智域 OS 企业使用手册

面向企业员工 管理员与技术团队

从首次任务到企业部署

使用桌面 AI 工作区完成任务，并在团队授权、资源和费用规则下保存与管理成果。

员工操作

安装登录、选择 Bot 与模型、使用插件、检查成果、分享文件、迁移对话、查询任务与账单。

企业管理

成员邀请、部门与角色、预算与容量、离职交接、触发器、软件更新和设备授权。

技术实施

平台开通、模型与插件发布、源码联调、部署配置、插件 SDK、备份恢复与故障处理。

版本 1.0　2026 年 11 月 5 日

提供编号截图、流程图、操作步骤、预期结果和排障清单。具体开放能力以交付版本及企业配置为准。

插图中的测试数据仅用于说明界面，所有流程示意图均有标注。

目录

可点击章节跳转。按角色选择阅读路径，见下一页。

阅读导览与使用准备 3
1 安装登录与选择团队 4
2 认识工作区与会话 5
3 完成第一个文件任务 6
4 审批执行与检查成果 7
5 选择模型与管理 Bot 8
6 查找并使用企业插件 9
7 安装授权与升级插件 10
8 上传文件与授予分享 11
9 文件版本容量与回收站 12
10 在设备间迁移对话 13
11 查询任务状态与费用 14
12 查看账单与分配预算 15
13 邀请成员与维护部门 16
14 设置角色与团队资源 17
15 停用成员与资料交接 18
16 创建并验证触发器 19
17 桌面软件更新与设备管理 20
18 平台管理员开通企业 21
19 发布模型与接入企业身份 22
20 上传审核与分发插件 23
21 本地开发与联调启动 24
22 部署配置与网络接入 25
23 初始化上线与验收 26
24 业务插件开发与能力接入 27
25 日常运维备份与版本升级 28
26 常见故障处理 29
27 企业培训与交付验收清单 30
28 术语能力范围与技术索引 31

阅读导览与使用准备

本手册用于员工上手、团队管理和技术部署。完成员工路径后，应能独立发起任务、检查成果、查看费用；管理员和技术人员按各自路径完成资源配置与运行维护。

读者	建议阅读	完成目标
员工与业务用户	第 1 至 12 章；第 16 至 17 章	完成任务并保存成果，理解文件与费用
Owner 与团队管理员	第 12 至 16 章；第 25 至 27 章	管理成员、权限、预算、交接与培训
平台管理员	第 18 至 20 章；第 25 章	开通团队，发布模型与插件
部署与研发人员	第 21 至 28 章	部署、接入、备份、升级和排障

开始之前

向企业管理员取得对应系统和 CPU 的安装包、企业服务地址、账号或邀请链接，以及使用规则。确认可用模型、试用预算、数据上传范围和支持联系人。平台管理账号与日常员工身份分别授权。

界面与插图约定

带有“测试界面截图”的图片来自当前 Web 端到端测试，使用模拟服务响应和示例数据；金额、人员、模型参数与日期均不是套餐或性能承诺。浅色与深色主题的操作路径相同。带有“示意图”的图用于解释流程，不代表额外界面或功能。

正文中的“设置 → 模型”表示从设置进入模型页。界面只显示当前身份获准的入口；缺少入口先检查团队与角色，不应直接认定为故障。交付版本的菜单和可用插件可能不同。

文档版本 1.0　核对日期 2026 年 11 月 5 日　示例时区 Asia/Shanghai

适用范围为智域 OS 桌面客户端及企业服务。移动渠道、支付渠道和特定业务系统连接器按项目开放。OS 是产品名称，不代表操作系统内核。

1 安装登录与选择团队

目标是进入正确团队，再开始任何付费调用或文件操作。



图 1 企业账户中的团队身份与切换入口

1. 安装企业分发的智域 OS 安装包。核对包版本、系统及 CPU；首次启动按系统和企业规定完成签名信任与本地权限授予。
2. 在桌面账户入口登录。受邀用户先打开邀请链接，按页面要求登录或注册并接受邀请；注册是否开放、是否验证邮箱取决于部署政策。
3. 从账户入口明确选择自己的团队。进入“设置 → 企业账户”，核对当前组织、套餐与我的角色，再开始工作。
4. 切换团队使用“切换组织”；退出使用“退出登录”。先保存编辑内容并结束需要保留的操作，切换会停止旧团队 Runtime 并清理相应凭据。

