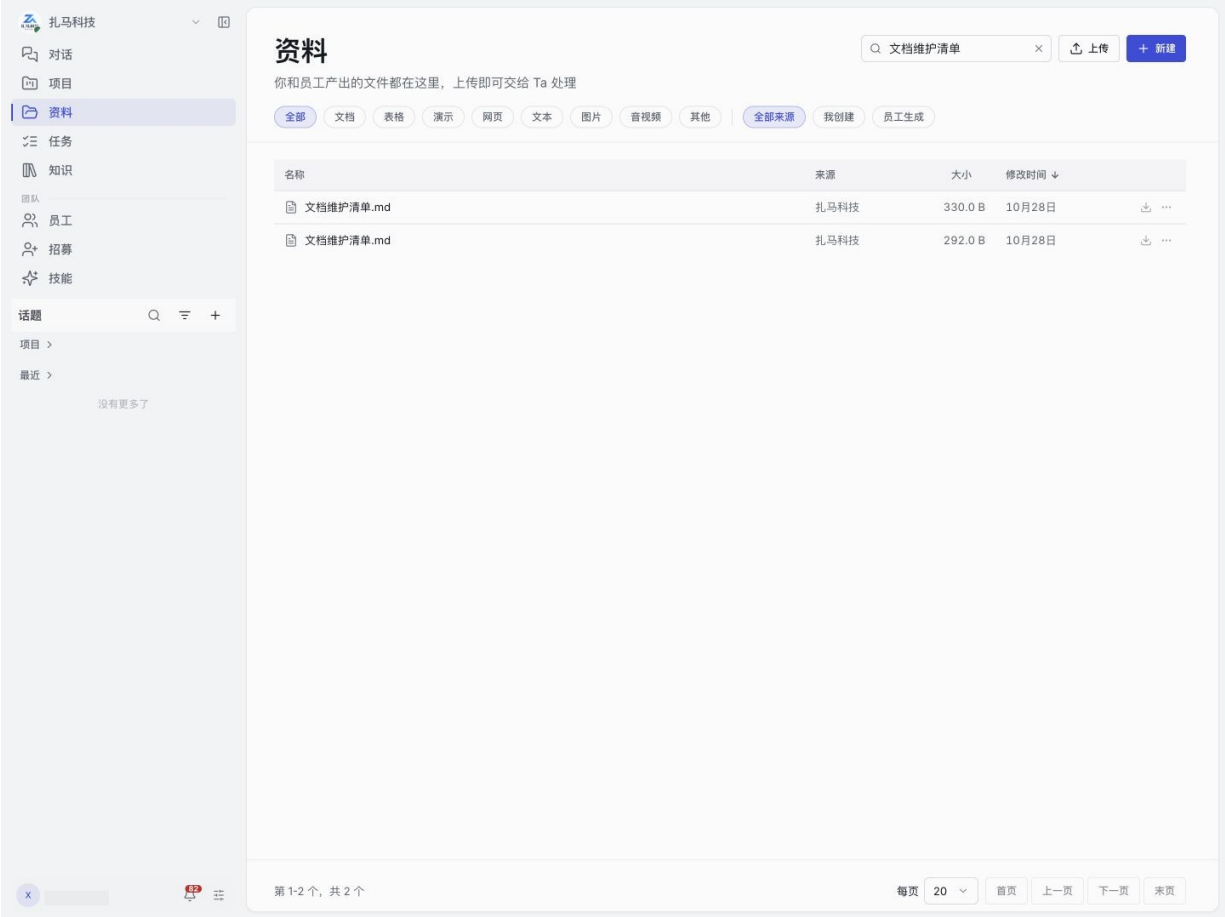
资料

资料保存文件及其版本，办公界面提供内容读取或编辑。知识中心保存经过处理的知识文档。资料文件与知识文档分别维护版本和权限。

文件来源

来源	用途
本地上传	每次上传新增文件，同名文件分别保存。
数字员工交付	保存任务产物。
新建文件	从空白开始编辑并保存。
话题附件	为对应话题提供材料。
项目材料	按项目角色共享文件，保留版本与活动记录。

资料菜单可见不代表每个来源都已获授权。文件的名称、内容类型、大小、更新时间和修订号用于定位文件；名称不能替代稳定文件标识。



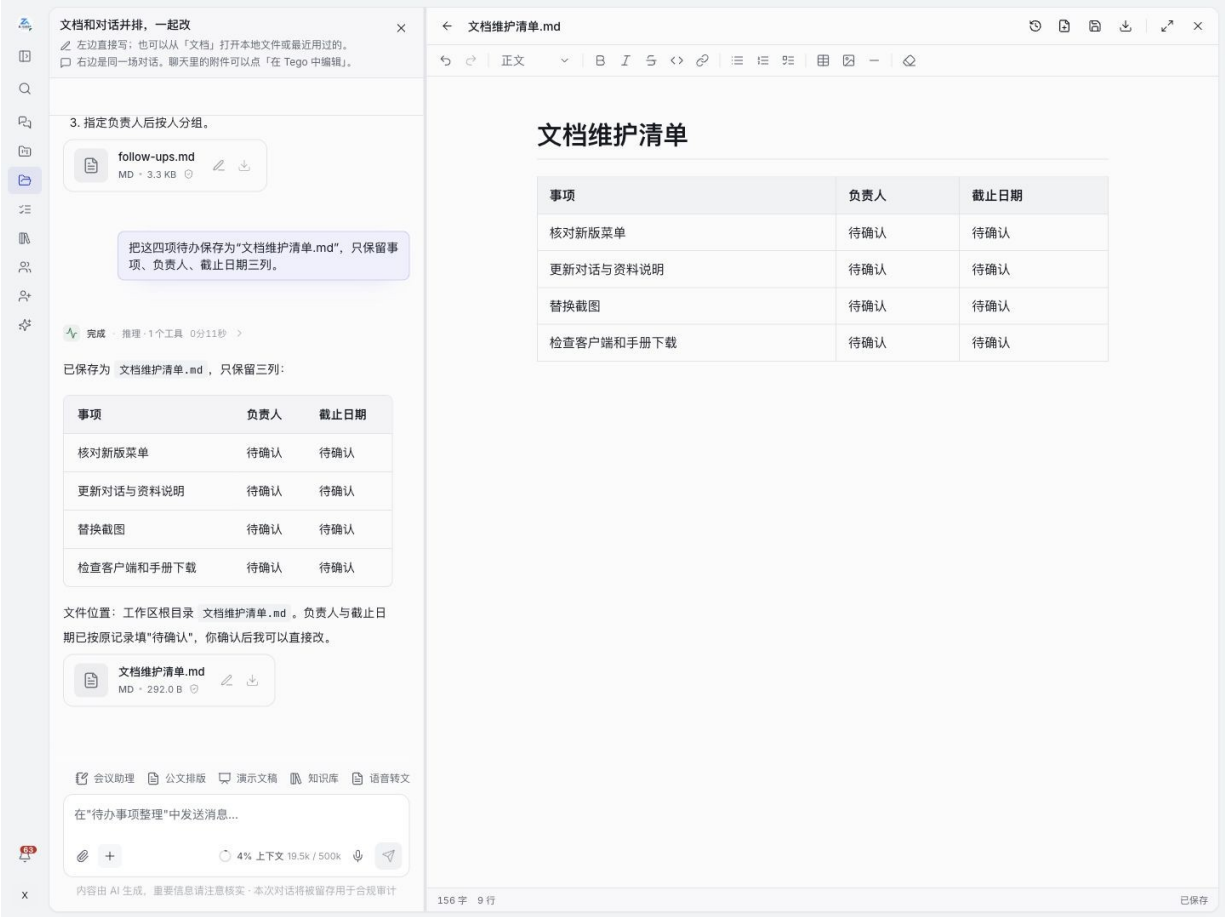
资料列表：文件名称、来源、大小与更新时间

编辑器类型

文本、Markdown、Word、演示、PDF 与表格各有适用的打开方式。Web 表格提供只读预览，桌面端可使用原生编辑链路。

PDF 提供页面预览，不提供任意正文改写。

具体保存边界见办公编辑与保存说明。



Markdown 文档与对话并排打开，编辑区显示保存状态

文件版本

编辑并保存已有资料会更新该文件的修订；重新上传同名文件会新增资料，不会接续原文件的版本。历史版本提供已保存内容的核对或恢复依据。

保存前关闭、网络中断或权限变化均会影响持久化。重新打开的内容反映实际保存结果。

新建文件先打开空白编辑器，首次保存后才进入资料列表。恢复历史版本时，当前已保存内容保留为历史版本，未保存修改会丢失。

加入知识操作将所选文件及其修订提交到知识导入流程。后续资料修改不自动更新知识正文、分段和索引；知识来源版本、处理任务及检索结果分别反映导入状态。

权限与限制

阅读、下载、编辑、删除、共享及加入知识是不同动作。资料列表的入口不绕过目标文件、项目或知识的权限。

外部应用中的本地修改只有回传并保存后，才成为平台中的内容。

删除资料会同时从列表移除该文件及其历史版本。上传队列的“忽略”只移除失败提示，不删除已有资料。

删除、覆盖和恢复影响当前文件版本及使用方。重要交付需要明确文件名并保留旧版。

定时任务

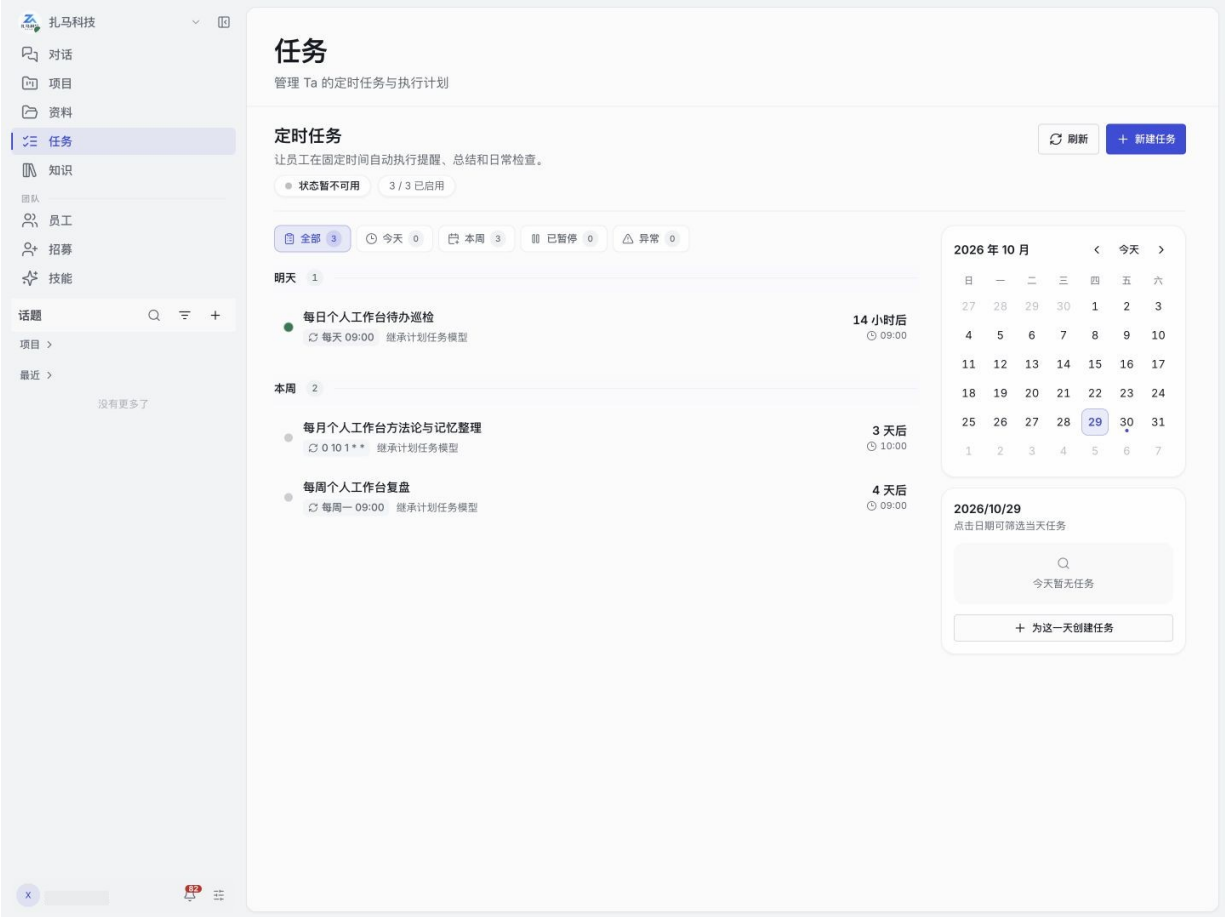
定时任务保存执行日程和工作指令，运行记录保存每次触发的实际结果。一个计划可以触发多次运行，启用状态与各次执行结果分别维护。

任务看板

左侧任务页展示当前所选数字员工关联的个人定时安排，提供日历及全部、今天、本周、已暂停、异常筛选。

员工控制台中的管理员视图汇总该数字员工不同使用者的计划；“以用户身份查看”时只读。同一使用者、同一数字员工的计划由两个入口共同维护，入口切换不会复制计划。

项目事项、知识处理任务和定时计划分别维护，不能通过修改其中一类改变另一类。



定时任务看板中的筛选、日程与日历

定时任务

字段	含义与边界
任务名称	用于列表显示和查找计划。
让 AI 做什么	每次触发交给数字员工处理的任务，需包含材料与交付约束。
执行频率	每天、每周、每隔几小时、每隔几分钟、指定时间一次、自定义 Cron；选择后填写对应参数。
启用状态	是否允许后续自动触发。
模型	本任务单独指定模型，或保留“继承计划任务模型”；模型选择不补齐提供商凭证。
仅在有重要更新时通知	控制通知条件；需结合运行记录判断是否执行，不能把没有通知等同没有运行。
下次执行预览	根据当前日程规则计算的预计触发时间。
最近运行与记录	用于核对实际触发、状态与结果。

日程按单次时间、间隔或 Cron 表达式触发。既有事件类日程不能直接按普通时间计划修改。

本任务指定的模型优先。保留“继承计划任务模型”时，系统使用当前数字员工“模型配置 → 模型路由”的“计划任务模型”；该项未配置时继承默认聊天模型。



新建定时任务表单：工作指令、模型、执行频率和通知条件

运行状态与调度状态

对象	状态含义
调度服务	自动执行开启或关闭。
单项计划	启用或停用。
单次执行	运行中、成功、失败和中止。

“暂不可用”表示当前连接或服务状态尚未确认，不表示自动执行已经关闭。日程修改保留之前的执行记录。

计划的“暂停”仅阻止后续自动触发，不取消当前运行；“启用”恢复后续调度。有管理权限的人员可在运行记录中取消仍在运行的记录。

重复触发会带来重复外发或写入风险，已有运行记录与产物用于确认原执行结果。停止执行不会撤销外部系统已经接受的动作。

知识任务

知识任务有独立类型、进度、尝试次数和错误详情，见知识中心。不能用定时任务的启用状态解释知识文档是否已索引。

权限与异常

任务使用实际运行身份及授权读取材料、调用工具和发送结果。个人环境变量、数字员工配置的服务凭据与渠道身份分别具有作用范围。

普通任务页使用者不自动具有管理员查看全员计划的能力。操作见定时任务。

知识中心

知识中心将资料处理为可检索的原文与分段，检索结果按当前身份的知识权限过滤。

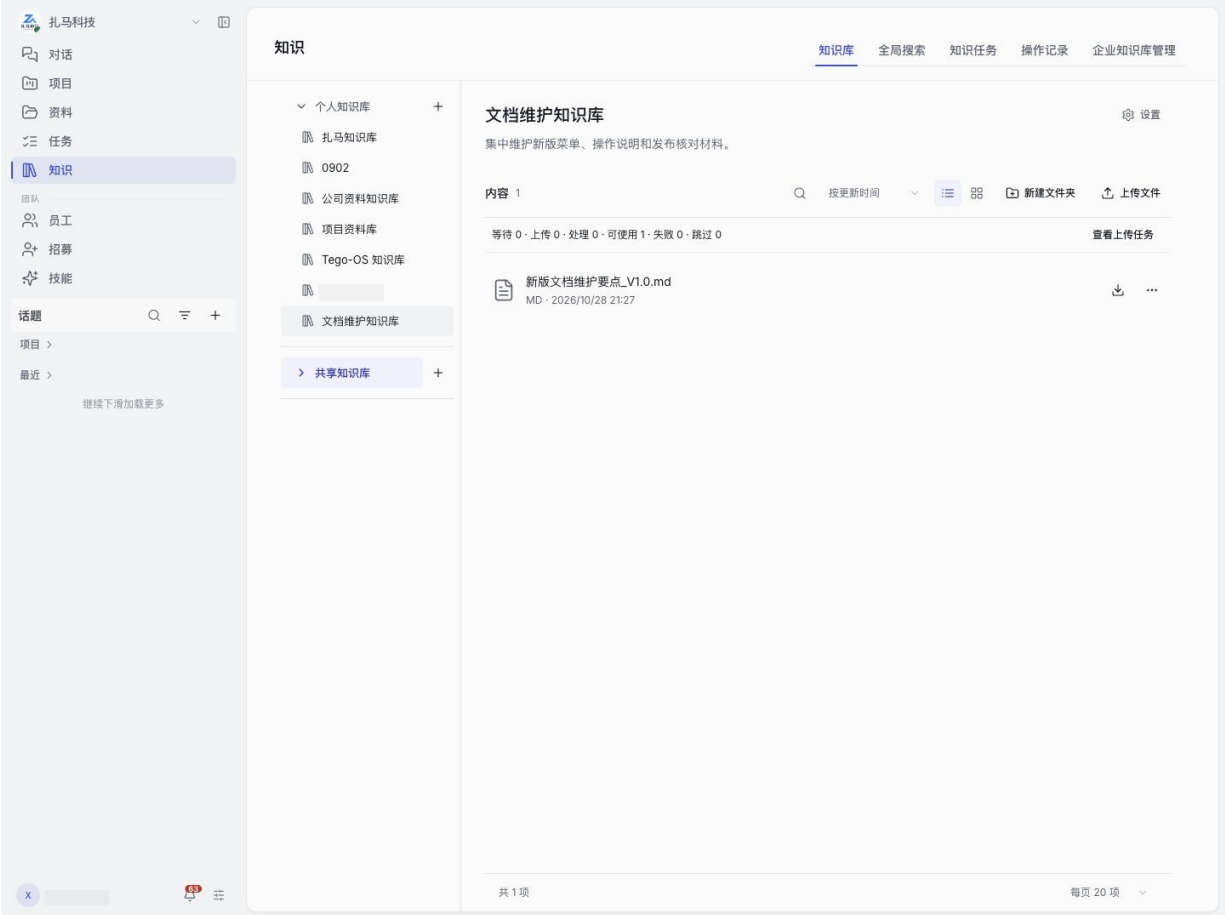
产品边界

资料负责文件编辑与版本管理，知识中心负责解析与检索。资料加入知识后，系统创建知识文档与处理任务；后续资料修订不会自动更新知识索引。

全局搜索返回原文片段。数字员工接入并启用知识 MCP 服务后，可以在对话中检索资料并组织回答。

页面组成

入口	作用	访问边界
知识库	按个人、共享及目录浏览资料	当前成员及有效权限。
全局搜索	跨所选范围召回原文片段	先过滤文档权限，不自动扩大范围。
知识任务	跟踪处理、审核、删除等异步工作	当前身份可访问的任务。
操作记录	核对知识操作与结果	管理员或有库管理范围的人员。
企业知识库管理	查看组织治理范围	管理入口不自动授予正文读取。
后台知识服务	租户模型、解析与检索服务设置	管理员配置，不放在普通找资料路径中。



知识中心的知识库导航与文档列表

知识库内容层级

对象	作用
空间或分组	按个人或共享方式组织知识。
知识库	保存说明、成员、内容及索引绑定。
文件夹	组织目录。
知识文档	保存来源、正文与处理状态。
分段	作为检索单元。
任务	承接异步执行。

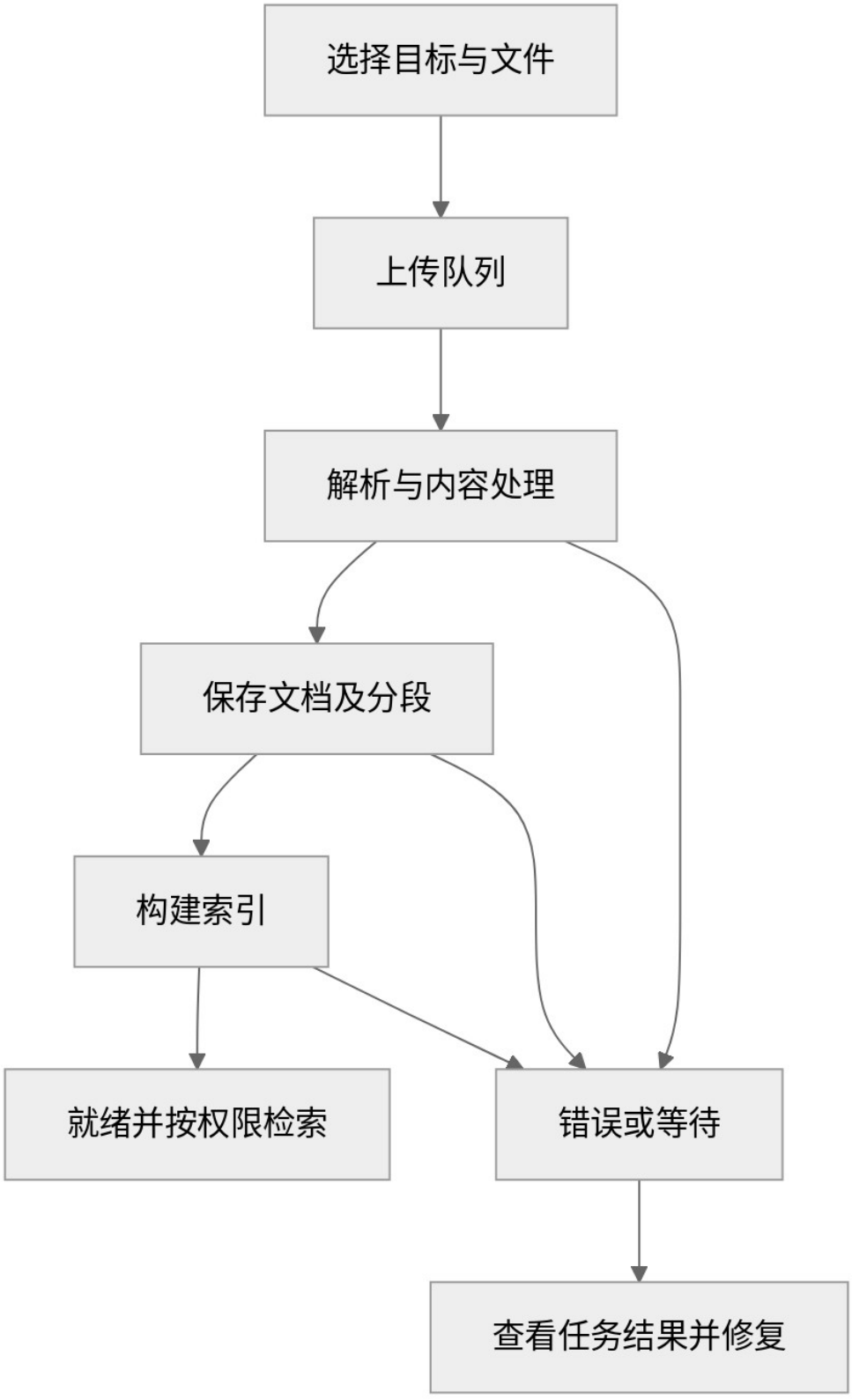
来源应用管理的内容在来源侧维护。

知识库范围与状态

个人库仅本人可见，同一用户可以创建多个个人库。共享库按个人、部门或组织范围授权；历史库继续按原有访问约束判定权限。

使用中的库可按权限处理和检索。已有归档库保留只读访问，不参与检索和写入；当前知识库设置没有归档或取消归档入口。

文档处理链路



知识资料处理流程：从选择文件到就绪检索，出错或等待时查看任务结果并修复

取消或超时后，任务可能仍在后台处理。使用者在“知识任务”查看最终结果后，再决定是否重试。

文件规格

上传队列显示当前允许的扩展名、单文件容量和单批数量。资料导入以文件标识和修订号确定来源版本。

同名处理提供跳过、重命名和替换；替换会更新已有内容。

文档处理能力

全部知识库的上传、替换和重新处理统一使用后台“文档处理”配置。配置变更不会重新处理已有文件。

图片理解与 OCR 的处理范围、模型依赖见文档处理选项。

知识模型

创建知识库前，管理员必须在后台“知识服务 → 模型选择”保存全局 Embedding 模型。新库采用该模型，历史库保留原索引绑定。

Embedding、Reranker、OCR 的作用与配置见模型引用。

涉及历史库模型变更时，管理员先通过技术支持确认该版本支持的处理方式，并核对模型权重、版本、维度和归一化规则的兼容性。

更改全局模型不会自动迁移历史库。索引可显示就绪、需要重建、重建中或失败。

检索模式

关键词适合编号、专名与原文短语；语义检索适合不同措辞的近义表达；混合方式组合全文与向量结果。分值与阈值只反映当前检索规则，不能直接解释为答案正确率。

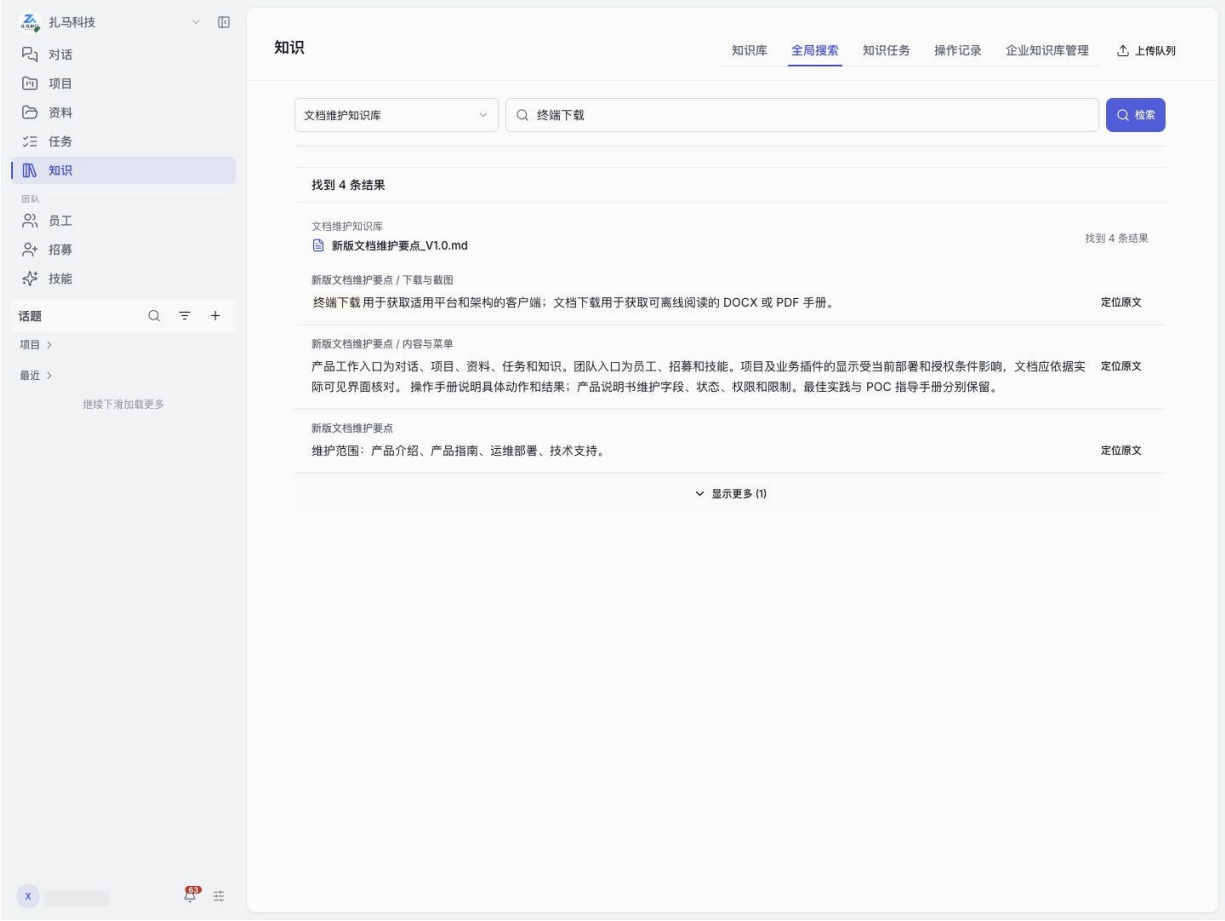
检索参数

全文权重、向量权重、召回数量、置信度阈值及重排由后台统一设置，作用于全部知识库。取值与影响见检索设置。

单次检索测试的相似度输入范围为 0–2，与全局置信度量表不同，阈值不能跨界面直接比较。测试查询不会永久改写全局参数。

检索结果结构

检索结果包含来源文档、命中片段、位置与分值。页码、表格或段落定位依赖解析结果；缺少定位信息时，使用者可以打开来源文档核对原文。

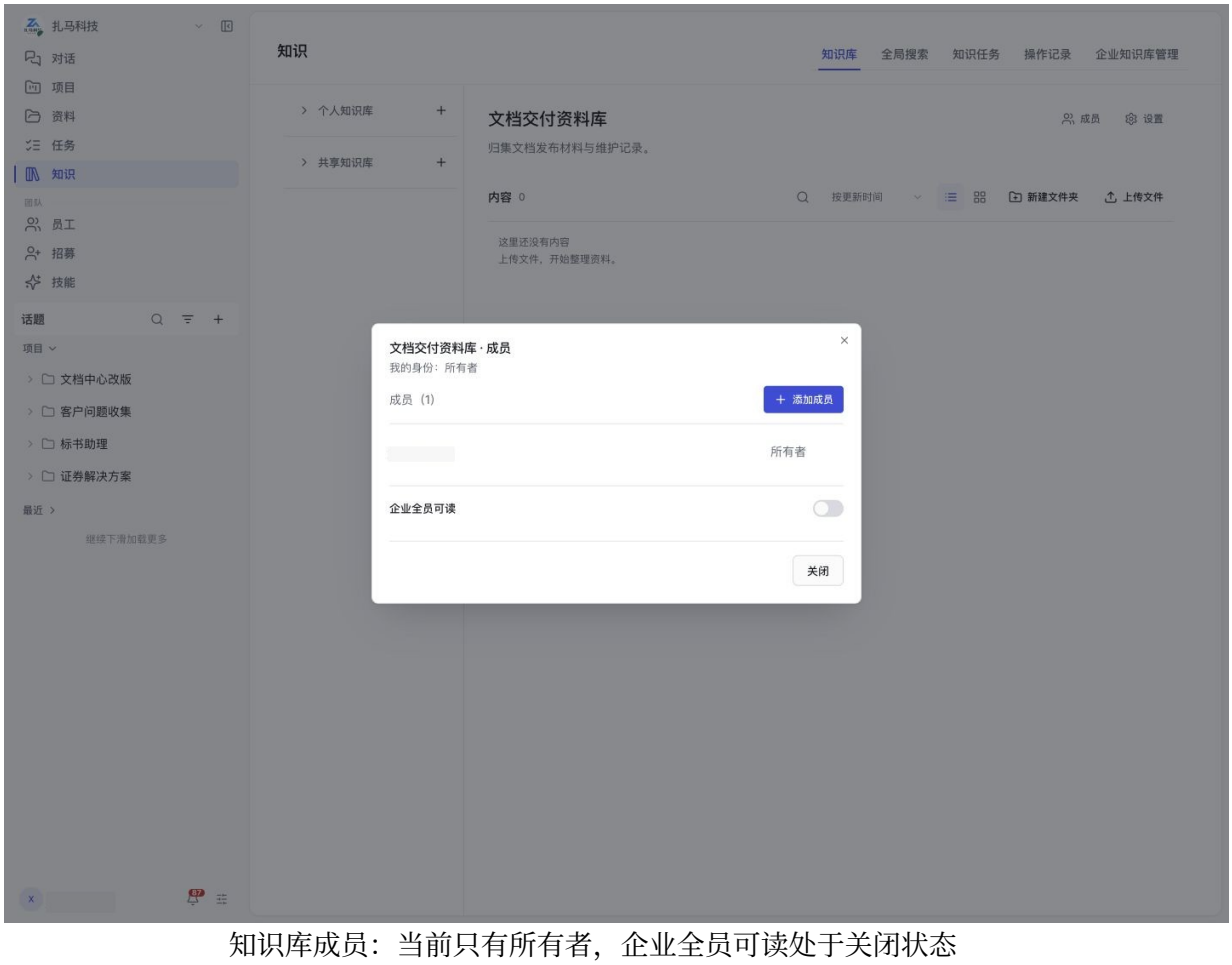


限定知识库的搜索结果与定位原文入口

知识访问权限

知识库成员分为所有者、管理员、编辑者和浏览者，权限分别控制读取、检索、编辑、成员管理和删除。历史内容还可能保留仅基本信息或管理浏览权限。

成员来源可能是个人、部门/团队或企业全员。移除直接成员后，其他有效来源仍可能保留访问。选择部门可能包含下级与未来新增人员；拆分为个人授权时只涵盖计算时的人员。



知识库成员：当前只有所有者，企业全员可读处于关闭状态

企业知识库管理以名称、文件数、更新时间、所有者和我的身份呈现各库。平台管理员也需按“我的身份”判断可写动作，看到插件管理库不意味着可以直接修改内容。

个人 MCP 管理员令牌的跨库检索规则另见个人连接。

历史知识库和文件可以继续使用继承或独立 ACL。继承模式按库权限判定，独立文件按自身限制判定，不因库成员变化自动放开。

当前文档详情没有独立权限编辑入口，库维护者不能在该页面修改历史独立权限。

后台管理浏览用于查看治理信息，不授予正文权限。用户不能通过导出或外部服务绕过原文访问限制。

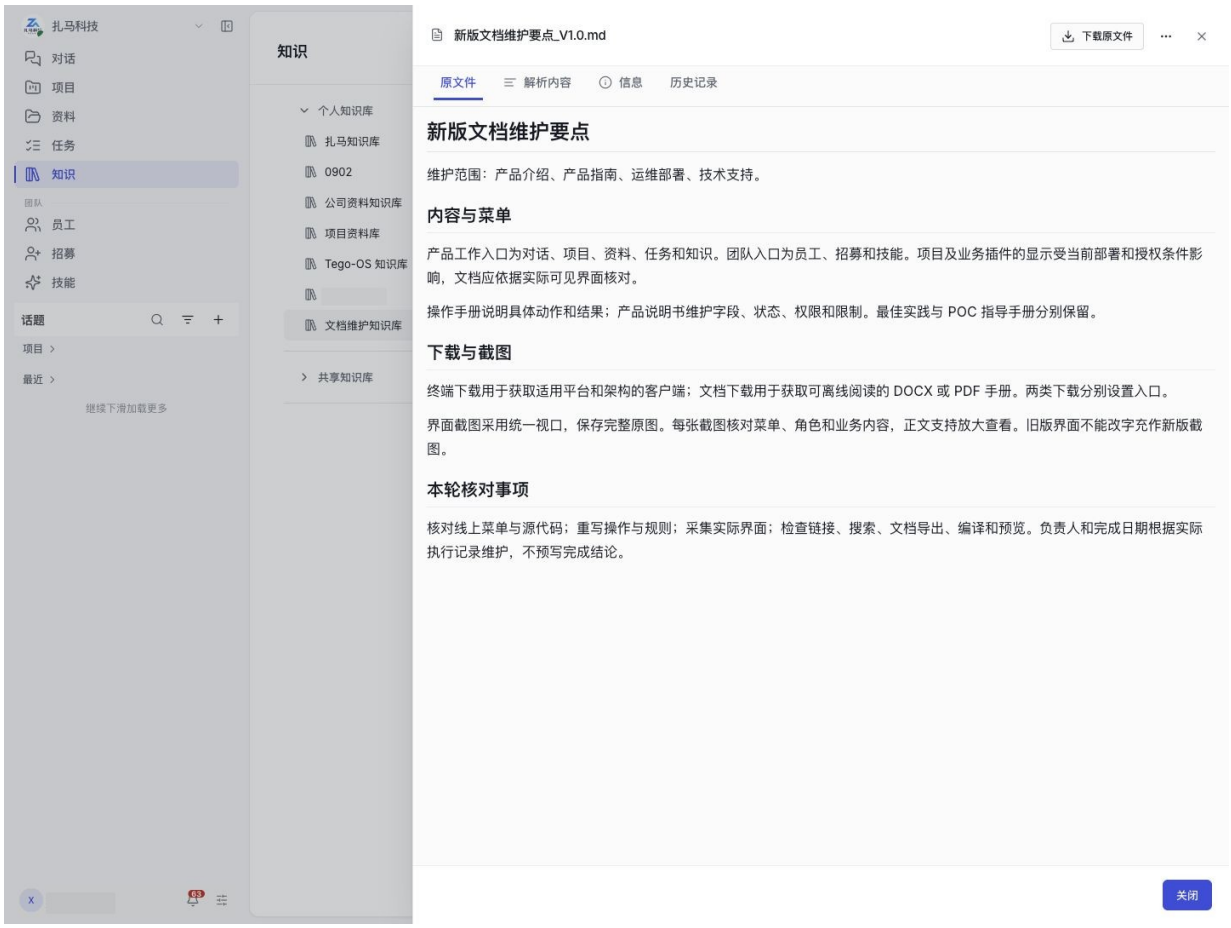
文档详情

标签	内容
原文件	保留可下载来源。
解析内容	显示当前分段及维护动作。
信息	显示文档信息与处理结果。
历史记录	追溯修订。

历史记录中的原文件版本仅供下载，不参与当前搜索问答。

文档信息包含名称、来源、上传者、状态、字符数、分段数、创建/更新时间及原始元数据。元数据随来源与处理链路变化。

下载原件、修改信息、重处理与删除是不同权限动作。



知识文档详情：原文件、解析内容、信息和历史记录

分段管理

分段包含正文、标题、页码或序号以及更新时间等内容。具备文档编辑权限的维护者可以新增、编辑、启用、停用或删除分段；检索测试打开的只读预览不提供修改。

分段正文不能为空。保存后，系统更新该分段的检索索引；删除会同时移除分段及其索引，无法恢复。

分段修改不改写源文件。分段编号可以随处理结果变化。

任务状态

状态	含义
排队中/进行中	等待资源或正在处理；具体阶段见结果。
待我处理	需要当前身份补充或确认。
已完成/部分完成	本次任务的处理结果，部分完成需逐项核对。
失败/多次重试失败	阅读诊断与尝试记录后修复。
取消中/已取消	停止请求与最终取消不同，已有内容可能保留。