结果检查与失败处理

成功后可看到目标团队名称及有效角色。没有目标团队时，请管理员核对邀请是否过期、成员是否有效、席位是否足够。停用成员需要恢复原关系，不能用重新邀请绕过停用。

邀请接受后直接加入，不需要二次审批。遗忘密码走公开账户页的恢复流程；修改部署初始化密码变量不会重置已有账号。

2 认识工作区与会话

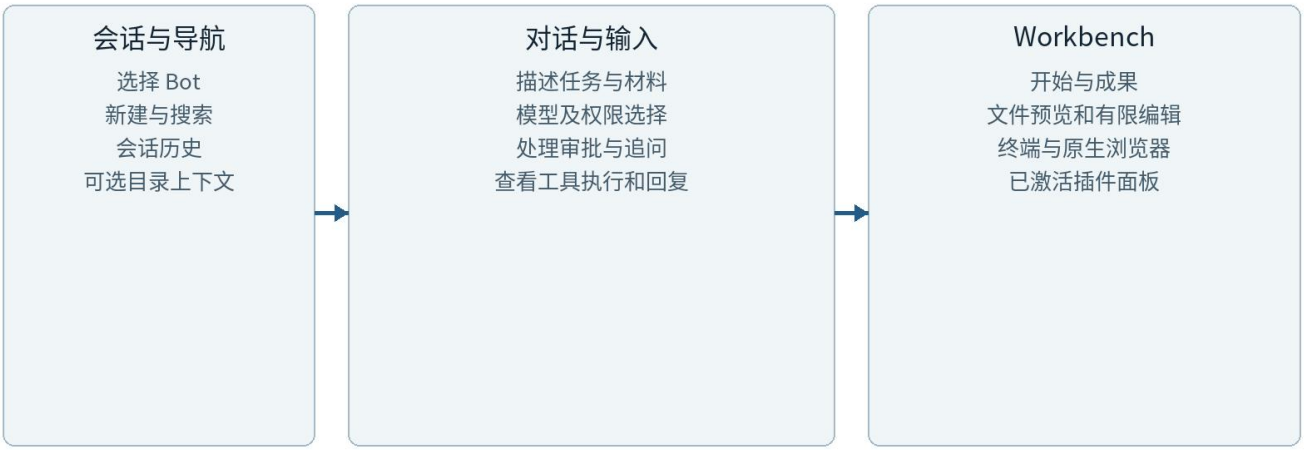


图 2 工作区的三个主要区域 示意图

1 在左侧选择 Bot。点击 Bot 名称打开或复用空白会话，展开箭头查看历史；“新会话”创建独立对话。

2 按任务需要添加上下文目录。目录是可选输入；已有会话添加目录只改变该会话的目录引用，不自动变成另一个 Bot。

3 在中间对话区描述目标、材料、限制和交付格式。输入区的模型与权限选项应在发送前核对。

4 从顶栏打开 Workbench，在开始页选择成果、文件、终端或浏览器；插件可以提供额外面板。

整理历史

使用侧边栏搜索定位标题、目录或对话内容。搜索默认围绕所选 Bot，可显式扩大范围。重命名便于后续检索；分叉从最后一个已完成轮次创建后续分支；归档用于隐藏历史，不等于把文件上传或做完整备份。

读懂状态

“等待审批”“计划待审”“等待回答”表示任务需要你的输入。侧栏活动定时任务标记只反映当前列表记录，不保证运行时在线。不可用 Bot 的历史仍可阅读，但不能据此创建新工作。

3 完成第一个文件任务

练习使用一份获准的非敏感会议纪要，生成可人工复核的行动清单。

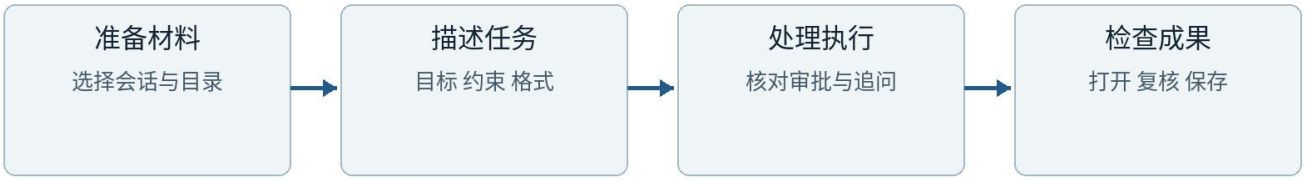


图 3 从任务输入到成果检查的操作顺序 示意图

1. 创建会话，选择可用的通用 Bot 与平台模型。在会话中关联练习目录，放入一份示例纪要；也可通过附件入口或拖放添加材料。
2. 确认附件上传完成。上传失败先重试；只看到文件卡片，不代表附件已被成功接纳。核对当前权限能否写入目标目录。
3. 发送下面的示例指令，检查计划或追问，补充缺少信息。遇到审批先读目标路径、命令及影响，再决定本次允许或拒绝。
4. 任务结束后打开成果文件，逐项核对原文、责任人和截止日期。对缺失信息保留“待确认”，确认后保存或下载交付文件。

请读取本次提供的会议纪要，整理行动清单。
字段：事项、责任人、截止日期、原文依据。
原文没有的信息写“待确认”，不要自行推断。
输出为 Markdown 文件，保存到当前获准工作目录。

预期结果：形成一份可打开的 Markdown 行动清单，内容能够追溯到材料。文件不在成果列表时到 Workbench 文件面板核对目录；模型回答“已完成”不能替代文件检查。

4 审批执行与检查成果

操作范围由当前会话权限决定

常见权限标签为“仅可查看”“工作区内修改”和“完全权限”。企业政策可能限制可选范围。通用设置中的默认权限只影响以后创建的会话；当前会话通过界面选项或 /permission 切换。完全权限需要显式确认。

遇到的情况	你的操作	继续前检查
等待工具审批	读操作详情，选择仅本次允许或拒绝	目标目录、外部地址和写入影响
等待回答或计划审阅	回答问题或修改计划	是否遗漏材料与验收要求
结果包含文件	在成果或文件面板打开	内容、版本、保存位置和可用格式
执行失败或中断	查看失败工具及任务状态	避免重复产生付费或外部写入

使用 Workbench 验收

1. 在“成果”查看当前会话成功变更工具产生的文件；选择条目打开相应预览。同名文件可能属于不同目录，核对来源路径。
2. 在“文件”手动刷新目录。文本和现代 Office 文件提供有限编辑；修改后保存。跨多个格式片段的文字替换可能减少局部样式，正式交付前使用原生 Office 复核复杂版式。
3. 源引用可以定位到 PDF 页、文本行、工作表单元格或媒体时间。原文件版本变化时旧坐标可能不再适用，应核对当前文件。

注意：表格预览显示已保存的公式结果，不重算公式，不执行宏；旧 DOC/PPT 等格式仅预览。未保存草稿主要保留在当前挂载会话内存中，刷新或切换前务必保存。原生浏览器与终端需要对应桌面能力。