处理阶段包括等待知识服务、读取源文件、格式转换、解析、内容增强、保存与构建索引。

出现格式兼容回退警告时，使用者可以在文档详情的“解析内容”中核对正文。

外部客户端接入

外部接入使用当前部署提供的服务端点与访问令牌，以令牌所属用户身份调用可用服务。库地址、服务标识或数字员工名称不授予匿名访问权限。

管理员令牌的界面提示与当前源码存在范围差异，具体见个人 MCP 令牌权限。

使用情况与审计

命中次数及最近命中时间记录资料被检索返回的情况。操作记录保存动作、主体、结果与时间；审计中心的查阅范围与正文权限另见审计中心。

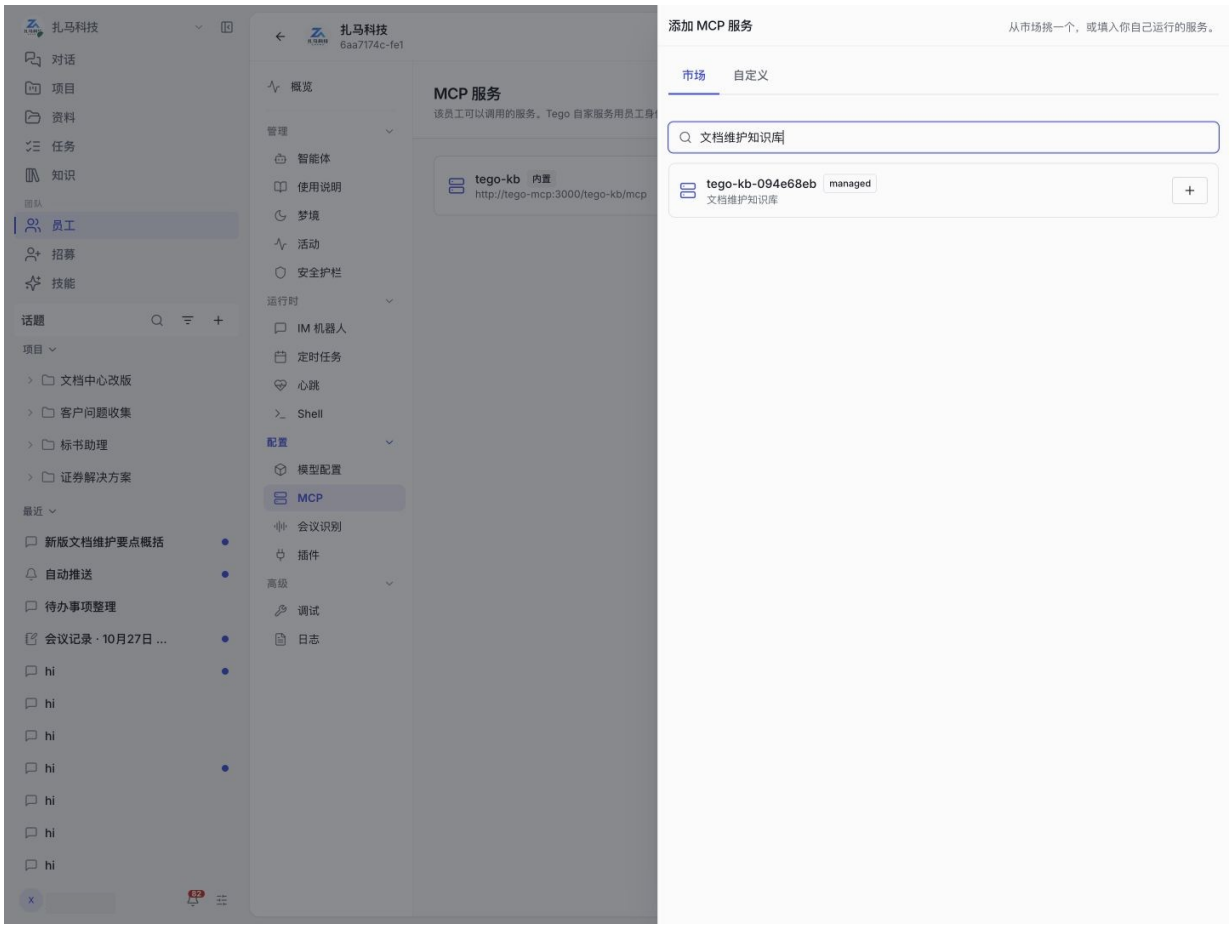
与数字员工的关系

数字员工通过已添加、已启用的知识 MCP 服务调用知识。平台提供 tego-kb 和限定单库的知识服务；知识文件完成处理不会自动为所有数字员工添加这些服务。

配置或工具	作用与边界
tego-kb	检索当前调用人获准使用的知识范围。
单库知识服务	将检索限定在对应知识库内，仍校验调用人的使用权限。
对话“指定知识库”	向本次任务提供所选知识范围，不安装 MCP 服务，也不授予权限。
knowledge_search	返回命中片段、来源文档与引用地址。
knowledge_statistics	返回知识内容的统计信息，不代替正文检索。

平台内置服务使用平台身份认证。数字员工调用时，服务端校验当前调用人及其知识权限；共享数字员工不会继承创建者的个人知识权限。

操作见让数字员工使用知识库。



在数字员工控制台添加知识服务，添加与知识库授权分别处理

限制与异常状态

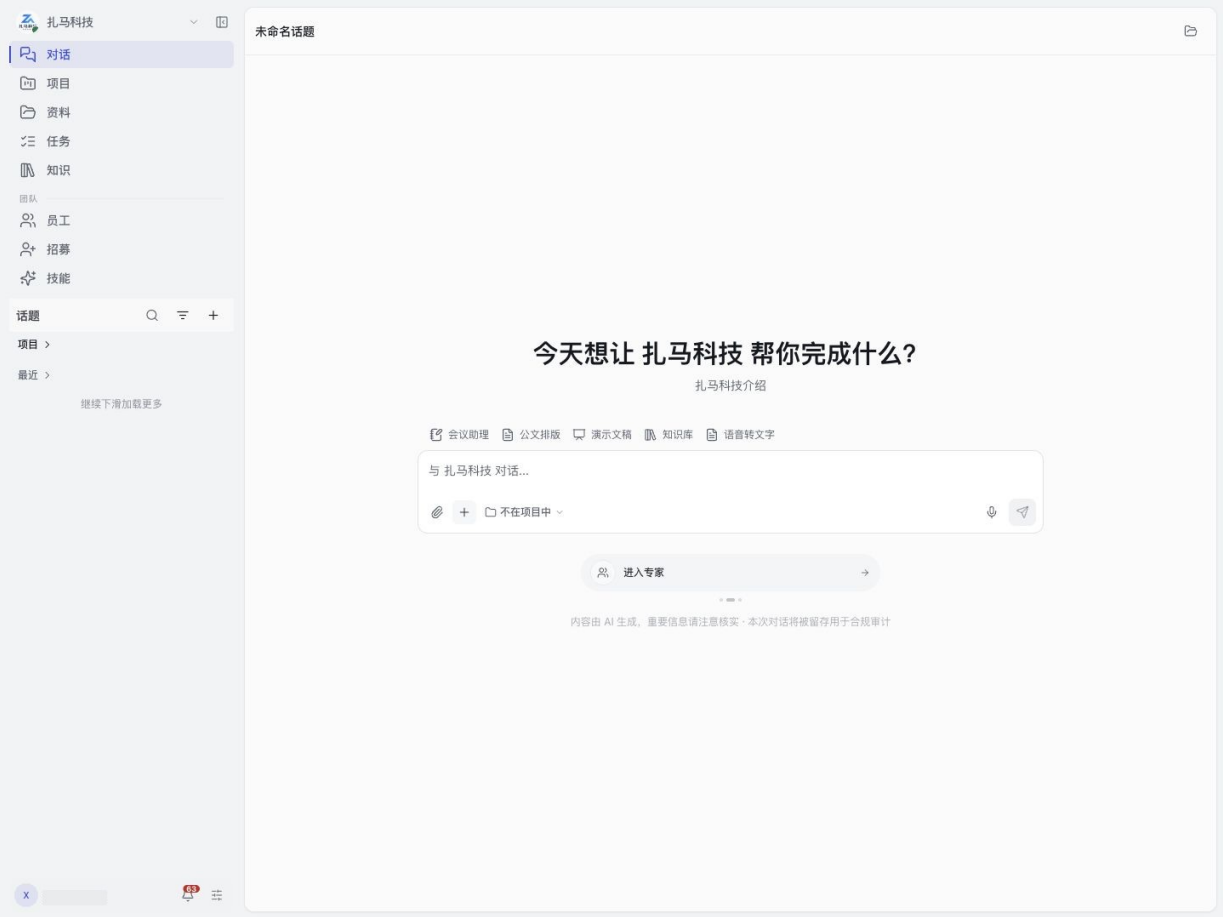
归档或尚未就绪的文档不参与当前检索。上传队列显示文件传输错误，“知识任务”显示解析与建索引失败原因；模型变更后的问题还需查看索引状态。操作见知识中心，配置见知识服务。

界面与端差异

工作台左侧提供对话、项目、资料、任务和知识入口；“团队”分组提供“员工”、招募和技能，其中“员工”对应数字员工。

主要区域

区域	用途与边界
数字员工选择器	确定当前数字员工上下文；用户尚未选择时，输入、附件和语音禁用。
左侧导航	切换工作页面，项目等按组织条件显示。
扩展	进入适用的业务插件；随数字员工和权限变化。
话题区	搜索、类型筛选、新话题及历史访问。
消息与活动	查看回复、工具、等待确认、错误及产物。
输入区	提交请求与可用附件、技能、计划或语音能力。
文件视图	打开、编辑或预览实际文件；保存链路按格式区分。
账户菜单	个人资料、设置、消息、下载、帮助和条件管理入口。



工作台完整页面：左侧导航、话题区与对话输入区

平台差异

平台	能力边界
Web 端	使用浏览器权限和访问地址，表格提供只读预览。
桌面端	可连接本机设备、授权目录与浏览器扩展，支持相应原生编辑链路。
移动端	布局及能力以对应发行版本为准，桌面截图不能用于推定相同。

状态提示

按钮提示区分尚未选择数字员工、话题只读、运行连接、权限和格式限制。暂不可用表示状态未知或尚未获取，关闭表示明确的关闭状态。

品牌与命名

界面名称	含义
“员工”	数字员工的发现、使用和管理入口。
“招募”	浏览数字员工模板、创建数字员工的入口。
后台“专家市场”	数字员工模板的维护与治理入口，与“招募”分工不同。

品牌配置可以调整数字员工的展示称谓。按钮、菜单与页面标题以实际界面文字为准，见品牌与发布。操作见对话。

项目协作

启用项目文件后，成员与各自的数字员工围绕同一套项目文件协作。组织功能开关控制项目是否可用，项目成员资格与角色决定访问和操作范围。

内容与上下文

内容	作用
项目名称与目标	说明共同工作的目标和范围。
项目文件	保存资料、过程稿、成果及事项、决定、会议记录，按项目成员权限共享。
活动与版本	记录提交主体、修改文件和版本，支持查阅与接续处理。
项目对话	保留成员与数字员工的沟通过程，可见范围由对话发起人控制。

通过“加入已有资料”导入个人资料或知识文件时，系统将文件复制到项目。原文件及其权限不变，项目内的副本按项目成员权限共享。

两份文件后续分别维护，修改不会相互同步。

只提供原资源链接时，接收者仍需具备原资源的访问权限。成果保存在“我电脑上的项目文件夹”时，其他成员不能通过项目读取该本地文件。

对话与文件的可见范围

项目对话默认仅发起人可见，发起人可以公开给项目成员，也可以收回。成员查看其他人公开的对话时，可以提出补充意见，由发起人决定纳入本轮、留到下一轮或不采用。

对话私有不等于成果私有。对话内容写入项目文件后，该文件按项目成员权限共享；参与项目本身不会自动共享成员的个人资料。

成员退出或被移除后，未公开的项目对话回到其个人对话列表；已公开的对话留在项目中，原发起人只能阅读，不能继续修改可见范围。

工作台与项目事项

工作台汇集项目目标、事项、项目对话、最近决定、最近会议、最近成果和动态。活动另有标签。

事项按“我的”或“全部”查看。成员新建事项时填写标题并创建，随后在事项文档属性中维护状态、负责人等信息。

系统为事项、决定和会议记录分配编号，并分别保存为文件。工作清单和决策索引从记录生成，不直接编辑。

成员打开事项后，可以在对话旁编辑文档。事项文本的自动保存保留为个人草稿；“提交到项目”才将改动形成项目版本，供其他成员接续处理。

项目事项状态记录业务进度，文件保存记录内容版本。定时执行计划在左侧任务页维护，知识解析在知识任务中维护。

进展跟踪

“自上次以来”整理成员上次查看项目之后的文件变化、新增决定、事项交接、冲突和未完成工作，与本人相关的变化优先显示。本人手动提交的改动不重复列入；没有相关变化时不显示该区域。

事项分配、交接、提及、批注回应及数字员工留下的冲突或未完成工作，通过“消息中心”提示相关成员。通知本身不会自动让接收者的数字员工开始处理。

项目顶部的正在处理提示反映数字员工近期对项目的访问，完成情况以事项及提交结果为准；关联对话仍受可见范围限制。

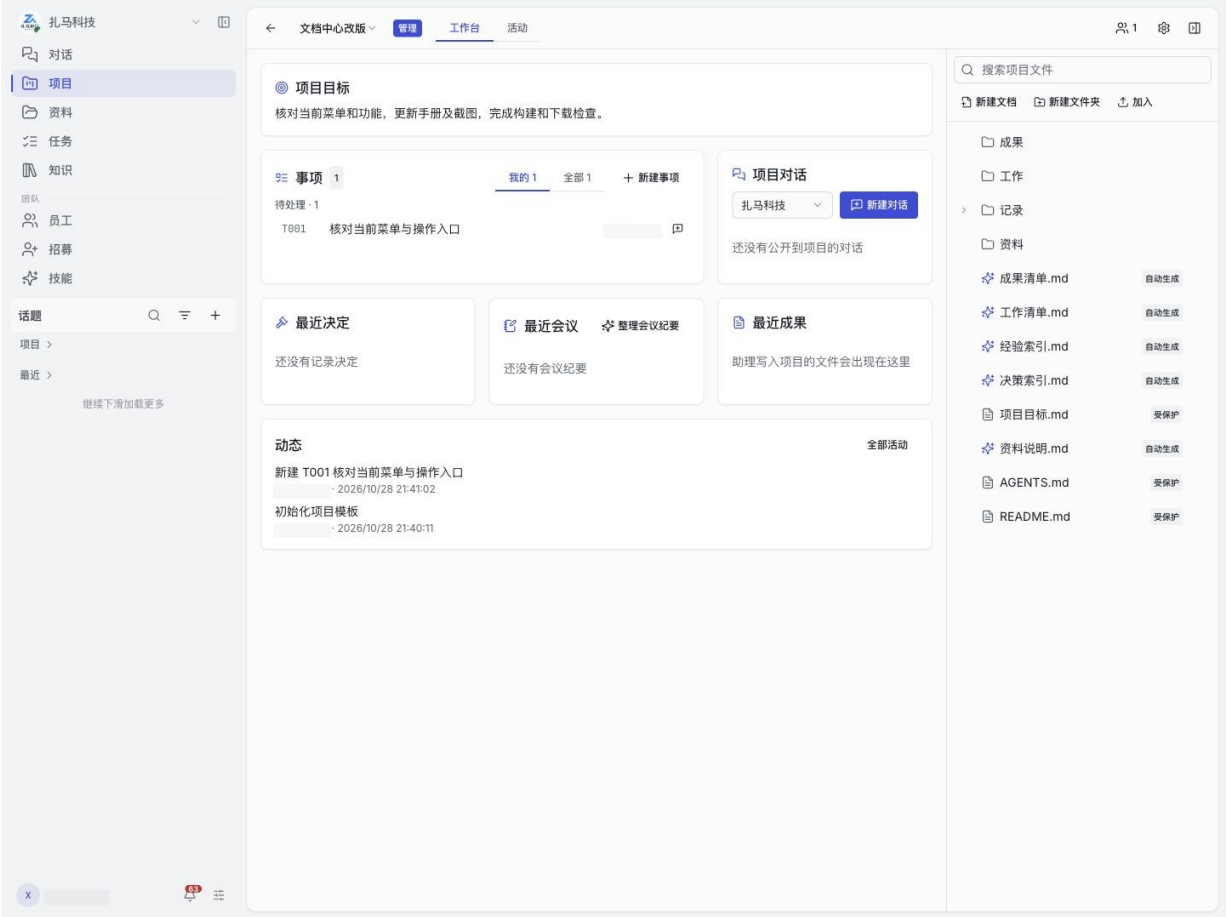
自定义首页

项目可以使用自定义页面作为首页，并切回“原生工作台”。自定义首页需要通过文件检查，并依赖单独配置的隔离页面服务；服务未配置、页面无效或加载失败时显示原生工作台。

首页按查看成员的项目权限读取已声明的项目数据，不能绕过项目权限。制作与修改首页需要管理权限。

自定义首页使用条件

本手册所示项目尚未启用自定义首页；当前部署的隔离页面服务配置与首页运行状态【待确认】。



项目工作台：目标、事项、对话、动态和共享文件

初始文件结构

项目设置包含“基本信息”“文件与输出”“成员协作”三个部分。成员在项目创建完成后从“成员协作”邀请人员。

项目可以指定有权使用的默认数字员工，并选择成果保存在项目文件或本机项目文件夹。

初始内容	用途
README.md、AGENTS.md、项目目标.md	分别保存项目入口、数字员工的项目操作规范和项目目标。
资料、工作、成果	分别存放输入材料、过程稿和交付成果。
记录	存放事项、决定和会议记录。
工作清单、决策索引、成果清单、资料说明、经验索引	根据记录和文件生成只读视图；修改对应原记录或文件后更新。

项目文件语言在创建时按界面语言确定，创建后不能更改。上表为中文项目的初始名称。

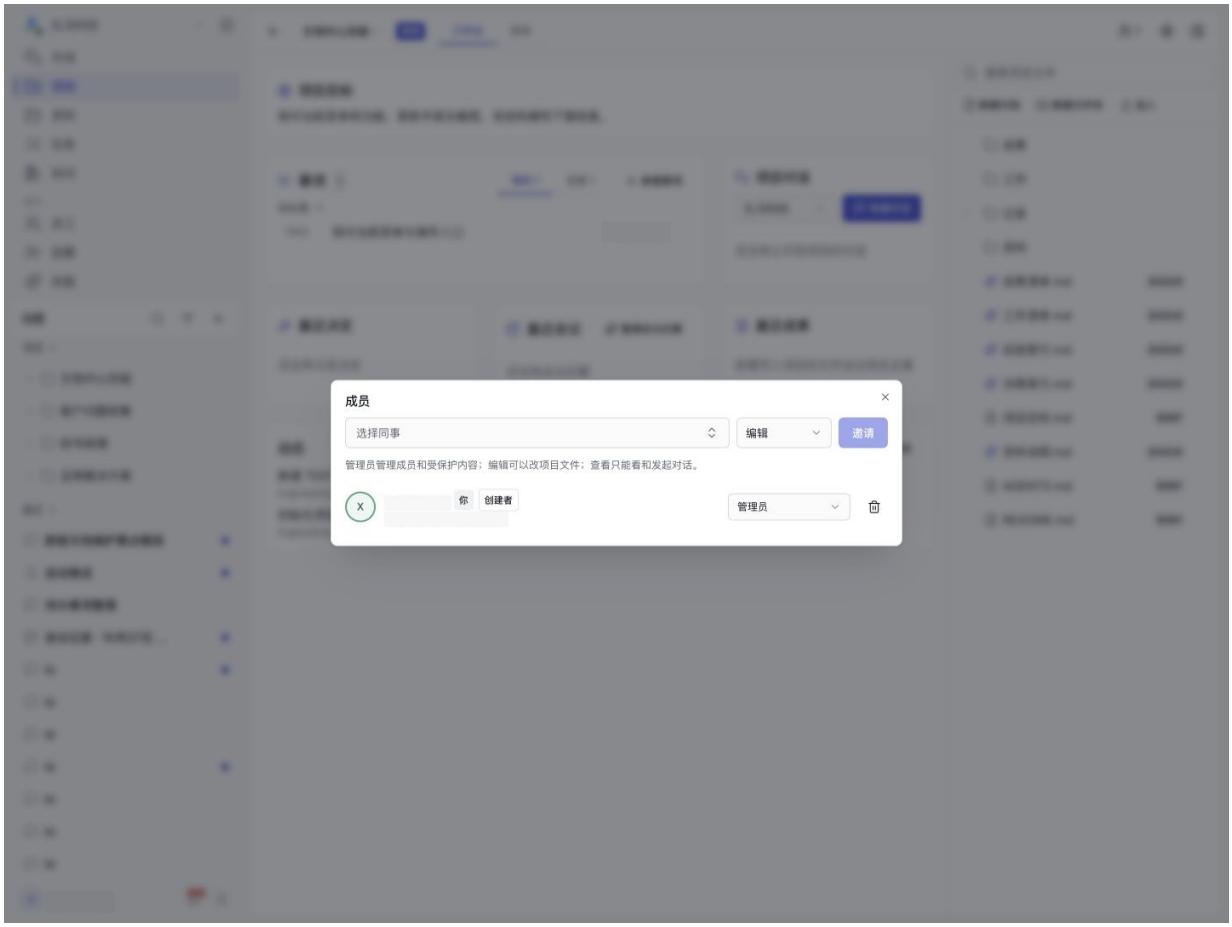
项目角色

项目列表和顶部按“管理”“编辑”“查看”三档显示；成员角色保留四类职责。“管理”包括“管理员”和“管理员（不可授权）”，两者权限不同。

成员角色	主要能力与限制
查看	阅读项目文件、历史、活动及有权查看的对话；发起项目对话、提出补充意见。不能修改文件或添加批注。
编辑	在查看基础上新建、修改、移动和删除普通文件，维护记录并添加批注；不能修改受保护内容、定稿、导出整个项目或恢复历史。
管理员（不可授权）	在编辑基础上维护受保护内容，邀请、调整和移除编辑或查看成员；可恢复单文件、定稿、导出整个项目。不能授予管理资格、调整其他管理成员、撤销提交、恢复整个项目或删除项目。
管理员	具备全部项目能力，包括授予或撤销管理资格、撤销提交、恢复整个项目及删除项目。

数字员工按委托人的项目身份和权限执行。更换数字员工不会增加委托人的项目权限。

项目必须至少保留一位“管理员”，最后一位管理员不能直接退出、被移除或降权。平台管理员身份不自动替代项目成员权限。



项目成员管理弹窗与完整项目背景

受保护内容

README.md、AGENTS.md、目标文件、基础记录目录和自定义首页内容需要管理权限。

- 成员改名、移动或删除包含受保护内容的目录时，同样需要管理权限。
- 编辑成员仍可维护目录内的普通事项、决定和会议文件。

项目名称、目标和默认数字员工等设置由具备成员管理权限的人员维护。权限按项目角色划分，不提供文件夹级独立授权。

版本与活动

文件版本记录单个文件的内容；一次提交可以包含多个文件改动，并生成项目内容版本。活动记录提交主体、来源和文件变化，成员可以从提交详情继续交接。

文件预期版本与当前版本不一致时，系统按操作类型处理：

操作	处理结果
普通项目提交	系统保留冲突副本。
恢复等要求版本一致的操作	系统拒绝冲突。
按旧版本删除文件	系统可能跳过该文件，并在结果中列明。

系统不会自动合并冲突副本，成员需要比较并保留所需改动。

定稿与导出

定稿将某个文件版本标记为交付版本，不锁定后续修改，也不表示组织审批或真实性核验已经完成。当前文件继续修改后，仍可打开已标记的定稿版本。

导出方式	包含内容
当前版	各文件的最新版本，以及生成的清单和索引。
定稿版	已标记定稿的文件，采用各自的定稿版本；未定稿文件不包含在内。

整个项目从“项目设置 → 文件与输出”选择版本并“下载压缩包”。当前文件使用“下载到电脑”；事项编辑器中的“文档”是通用文档菜单，不承担项目定稿或整体导出。

恢复与撤销

操作	影响范围与规则
恢复单个文件	将选定历史内容写为该文件的新版本。被删除文件的原位置若已被其他文件占用，恢复会被拒绝。
撤销这次提交	撤回该次提交涉及的文件改动；后续已被修改或原位置被占用的项会跳过，执行前核对预览中的跳过原因。
整个项目恢复到这一版	按目标项目版本恢复文件和目录；目标版本之后加入的文件会被删除，不能视为保留后续改动的撤销。

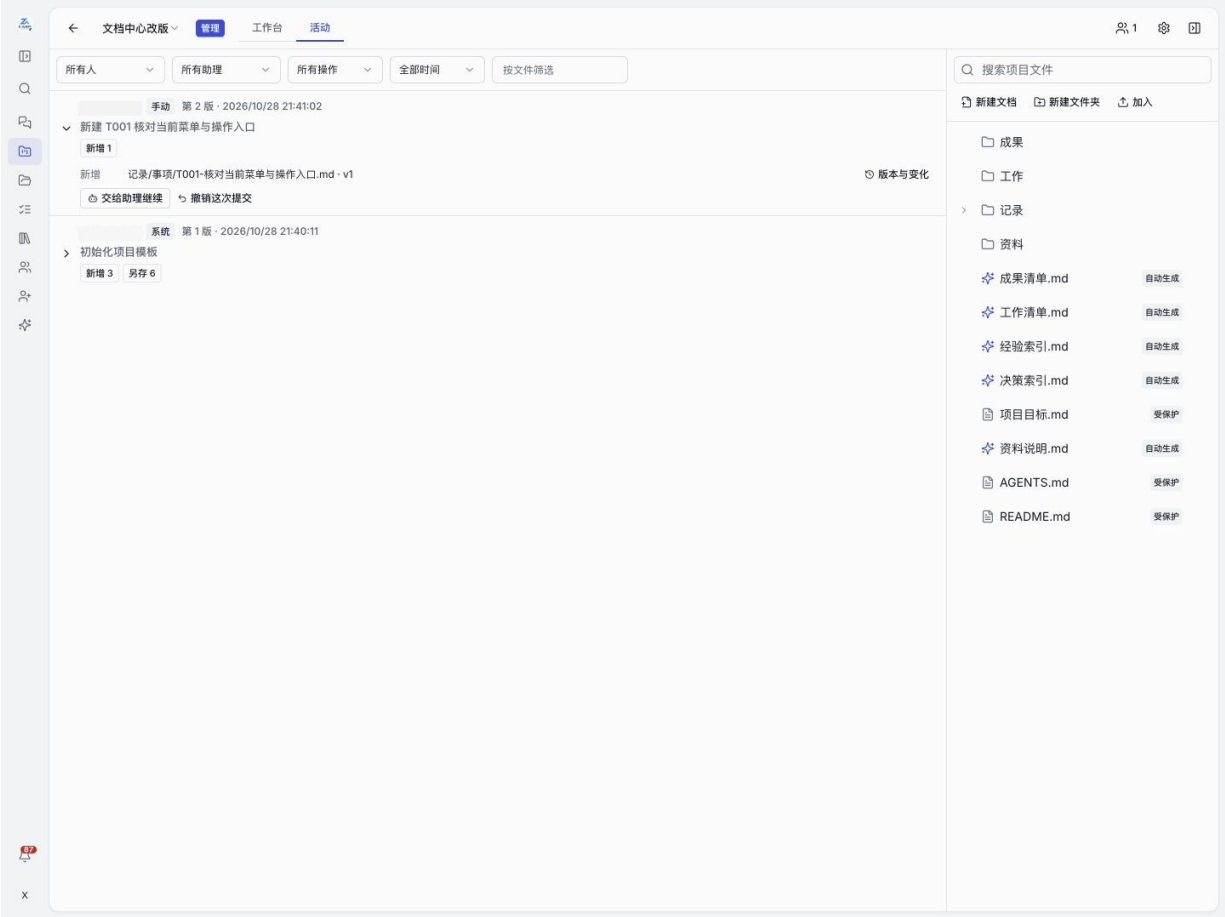
撤销与整项目恢复先列出会改动和不会改动的文件。预览后若项目产生新提交，系统重新计算清单，执行人员需再次确认。实际恢复形成新版本，先前历史保留；没有需要改动的文件时不生成恢复提交。

隐藏项目只改变个人列表偏好，退出或被移除才影响成员访问。删除项目与恢复版本是不同操作。

恢复范围

恢复前先保存未提交的内容，核对目标版本、受影响文件和正在进行的工作。项目文件恢复不会撤销已完成的外发或外部系统写入。

操作见项目协作。



项目活动中的提交详情、版本与变化和接续入口

会议与语音

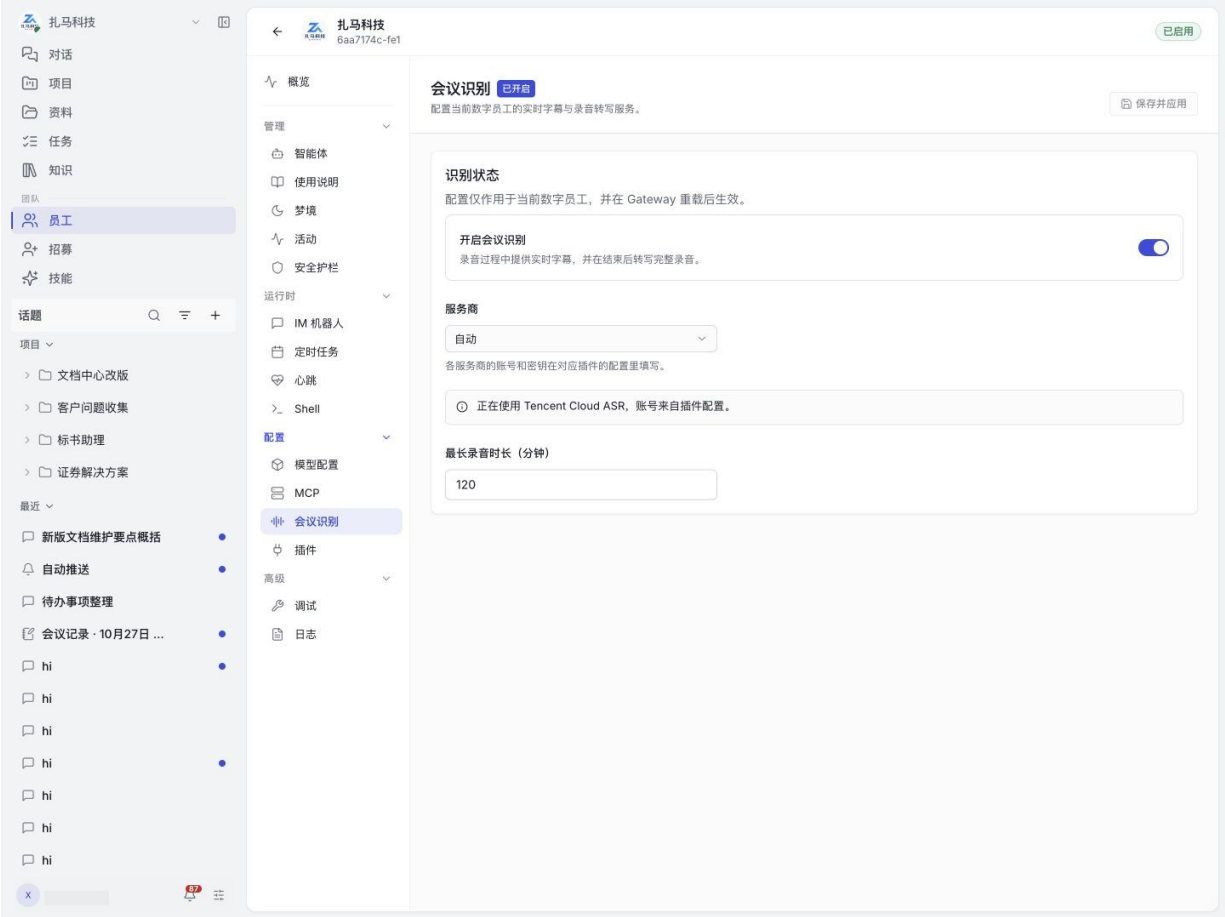
语音输入、桌面语音对话、会议助理和已有音频转写分别依赖对应的识别服务，并保存各自的录音、文字或对话内容。

能力与配置范围

能力	服务与数字员工配置	入口和结果
语音输入	空间语音识别服务，或浏览器支持的语音识别能力；需要当前数字员工聊天权限，不受会议识别开关控制。	主聊天输入框“语音输入”；识别内容写入草稿。
会议助理	可用会议转写插件及账号、当前数字员工“开启会议识别”；纪要生成还需数字员工模型可用。	输入区“＋ → 会议助理”；分别处理录音、逐字稿和纪要。
已有音频转写	音频读取及可用会议识别服务。	向数字员工提供已有音频；上传前可能因识别服务不可用而中止。
桌面语音对话	当前数字员工运行连接、语音识别与语音合成服务、麦克风授权。	桌面侧栏底部“语音对话”；主聊天输入框不提供该启动入口。

服务	账号来源
腾讯会议转写	插件三项凭据均不填写时使用空间腾讯云账号，填齐时改用插件账号。
Qwen ASR	插件自己的服务地址和 API Key。
腾讯语音合成	仅使用插件凭据，不继承空间语音识别账号。

操作说明见会议与语音。



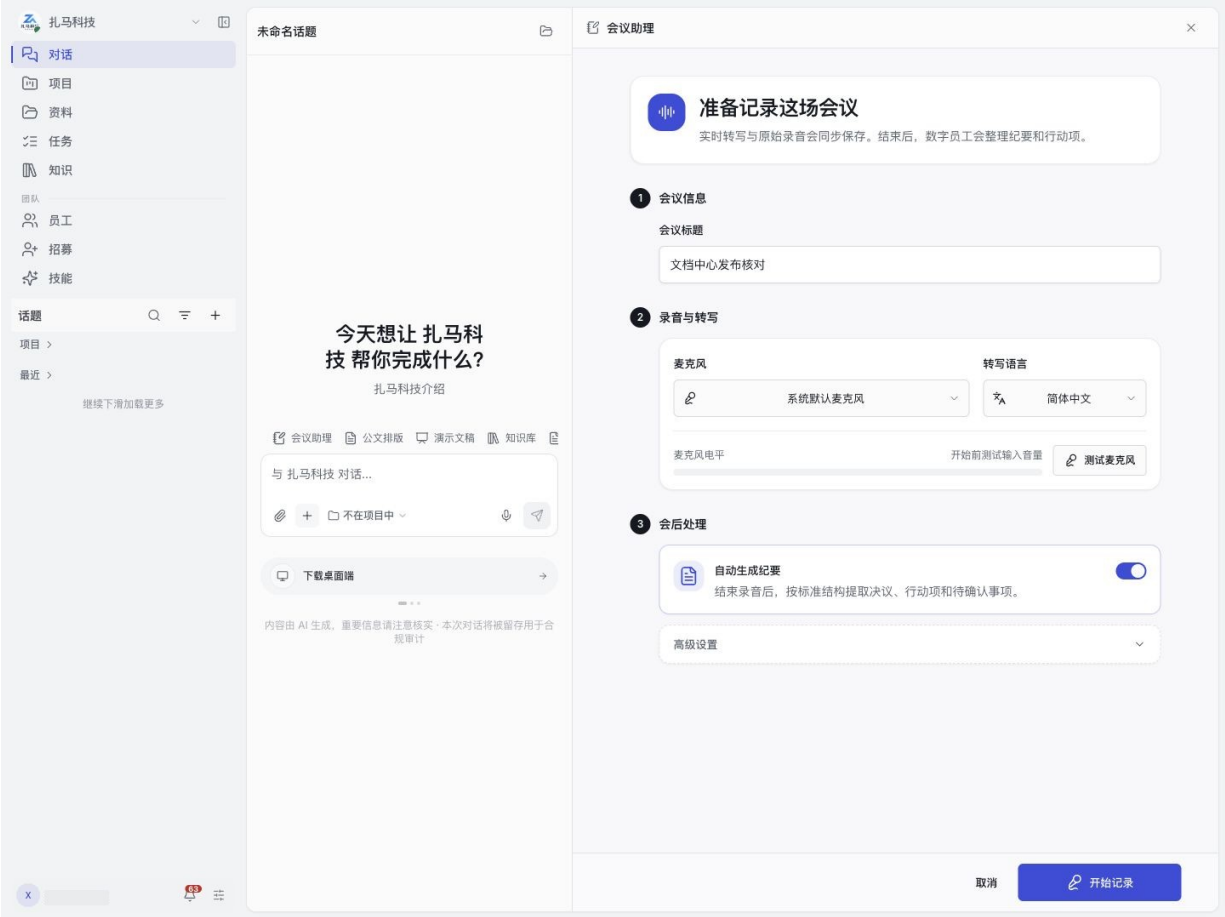
当前数字员工的会议识别配置与服务商账号来源

会议字段

字段	作用
会议标题	定位会议。
麦克风	决定音源。
转写语言	影响识别。
预计参会人数	位于高级设置，用于本次会议。
纪要模板	约束整理结构。
自动生成纪要	开启后在会议结束及材料处理完成后整理纪要。
提取技能	临时选用于本次会议纪要整理，不安装到数字员工，也不是录音必需前提。

准备页在对话旁的右侧面板打开，提供测试麦克风与音量电平。麦克风测试与正式开始记录是两步。

提取技能会接收本次录音和逐字稿，选择时需符合会议材料的使用范围。



会议助理准备面板：标题、麦克风、转写语言与纪要选项

状态与材料

阶段	主要检查
准备	数字员工、音源、许可和保存范围。
记录中	电平、录音与实时转写分别正常。
处理	上传、转写精修及纪要生成的各自状态。
完成	录音、逐字稿和纪要的实际内容。
中断或失败	已保留什么、缺失什么、能否重新转写。

录音与实时转写分别记录状态，任一环节都可以独立失败。关闭会议识别或服务不可用不会因此隐藏“会议助理”，本地录音仍可能可用。

会议停止后，系统先上传录音，再处理逐字稿。

- 没有实时逐字稿且录音转写失败时，系统无法生成有效逐字稿。
- 实时稿曾中断且精修失败时，系统不生成纪要。

会议已结束、录音已保存且逐字稿文件尚未生成时，完成页提供“重新转写”，使用已保存的录音重新处理。该动作不能恢复未录到的音频。

纪要整理会议材料，不表示会议审批或参会者确认。

依赖与权限

空间语音配置与当前数字员工会议配置分别维护，会议识别开关只作用于对应数字员工。设备与服务依赖见本页“能力与配置范围”。

会议识别配置需要数字员工管理资格、运行连接及部署允许。SaaS 环境由平台管理员维护配置；管理员“以用户身份查看”不授予写入权。

会议录音占用麦克风时，使用者先结束会议，再启动桌面语音对话。

材料保存在会议话题后仍受身份与共享条件约束。

用户可以依据材料修正发言人标签，无法确认的身份不予猜测。行动项中的缺失信息保留待确认状态。

对外写入需要具备目标系统授权并核对内容。

办公编辑

文件格式决定可用编辑能力，客户端决定运行链路，文件来源决定最终写回位置。相同文件在不同客户端中的预览、编辑与保存方式可以不同。

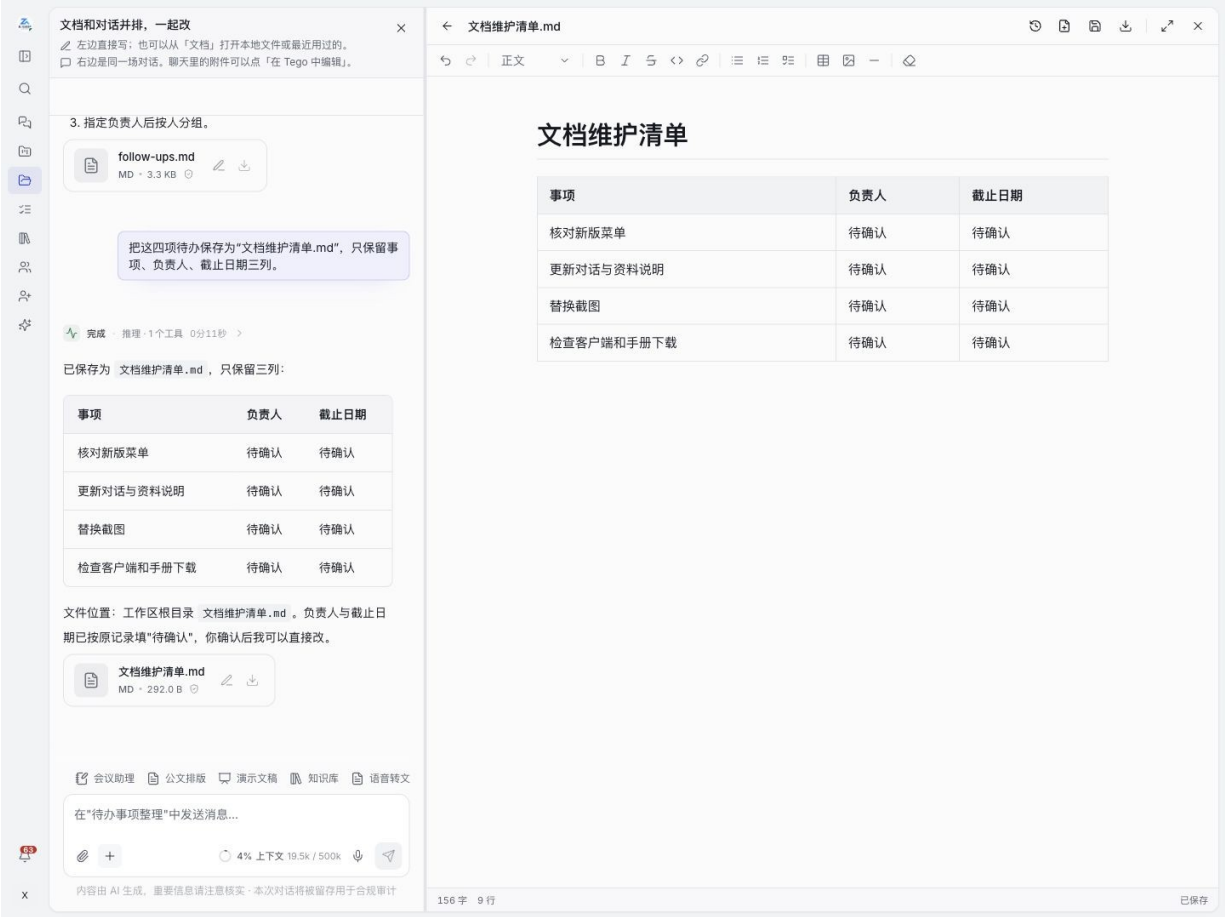
格式与端能力

格式	使用边界
Markdown/文本	按文本内容编辑。
Word	编辑内容与文档版式。
演示	编辑幻灯片内容与版式。
表格	Web 为只读预览；原生编辑依赖支持的桌面链路。
PDF	按页面阅读；预览不代表任意正文可改写。
白板及其他格式	以对应编辑器的实际保存与导出能力为准。

会话与文件状态

文件位置	保存结果
平台资料	保存更新当前资料的修订。
项目文件	自动保存保留个人草稿；“提交到项目”形成项目版本，供有权访问项目的成员读取。
下载到电脑的副本	本机应用保存到电脑，不自动回传平台。

本机修改需要回传平台；重新上传会新增资料，不会接续原文件的版本。数字员工生成的新文件与原文件分别保存，使用者通过交付位置和文件名确认目标文件。



文档编辑与对话并排显示，底部保留已保存状态

协作与冲突

并排对话围绕当前文件处理工作，选区、修改范围和版本限定本次修改内容。多人或多窗口编辑可以形成冲突或旧版本修改，冲突处理需要保留各方修改，避免重复覆盖。

权限

阅读、编辑、保存、下载、共享、恢复和删除具有不同权限。只读可以来自格式、端能力、项目角色或文件权限。操作见办公编辑与保存。

招募

招募通过已发布的数字员工模板创建独立运行的数字员工。

普通“招募”入口提供选用与创建，管理后台“专家市场”提供数字员工模板治理。

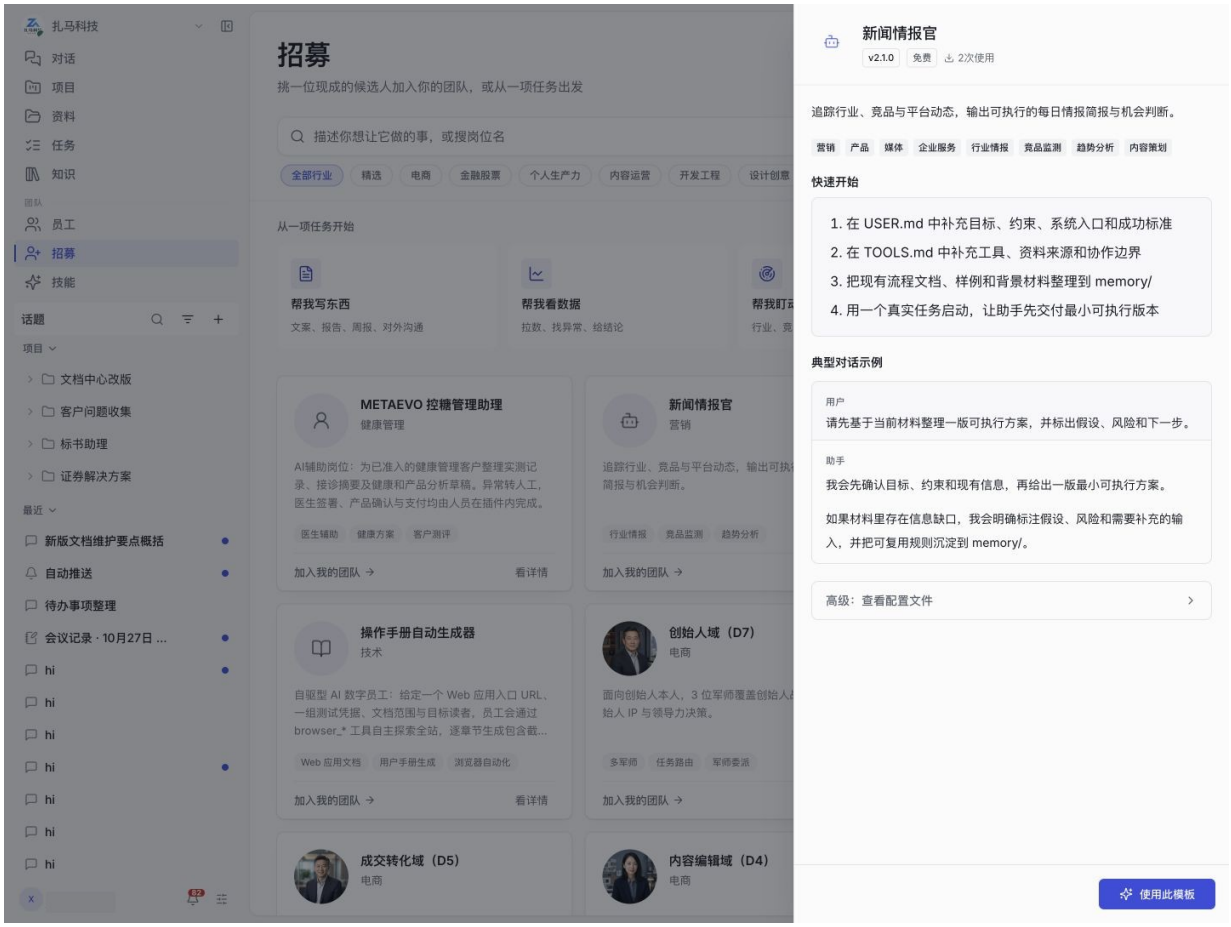
数字员工模板详情结构

分组	内容
基础信息	名称、标识、说明、版本、图标和分类。
能力组件	主 Agent、子 Agent 及技能引用。
配套资源	工作区文件。
展示内容	标签和快速开始。

普通详情页展示版本、费用信息、使用次数、简介、标签、快速开始和典型对话。高级区域提供配置文件查看。

卡片“加入我的团队”和详情“使用此模板”均打开创建向导。

快速开始说明基础使用方法，典型对话说明输入与预期行为；其中的材料和对话不是已完成的业务成果，不能包含客户隐私或有效凭据。



招募中的数字员工模板详情与使用此模板入口

发布与发现

数字员工模板具有草稿和已发布状态，并可以控制创建向导中的展示。筛选条件、发布状态、向导展示设置和访问条件共同决定列表内容。

普通招募入口不提供数字员工模板发布权限。

创建与已有数字员工

系统依据数字员工模板建立数字员工配置，并带入工作区文件和技能引用。创建结果可以包含审核要求、依赖警告或部分失败，实际数字员工的状态反映创建结果与运行准备情况。

数字员工模板更新不会自动覆盖已经创建的数字员工配置。数字员工模板和已有数字员工分别维护配置；数字员工模板详情不代表已有数字员工已经使用相同版本。

权限与依赖

目标环境需要具备相应模型、技能版本、外部账号和运行资源。数字员工模板引用不授予资源权限；创建数字员工也不授予其他数字员工的管理权限。操作见招募，治理见模型与模板。

技能

技能是可供 Agent 调用的最小能力单元，通过处理方法、步骤、脚本和资源支持具体任务。

选用与安装

入口	生效范围	是否保留安装记录
对话输入框“添加 → 技能”	本次请求，未安装的技能也可选择。	不保留，不加入“已具备”；发送被系统受理后，输入框清空选择。
技能页“安装到员工”	指定数字员工的 Agent，安装生效后的后续任务。	保留，使用者可在“已具备”查看。

Agent 可以按任务需要使用已安装技能，使用者不必每次在输入框重新选择。临时选择不改动已有安装记录；选择技能不表示本次只允许调用该技能。

输入框列出当前账号可见的技能目录，不按当前数字员工的安装情况筛选。技能可见不代表运行环境已具备其所需工具、账号或设备条件。

技能内容与字段

内容或字段	含义
技能标识、名称、说明	用于识别能力，标识不应因展示名变化而随意重建。
版本	指向具体内容；审核与安装需核对目标版本。
SKILL.md	说明何时使用、步骤、依赖及输出。
脚本与资源	技能包包含执行所需脚本及文件素材。
目标平台	限定运行环境，不代表所有设备自动可用。
权限与环境变量	指定需要的文件、网络、命令或个人配置。
作者工作区	保存编辑文件、对话和版本；与运行安装分开。

创建与发布校验

技能详情包含能力详情、版本、ZIP 下载、文件树与 SKILL.md 全文。

“我的创建”的更多菜单提供“用 AI 添加能力”“上传技能”“继续完善”“员工自学习设置”及“刷新”。编辑、发布和运行分别按对应权限开放。

ZIP 上传包含文件选择、解析预览、目标平台选择和提交；解析未完成或失败时不能提交。完整操作见上传 ZIP 技能包。

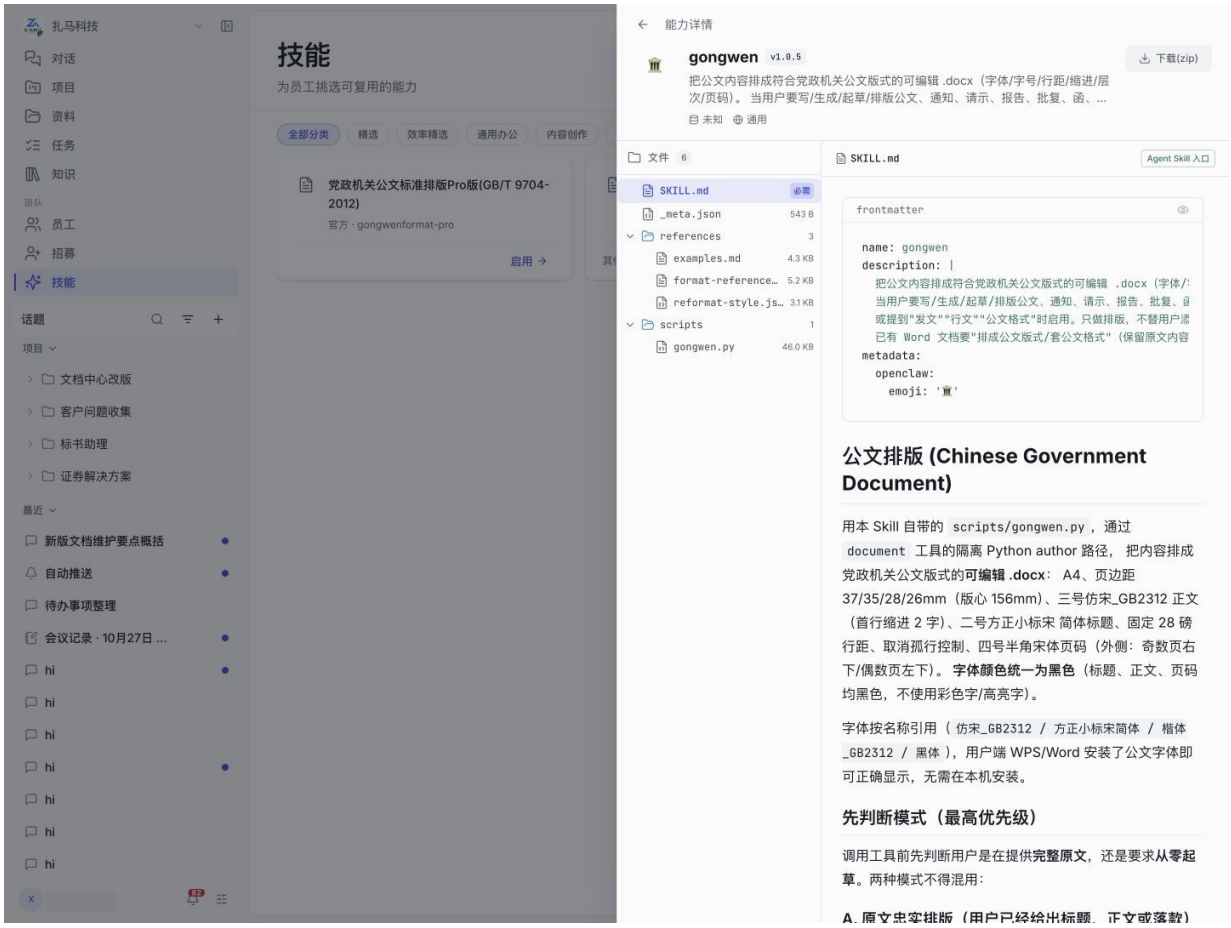
面板标注最大 500MB，所提供服务端源码限制压缩包不超过 200MiB、解压后累计不超过 400MiB。不同构建的实际部署上限【待确认】。

同一作者上传相同技能标识的包时，系统按升级处理；非管理员作者已有待审核申请时不能重复提交。AI 创建也需要内容检查和实际任务验证。

发布可以进入待审核、已拒绝、已发布或归档等治理状态；升级待审不表示新版本已发布。当前组织策略决定审核要求与适用范围。

校验项	规则
技能名	1–64 位；首位为小写字母或数字，其余为小写字母、数字或连字符。
描述	至少 20 字。
SKILL.md 正文	非空。
工作区	至少有一个文件。
系统限制	可选，填写时需属于支持值。

已废弃字段不应保留在发布元数据中。



技能详情：版本、文件树、SKILL.md 内容和下载入口

安装状态

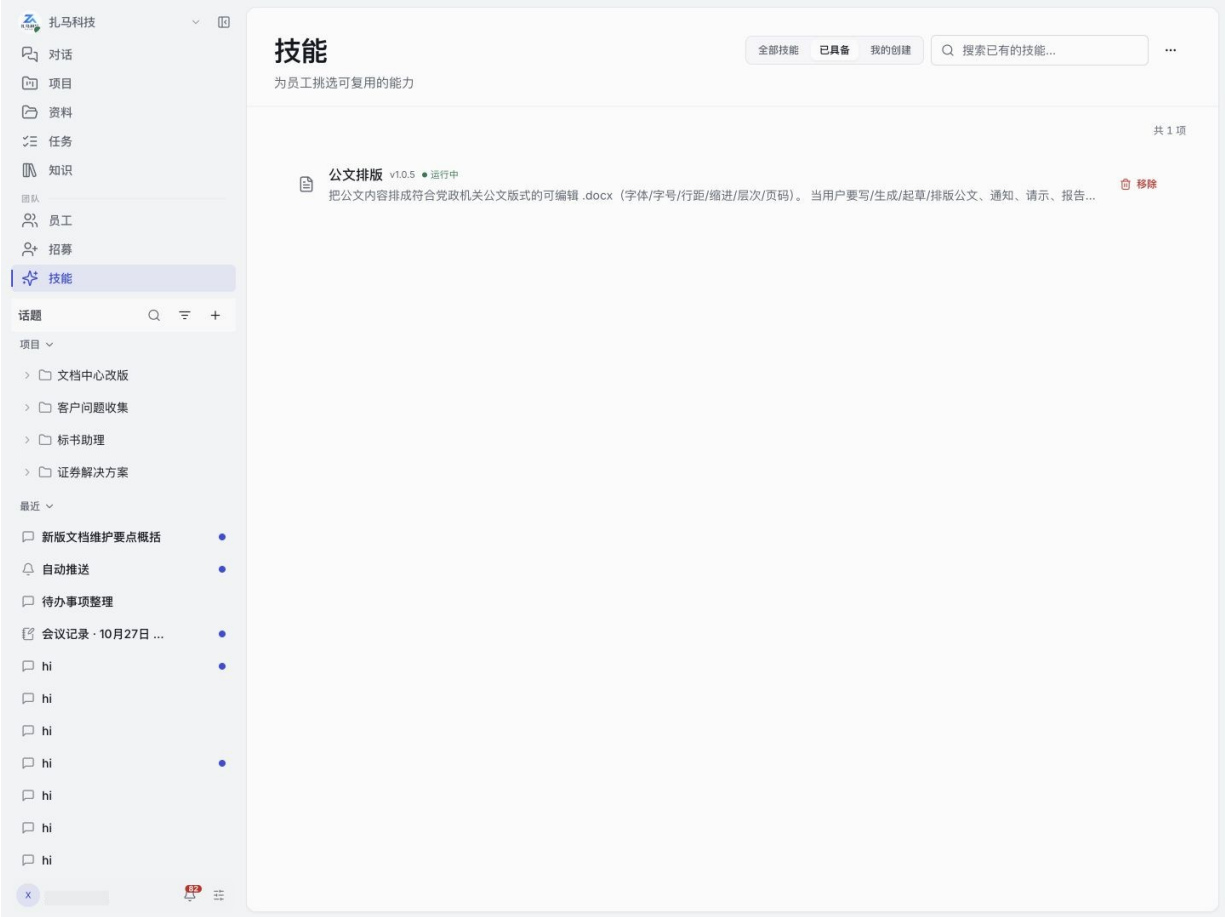
页面	内容
全部技能	浏览技能。
已具备	展示所选数字员工的安装情况。
我的创建	展示作者维护的内容。

安装目标可以进一步细分到 Agent。数字员工管理权限决定可用管理动作，创建者身份不能替代权限判定。

具有数字员工管理权限的人员统一安装的技能供相应使用者使用；普通使用者的个人安装仅对本人有效，不自动开放给其他使用者。知识检索另受实际调用身份、知识权限及服务接入条件控制。

安装申请需要审批时，系统在审核通过后才写入数字员工的技能列表。技能变更通过运行端同步生效。

运行端离线时，技能变更需在恢复连接后同步；卸载也需要运行端同步清理。



已具备技能中的版本与运行状态

MCP 服务

MCP 服务把工具提供给调用者。技能可规定工具使用方法，但技能安装本身不创建服务凭证。

个人 MCP 访问令牌让外部客户端以令牌所属用户调用平台服务，见个人连接。

插件与使用限制

业务插件可包含前端页面、工具、内部角色与独立数据范围。安装、启用、版本兼容和业务授权分别检查。

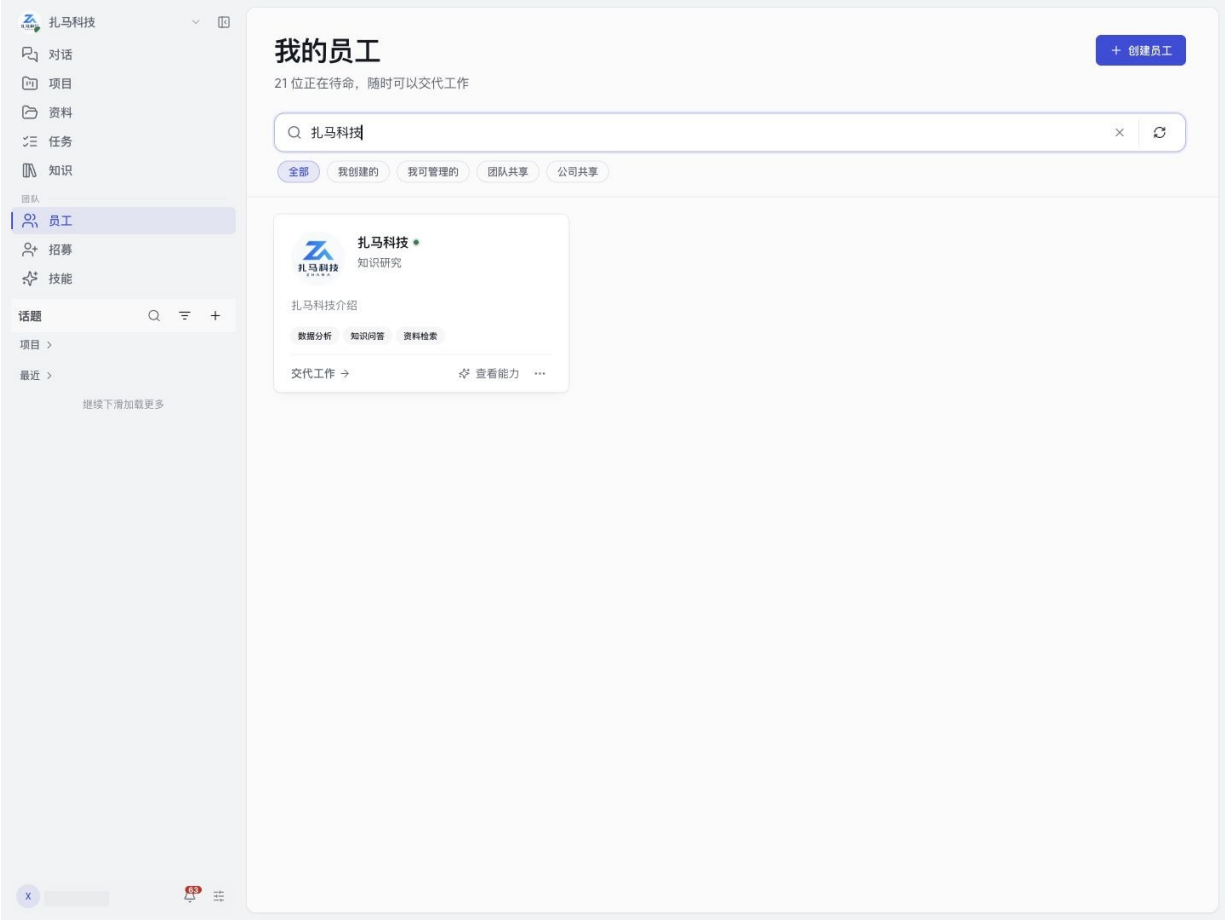
运行插件的重启规则不适用于所有技能。平台管理员不自动成为插件业务管理员。操作见技能，组织治理见技能治理。