5 选择模型与管理 Bot



图 4 默认模型与可用模型分别管理

1 进入“设置 → 模型”，在“可用模型”确认名称、能力与限制，在“默认模型”设置后续请求使用的选项。企业客户端不在此填写供应商密钥或地址。

2 任务需要图片、文件或其他输入时，先核对模型声明的输入能力。目录中出现媒体模型，不表示它适用于所有生成参数或插件。

3 进入“设置 → Bot 管理”，查看可用预设与受管理版本。新会话在侧栏选择 Bot；标题中的 Bot 标签用于确认当前会话身份。

4 需要自定义 Bot 时，从可复制预设创建副本。预设文件在界面外编辑；受管理副本仍保留来源要求，不能靠复制绕过插件授权。

结果检查

更改默认 Bot 不会改写已运行会话。模型选择作用于后续请求；服务端会再次检查可用性。目录没有目标模型时，由平台管理员检查供应商、模型启用与团队发布范围，员工不能输入上游模型名代替平台模型 ID。

图中模型名称、上下文及输出限制来自测试配置，实际能力以当前平台目录和供应商为准。

6 查找并使用企业插件



图 5 插件市场的发现 已安装与可更新入口

1 从侧栏插件市场或“设置 → 企业插件”进入。在发现页使用搜索、类型和分类筛选，并翻页浏览；每页最多 24 个。

2 打开目标版本，核对发布方、产品、版本、执行目标和权限。相同商品名可能来自不同发布方，不能只凭名称判断来源。

3 已获准安装并激活后，回到会话。通过输入区添加插件菜单或 @ 建议选择当前 Session 可见的插件；也可从 Workbench 打开它贡献的面板。

4 核对引用再发送指令。不需要时删除引用；发送前平台会重新检查可用性。选择引用本身不会完成安装、启用或授权。

结果与常见问题

预期看到插件引用、工具、Skill 或相应界面。市场空白目录可能是没有可见产品；先清除筛选并确认团队发布范围。已安装却不能选择时，检查本机授权、激活错误及当前会话的能力范围。

插件引用可能把工具名称和用户可调用 Skill 正文加入请求，增加 token。浏览菜单不会增加模型 token。未经审核的 Host 代码不应作为普通业务附件运行。

7 安装授权与升级插件

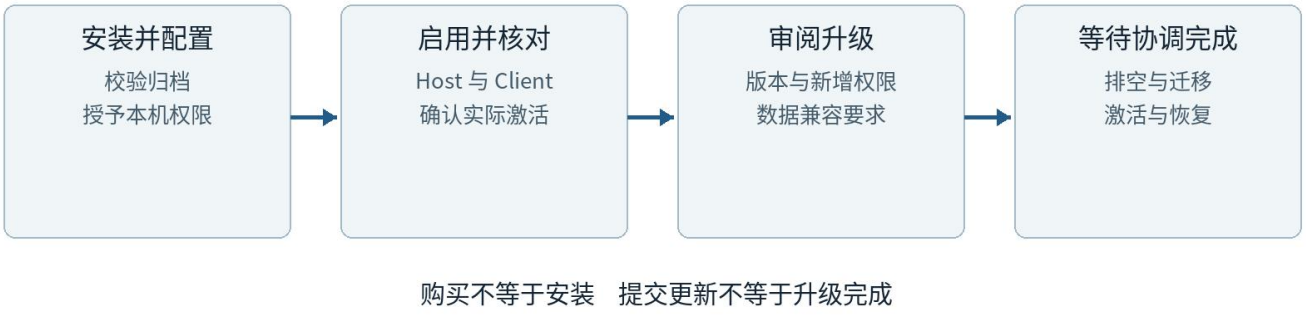


图 6 从安装到升级完成的检查流程 示意图

1. 有 plugin.manage 权限的管理人选择版本并确认安装。平台下载并校验归档后记录安装；根据 Host 或 Client 目标分别完成配置、集成登录和本地授权。
2. 启用目标并等待协调完成。刷新已安装页，确认状态正常；失败时读取具体 target 错误。安装记录存在，不代表本设备已经可执行。
3. 升级时比较当前与目标版本、新增权限、数据迁移和适用设备范围；确认后观察等待排空、迁移和激活进度。提交成功不代表升级完成。
4. 升级失败保留当前操作与错误，按界面重试所选更新。持续维护状态先联系管理员，不反复创建安装，不手工修改迁移数据。