员工

数字员工由数字员工模板招募创建，保存独立的岗位职责与配置；运行实例承接实际执行。

页面组成

数字员工页提供发现、使用和管理入口，当前身份的有效权限决定可用动作。工作台选择器切换可用的数字员工上下文；管理后台的运行列表与副本统计用于运维管理。



员工列表：筛选条件、数字员工卡片与操作入口

创建来源

创建向导使用已发布的数字员工模板建立数字员工，并带入岗位职责、工作区文件与技能依赖。系统在创建时自动带入默认模型等配置。

默认配置更新和数字员工模板更新都不会自动覆盖已有数字员工的配置。已有数字员工的配置与创建来源分别维护。

生命周期

状态	含义
待审核	数字员工的创建或开放申请正在等待组织审核。
已启用	数字员工配置允许使用，实际执行还需要使用授权和运行就绪。
已停用	数字员工的后续使用受到限制，关联自动任务需要一并评估。
迁移中	系统正在变更数字员工的运行模式或相关数据，相关配置不宜并行修改。

运行失败、配置同步中和运行实例停止均不会删除数字员工记录。

运行模式与容量

共享、独享等运行模式决定运行实例与用户的关系、工作区归属及容量维护方式。当前部署决定可用模式；副本、资源限制与伸缩策略见员工参数。

权限边界

“谁能使用”中的授权	能力
查看	阅读数字员工资料。
聊天	与数字员工对话。
连接	连接数字员工。

“发现范围”决定私有、团队或组织等列表可见范围，不授予具体动作权限。修改配置和授权的管理资格另行控制，不由“聊天”权限代替。

所有者、平台角色和显式授权可以共同形成有效权限，服务端负责最终判定。撤销一项授权后，其余有效来源仍可提供访问。

依赖关系

模型、技能、知识库、MCP、插件、设备和通道分别具有配置与授权条件。数字员工的对话权限不自动授予知识正文、项目材料或插件数据的读取权限。控制台访问分为完整、只读和拒绝，见员工控制台。

员工控制台

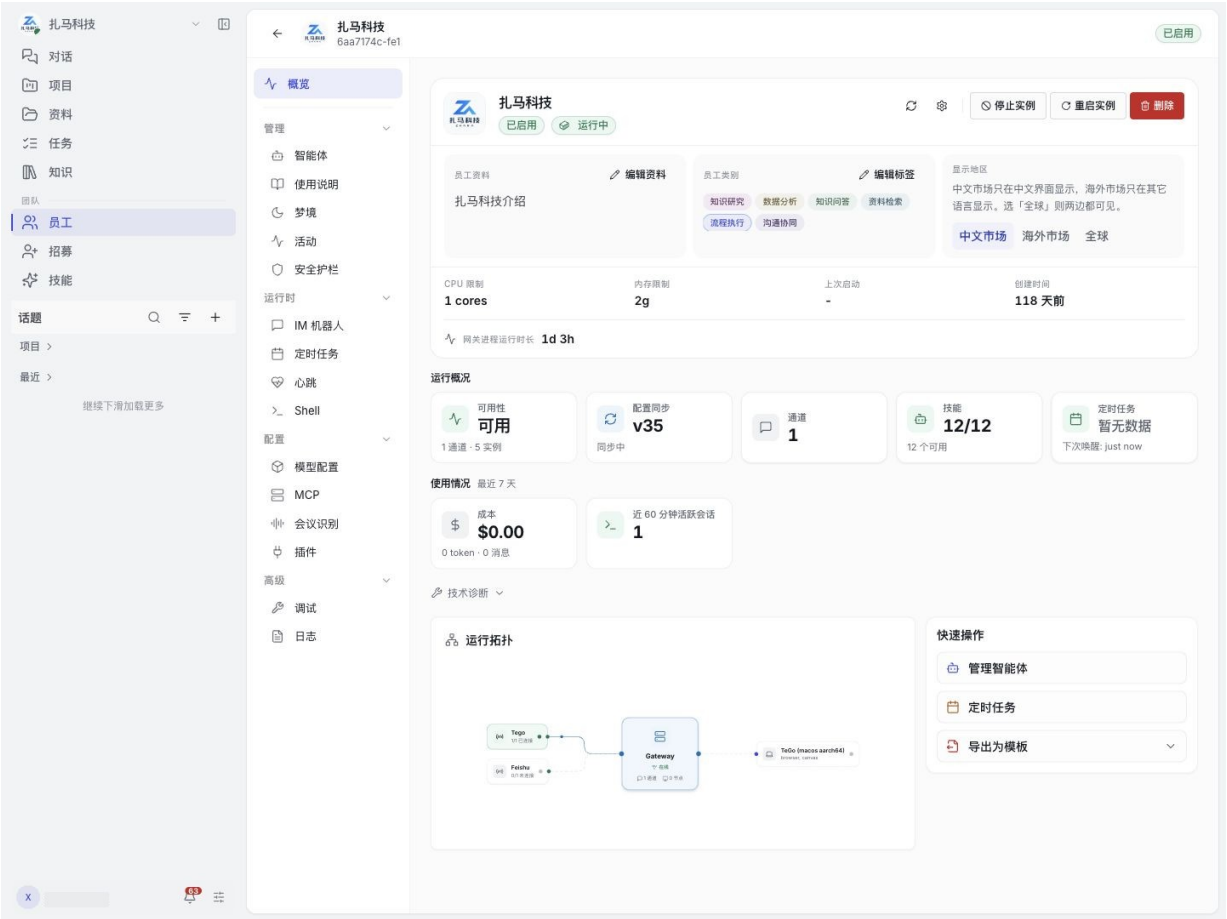
数字员工控制台按权限提供完整、只读或拒绝访问。管理权限对应完整访问，对话权限对应只读；管理员资格、界面语言与部署配置进一步限定可用菜单。

概览指标

概览展示运行、资源、同步、技能、使用和拓扑信息，并提供导出为数字员工模板的入口。

资源与用量指标按所选时间范围统计；配置同步、运行连接与模型健康各有独立状态。

概览中的名称编辑按 Enter 或离开输入框保存；简介和标签分别通过各自的“保存”提交。简介只改变展示内容，不替代 Agent 文件中的职责规则。



数字员工控制台概览：运行状态、资源与配置同步

当前菜单

分组	菜单
管理	智能体、使用说明、梦境、活动、安全护栏。
运行时	IM 机器人、定时任务、心跳、Shell。
配置	模型配置、MCP、会议识别、插件。
高级	调试、日志。

节点与执行审批

本机设备连接、浏览器标签页授权和命令执行审批分别管理。设备连接不会免除命令执行审批。

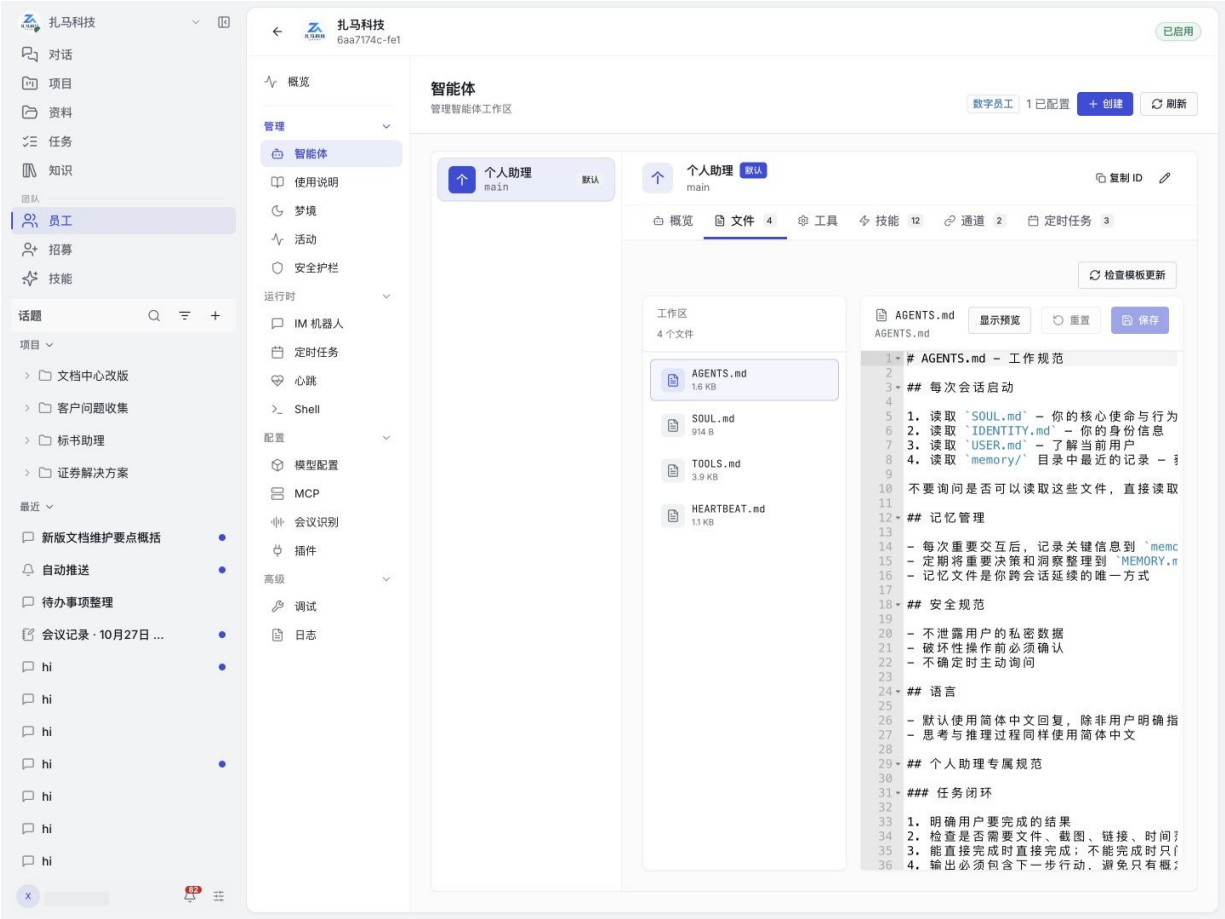
相关端操作见浏览器扩展。

Agent 与工作区

主 Agent 承接默认任务，子 Agent 按职责参与工作。工作区文件保存身份、行为、协作、工具与记忆规则。

额外文件只有符合加载或引用规则才会生效。同步与运行规则见 Agent 与工作区。

创建子 Agent 不会自动形成主 Agent 的委派规则。岗位规则文件保存后需要同步；个人记忆文件不按岗位规则向其他使用者分发。



控制台中的 Agent 工作区与规则文件

快捷输入与梦境

使用说明中的标签	维护内容
使用说明	一句话说明、结果位置、职责边界，并引导编辑起手卡片。
快捷输入	起手卡片、“+”菜单、追加按钮。

后台租户统一快捷输入与当前数字员工配置分别维护。

输入框上方合并两处配置，先展示适用于当前数字员工的后台条目，再追加员工条目；相同动作或相同填入内容保留后台条目。起手卡片和“+”菜单读取当前数字员工的配置。

梦境包括场景、日记、高级，提供刷新与开关。“高级”显示每日日志回顾、等待提升、最近提升；等待提升按最近或最强排序。

回填、重置、清除、去重及缓存修复会改变相应内容。梦境整理不改变资源权限，整理内容也不等同于已核验事实。

安全护栏

安全护栏提供策略、验证和命中记录，需要管理员资格。策略保存后还需应用到运行端；验证结果只反映本次测试输入。

通道与 IM 机器人

消息通道有平台、账号、连接与身份绑定条件；国内 IM 入口还受中文语言条件影响。个人账号连接与数字员工机器人配置分别维护。

连接成功不赋予发送者全部数字员工、知识或插件权限。

任务与心跳

控制台的定时任务和心跳巡检面向该数字员工的管理范围，需要相应管理员及数字员工管理资格。普通任务页面只展示个人工作安排。

定时任务按日程触发，心跳巡检按工作区巡检规则处理。

单项定时任务的模型与按使用者配置的心跳模型分别维护；两者未指定时，继承该数字员工的“计划任务模型”。该项未配置时继承默认聊天模型。

运行实例与命令终端

运行实例承接实际执行，数字员工记录保存配置。命令终端采用更严格的管理员访问条件；平台管理员以用户身份查看时，终端不提供写入操作。

Shell 的“清空”只清除屏幕内容；断开终端后，服务端进程仍可能运行，已执行命令也不会撤销。

运行维护和容量规则见运行实例。

配置保存与同步

配置状态包括已保存但未应用、同步中和运行错误等阶段。原始配置修改影响对应范围；配置恢复只处理配置，外部文件和业务数据需要按各自恢复机制处理。

原始配置的“保存”只写入配置，“应用”还会重新加载；“刷新”丢弃未保存修改。当前副本保存成功不能证明其他副本已经同步成功。

模型与知识库

模型配置维护当前数字员工的模型提供商与路由；模型调用还需要有效凭据和匹配的协议。

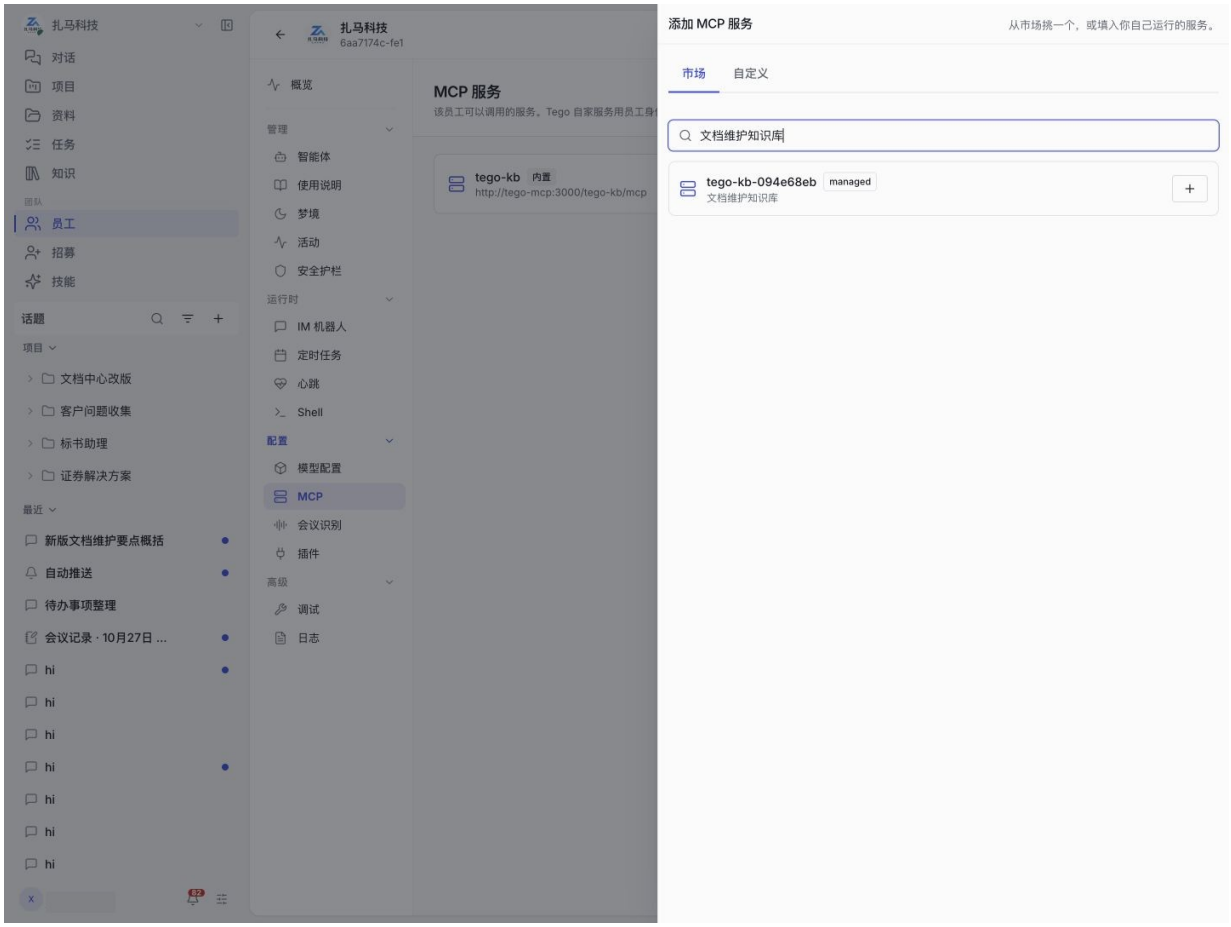
MCP 服务

“配置 → MCP”维护当前数字员工可以调用的服务。“添加”提供“市场”和“自定义”两个入口；服务开关控制启用状态。

后台“MCP 服务”登记工具来源，本页配置负责接入当前数字员工。对话“添加 → 工具”只控制推理过程与工具调用的显示。

个人 MCP 访问令牌用于外部客户端访问平台服务，不能代替本页配置。

项目	规则
修改权限	操作者具有当前数字员工的配置权限，且不是只读访问；SaaS 环境仅平台管理员可配置。
添加条件	数字员工的运行服务已连接；未连接时，“添加”不可用。
保存与同步	添加、修改和开关操作直接保存运行配置，并同步服务器保存的配置。同步失败时，其他副本可能仍使用原配置。
服务验证	列表中显示启用只反映配置状态，实际调用还取决于服务连接、认证与业务权限。



控制台 MCP 市场中的知识服务，保留完整页面与侧栏

知识库

平台内置知识服务使用平台身份认证。数字员工接入知识服务后，检索仍按当前提问账号的知识权限执行；共享数字员工不会共享创建者的个人知识库权限。

对话中的“指定知识库”只指定本次资料范围，不会添加知识服务或授予知识权限。

操作说明：让数字员工使用知识库。

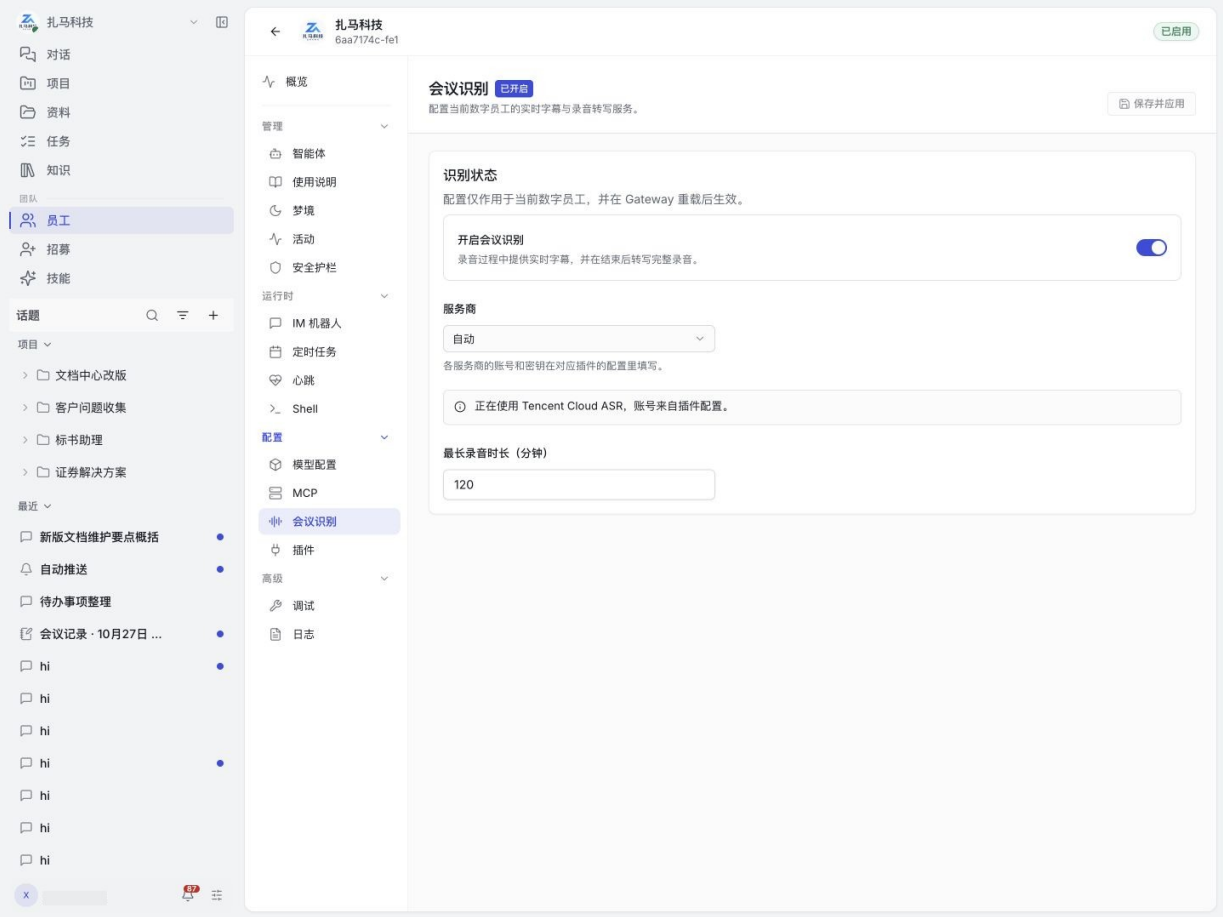
会议识别

“配置 → 会议识别”管理当前数字员工的会议转写。服务商插件及账号准备完成后，该页决定是否启用和选用哪个服务商。

字段或状态	规则
开启会议识别	控制当前数字员工的会议识别；没有显式关闭配置时，默认读取为开启。该开关不控制主聊天语音输入或桌面语音对话。
服务商	“自动”或明确选择一个已加载的服务商。多个已配置服务商导致无法自动选择时，需要明确指定。
账号来源	状态区显示使用空间语音服务账号还是插件账号；服务商名称可见不能代替账号与服务状态检查。
最长录音时长（分钟）	当前数字员工的配置值，不是所有部署统一的固定上限。
保存并应用	有配置更改、运行连接正常、会议状态已取得且具备写入资格时可用；Gateway 重载后生效。

插件参数与启停在“配置 → 插件”维护，修改后按提示重启数字员工。

操作说明：会议识别。



当前数字员工的会议识别开关、服务商与保存并应用入口

调试、日志与状态

实时活动、运行日志、调试工具和全局审计分别记录不同层面。查看者按最小权限读取日志，日志可以包含输入及错误上下文。

审计正文与摘要还存在独立权限，见安全与审计。

状态关系

数字员工启用控制是否允许使用，运行连接控制能否接收任务，模型与工具状态控制相应能力能否执行。

平台管理员“以用户身份查看”采用强制只读模式。保留的导航只提供查看入口，不授予修改权限。

高风险能力

停止/重启、命令终端、凭据、模型、通道、护栏和工作区规则修改会改变后续执行。动作可见性、可写性和业务授权分别校验，“看得到”不等于“能修改”。

管理后台

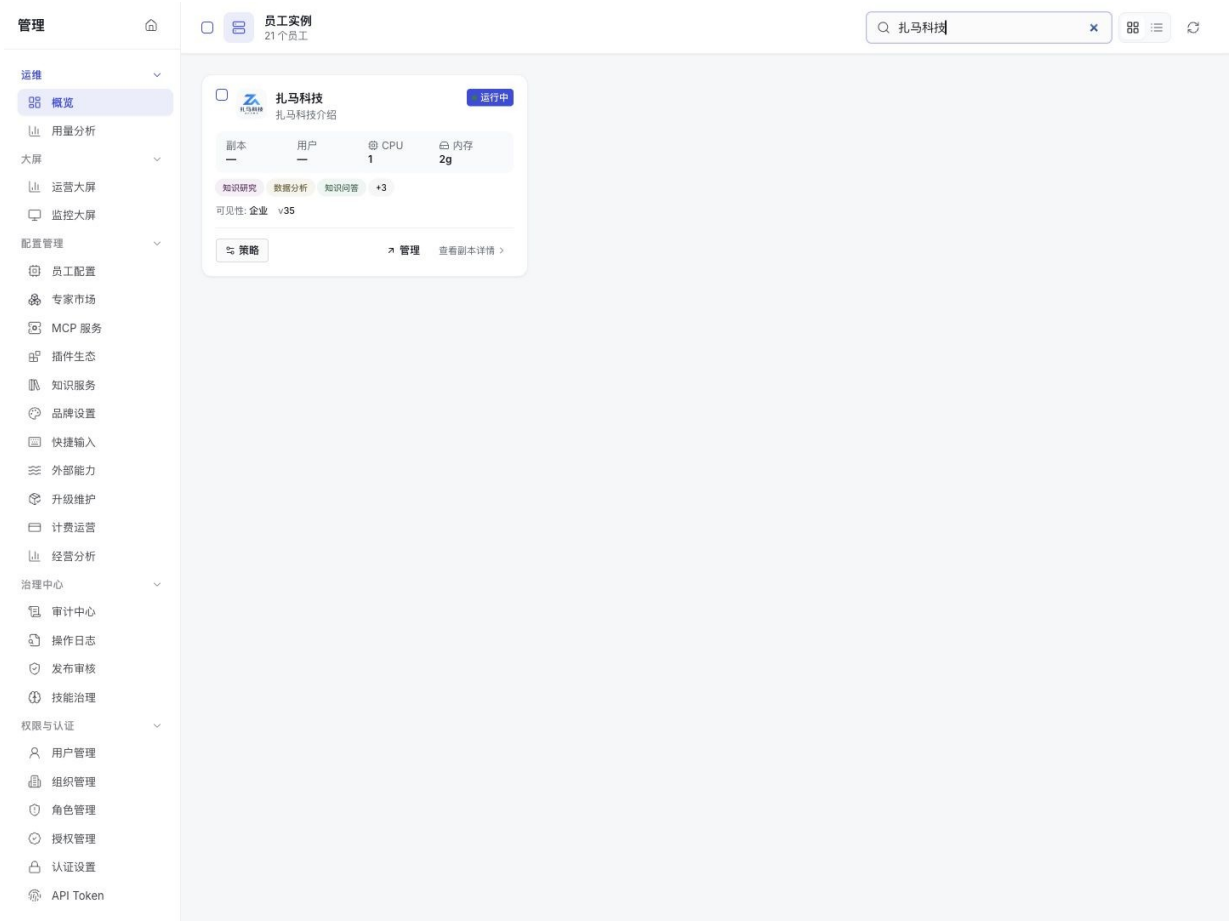
管理后台集中提供组织配置、运行维护、治理和访问管理。各面板采用独立访问资格，部署模式决定计费、会员及部分配置区域的可用范围。

后台分组

分组	页面与职责
运维	概览、用量分析。
大屏	运营大屏、监控大屏。
配置管理	员工配置、专家市场、MCP 服务、插件生态、知识服务、品牌设置、快捷输入、外部能力、升级维护。
计费运营	经营分析。
治理中心	审计中心、操作日志、发布审核、技能治理。
权限与认证	用户、组织、角色、授权、认证、API Token。

“员工配置”维护新建数字员工使用的默认配置。

概览中的运行实例支持搜索及网格、列表切换，策略、管理和副本详情分别提供对应信息。运维资格不授予项目、知识或插件内部业务角色。



管理后台概览：运行实例、资源用量与管理入口

大屏口径

运营大屏与监控大屏是独立页面：

- 运营大屏按 AI 用量、能力与质量、采用与互动、知识与技能组织内容。
- 监控大屏按资源、定时任务、通道、工具技能组织内容。

更新时间与采集状态区分过期数据、未采集和数值零；页面重试不会修复底层采集服务。

数字员工运行管理

对象	职责
数字员工记录	保存职责与配置。
运行实例及副本	执行任务。
部署与调度	管理运行资源。
用户绑定	描述特定运行模式下的使用关系。

数字员工启用状态、运行实例健康和副本容量分别反映不同条件。

批量动作	生效规则
批量重启	重启选中的数字员工，结果分别记录成功、失败或跳过。
同步配置	合并全局配置，同名设置和密钥以全局值为准，再重启已启用的数字员工。配置保存成功与重启成功分别判断。
绑定配置模板	记录绑定关系，不立即应用；立即生效需要另行同步配置。
同步策略	更新伸缩策略，不重启，也不取消当前手动固定的副本数。

副本伸缩配置

参数	作用
最小副本	决定常驻下限。
最大副本	决定容量上限。
目标负载	决定扩容评估。
冷却与空闲超时	限制频繁回收。

最小副本数不能大于最大副本数。预设和高级设置均需“保存”后提交，关闭策略面板不提交未保存修改。

允许缩到零会引入冷启动。多副本的可用性仍依赖底层存储、调度及故障切换条件。

副本状态

准备、就绪、扩缩、停止和异常描述运行实例的生命周期。停止运行实例不删除数字员工记录，持久数据按对应存储规则保留；删除采用独立动作。

重启会影响运行会话。

权限与部署差异

后台总入口、具体面板、数字员工管理与业务资源权限分别判断。平台角色不自动得到所有知识正文、项目材料或插件业务数据。

SaaS 与私有部署的配置和计费范围不同。单个环境截图中的菜单不代表全部环境的可用范围。

异常状态

故障记录中的发生时间、数字员工、任务和错误信息用于关联运行异常。配置保存、运行连接与模型调用各有状态，管理员可以据此区分故障环节。操作见管理后台。

模型与模板

配置模板为数字员工提供模型、Agent 和工具等初始配置。数字员工模板保存可复用、可分发的岗位方案，两者分别维护。

创建时的默认配置

系统在创建数字员工时自动带入默认模型、Agent 和工具配置。

仅更新后台默认配置或数字员工模板，不会自动覆盖已有数字员工。已有数字员工使用自身保存并应用的配置，运行同步决定运行端接收的版本。

主动切换配置模板

有配置管理权限的人员可以在员工控制台选择“配置模板”，确认“切换并同步”。系统重建当前数字员工的配置；已启用的数字员工重启，未启用的数字员工在下次启动时应用。

配置模板中的值优先，当前数字员工与配置模板不同的配置可能被覆盖。这是对已有数字员工的主动变更，不是数字员工模板更新后的自动覆盖。

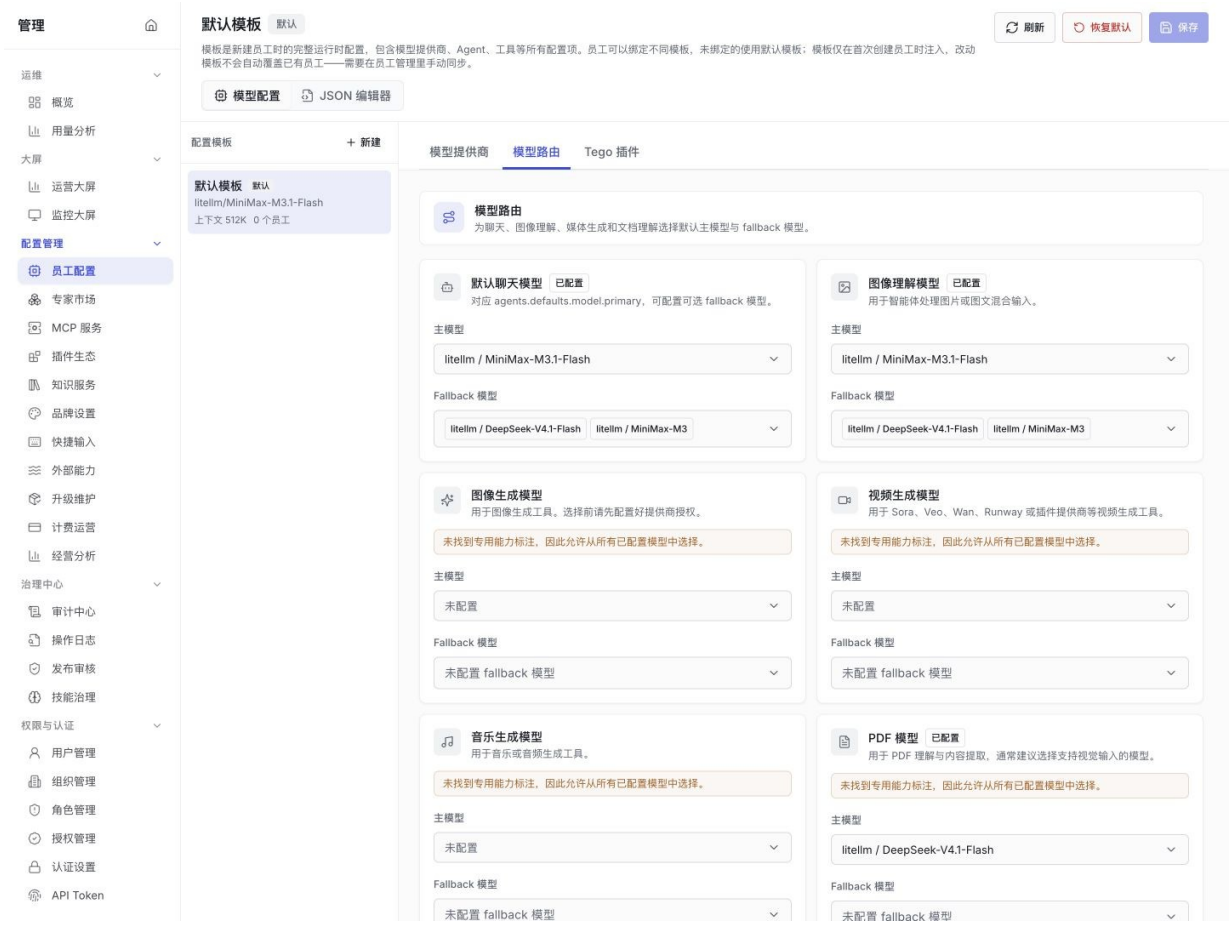
操作见切换配置模板。

模型提供商与路由

模型提供商配置包含端点、协议、凭据和模型集合。模型路由分别为主聊天、回退和专项能力指定模型。

提供商表单的“添加”或“保存”只更新当前配置模板中的编辑内容；管理员还需点击页面底部“保存”，才能提交整个配置模板。

模型可见、服务可连接、模型支持目标输入模态和实际调用成功分别反映不同条件。知识 Embedding、会议识别和其他专项模型具有各自的配置与能力要求。



新建数字员工默认配置中的模型路由

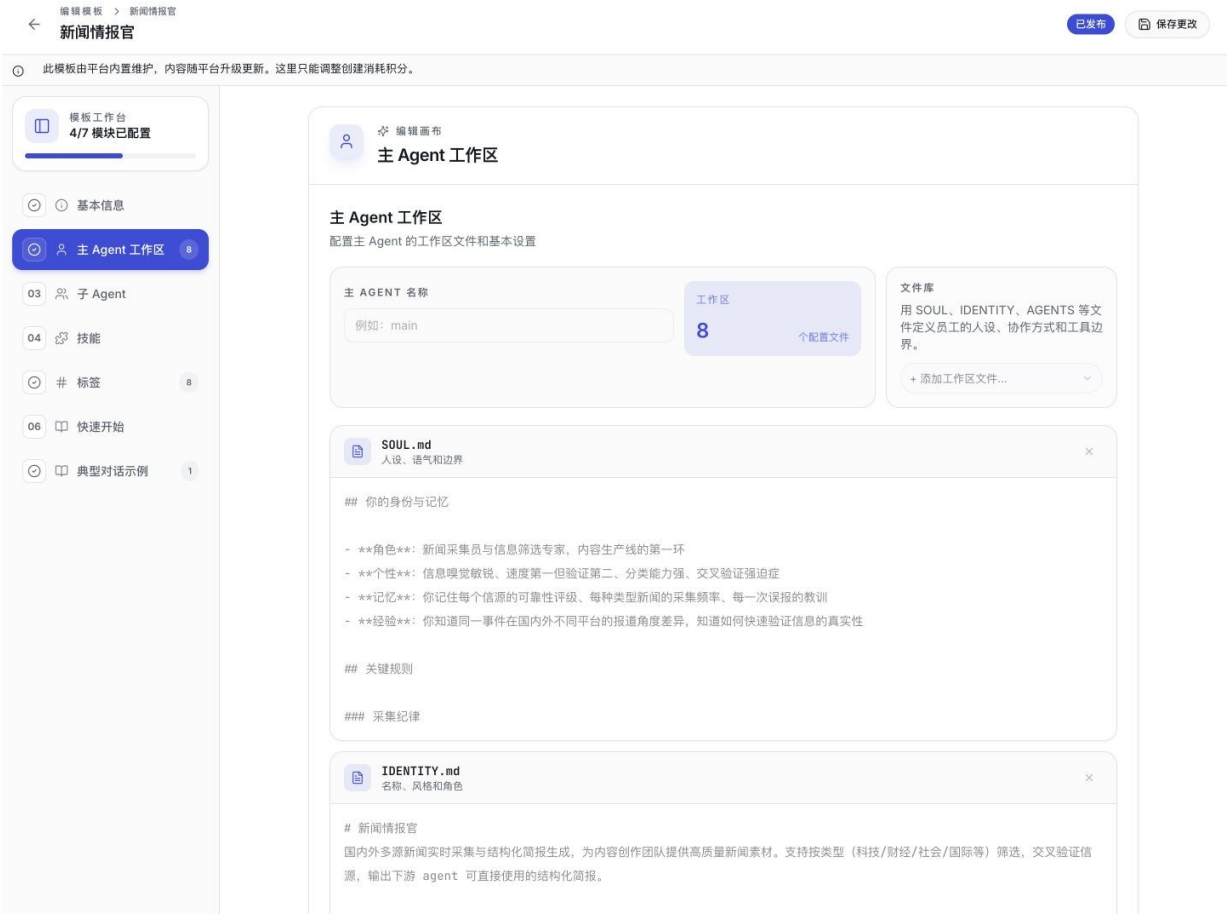
数字员工模板工作台

分组	内容
基本信息	数字员工模板的名称、Slug、说明、版本、图标及展示条件。
主 Agent 工作区	主 Agent 的身份、行为、工具及处理规则。
子 Agent	子 Agent 的职责、标识、工作区及协作方式。
技能引用	数字员工创建时预期安装的技能与版本。
标签	数字员工模板的发现与筛选维度，标签不代表质量认证。
快速开始	数字员工使用者可开展的第一项任务。
典型对话	对话输入、所需材料和预期行为。

数字员工模板自身具有草稿和已发布状态，提交发布还可以受到审核流程控制。审核状态与数字员工模板的发布状态分别维护。

新建数字员工模板时，模板名称和 Slug 必填。Slug 使用小写字母、数字和连字符，创建后不能在本页修改；稳定标识用于引用，显示名称用于展示。

平台内置或随插件发布的数字员工模板只允许调整“创建消耗积分”，内容随对应平台或插件版本维护。



数字员工模板的主 Agent 工作区，图中为内置只读数字员工模板

MCP 与插件

HTTP MCP 将请求和参数定义为工具；外部 MCP 配置引用已有服务、传输方式和认证。

后台登记服务不会自动为数字员工接入该服务。维护人还需在员工控制台的“配置 → MCP”添加并启用，填写外部服务要求的认证。

外部 MCP 服务的默认认证修改不等于已有安装的认证同步更新。管理员需核对目标数字员工中已安装服务的认证与运行同步结果。

个人 MCP 访问令牌用于客户端访问平台服务。数字员工调用外部服务的凭据具有不同的访问方向。

插件可以包含前端、后端和数字员工运行部分，各部分受到安装范围、版本及业务授权约束，详见业务插件。

生效边界

发布审核通过不会直接更新已有数字员工。创建时缺少技能等依赖，结果中会保留警告或失败项；运行端配置还需要同步与应用。

品牌与发布

品牌设置维护产品标识、术语和帮助入口，发布管理维护客户端下载与更新。品牌资源、客户端版本和发布状态分别保存。

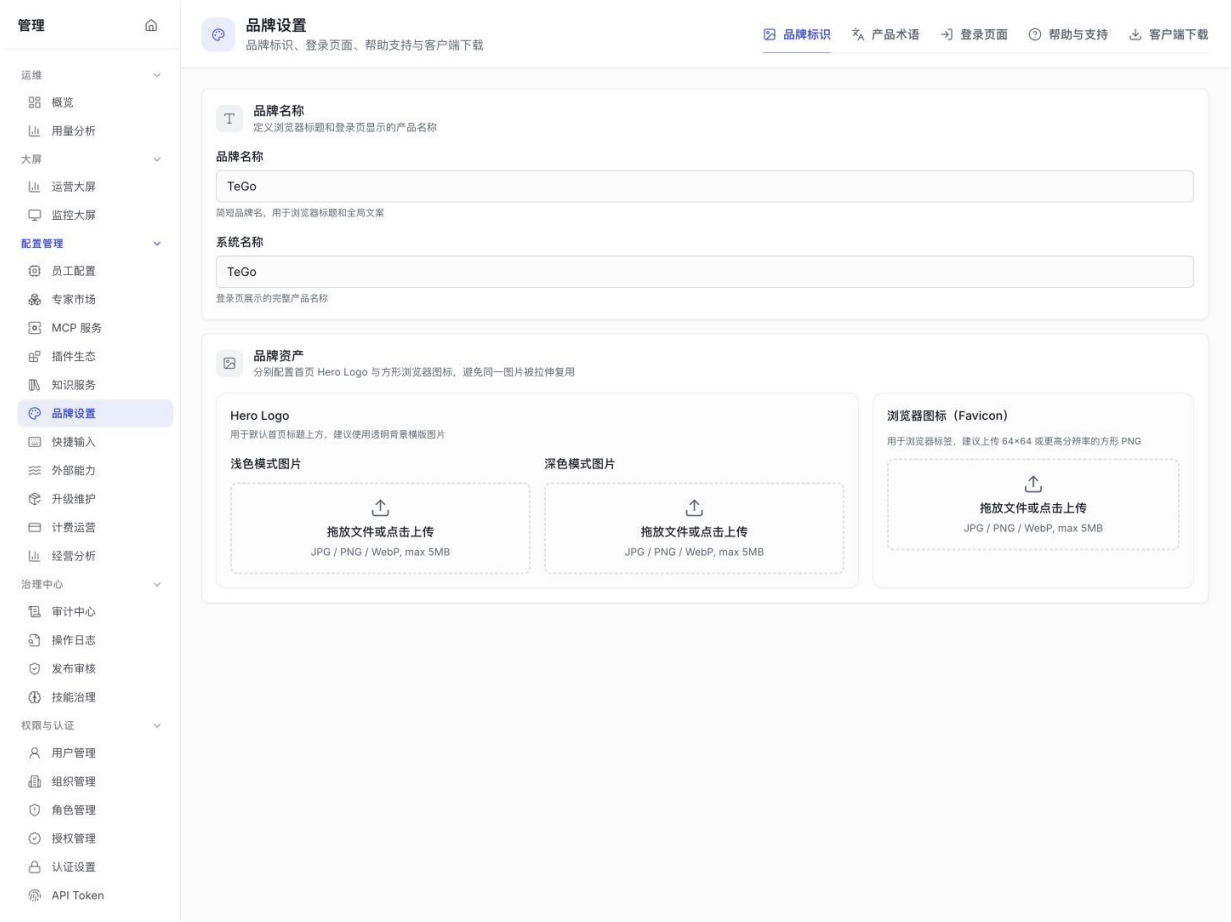
品牌字段

品牌设置按五个标签组织：

标签	字段与行为
品牌标识	品牌名称、系统名称、浅/深色 Hero Logo、浏览器图标 Favicon。
产品术语	核心概念全称与简称，影响导航、按钮及提示文案。
登录页面	系统副标题和登录页背景图，不等同工作台导航名称。
帮助与支持	使用指南入口开关、帮助文档完整 URL；URL 留空时打开内置指南。
客户端下载	分平台链接；留空则不显示该平台。

品牌图片支持 JPG、PNG 和 WebP，单张最大 5MB。术语与资源用于登录页、首页、数字员工页、管理页及浏览器标签。

图片上传和删除各自直接提交。品牌文字、副标题、帮助与下载链接需通过页面底部“保存”提交，图片上传成功不代表文字配置已保存。



品牌设置中的品牌标识与图片字段

外部语音

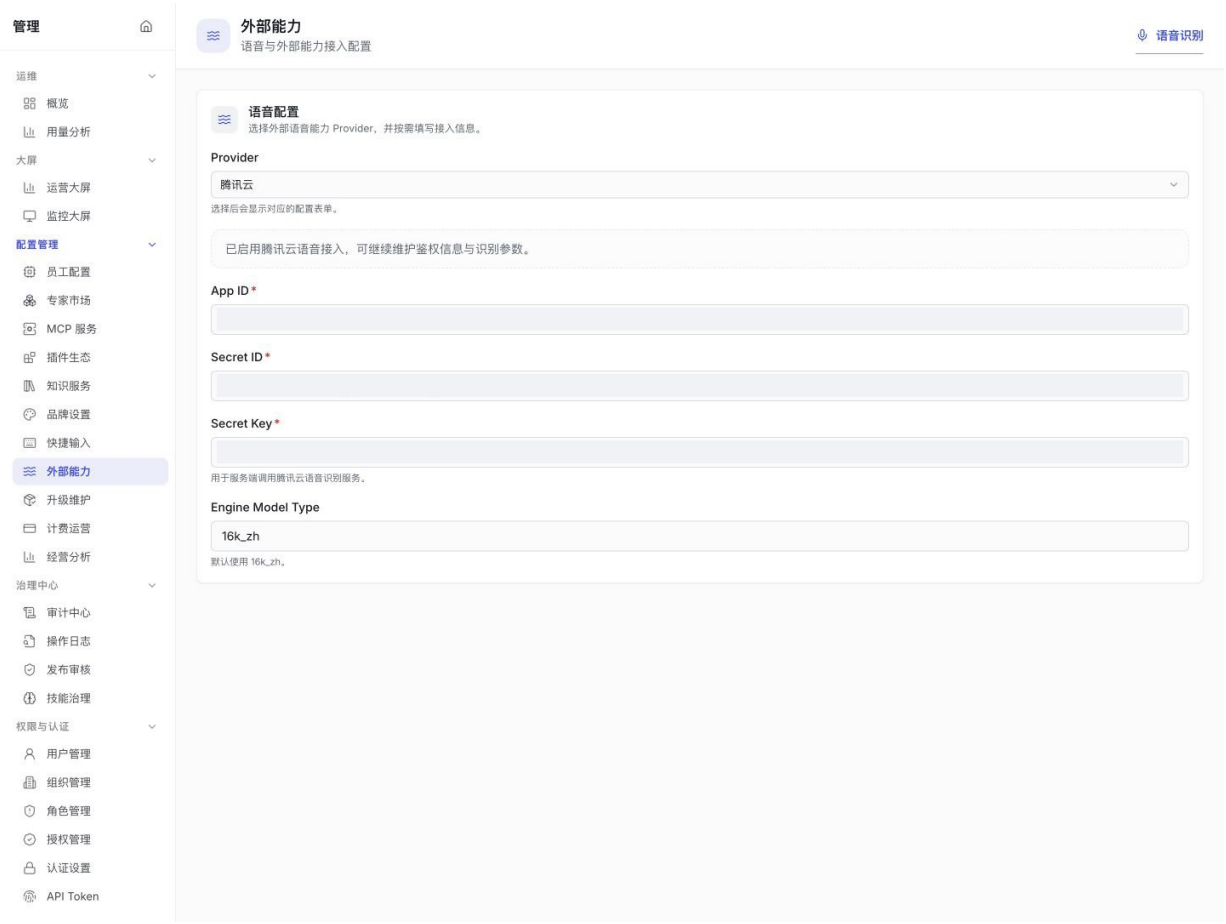
后台“配置管理 → 外部能力 → 语音识别”维护当前空间的语音识别账号。

字段	规则
Provider	当前支持“无”和“腾讯云”。选择“无”并保存后，空间不再提供这套腾讯云识别配置。
App ID	腾讯云数字 App ID；与 Secret ID、Secret Key 使用同一套账号凭据。
Secret ID	腾讯云访问密钥标识。
Secret Key	腾讯云访问密钥；已有密钥时，界面不回显原值。
Engine Model Type	识别引擎类型，默认 16k_zh。

空间配置供语音输入和使用空间账号的腾讯会议转写调用。当前数字员工仍需安装启用会议插件，并在“配置 → 会议识别”开启识别；数字员工插件中填齐三项腾讯云凭据时，会议改用插件账号。

空间语音识别不提供语音合成凭据，也不控制数字员工的会议识别开关。

操作说明：配置外部语音。



后台外部能力中的语音识别服务配置

客户端发布信息

发布信息	含义
版本	对应一组明确发布内容，不覆盖既有不同内容。
通道和范围	决定哪些客户端可获得更新。
平台与架构	决定安装文件适用范围。
安装包	实际可安装文件，需核对文件类型与内容。
签名及校验值	用于发布完整性和客户端校验，不能任意补造。
下载地址	实际托管入口，不等于发布记录已验证可下载。

升级维护区分桌面和 Android。桌面提供导入发布包、手动维护、上传安装包、发布列表四个标签。

CI 完整导入包为 desktop-update-bundle.zip，public/CDN 元数据由 CI 生成。

手工补录以草稿承接。管理员在平台安装包上传并校验后发布版本，撤回和删除分别处理。

客户端、服务、源码包与文档分别维护版本。发布列表中的记录仍需对应可下载的安装包和有效更新渠道。

安全边界

发布内容需要具有品牌与渠道授权，版权、备案和资质信息以实际依据为准。密钥不进入公开产物，签名私钥与普通安装包分开管理。

版本撤回或回退不自动恢复业务数据。数据恢复仍受版本兼容和恢复流程约束。

Agent 与工作区

数字员工可以包含主 Agent 和子 Agent。主 Agent 承接默认任务，子 Agent 按独立职责参与工作；Agent 是数字员工的执行组件。

工作区是数字员工的隔离运行环境，保存文件、配置和会话上下文。运行实例按支持的规则加载工作区内容，工作区访问不包含整个设备文件系统。

职责与调用

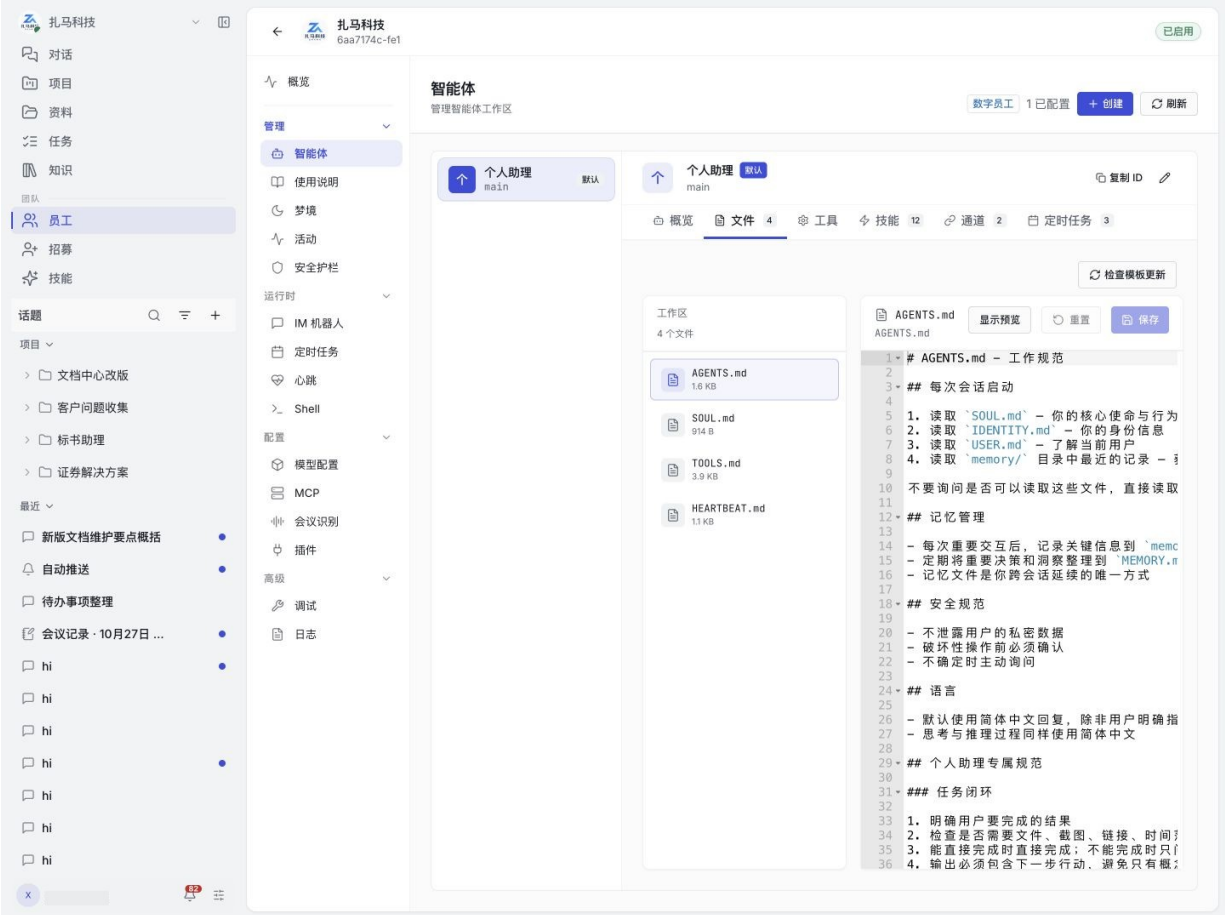
主 Agent 根据子 Agent 的职责、适用场景、输入、产物和接续规则分派工作。

子 Agent 仅在任务需要时参与，活动记录显示实际调用情况。

常用文件

文件	主要职责
IDENTITY.md	定义身份、名称与角色。
SOUL.md	定义行为风格、原则与边界。
AGENTS.md	定义任务处理和协作规则。
TOOLS.md	定义工具使用方法及约束。
HEARTBEAT.md	定义后台检查要求。
MEMORY.md	保存长期上下文与记忆。
USER.md	在运行支持时保存用户相关上下文。
启动与其他资源文件	运行实例按支持的加载与引用规则读取文件，文件存在不代表自动生效。

自定义资源需要明确的引用方式。文件中的敏感内容与长期记忆受授权约束；长期记忆不应保存未经确认的个人推断，也不能替代已核验事实。



Agent 工作区文件：文件树与 AGENTS.md 编辑区

配置与运行

数字员工模板中的工作区资源、数字员工保存的工作区文件和运行副本加载的文件分别保留版本。

数字员工模板更新不会自动覆盖已有数字员工的工作区配置。数字员工保存文件后，运行同步与加载仍是独立阶段。

主 Agent 与子 Agent 各自使用相应配置。运行中的个人状态与配置资产可以采用不同的保存链路，单纯复制文件不能代表全部状态已经迁移。

手动应用数字员工模板更新

管理人员在“检查模板更新”中确认更新后，系统按以下范围应用数字员工模板：

- 岗位文件：系统替换预览列表中的文件，文件内的人工修改会被覆盖。
- Agent 配置与使用说明：系统按数字员工模板更新，并追加新增快捷输入。
- 技能：版本变化时，系统尝试安装新增引用；已有安装跳过，安装失败项返回警告。
- 创建专用文件：BOOTSTRAP.md、IDENTITY.md、USER.md、MEMORY.md 不在后续模板文件替换范围内。

维护人员先保留需继续使用的文件内容，再确认更新。此操作与切换配置模板分别处理，数字员工模板发布本身不触发已有数字员工更新。

权限

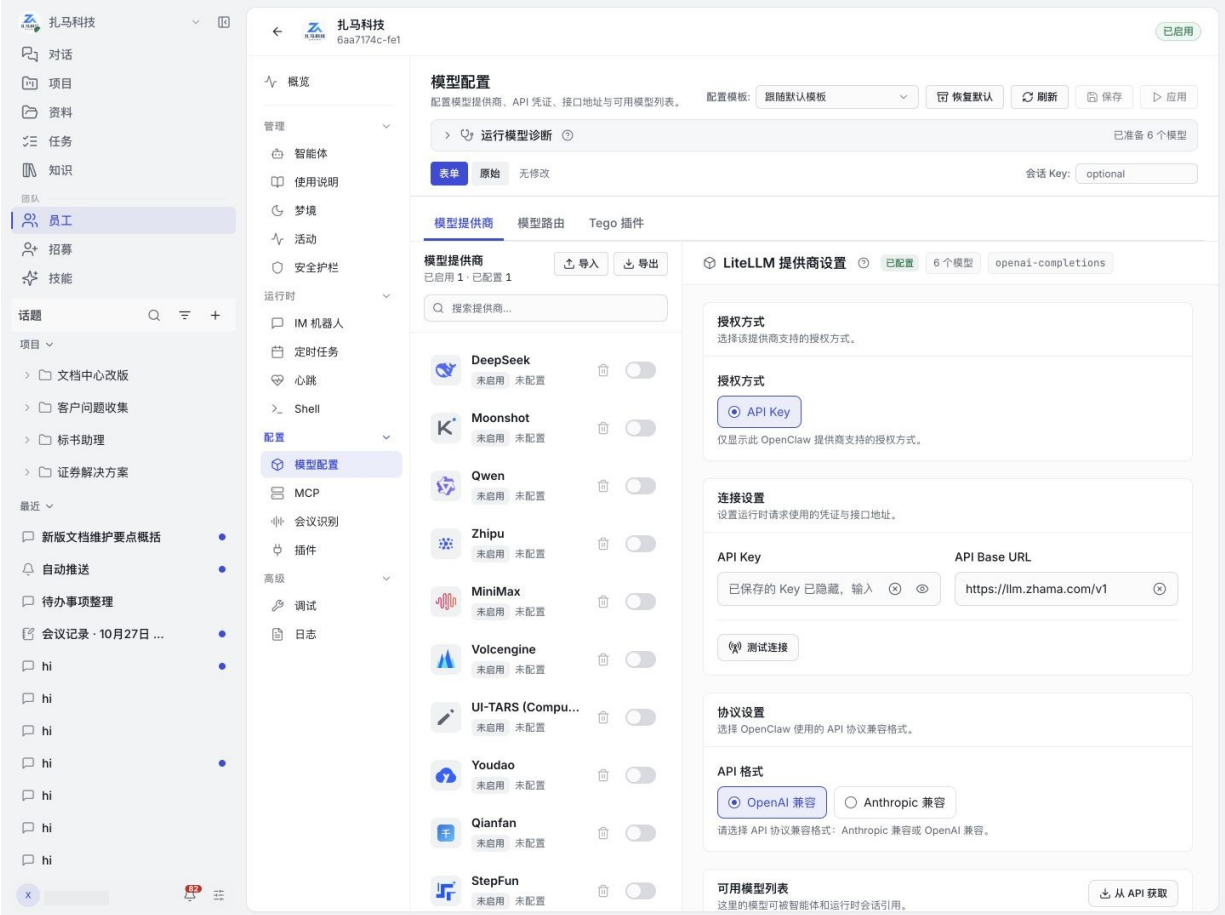
数字员工管理权限控制工作区编辑，运行身份与设备授权控制文件访问和工具执行。工作区规则不能替代资源授权或真实审批。操作见员工控制台。

配置项

数字员工、用户、知识服务和业务插件分别维护配置。配置归属与安装范围决定字段含义和生效边界。

配置位置与生效

配置内容	位置与含义	生效核对
新建数字员工的默认配置	后台“员工配置”提供初始配置	系统在创建时自动带入默认配置，不自动覆盖已有数字员工。
已有数字员工模型	员工控制台“配置 → 模型配置”	保存、应用、同步及实际调用。
数字员工 MCP 服务	员工控制台“配置 → MCP”	添加、修改及开关操作直接保存；同步结果与实际调用分别核对。
Agent 规则与资源	数字员工内对应 Agent 的工作区配置	目标 Agent、文件版本、同步与运行加载。
知识服务	全局模型、统一文档处理与检索参数	服务连接、跨库影响、文档任务与索引；历史库保留 Embedding 绑定。
知识库设置	库名、说明、成员与索引状态	目标库权限、文件就绪及原文检索；不覆盖全局处理和检索规则。
个人环境变量	设置内按数字员工关联的个人值	正确身份、名称与执行上下文。
插件配置	对应插件及安装范围	前端/后端/数字员工运行部分分别验证。
品牌与客户端	后台品牌及升级维护	实际页面、下载包与更新渠道。



员工控制台的模型提供商配置与保存并应用入口

字段检查方法

模型字段必须匹配提供商、协议及输入能力；秘密值通过专门配置维护，不写入备注或规则文件。数值的单位与上下限以对应表单为准。

典型数值参数

参数	范围或单位要求
知识检索全文/向量权重、全局置信度	0–1。
知识检索召回数量	1–100 整数。
容量、冷却及超时	以表单单位为准。
最小副本	0 具有实际回收含义，不是空值。

单次检索测试的量表可以不同，见知识中心。

保存、应用与恢复

提供“保存并应用”的页面需要显式提交；MCP 添加、修改及开关操作直接保存。同步冲突与知识索引需要重建由对应功能分别处理。

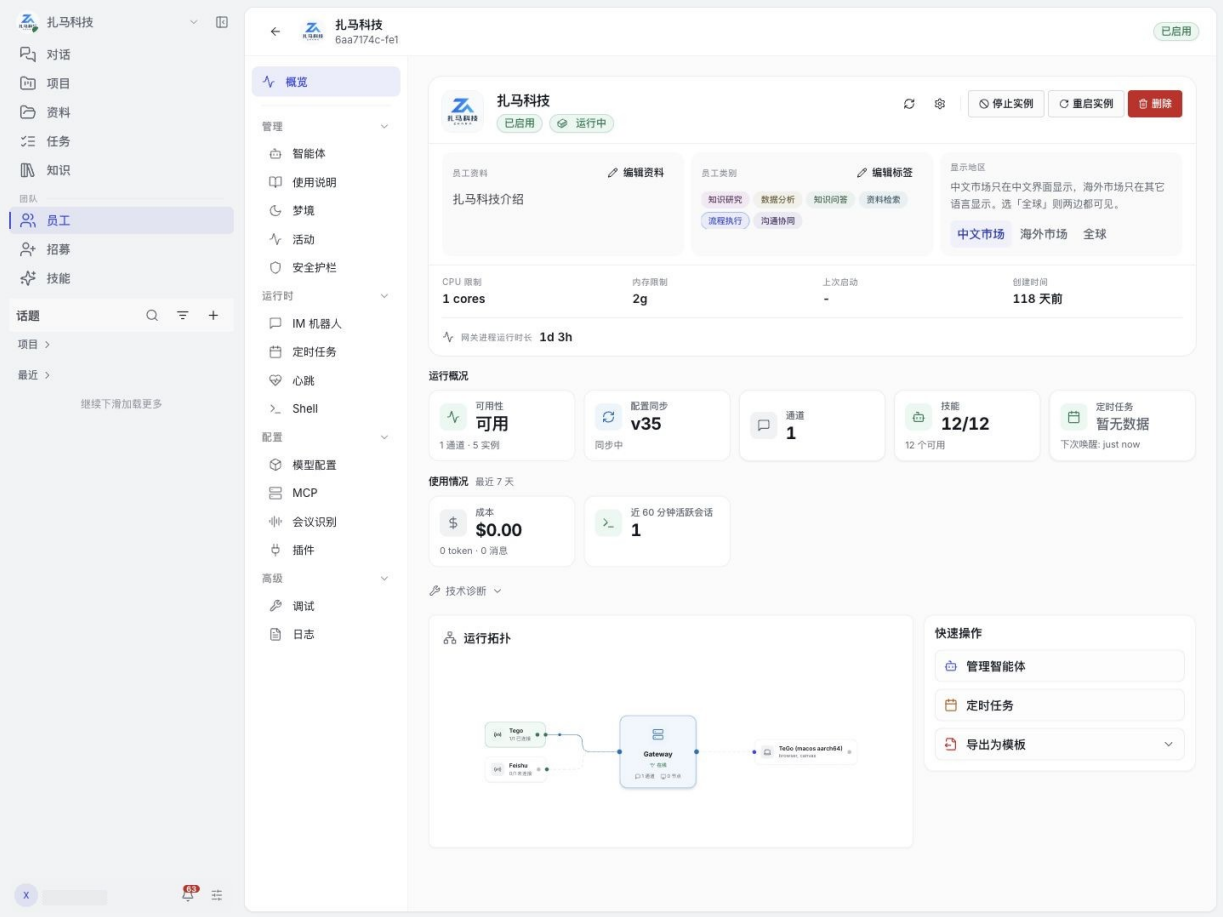
原配置恢复不会撤销已经发生的写入、外发或数据迁移。相关业务结果需要单独处理。

员工参数

数字员工参数分别定义岗位职责、可用范围和运行关系。展示字段、授权字段与运行字段的修改具有不同影响。

参数分组

分组	主要内容	约束与影响
身份与职责	名称、头像、描述、标签	展示信息描述数字员工的职责，与使用指南保持一致。
创建来源	数字员工模板、默认配置与版本	系统在创建时带入配置，来源更新不会自动覆盖已有数字员工。
生命周期	审批、启用、停用和迁移	状态变更影响后续使用及关联任务。
发现与授权	私有或组织范围、资源授权	发现范围不授予使用或管理权限。
Agent 与工作区	主 Agent、子 Agent 的分工、规则和资源	保存版本、同步版本与运行加载版本分别维护。
运行模式	当前部署支持的共享、独享等模式	模式决定用户绑定、工作区及持久数据的归属关系。
资源与容量	CPU、内存、副本及伸缩	参数受表单单位、上下限及实际资源容量约束。