换设备与停用

账号可恢复所选版本、普通配置和启用状态；Keychain 凭据、API key、本地路径、系统和 Shell 权限不随账号复制，新设备需要重新授权。停用、卸载与强制清除按界面权限和确认执行，保留数据行为需读当前提示。

回退与购买

普通更新不提供降级。代码回退需要平台审核、兼容目标和数据声明，不能保证迁移后随时回退。购买或续费仅处理权益，不自动安装；销售开关默认关闭，未开放时不作为使用前提。

8 上传文件与授予分享



图 7 云盘的空间切换 搜索 上传与新建文件夹

1 打开云盘，选择个人、团队或“与我共享”范围，先确认目标空间和文件夹。个人所有权与团队管理权限不是同一概念。

2 通过“上传文件”添加获准材料，等待提交完成；通过“新建文件夹”整理结构。上传会检查容量与权限，失败不能直接认为已经保存。

3 打开文件详情，查看有效受众、继承权限、可访问人数与自己的权限。分享管理员选择成员、部门或团队全员，授予查看或编辑权。

4 保存后让目标成员实际打开验证。部门范围按具体部门 ID 保存，是否包含下级需要明确选择。撤销后再次核对访问。

分享与索引

分享只授予指定访问，不复制文件字节。资料索引由用户或 Agent 填写类型和描述，新索引关联当前不可变版本，可供搜索；它不会自动提取或索引文件全部正文。保存冲突时保留草稿，刷新版本后核对再提交。