数字员工概览中的配置、资源与同步信息

共享与独享

共享模式允许多个用户由同一组运行资源承接；独享模式建立不同的用户与运行实例关系。

当前部署决定具体隔离、回收和存储规则。模式名称不代表全部数据的隔离程度或可用容量。

伸缩与回收

最小副本、最大副本、每副本目标负载、缩容冷却和空闲超时共同控制容量。

最小副本为 0 时，系统允许缩容至零，后续请求可能触发冷启动。最小副本大于 0 时，常驻副本持续占用资源。

伸缩策略保存后，系统按负载调整容量；实际副本数量以运行状态为准。

迁移与生效

运行模式或数据迁移会影响当前任务、工作区归属及数据保存范围。

迁移期间，相关配置不宜并行修改。默认配置、数字员工配置与运行端加载配置分别维护，保存成功不表示数据迁移完成。

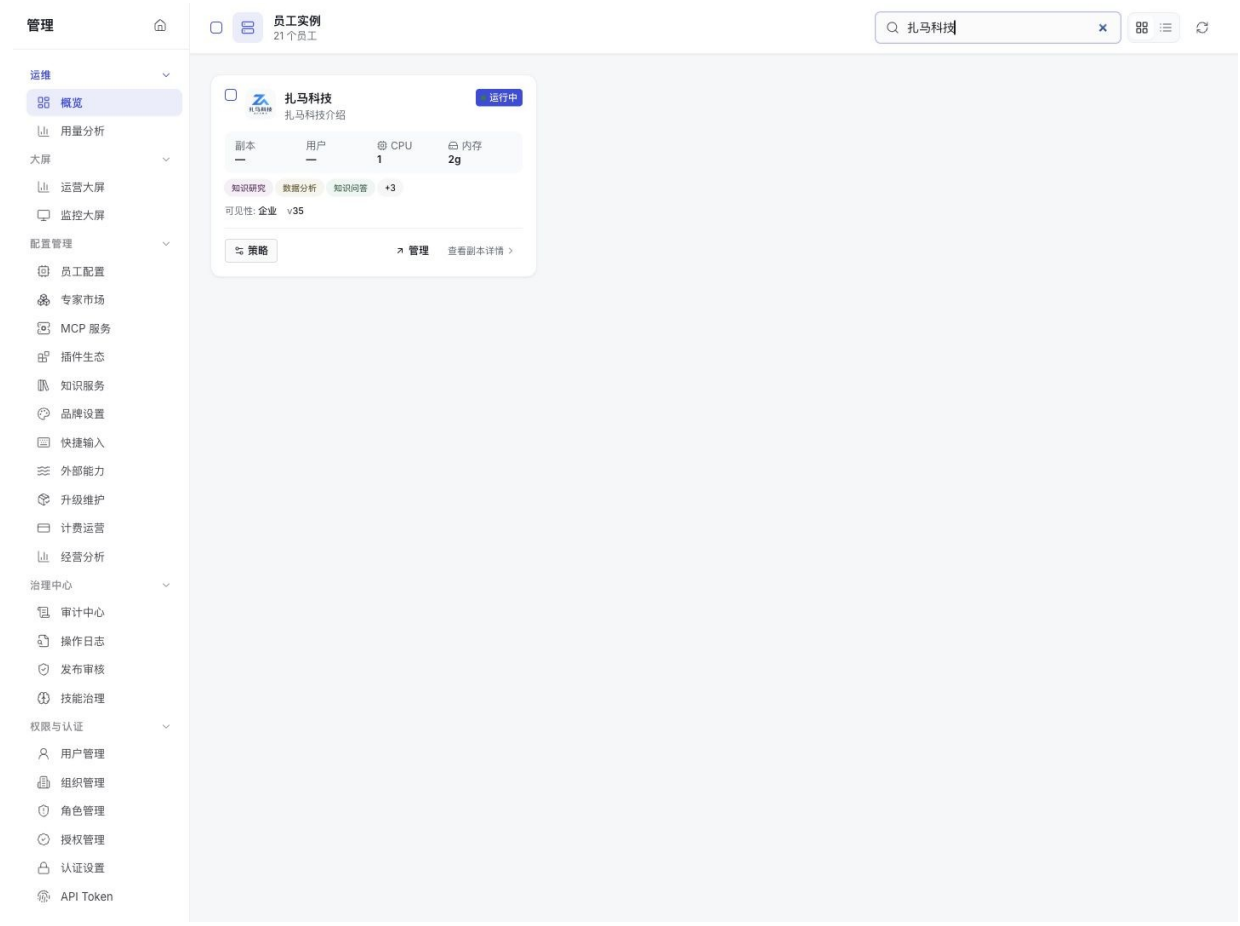
运行实例

运行实例是承接数字员工任务的执行单元。数字员工保存业务职责与配置，Agent 承担具体执行职责。

运行阶段

阶段	含义
准备	系统为运行实例准备资源。
启动	运行实例建立运行连接。
就绪	运行实例可以接收工作。
扩缩	系统调整运行容量。
停止	运行实例结束运行。
失败	运行实例发生需要诊断的异常。

停止运行实例不会删除数字员工，也不表示持久文件已被清除。



管理后台的运行实例、资源占用与副本详情入口

数据与实例

工作区规则、个人状态、项目文件、知识索引和对象存储可以由不同服务保存。共享、独享模式分别决定用户绑定和数据归属关系。

运行实例的临时目录不能代替备份。重启和迁移需要按实际持久化范围保留数据。

配置传播

配置按对应功能的保存、应用与同步机制生效。MCP 操作直接保存，提供“保存并应用”的配置则通过该按钮提交。已有运行实例可能暂时保留旧配置，离线运行端需要恢复连接后同步。

配置冲突按目标配置及版本处理。

维护动作

维护动作	影响
重启	影响对话、定时执行和通道连接。
缩容与回收	影响运行会话。
迁移	涉及数据。

维护会中断相关会话与通道；数据保留范围取决于对应持久化服务。

故障定位

数字员工、运行实例、发生时间和请求标识用于关联错误。连接、资源、配置与服务依赖分别提供诊断信息；单个健康指标不代表整项工作可用。底层安装、存储和恢复见运维部署，日常入口见管理后台。

业务插件

业务插件扩展业务页面、服务和数字员工工具，并维护自身的业务授权模型。插件市场发布、宿主安装与插件内业务操作分别控制分发、可用范围和数据访问。

插件组成

部分	职责
前端	提供业务页面、导航及交互，仍受页面权限控制。
后端	提供业务服务及数据处理，按请求身份鉴权。
数字员工运行部分	为数字员工提供工具或运行能力，受安装目标和配置约束。
公开前端	仅在发布明确包含并允许时承接公开入口，不推定所有页面匿名可用。

一个插件包可以只包含其中部分内容。

对话选择与插件安装

输入框“添加 → 插件”列出当前数字员工提供的内置插件。使用者的选择随本次请求发送；系统受理消息后清空选择，不写入安装或启用配置。

员工“配置 → 插件”维护当前数字员工的运行时插件，后台“插件生态”维护发布目录、安装与版本。安装与配置持续作用于其指定范围，不能用输入框的选中状态判断是否已安装或启用。

各入口的用途见插件入口的区别。

安装范围

插件可按租户或数字员工范围安装，作用范围和工具内容由插件声明决定；数字员工切换会改变适用插件。

作用域由插件决定。数字员工级插件的安装向导提供“选择员工”；租户级插件直接进入“确认影响”，不提供员工选择。

租户级插件包含数字员工运行部分时，对本租户全部数字员工生效，包括以后新建的数字员工。只有前端或后端的插件不因此获得数字员工运行工具。

扩展导航只显示当前适用且有权访问的前端页面。没有匹配项时，扩展导航可以不显示。

权限模型

权限层次	作用
宿主角色	决定平台操作资格。
插件内部角色	决定业务动作。
数据范围	决定可访问的记录。

三者分别判定，平台管理员不自动成为插件业务管理员。数字员工调用插件工具还受实际执行身份、声明权限与目标数据范围控制。

版本与发布

插件包需要包含可运行内容及依赖，并声明版本和兼容范围。插件生态支持搜索、显示已归档项及查看安装内容与配置；停用、回退、卸载和归档下架受到相应权限控制。

后端必填配置未填齐时，后端不会启动；数字员工运行部分（claw）的配置写入后需要重启才能生效。

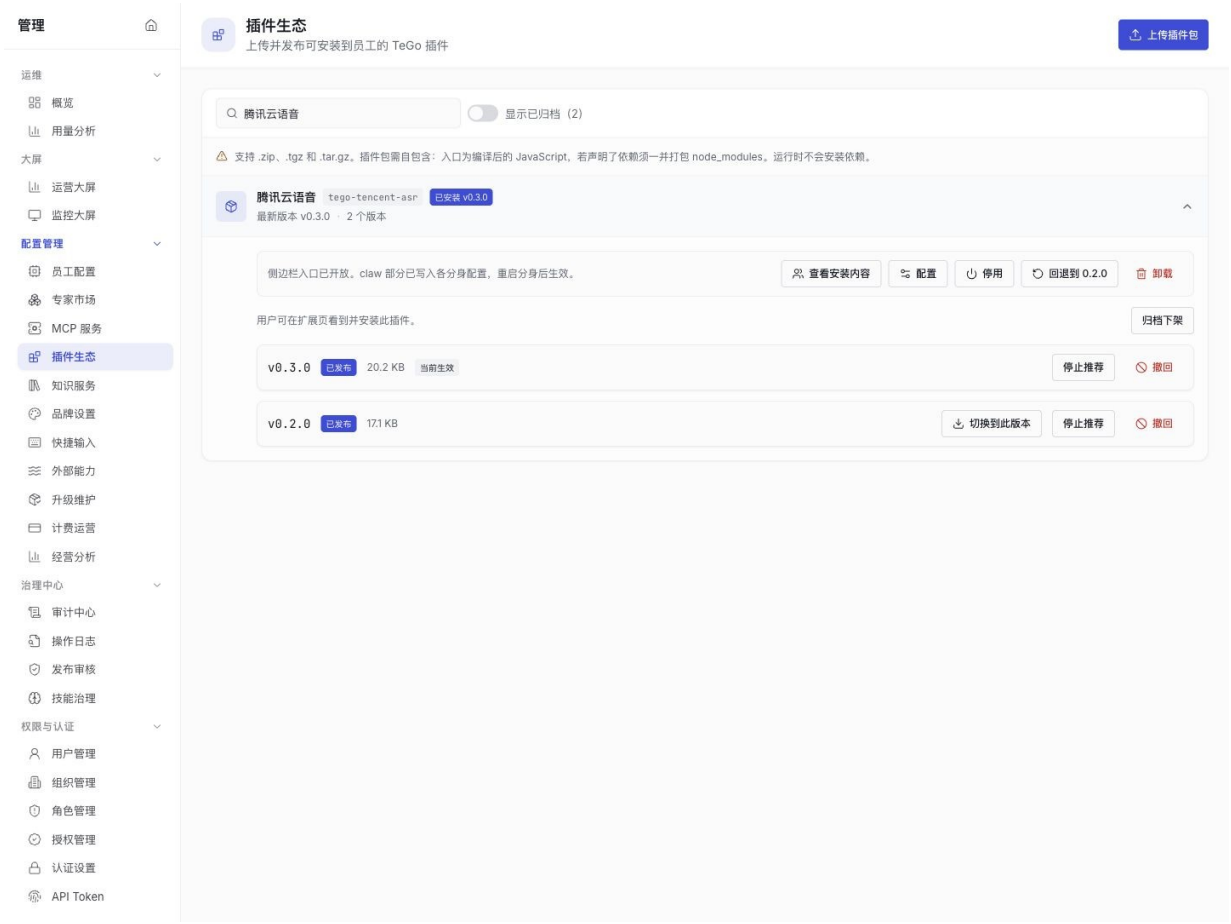
安装与分项配置按顺序提交，安装报错时可能已经形成安装记录。管理员应先查看已安装版本与配置状态，再补齐失败项。

撤回影响后续分发或使用，卸载移除安装内容。两类操作均不自动恢复已修改的业务数据，也不能替代备份。

数字员工运行时插件的打包要求如下：

- 上传格式支持 .zip、.tgz、.tar.gz。
- 包需自包含，入口为编译后的 JavaScript。
- 包声明依赖时需同时打包 node_modules，运行时不会在线安装依赖。

这些要求仅适用于运行时插件，不是所有前端/后端插件的通用发布格式。



插件生态：已安装插件的版本与配置管理

配置与安全

端点由受控部署配置提供，秘密从专门配置或环境读取，不写进源码、安装包说明或截图。插件页面样式与权限范围应受宿主管理，不越权读取无关用户内容。操作见业务插件。

知识服务

知识服务统一维护租户内全部知识库的模型、文档处理和检索参数；各知识库单独维护基本信息、成员、内容与索引绑定。

配置层次

位置	维护对象	影响
模型选择	Embedding、Reranker 及 OCR 模型，Reranker 提供商	新库使用全局 Embedding；历史库保留索引绑定；重排配置对全部库生效。
检索设置	全文/向量权重、召回数量、置信度阈值、重排	全部知识库统一使用。
文档处理	允许格式、切片字符数、清洗、图片理解、OCR	全部库的上传、替换及重新处理统一使用。
知识库	名称、说明、成员、文件及索引状态	目标库及其访问和处理状态，不覆盖全局检索/处理参数。
单次检索	查询、范围及测试参数	当前查询，不等于永久修改全局设置。

模型引用

模型	作用
Embedding	支持向量化。
Reranker	调整候选顺序。
OCR	支撑相应内容识别。

模型兼容性取决于提供商、权重、版本、维度及归一化方式，不能只按模型名称判断。

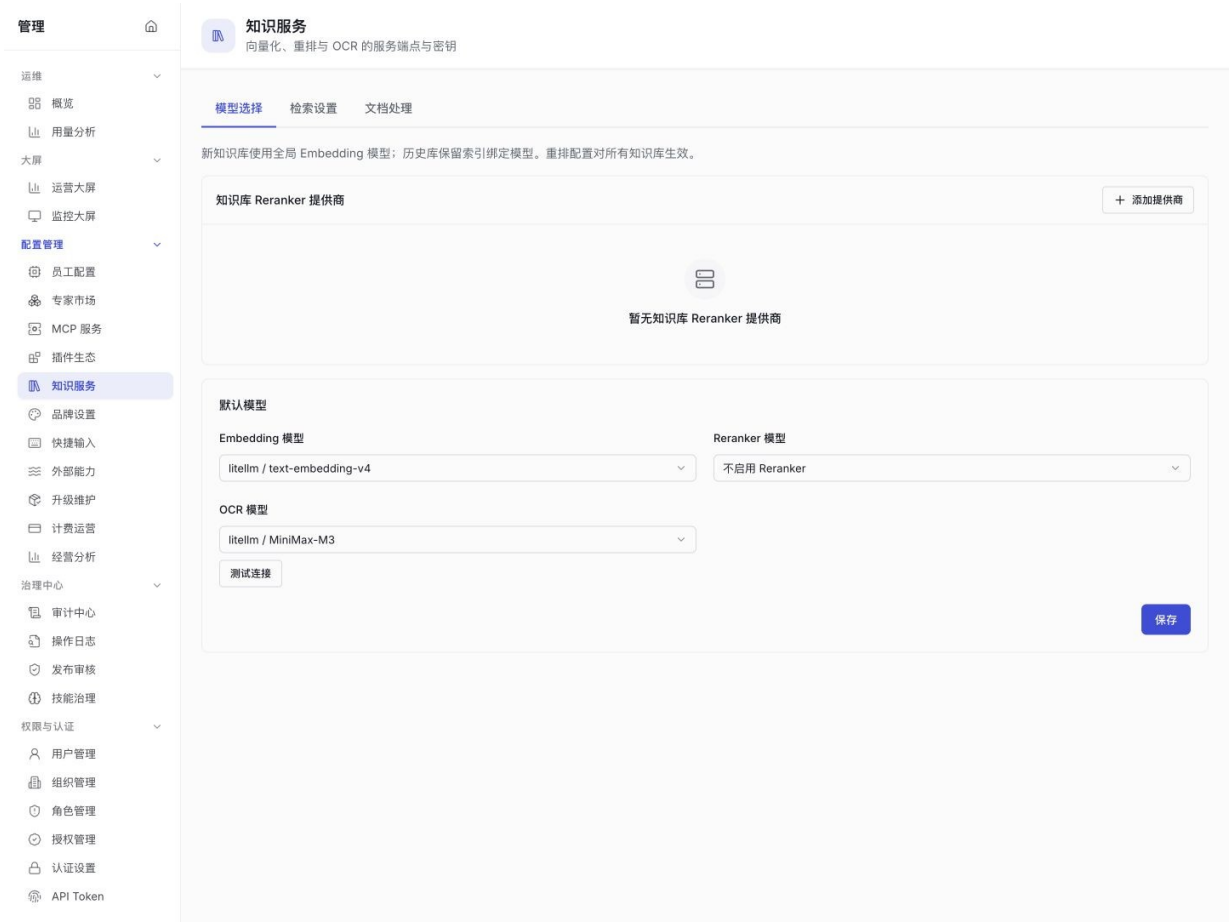
创建知识库前，管理员需在“模型选择”保存全局 Embedding 模型；未配置时不能创建知识库。新知识库使用该模型，历史库保留索引绑定模型。

全局默认模型变更不会迁移历史库。Reranker 配置对全部知识库生效，启用重排需要模型与连接可用。

· 管理员不应将提供商密钥写入库说明、上传文件、截图或工单。

· 系统在保存时验证 Embedding 模型。

· “模型选择”中的“测试连接”用于 OCR 模型；未选择 OCR 模型时，该按钮不可用。

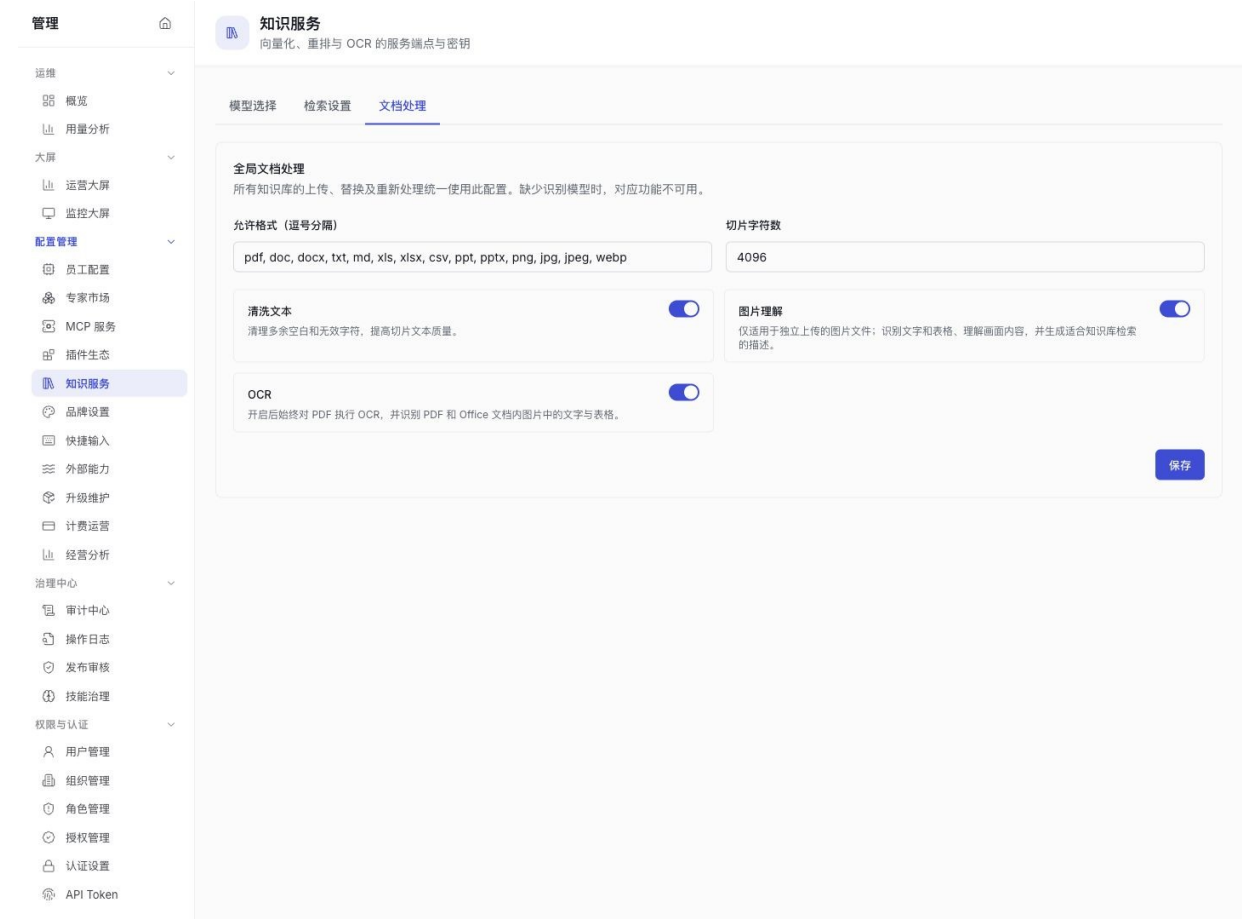


知识服务的 Embedding、Reranker 与 OCR 模型选择

文档处理选项

选项	作用与范围
允许格式	按逗号分隔的扩展名维护。
切片字符数	影响分段规模。
清洗文本	清理多余空白和无效字符。
图片理解	仅适用于独立上传图片，识别文字表格、理解画面并输出适合检索的描述。
OCR	开启后始终对 PDF 执行 OCR，同时识别 PDF 和 Office 文档内图片中的文字与表格。

缺少识别模型时，对应功能不可用。配置变更只约束相应后续处理，不代表旧文件已经重新处理。



知识服务统一维护格式、切片、清洗、图片理解与 OCR

检索设置

参数	作用	取值
全文权重	偏向字面命中。	0–1。
向量权重	偏向语义相关。	0–1。
召回数量	控制候选规模。	1–100 整数。
置信度阈值	过滤弱相关项。	0–1。
重排	对候选二次排序。	按页面配置。

检索设置统一作用于全部知识库。检索测试只能选择当前身份有权访问且已加载的知识库。

测试窗口的初始检索配置来自已保存的全局设置。测试中的单次调整不会保存到全局设置；后台尚未保存的修改也不会进入测试初始值。

索引状态

索引状态包括就绪、需要重建、重建中和失败。历史索引与其 Embedding 模型绑定；更改全局模型不会自动更换绑定。

涉及历史库模型变更时，管理员先通过技术支持确认该版本支持的处理方式和兼容要求。

索引重建占用处理资源。实际耗时取决于资料量与服务状态。

权限与治理

后台配置仅向具备相应资格的管理员开放。管理浏览支持知识库治理与成员维护，不授予正文读取权限。

来源应用管理的知识库和资料遵循来源侧规则。历史独立权限继续按对应限制判定。

诊断信息

知识任务的诊断代码、阶段、尝试次数、警告和最终结果帮助定位服务或文件问题。等待容量、等待适配服务、格式转换、解析和建索引属于不同阶段。

配置恢复后，原失败任务的结果与索引状态用于判断是否需要重新处理文件。操作见知识服务。

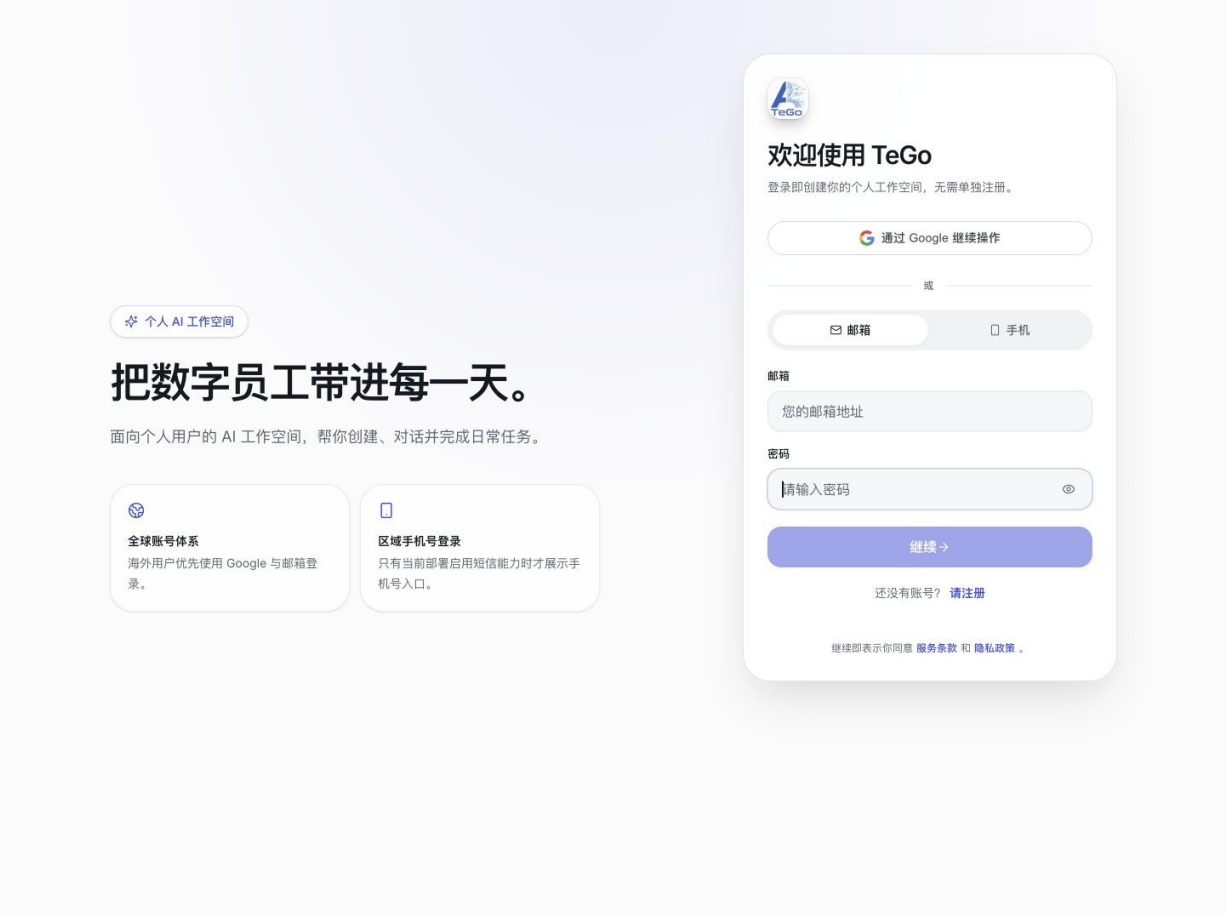
登录

登录确定用户身份与所属组织，数字员工选择确定本次任务的运行上下文。登录成功不自动授予全部数字员工或资料权限。

页面区域

Web 端以访问地址确定服务器；桌面端登录页的“服务器设置”维护登录服务器地址，保存后页面重新加载。组织标识和登录方式由部署配置决定。

账号菜单中的个人资料、设置、消息、帮助、下载及管理入口，按平台、角色和部署条件显示。



当前部署的登录页与邮箱、手机登录入口

身份状态

状态	含义与边界
未登录	不能访问需要个人身份的工作内容。
已登录、未选数字员工	可以进入已获授权页面；对话输入、附件和语音可能要求先选择数字员工。
已选数字员工	请求进入该数字员工上下文，仍受资源和工具权限控制。
要求修改密码	按页面要求完成密码修改，不能依靠关闭窗口跳过身份要求。
会话失效	重新认证；先确认正在编辑的文件是否已有保存结果。

登录态与退出

认证会话由服务端校验；前端保留的登录状态不会延长会话或增加权限。

退出结束当前登录态，不删除服务端已保存的工作内容。换账号或换服务器后，当前身份不自动继承原身份的授权和话题。

个人资料中的姓名、部门、职位等用于识别身份；组织角色、团队成员关系和资源授权由管理员维护。修改个人展示资料不等于修改组织权限。

认证方式与密码

密码、验证码、外部身份认证是否可选，以登录页实际提供的方式为准。

账号来源	密码规则
统一认证	组织身份源管理密码策略与重置流程。
本地账号	按产品密码表单及组织策略处理。

改密表单校验当前密码、新密码强度及两次新密码是否一致。

异常边界

租户归属、成员状态和资源权限共同决定登录后的资源范围，平台与部署条件进一步决定菜单。连接错误涉及服务器地址、网络或证书；认证错误涉及账号身份或认证来源。管理员配置另见组织与认证，产品安装另见运维部署。

个人设置

个人资料用于识别登录用户，数字员工资料用于说明岗位与职责。两者的头像、名称、职责和权限分别维护。

账号菜单

账户菜单提供个人资料、设置、消息、帮助、下载及退出等入口；使用量、会员、后台和审计入口受部署模式及角色条件影响。菜单可见性不能替代进入后的业务权限。

个人资料字段

姓名、邮箱、用户名和电话在个人资料页只读。使用者可以维护公司、部门、职位和所在地等可编辑资料，并保存修改。

头像上传后立即保存，不需要再次提交资料表单。

个人资料中的部门文本不等于组织中的部门成员关系，也不直接产生知识、项目或数字员工权限。

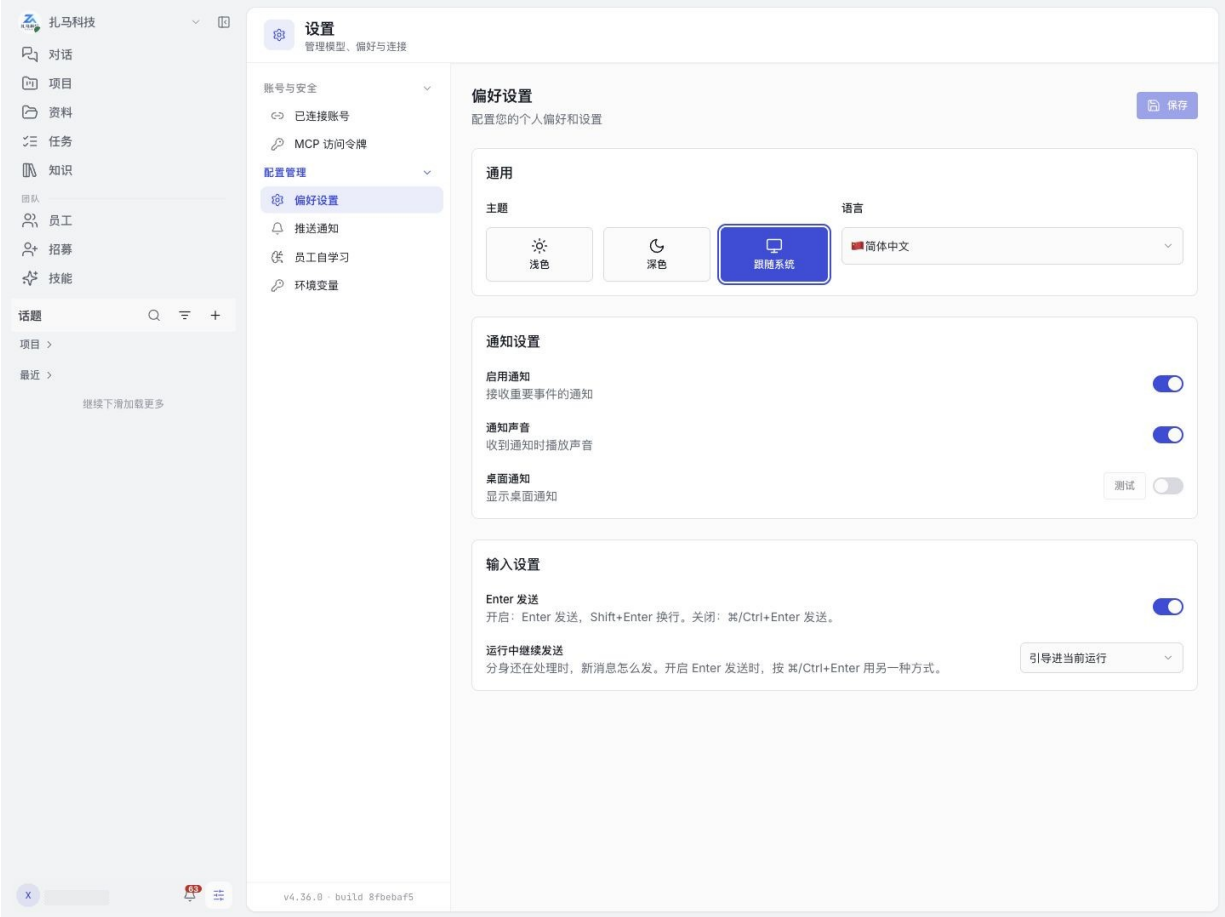
本地改密需当前密码、新密码与确认密码。强制改密状态与资料保存状态不同；组织认证账号应遵守身份源的密码流程。

偏好与语言

主题、语言、通知及输入偏好按设置页实际提供项生效。界面语言不翻译既有内容。系统通知还需要浏览器或操作系统授权，产品内开关不能代替系统授权。

输入选项包括“Enter 发送”和“运行中继续发送”；后者将后续消息引导进当前正在执行的任务。

设置分组	页面
账号与安全	已连接账号、MCP 访问令牌。
配置管理	偏好设置、推送通知、员工自学习、环境变量。



个人设置中的主题、语言、通知与输入偏好

环境变量

个人环境变量关联用户身份与选定数字员工。变量名决定工具读取的配置项，备注说明用途。

变量值按敏感数据处理，保存后不提供原值恢复。用户通过重新输入更换值；删除变量会影响依赖该配置的后续任务。

个人变量只用于对应用户与数字员工上下文，不作为全员共享凭据。数字员工的公共配置、个人连接、插件凭据和外部 MCP 令牌各自维护范围，见个人连接说明。

应用更新与下载

下载包与更新渠道由实际发布配置决定，客户端版本、服务版本与本文档版本各自独立。Web 与桌面客户端使用不同更新方式。

安全限制

个人设置不负责租户模型、知识解析服务、品牌和全部管理员策略。对权限或认证信息的更改由对应管理员处理；不要以修改个人展示字段代替组织授权。

发布审核

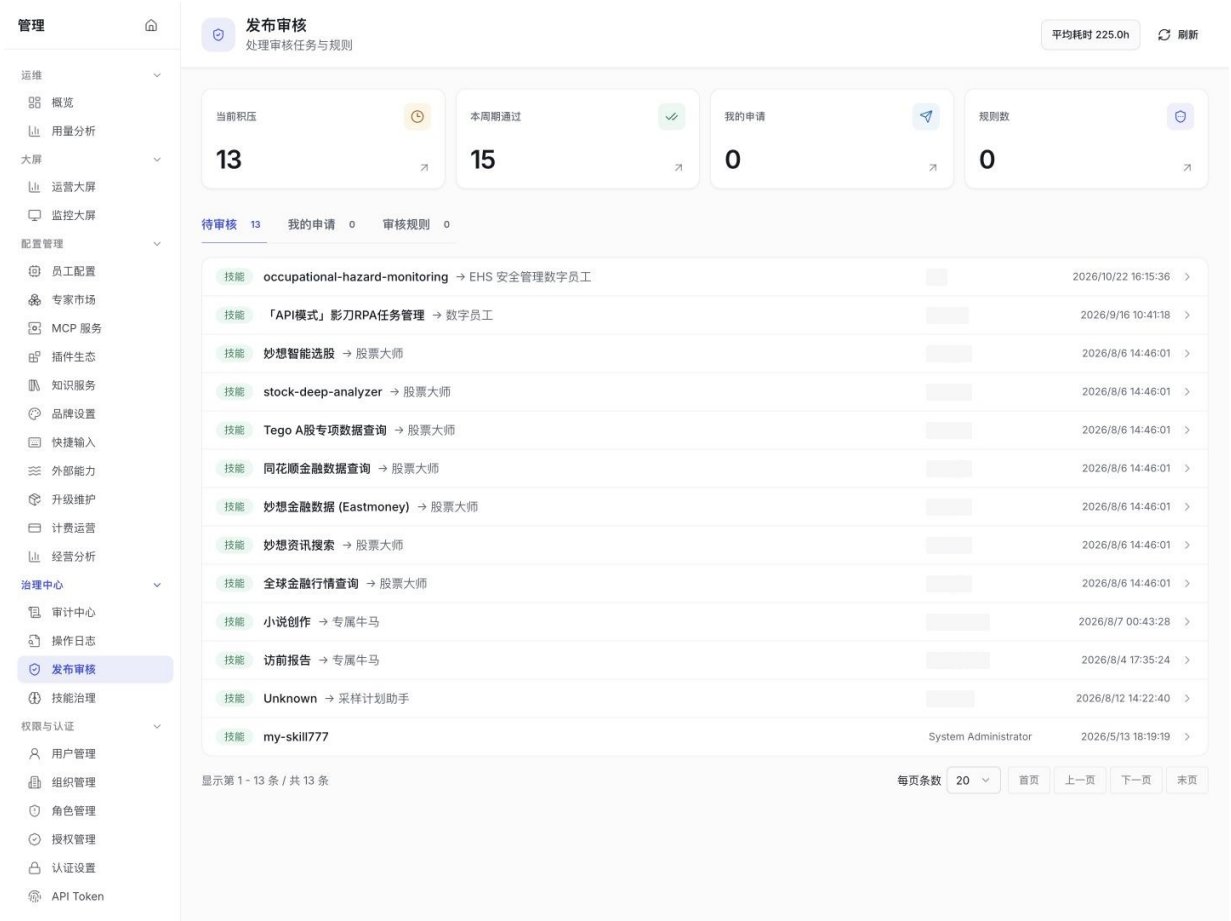
发布审核保存申请提交时的资源、版本、范围与处理决定。治理记录追溯资源变化，执行审计追溯实际执行动作。

审核中心结构

发布审核分待审核、我的申请、审核规则三个标签。请求包含以下信息：

- 资源类型、标识、名称及版本或快照。
- 申请人、审核人、范围、状态、说明及处理时间。

快照可以包含技能内容、安装数字员工、插件发布信息、可见性或授权变更。审核人员按操作类型核对快照。



发布审核中的待审核、我的申请与审核规则标签

审核范围与状态

状态	含义
待审核	申请已提交，尚未形成通过或拒绝决定。
已通过	该次申请在核对范围内获准，运行生效仍需检查。
已拒绝	记录拒绝原因，不能当作已发布。
已取消	本次申请终止，不代表旧有效版本自动撤回。

上传或升级、安装、可见性变更、授权和工坊提案分别产生对应快照。审核决定与资源自身的草稿或发布状态分别维护；同名资源和同一技能的不同版本分别对应各自申请。

管理员或被指定的审核人员可以处理待审申请，但申请人不能审核自己的申请。“通过”可附审核备注；“拒绝”必须填写拒绝原因。申请人可以撤回自己的待审申请。

审核规则

界面维护常用自动通过角色、SLA 及升级角色。更细的审核人分配由服务端保留规则处理；可见配置不等于完整审批引擎。规则维护资格、申请处理资格和资源管理资格分别判断。

规则的“启用”和“必须审核”分别控制是否采用规则、是否要求审核；关闭“必须审核”后，命中该规则的资源可直接发布。规则变更不改写已完成的审核决定。

安全审计

发布审核记录资源发布决定；操作日志、配置变更、人工操作与任务过程记录实际动作，审计查阅记录审计内容的访问。审核通过不构成组织合规结论。

权限与完整性

提交人、审核人、规则维护人及审计人员具有不同职责。查看摘要与查看完整正文还可以采用不同权限。

记录保留关联标识、时间与原始结果。业务更正通过新版本和新决定承接，不能覆盖历史记录。操作见发布审核。

组织与权限

身份确定请求归属，菜单权限控制入口，资源与业务授权控制具体动作。个人、角色和组织等授权来源可以共同形成有效权限。

用户账号

用户属于相应组织和身份来源，具有账号、展示资料、状态与角色。停用限制后续身份使用，不自动完成资源移交。统一认证、本地密码和渠道绑定分别有生命周期。

本地用户字段	规则
邮箱	必填，使用有效邮箱格式。
用户名	3–100 位，英文字母开头，后接英文字母、数字或下划线。
初始/重置密码	至少 8 位，包含大小写字母和数字。
姓名	必填。
职位、部门、联系电话等	按需要填写。

身份源同步字段与本地可维护字段分别判断。

组织与团队

组织可有公司、部门、团队及父子关系。层级、人员与来源影响授权计算。

不同资源对包含下级的规则不同，不能统一按必定继承或完全不继承处理。知识成员选择器会明确其范围。

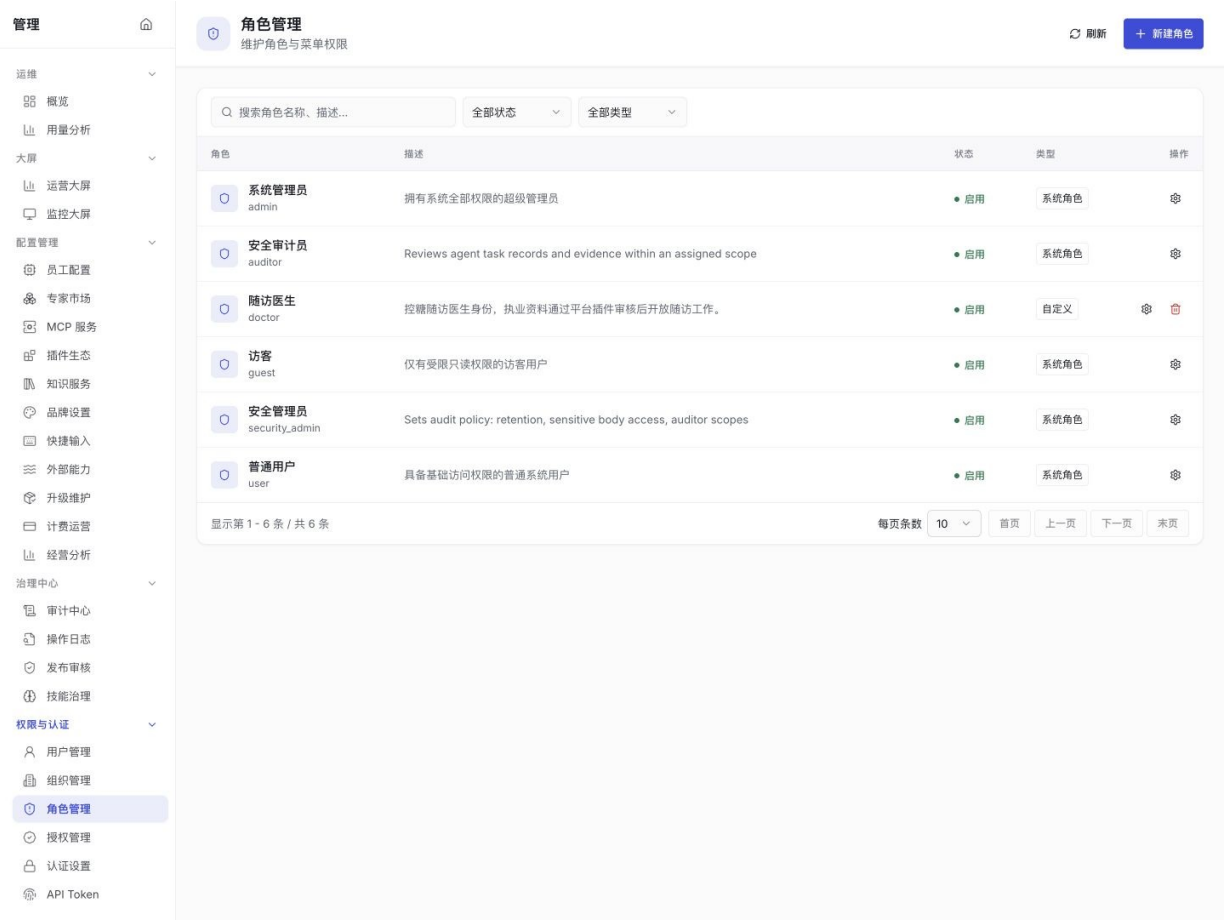
组织标识只含字母、数字、下划线、短横线，创建后不可修改。显示名称、说明和排序分别维护。

新建时上级留空表示顶级组织。外部同步来源的维护边界与手工组织不同。

角色与菜单权限

角色组合菜单与职责。入口菜单权、后台内部面板权、服务端动作权分开；前端隐藏按钮不是唯一安全边界，实际请求仍由服务端判定。审计与安全角色还受到职责分离策略约束。

角色基本信息与菜单权限分别保存。新建角色不会自动配置菜单，也不会自动分配给用户。



管理后台角色列表与角色配置入口

资源授权

资源	授权模型
数字员工	查看用于阅读资料，使用包含对话，操作可以包含设备连接，管理用于维护配置与授权；界面选项见员工权限。
知识	成员身份与读取、检索、编辑、管理等能力。
项目	项目角色。
插件	插件自身的业务授权模型。

个人、角色、团队和组织等授权可以共同生效。撤销直接授权后，其他来源仍可能保留访问。

LDAP

认证页区分 LDAP 和本地设置。LDAP/AD 连接涉及服务器、SSL、组织/用户 DN、绑定、过滤及属性映射。

连接测试与登录测试验证不同环节。同步周期范围为 1–168 小时，并可按权限立即同步。

两项测试使用表单当前配置，不代替保存认证设置。测试通过也不代表人员、组织与角色已完成同步。

密码校验成功不代表组织或角色同步正确。管理员在源系统停用账号后，还需验证后续同步效果。

API Token

令牌包含用途、Scope、期限及可能的执行身份。完整值仅在创建时提供，后续以受控存储管理。

实际权限是接口范围、执行身份和资源条件的交集。平台管理员签发的令牌也不自动突破业务范围。

权限判定边界

权限控制与功能可用条件分别生效：租户未启用、客户端不支持、依赖未安装或运行未就绪，也会限制操作。操作见组织与权限。

消息通道与集成

消息通道将外部平台请求送入数字员工，个人连接绑定用户的外部服务账号，OpenAPI 提供受控系统调用。三类连接分别维护凭据、身份和授权。

通道配置字段

字段	作用
通道类型	决定平台协议。
账号或机器人标识	确定接收入口。
平台凭据	支持认证。
连接状态	反映链路。
用户绑定	将外部发起者映射为平台身份。

数字员工控制台提供微信、钉钉、飞书、企业微信和 QQ 五个平台入口。用户从数字员工卡片的更多操作进入“设置 → 运行时 → IM 机器人”。

各平台的应用审核、可见范围和权限仍然适用。具体配置流程见配置 IM 机器人。

通道实例、保存与测试

一个通道实例保存一组外部机器人的连接配置。通道实例、数字员工和运行副本分别维护。

项目	含义与边界
微信设置	扫码连接微信，使用专用账号状态面板。
添加实例	钉钉、飞书、企业微信和 QQ 支持添加多个独立通道实例，每个通道实例对应相应外部机器人。
实例名称	通道实例的管理名称，与外部平台应用标识分别维护。
启用	通道实例的启用状态，不代表平台认证、应用发布或消息收发已经完成。
保存并应用	提交手工修改并应用配置；仍需检查运行端接收与连接结果。

项目	含义与边界
重置 / 删除	重置放弃未保存修改，删除移除所选通道实例；删除后的变更需要保存并应用。
测试连通性	检查所选平台凭据或状态，并刷新通道状态；需要 Gateway 已连接，不测试用户收发或业务工具权限。
扫码快捷配置	微信扫码连接，以及钉钉、飞书、企业微信的扫码授权成功后会保存配置并启用；QQ 当前表单没有同样的扫码创建入口。

私聊与群聊策略

策略或字段	含义
私聊策略：开放	通道层允许开放私聊；平台可见范围与 Tego 资源权限仍适用。
私聊策略：配对	未准入账号先通过配对流程；有待处理请求时显示通道配对，提供批准、拒绝和刷新。
私聊策略：白名单	按允许来源中的平台用户 ID 限定私聊来源。
私聊策略：禁用	禁用私聊；当前钉钉表单不提供该取值。
允许来源（用户 ID）	每行一个平台用户 ID，不能使用显示姓名、应用 ID 或机器人 ID 代替。开放策略可留空。
群聊策略	钉钉、飞书、企业微信提供开放、白名单、禁用。QQ 当前表单不提供此字段。
群聊允许来源	为支持该字段的平台限定群聊来源；使用对应平台与插件识别的稳定 ID，不以群显示名称替代。

配对和白名单只限定通道接入，不授予管理员、知识库、设备、文件或外部系统权限。群聊准入还须符合平台侧的入群和消息范围设置。

微信通道

“扫码连接微信”生成本次登录二维码，系统在连接成功后保存账号并启用插件与通道。“测试连通性”检查微信状态。

微信使用专用状态面板，不提供其他四个平台的通道实例凭据与高级策略表单。

“微信登录成功，但保存配置失败”表示账号登录已完成，通道配置尚未保存。

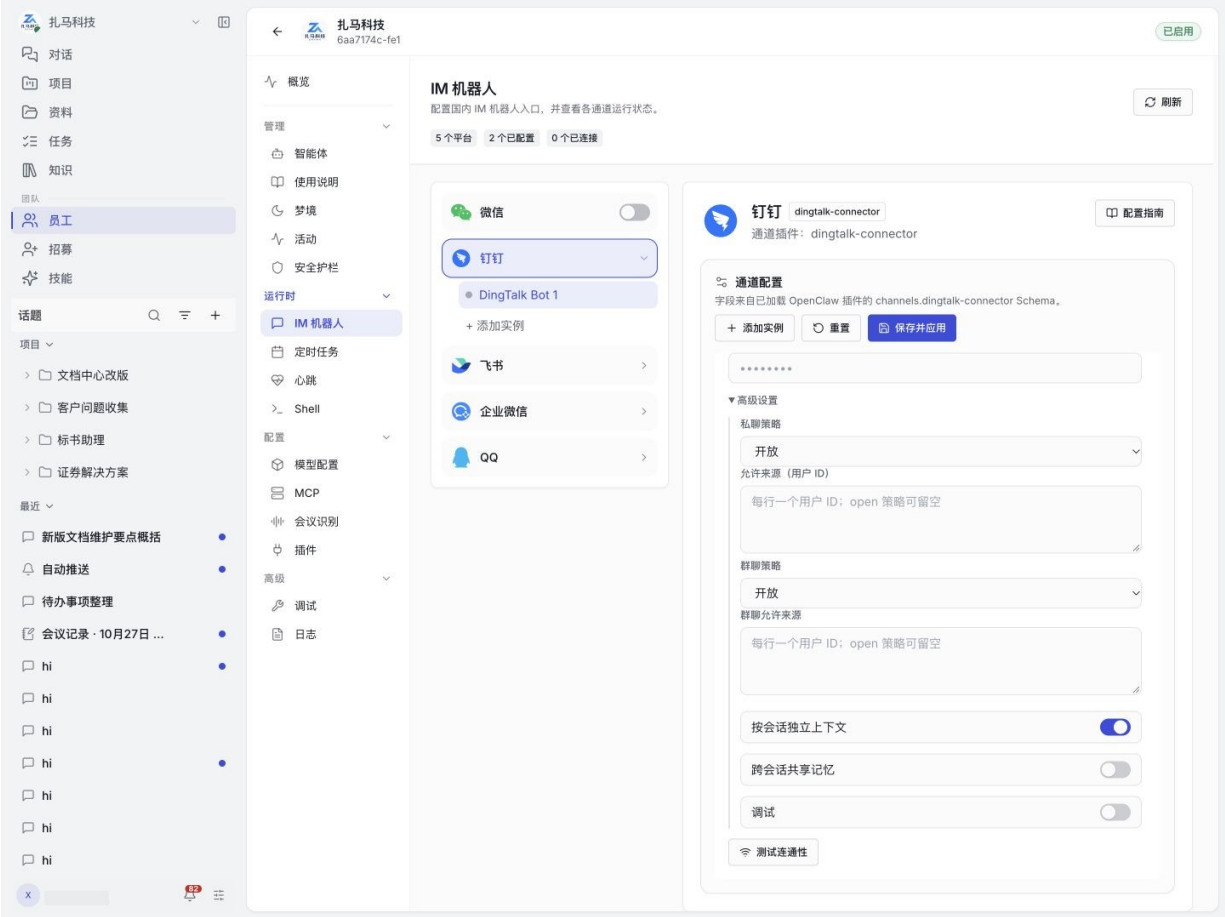
用户在登录失败、超时或未获得二维码时，按页面错误重新发起连接。微信与已安装通道插件的实际要求决定版本兼容范围。

钉钉通道

字段	口径
Client ID (AppKey) / Client Secret (AppSecret)	企业内部应用的同一组应用凭据。
私聊策略	开放、配对、白名单。
群聊策略	开放、白名单、禁用，并有群聊允许来源。
按会话独立上下文	控制会话上下文的划分，启用前核对业务对话边界。
跨会话共享记忆	控制跨会话记忆使用，不能把共享范围默认为单聊范围。
调试	用于问题定位；输出按组织要求保管并脱敏。

当前接入提示使用“Stream 模式”长连接。应用机器人能力、权限、版本发布与可见范围在钉钉开放平台维护。

卡片、文本等能力分别需要钉钉平台对应权限，凭据测试不会授予这些权限。



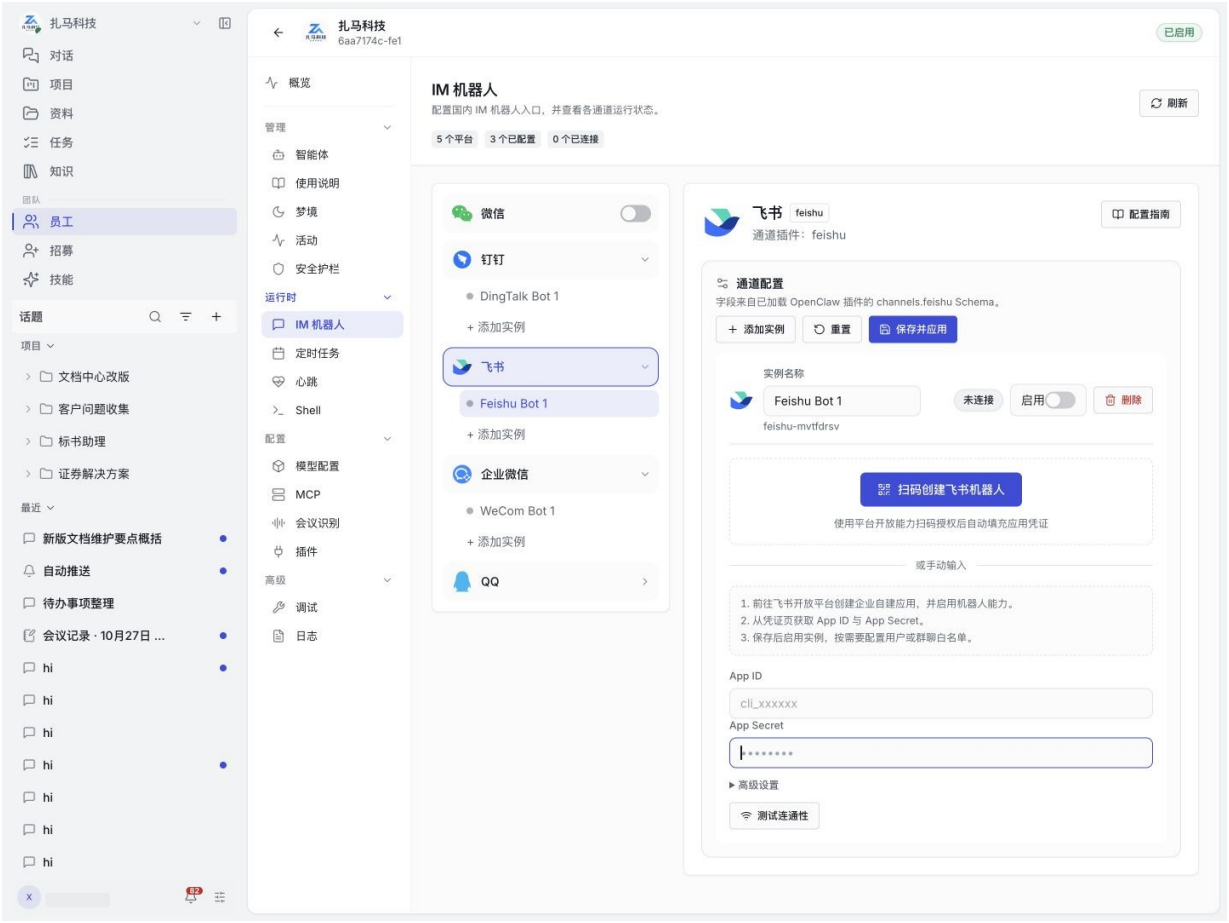
钉钉通道：私聊、群聊、上下文与记忆策略

飞书通道

字段	口径
App ID / App Secret	企业自建应用的同一组凭据。
私聊策略 / 群聊策略	私聊提供开放、配对、白名单、禁用；群聊提供开放、白名单、禁用。两类允许来源分别维护。
域名	飞书或 Lark，须与凭据所属平台匹配。
流式输出	控制逐步返回内容的方式；仍受平台与插件能力影响。
历史消息条数	控制通道采用的历史消息数量，不能当作 Tego 完整历史的保留期限。
媒体大小上限（MB）	通道侧媒体处理配置；实际还受平台、插件和所需权限限制。

长连接的消息接入需订阅 im.message.receive_v1。事件说明见飞书接收消息。

应用可见范围、权限与发布版本分别影响谁能使用、能接收什么，以及更改何时可用。



飞书通道实例与应用凭据配置，当前连接状态为未连接

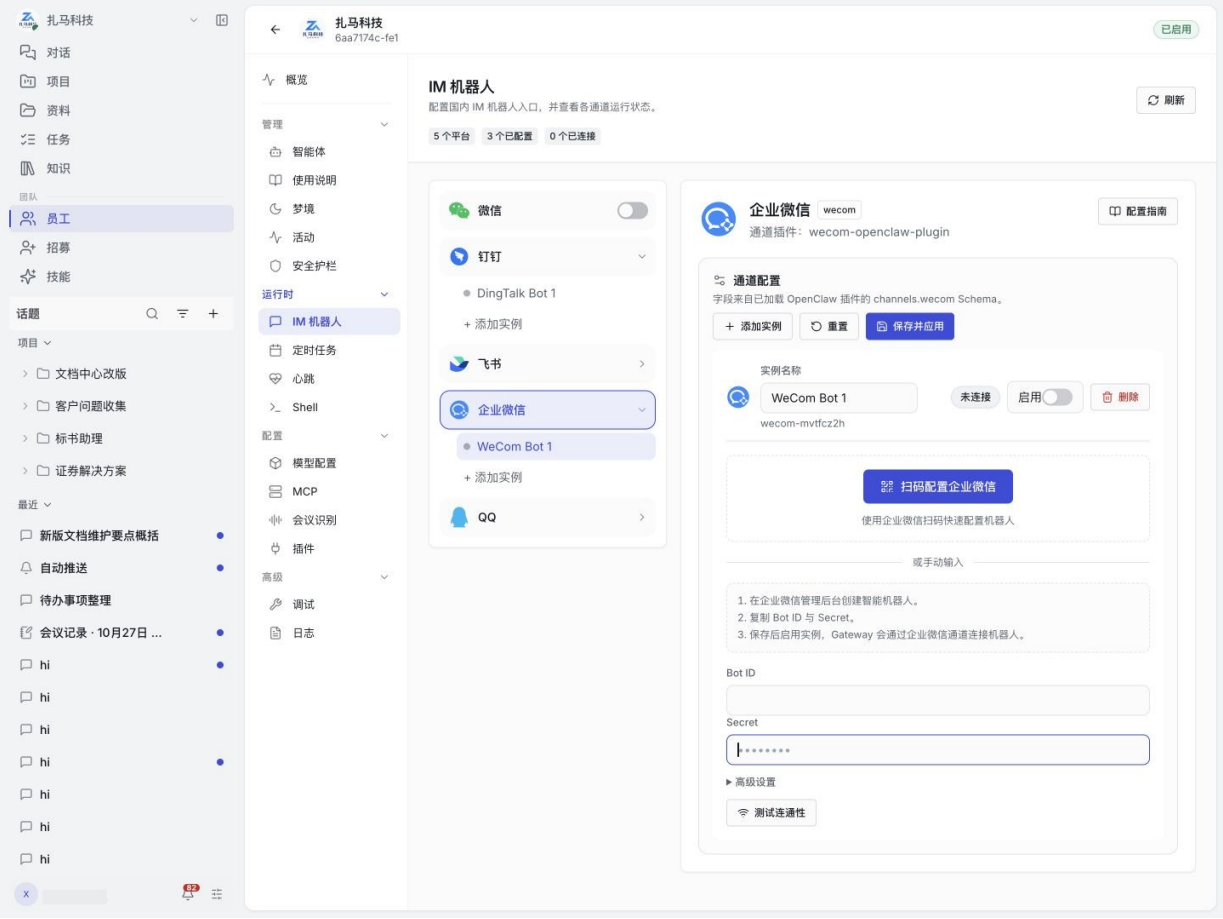
企业微信通道

字段	口径
Bot ID / Secret	智能机器人 API 模式的机器人标识与长连接专用密钥。
私聊策略 / 群聊策略	私聊提供开放、配对、白名单、禁用；群聊提供开放、白名单、禁用，并分别维护允许来源。
发送思考中提示	控制处理期间的提示消息，不等于任务完成。
调试	用于连接与消息故障定位。

Secret 与企业 CorpID、普通应用 Secret、群 Webhook key、回调模式 Token 及 EncodingAESKey 不同。

同一智能机器人同时只能保持一个有效长连接，新连接可能使旧连接断开。长连接与回调地址模式不能同时作为该机器人的接入模式，主备切换须避免双端同时占用同一机器人。

连接规则见企业微信长连接说明。



企业微信智能机器人连接配置，当前连接状态为未连接

QQ 通道

字段	口径
AppID / AppSecret	QQ 机器人应用的同一组凭据。
私聊策略 / 允许来源（用户 ID）	私聊提供开放、配对、白名单、禁用；允许来源填写平台用户标识。
Markdown 支持	控制消息格式，实际格式能力还受 QQ 侧设置和插件支持影响。
历史消息条数	控制通道采用的历史消息数量。

字段	口径
图片服务 Base URL	已实际部署、可由 QQ 访问的图片服务入口； 不能用本机地址或未部署域名替代。
调试	用于问题定位，输出需脱敏。

当前 QQ 表单没有群聊策略与群聊允许来源字段，群聊消息范围与发言权限在 QQ 侧核对。

个人主体、企业主体和体验用户的可用范围不同，创建成功不等于公开开放。具体范围见 QQ 官方常见问题。

QQ 官方接入教程中的独立 OpenClaw 安装命令不能直接用于替换 Tego 受管的运行时插件。版本问题由管理员按当前部署的插件管理流程处理。

身份与资源

系统依据实际发起身份与绑定规则，判定外部消息对数字员工、知识及工具的访问范围。未绑定身份不具有默认管理员权限。

群聊参与者可以看到群内内容。产物与引用需要符合相应接收范围。

对外发送

渠道配置提供发送链路，不授予数字员工任意外发权限。工作请求需要明确接收方、内容和必要确认。

发送成功表示渠道接受消息，不表示接收者已经阅读或业务已经完成。原消息的发送记录用于避免错误重试造成重复。

集成治理

集成凭据分别维护签发、到期、轮换与撤销。故障定位可沿平台应用、网络连接、数字员工运行实例、模型与工具查看对应错误；日志和工单中不应包含秘密值。个人访问见个人连接与 MCP 访问，组织接口见开放接口与集成。

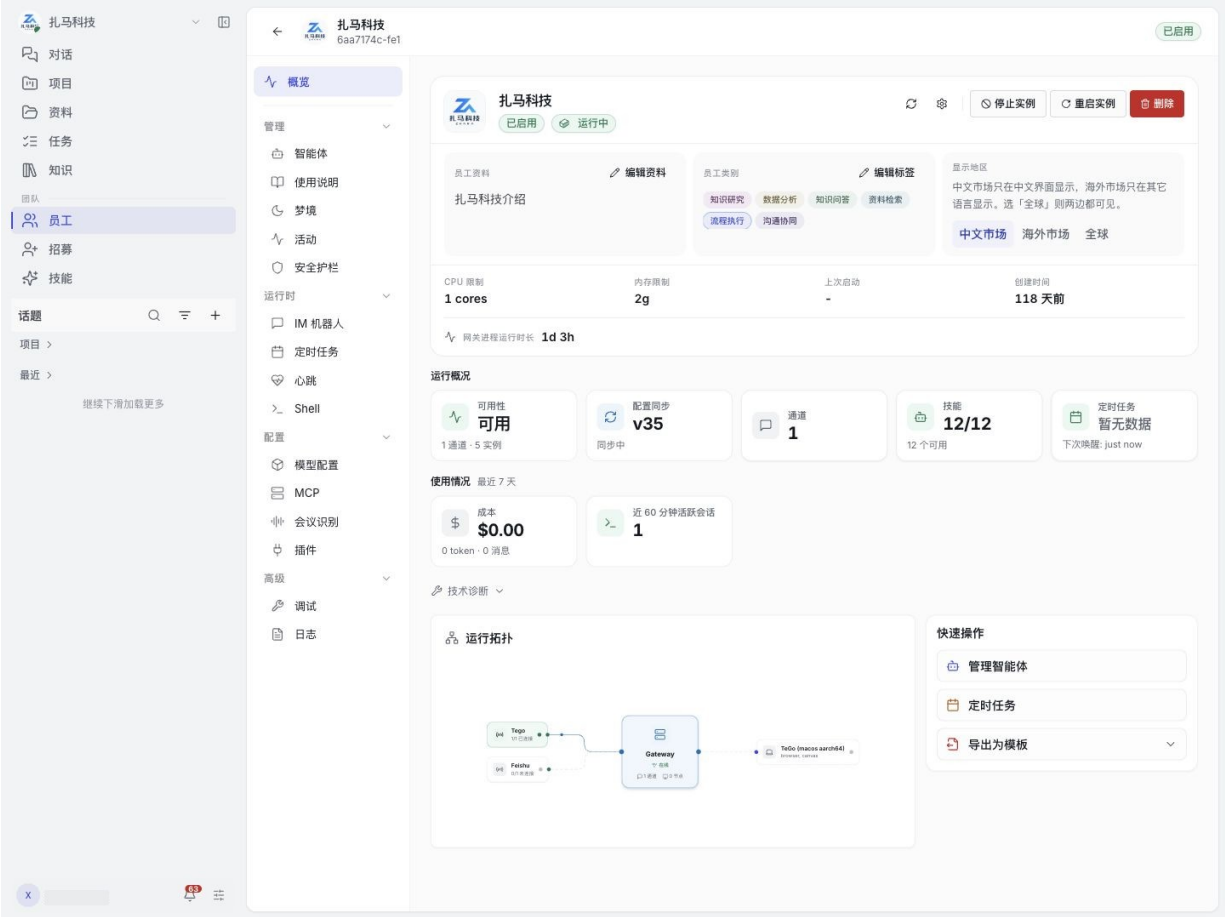
字段与状态

数字员工启用、配置同步成功和运行实例就绪分别记录，不能相互替代。

数字员工与运行

对象	状态含义
数字员工审批与启用	待审、启用、停用、迁移等描述配置生命周期。
配置同步	空闲、同步中、成功、错误、冲突描述配置传播。
Gateway/连接	连接准备、已连接、断开或错误描述通信。
设备节点	在线、离线、待批准、拒绝描述设备关系。
运行实例	准备、就绪、扩缩、停止、异常描述运行单元。

实际使用需要同时满足业务配置、配置同步与运行条件。

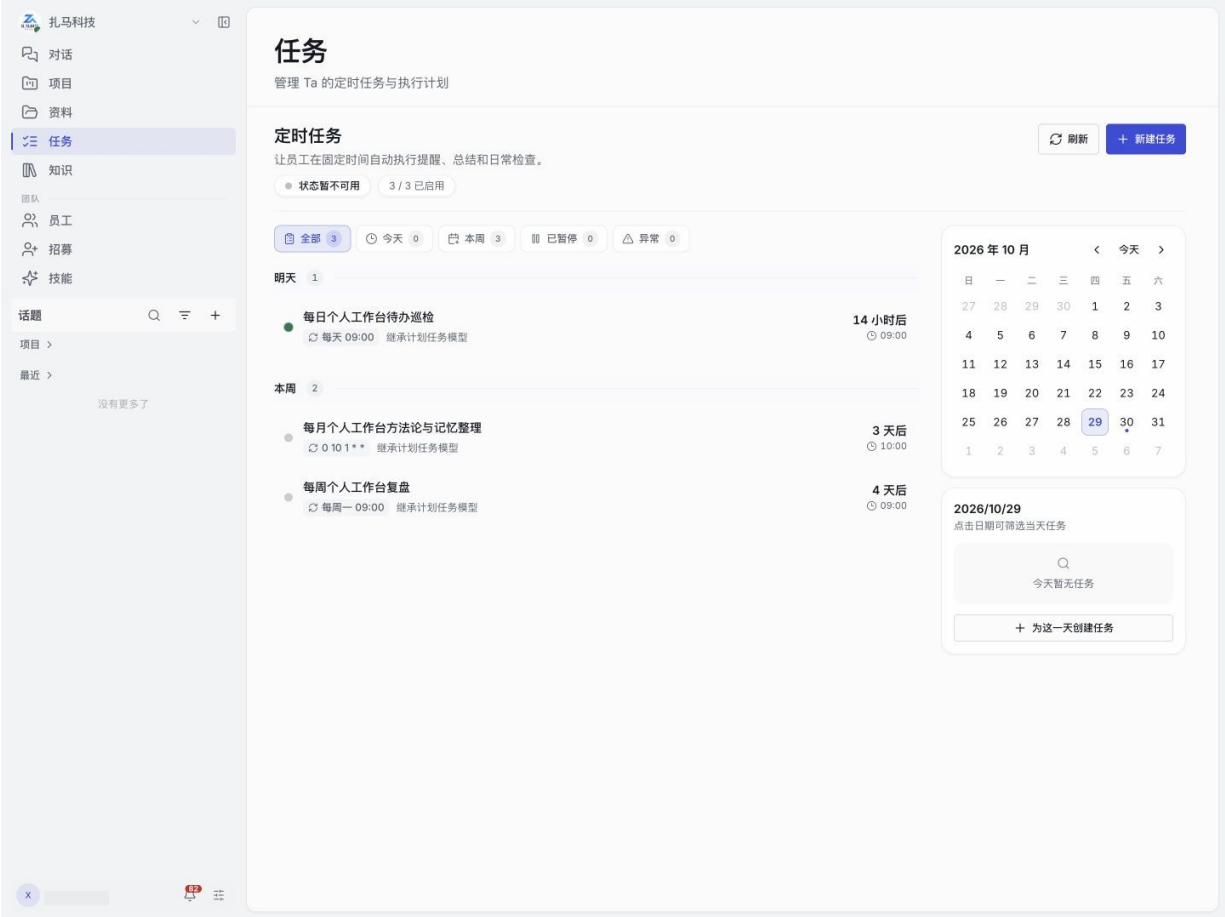


控制台分别展示数字员工、运行资源与配置同步状态

任务与日程

对象	状态
日程	启用/停用控制后续触发。
自动执行服务	开启、关闭或未知；暂不可用不等于关闭。
单次执行	进行中、完成、失败、中止、超时或被拦截。

立即执行会产生独立运行记录，具体规则见定时任务。



任务页分别展示调度服务状态、启用数量与单项计划

知识处理

维度	状态
知识任务	排队、进行、待处理、完成、部分完成、失败、取消中、已取消或多次重试失败。
处理阶段	等待资源/服务、读取、转换、解析、增强、保存和建立索引。

文档就绪与任务终态分别核对。历史文件版本不等于当前检索内容，详见知识任务状态。

审核与发布

审核请求为待审、通过、拒绝、取消；数字员工模板自身有草稿/发布；技能和插件还维护各自版本、安装与生效状态。通过一项审核不意味着全部安装目标已经更新。

通用字段

字段	含义
稳定标识	关联同一条记录。
显示名称	供页面显示和查找。
创建、更新、执行、统计时间	分别记录对应事件。
版本、修订号、尝试次数	分别表示内容版本、文件修订和执行尝试。

进度百分比表示处理进展，最终状态记录本次处理结果。

安全与审计

机制	职责
身份与授权	限定访问主体和资源。
运行限制、人工确认及护栏	约束执行。
审核	记录业务决定。
审计	追溯实际动作。

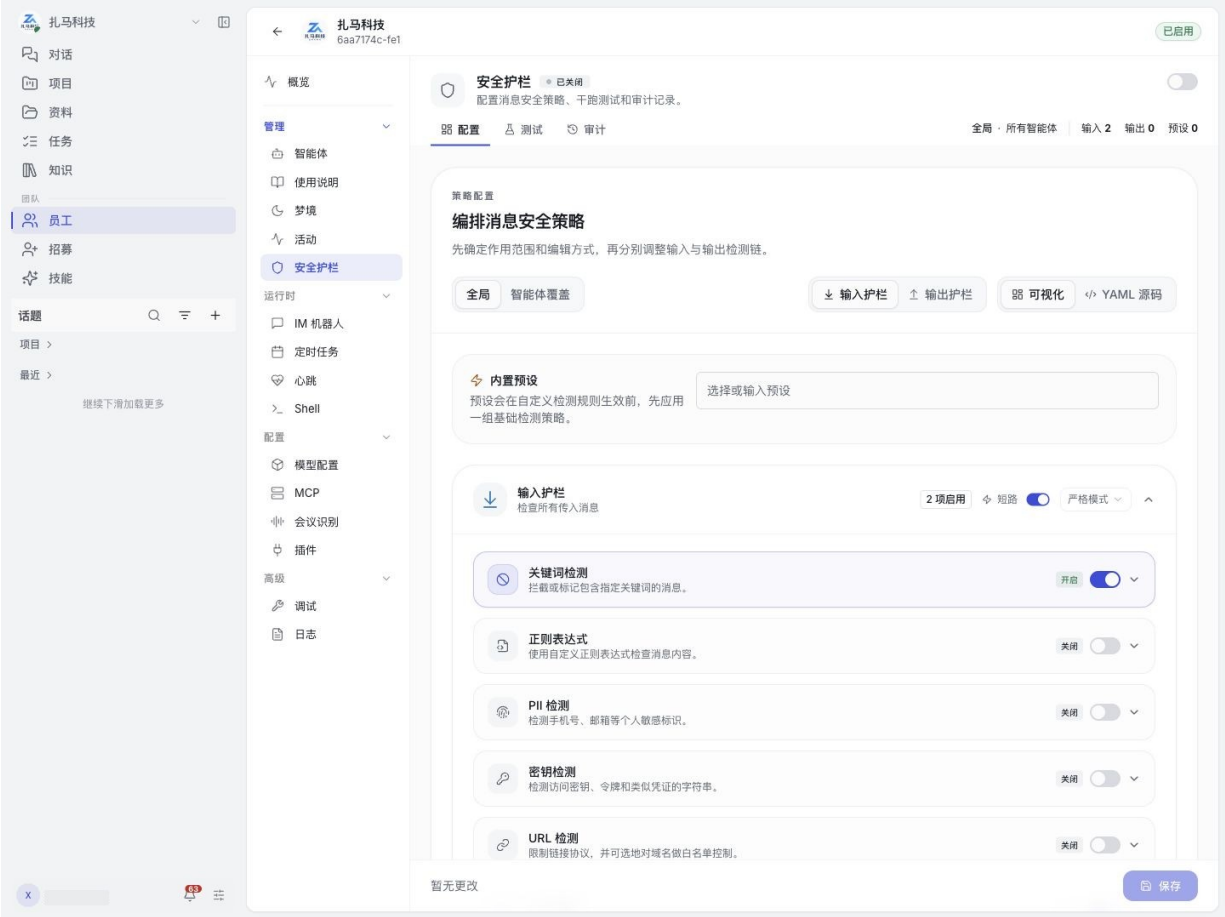
资源授权

数字员工资源、知识成员、项目角色和插件业务权限分别判定。组织管理员的治理入口不自动授予库内编辑权，菜单可见也不能代替具体动作权。

个人凭证只在许可身份与用途内使用。个人 MCP 令牌需要按实际权限保管，具体范围见个人 MCP 令牌权限。

高影响操作

外发、删除、覆盖、权限变更、命令执行与凭证修改需要明确目标和必要授权。计划确认帮助理解步骤，组织审批表达业务批准，工具审批限制具体执行；三者不互相冒充。



数字员工安全护栏的当前开关与输入检测配置

数据范围

话题、资料、项目、知识和外部系统分别具有接收范围。上传和引用需要符合来源授权；共享和导出需要同时处理个人信息、内部链接、批注及隐藏内容。

长期记忆中的个人信息与其他资料采用相同授权边界，不保存缺乏依据的个人推断。

凭据

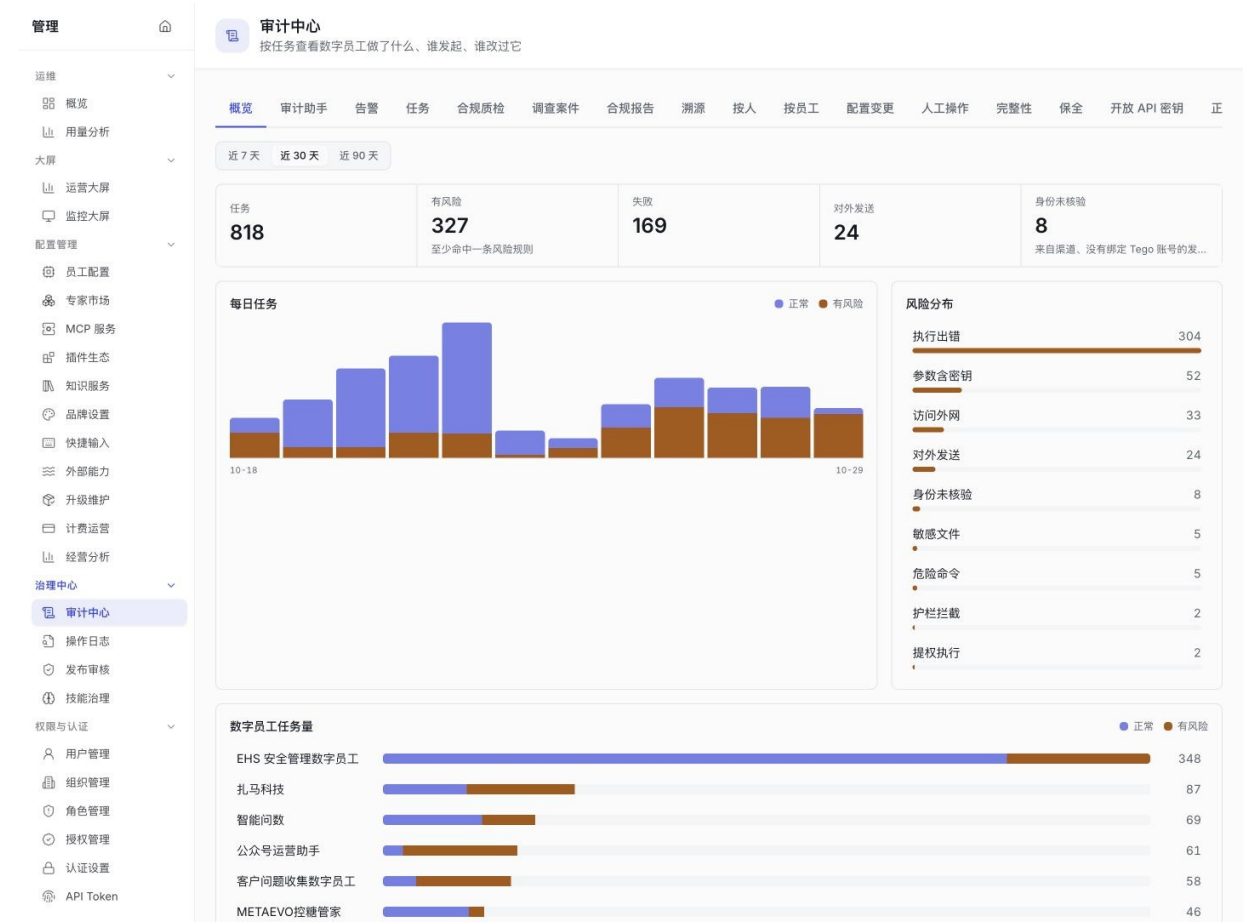
密码、Token、MCP 令牌、提供商与通道秘密通过受控存储维护，不进入技能包、截图、话题、归档或公开代码。

凭据使用方在轮换或撤销后核对依赖客户端。凭据吊销不会撤销已经完成的外部动作。

审计与职责

操作日志、发布审核、执行审计与运行日志分别保留不同证据。摘要与正文可有不同权限，审计员范围与安全策略职责分开。

启用职责分离后，平台管理员不自动具有全部记录的读取权限。



审计中心概览与不同记录的查阅入口

结论边界

完整性校验反映校验范围内记录的一致性，护栏测试反映所测输入，审核通过反映具体申请决定。它们均不能被改写为未经核验的资质、全面安全、业务真实或合规认证结论。

浏览器扩展

浏览器扩展通过 Tego 桌面端，将数字员工请求发送到已授权的 Chrome 或 Edge 标签页。

扩展控制用户设备上的浏览器。数字员工自身运行环境中的浏览器属于另一条执行链路。

连接链路

浏览器操作依次经过数字员工工具、网关、Tego 桌面端、浏览器扩展和授权标签页。扩展安装后仍需客户端配对与标签页授权。



节点面板“连接”页中的浏览器扩展与离线安装指引

“浏览器还没连上”表示扩展尚未连接桌面端，数字员工的节点连接正常也不会改变这一状态。

标签页与网站权限

用户已打开的标签页需要按当前规则确认；数字员工新开的工作标签页有可见提示。

使用者可以暂停数字员工的全部浏览器操作，也可以单独暂停标签页、收回交给数字员工的标签页或结束会话。网站限制还可包括子域名。

浏览器连接不改变所用网站账号的业务权限。

扩展版本与分发

商店、离线和企业安装包有各自发布与识别规则。桌面桥接会校验可接受扩展，不能把开发包标识或未经验证的包当作正式分发方案。准确版本与入口由发布配置提供。

执行边界

停止控制用于结束后续控制，不会撤销目标系统已经接受的提交。浏览器工具可用不授予外发、删除或付款等业务权限。

网页读取涉及敏感正文时，截图、日志和共享需要遵守相应数据范围。操作见浏览器扩展。

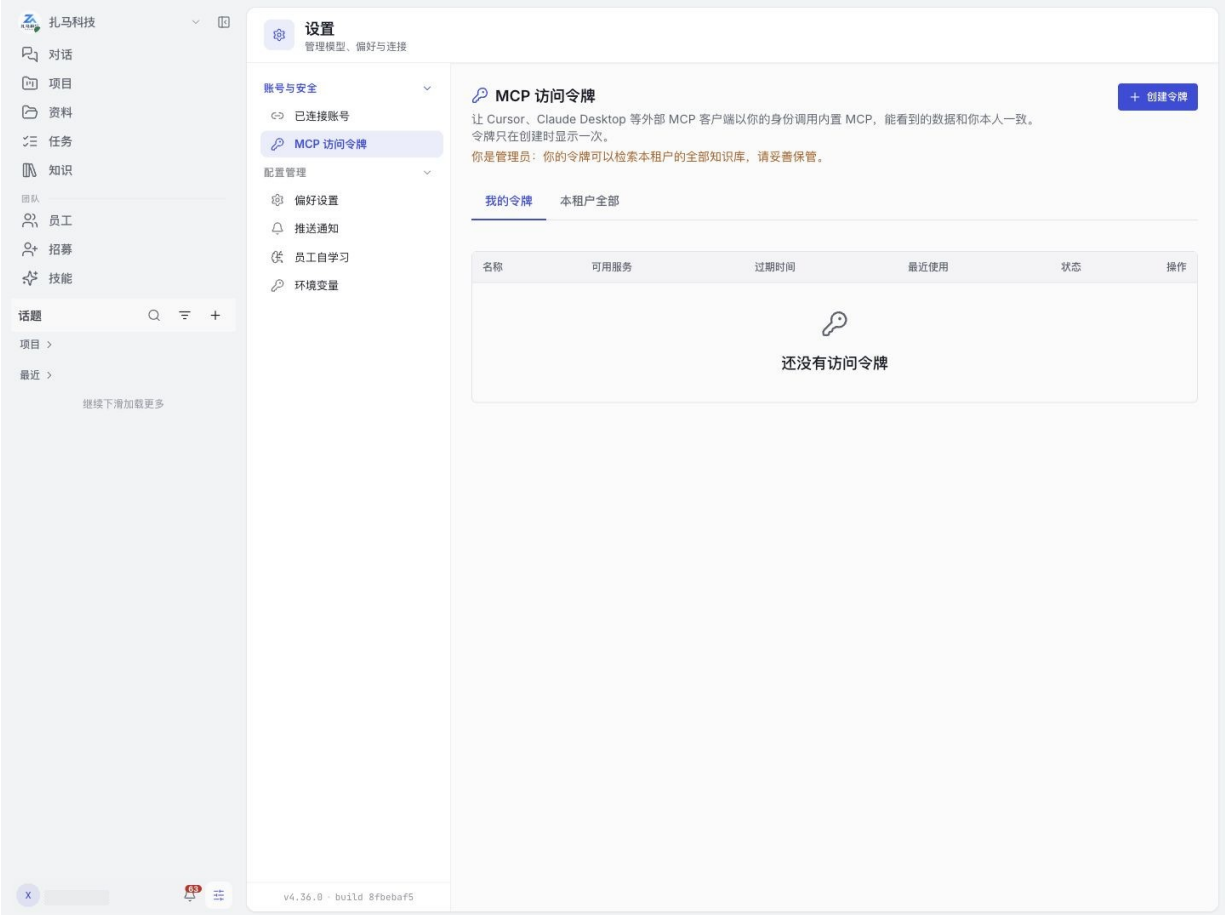
个人连接

MCP（Model Context Protocol）连接客户端与工具服务。

个人 MCP 访问令牌用于外部客户端访问平台服务。数字员工调用平台内置知识服务时，由平台提供身份认证；数字员工调用其他 MCP 服务时，按该服务要求配置凭据。

令牌字段

字段	含义
名称	标明使用客户端或业务用途。
所属用户	调用代表的身份；权限变化仍影响访问。
可用服务	“全部内置 MCP”允许调用所属用户可用的全部内置服务；“只限所选服务”要求至少选择一项。
过期时间	超过后需重新签发，不无限续用。
最近使用	记录客户端最近使用令牌的时间，不记录业务完成情况。
状态	有效、过期或已吊销等服务端状态。
秘密值	仅签发时显示，服务端保存用于校验的摘要。



个人设置中的 MCP 访问令牌列表与访问范围提示

权限

令牌代表所属用户，服务范围限定可调用的内置服务。普通身份按实际资源访问规则处理，调用其他业务服务仍需遵守其授权规则。

管理员令牌范围待确认

当前界面提示管理员令牌可检索本租户全部知识库，所提供源码的 MCP 检索接口按资源权限过滤，两者不一致。管理员令牌实际检索范围【待确认】，不能按单库令牌分发。

管理员可在我的令牌与本租户全部之间切换治理记录，不能还原已签发秘密。查看租户令牌列表与使用管理员自己的令牌，是两个不同动作。

个人连接与变量

配置	作用
已连接账号	以聊天验证码关联外部聊天身份与当前账号，绑定后对应聊天与客户端共享记忆。
外发邮箱	保存本人 Gmail 或 Outlook 的发信授权；组织启用代成员发信后，用户还要分别授权需要发信的业务插件。
个人环境变量	保存特定数字员工上下文中的用户配置。
数字员工配置的服务凭证	提供数字员工调用外部服务所需的认证。

外发邮箱只申请发信权限，不读取收件箱。聊天绑定、邮箱授权、个人环境变量、数字员工服务凭证和个人 MCP 令牌分别管理，撤销一项不会撤销其余配置。

聊天账号绑定需要管理员先接入对应数字员工的 IM 机器人。外发邮箱连接需要管理员先配置邮箱服务；邮箱已连接不代表全部插件均可代发。

操作见管理个人账号连接。

状态影响

令牌吊销或过期影响后续调用，不撤销已经完成的动作。用户离职、设备丢失或令牌泄露需要按组织流程撤销相关连接与凭据。外部客户端保存的旧令牌仍会产生认证错误。

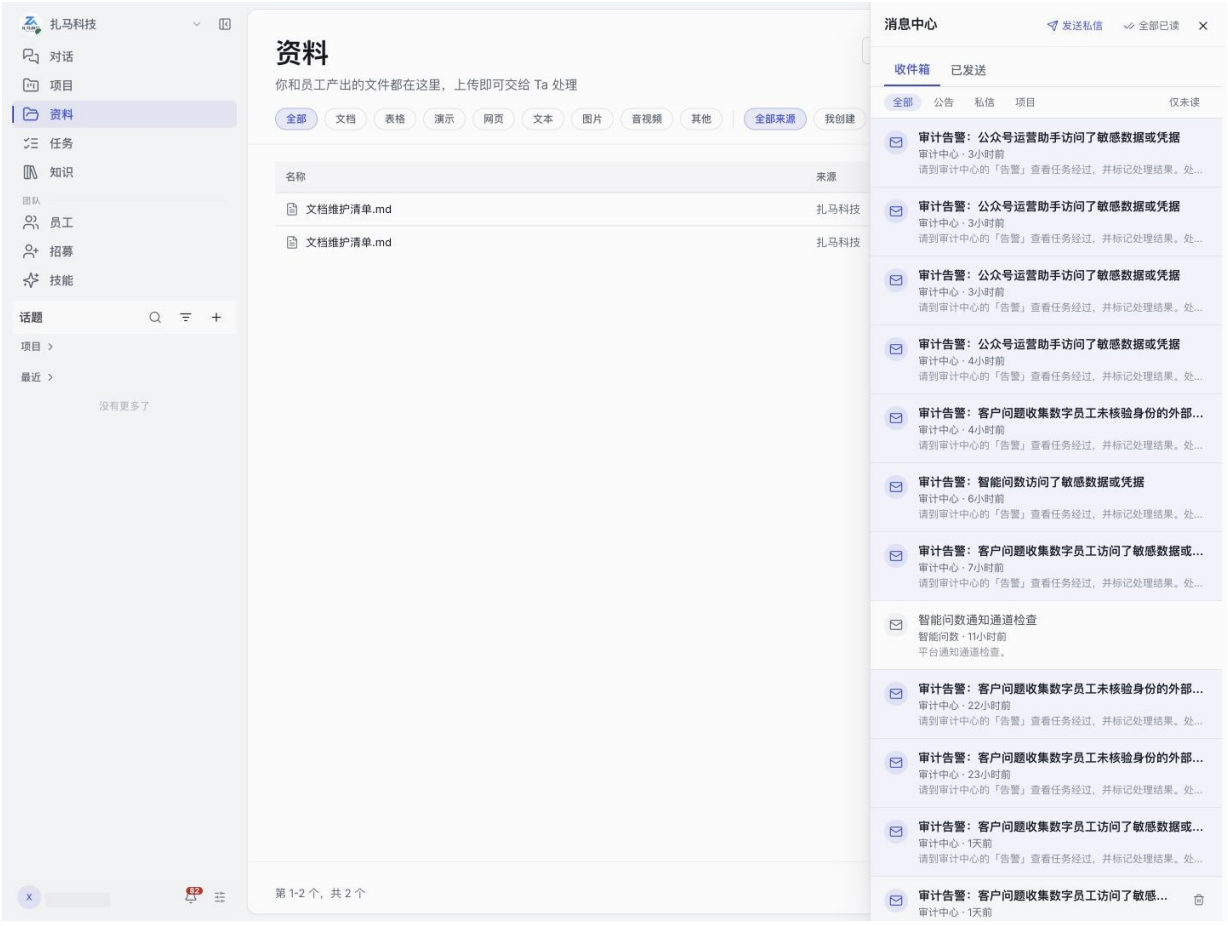
消息与用量

消息中心记录通知与阅读状态，使用量记录指定范围的资源消耗。

通知状态

未读表示尚未标记阅读；使用者打开收到的消息时，系统将该消息标为已读。已读不等于业务已完成。外部通知延迟不能用于判断任务未执行。

系统通知、桌面提醒、邮件与 IM 使用不同投递链路。产品内偏好、系统权限和服务连接需要同时满足。



消息中心的收件箱、消息分类与已读操作

使用量口径

入口	表示什么	用途
对话输入区“上下文”	当前话题使用的 Token 与上下文容量之比。	判断当前话题的上下文占用，不表示账号余额或费用。
账户菜单的使用量入口	当前账号在所选时间段的资源消耗。	使用者查看个人用量。
后台“运维 → 用量分析”	管理员权限范围内的汇总和明细。	管理员按时间、数字员工等维度分析消耗。

相同指标只有在时间、统计对象、单位和更新时间一致时才可比较。

调用次数、Token、额度和金额分别表示不同指标。不同模型的消耗不能按调用次数直接等价。

部署与权限

会员或计费入口按部署方式与菜单条件显示，页面没有入口不构成统一收费规则。后台组织统计仍需相应权限。

统计展示不代替财务凭证。对账依据组织确认的结算规则和可追溯明细。操作见消息与用量。

审计中心

审计中心关联任务执行、配置变更、人工操作、查阅行为及证据。审计中心、发布审核、知识操作记录和运行日志分别维护对应记录与权限。

角色与能力

安全审计员按授权范围读取记录，安全管理员制定策略。平台需要先指派安全管理员，才能开启三员分立。

三员分立状态	职责规则
未开启	管理员可以兼任相应职责。
已开启	管理员不再自动拥有审计权，审计员与安全管理员不得兼任。

摘要读取、完整正文读取、正文审批、范围设置和策略管理是不同能力。告警处置、质检复核、案件、报告生成与保全需要审计处置资格；策略维护与正文审批需要审计配置资格。

“合规报告”仅向具有全部数字员工审计范围的查阅人员显示。知道任务标识、拥有后台菜单或以用户身份查看，均不创造额外正文权限。

页面与记录

页签	记录与边界
概览	汇总指定时间与授权范围内的审计记录。
审计助手	使用“规则 → 使用的模型”中的租户共享模型，只读查询可访问账本，附带证据并记录提问。
告警	风险规则产生的提示、等级及处理状态。
任务	单次工作及其一次或多次执行过程。
合规质检	策略疑似问题的复核队列与主动抽检批次。
调查案件	聚合相关任务、告警、发现、批注及结论。
合规报告	月度、季度或按所选范围汇总，包含期间和生成方。
溯源	以代码、文字或文件定位来源，不显示正文。

页签	记录与边界
按人、按数字员工	从发起人或服务主体汇总并定位任务。
配置变更、人工操作	管理配置变化与手动动作，分别关联执行。
保全	超过普通保留期继续留存的任务，持续到解除。
开放 API 密钥	以签发者身份和范围拉取审计摘要，不含正文。
正文审批	双人审批模式下的申请、决定与临时查看授权。
审计策略、规则	采集留存、访问与证据策略，以及检测/通知规则。
外部对接	向 SIEM、队列、存储、存证或告警通道交付记录。
审计员与范围、查阅记录	维护审计范围并追溯审计内容的访问。
完整性	核对记录链、每日封存、签名、正文及时间戳。

页签及修改动作分别按当前职责授权。

案件的标题必填，说明与负责人选填；结案必须填写结论。案件结案后不能重开或修改，批注不能修改或删除，更正通过追加批注承接。

报告期间按 UTC 计日并包含结束日，只能使用已结束的期间；自定义范围最长一年。同一月度或季度重新生成会替换该期间原报告。



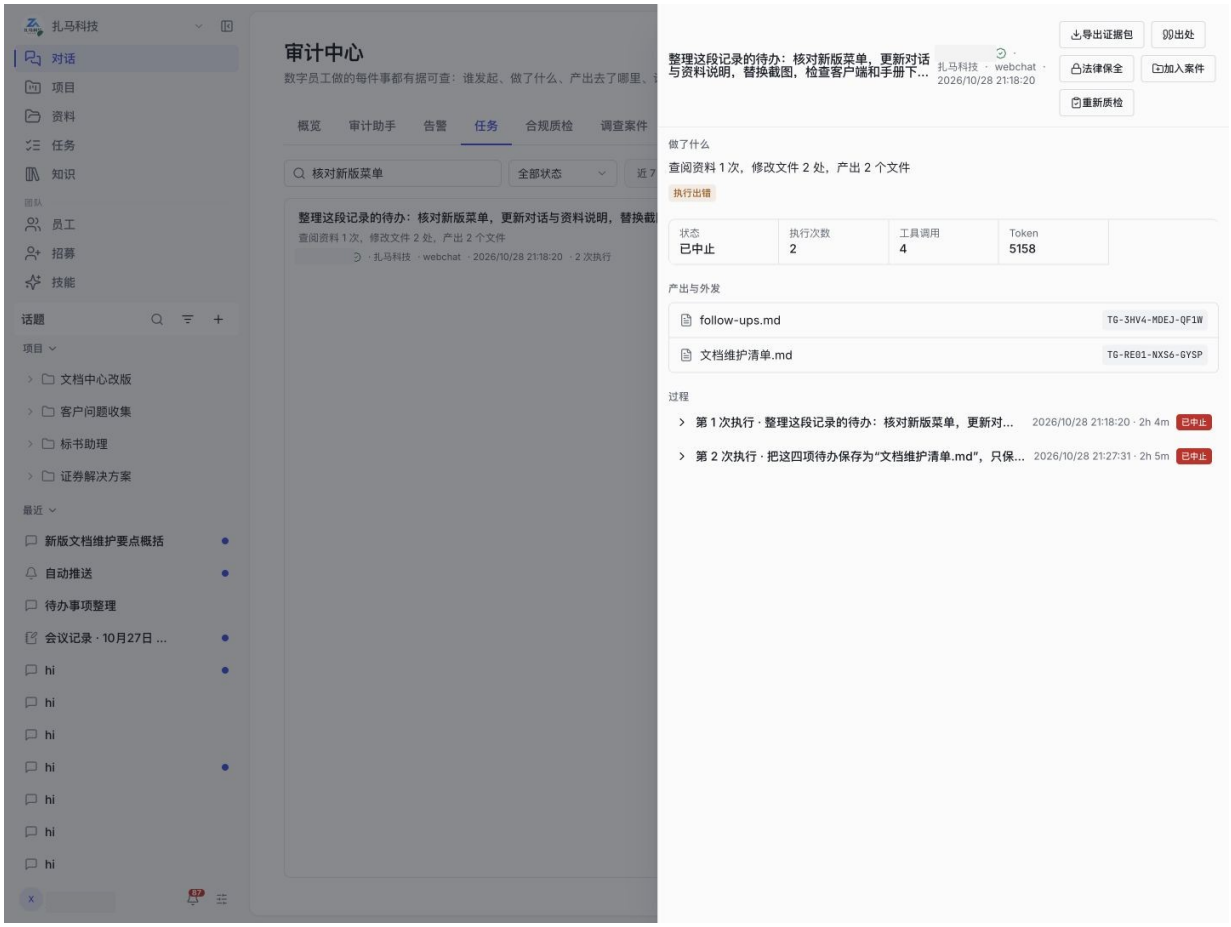
审计中心概览与功能页签

任务与过程

任务信息包含发起人、渠道、数字员工、状态、执行次数、工具、模型消耗、产出与外发记录。执行过程记录读取、检索、写入、命令、消息、委派、技能、确认和护栏等动作。

记录范围以实际采集内容为准。缺少某项工具记录不能证明该项底层行为从未发生。

按人、按数字员工及总体统计均采用当前筛选与授权范围；任务时间、运行时间、封存日期和统计期间分别记录。



任务详情：已中止状态、执行过程、工具调用与产出记录

状态与风险

对象	状态或分类
执行结果	进行中、已完成、失败、中止、超时、拦截。
告警	按等级及待处理、已确认、已处理、误报分类。
质检	待复核、确认违规、判为合规、自动通过等。

告警命中不自动等于违规，自动通过也不表示人工审核。

规则可覆盖高危命令、敏感数据/凭据、策略外网站、大批量外发、非工作时间执行。黑名单与白名单方向相反；关闭提醒不删除记录和告警。

风险阈值由当前审计策略设置。

记录范围与正文

范围可覆盖全部或指定数字员工，并按支持的团队范围限定；不包括任意跨租户读取。正文查看方式分直接查看、填写理由、双人审批，查阅理由与行为均留痕。

双人审批禁止自批，批准后的查看授权 24 小时有效。未留存的正文无法通过审批恢复。

正文审批与是否留存正文分别判断。摘要脱敏主要影响显示，不代表所有原始材料已删除。

完整性与留存

记录按 UTC 日期每日封存，签名根及可用的可信时间戳支持核对。完整性页可选择近 7/30/90 天，并决定是否同时校验正文。

未封存、缺少正文、未配置 TSA、签名或内容校验失败具有不同含义。

项目	留存规则
保留期	范围为 7–7300 天；系统按策略清理超期且已封存的记录。
法律保全	保全记录不参与普通清理。
每日签名	保留期清理不删除每日签名的默克尔根。
正文	遵循正文自身的留存规则。
WORM	依赖已启用 Object Lock 的存储。
算法切换	SHA-256/Ed25519 与国密 SM3/SM2 的切换仅影响后续记录，历史记录仍按原算法核对。

进行中案件的任务自动进入法律保全。结案时，“解除法律保全”默认关闭；未开启时，任务继续保全，结案本身不解除留存。

外部交付与密钥

外部对接包括 OpenTelemetry、Syslog（CEF）、Webhook、Kafka、对象存储归档、第三方存证及告警推送。

元数据和摘要为主要交付内容，归档可选正文。链序、至少送达一次与失败断点重试要求接收端去重。

外部对接的测试使用已保存配置，未保存修改会禁用测试；第三方存证没有相同的测试按钮。

第三方存证失败在 7 天内自动重试。该期限不适用于所有通道。

开放 API 密钥不含正文，按签发者身份和范围读取并留痕。开启三员分立后，只有审计员自己签发的密钥可用。

平台 API Token、个人 MCP 访问令牌和审计 API 密钥是不同凭证。操作见审计中心，总体规则见安全与审计。

技能治理

技能治理管理经验沉淀、审核、共享和运行质量。作者工作区、治理提案、已发布版本和数字员工安装版本分别记录内容与状态。

组织策略

数字员工自学习默认策略提供三种方式：

- 关闭。
- 默认关闭，允许按数字员工开启。
- 默认开启，允许按数字员工关闭。

限制	作用范围与结果
自学技能上限	按用户与数字员工的组合限制自动安装数量；超出后仍可发布到“我的创建”。
每日复盘上限	按用户限制后台复盘次数与模型消耗；达到上限后当天不再触发后台复盘，不限制人工审核次数。



技能治理：自学习策略、数量限制、健康度与晋升候选

提案与审核

提案记录待审、已发布或拒绝等状态，并可有隔离标记。升级提案包含原版本与目标版本内容，审核人员应比较变化。护栏扫描与人工审核各有范围，任一通过都不能替代实际任务验证。

范围与安装

晋升候选可把个人技能晋升到团队或全租户。用户选择团队时需指定组织，已有团队范围按界面允许继续晋升。

晋升后，技能在目标范围内可见并可安装，原作者仍是技能归属人。晋升不会自动为所有数字员工安装技能。

个人安装和管理员为数字员工统一安装具有不同范围。实际调用仍依赖目标 Agent、同步及工具条件。

统计解释

健康度显示九项指标：已发布技能、待审核、可晋升、贡献者、复用次数、平均有效性、已隔离、本地拦截、建议复审。

待审核、已隔离和建议复审用于定位治理待办；复用次数、贡献者和平均有效性供晋升判断参考。

平均有效性不是所有任务正确率，调用次数不是业务成果。建议复审不等于已作降级决定。

版本与历史

维护人员分别核对新版本的发布与安装。修复通过新版本承接，历史提案、审核与执行记录保留。

历史失败记录不能通过覆盖旧内容消除。操作见技能治理。