已签发下载链接在撤销后可能仍有效至过期。对保密材料应控制分享范围和链接转发。管理员拥有治理权限不代表可以读取所有文件正文。

9 文件版本容量与回收站

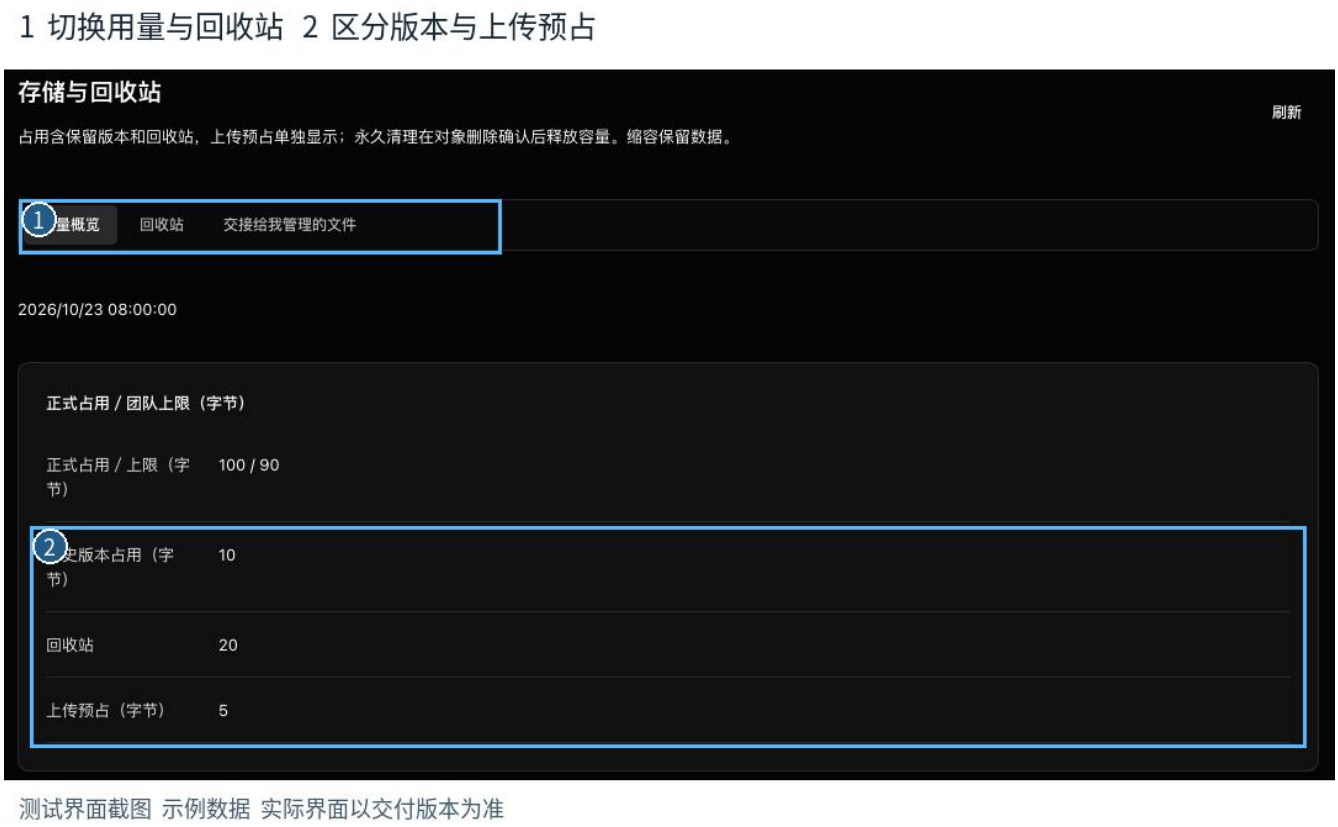


图 8 存储容量与回收站的管理入口

1 在“设置 → 存储与回收站”查看占用构成，区分当前文件、保留版本、回收站与上传预占。

2 需要恢复时切换回收站，选择目标工作区并找到记录，按当前授权执行恢复；恢复后核对原路径、版本及分享。

3 确需释放空间时，先确认备份及保留要求，再由授权人员永久清理。物理删除完成后才释放容量，失败清理需要等待或重试。

操作或对象	容量影响	使用规则
分享	不新增文件字节	仍需明确内容访问授权
复制与保留版本	增加占用	确认目标空间和个人上限
进入回收站	仍然占用	删除到回收站不是立即释放
未清理上传预占	减少可用空间	清理确认后才归还
缩小容量	不自动删除历史	可能阻止新增写入

团队总量包含个人与团队空间，Owner 也受容量限制。直接跨团队移动会被拒绝；同团队移动仍检查目标归属和分享。上传或恢复失败时保留任务标识，不通过重复复制规避容量策略。

10 在设备间迁移对话



图 9 手动上传与下载对话入口

1. 在源电脑保存所有正在编辑的文件，并结束需要归档的会话写入。进入“设置 → 企业账户”，核对账号与团队。
2. 点击“上传本地对话”，等待当前批次完成。失败前已完成的页会保留；在相同账号与团队下重复操作可以续传。
3. 在目标设备登录相同账号并选择相同团队。先关闭仍在写入的本地会话，再点击“下载云端对话”。
4. 下载完成后检查历史列表与消息完整性；单独迁移附件、外部目录和工作区文件，并核对文件引用是否可用。

传输规则

这是一项手动操作，没有后台持续同步。存档包含对话记录，不包含附件和工作区文件，也不复制设备凭据。两个设备的记录需要保留一致前缀；发生分歧会被拒绝，不会自动合并、覆盖或挑选一端。

失败处理

遇到冲突先停止两端写入，保留本地数据和错误信息，联系支持确认差异。不要删除其中一端来试错。对大体积历史应预留内存和传输时间；会话存档不能替代电脑与业务文件备份。

11 查询任务状态与费用



图 10 任务历史分别显示执行 结算和结果保存状态

1 进入“设置 → 任务与结果”，按关键词与状态筛选，使用上一页和下一页检查服务端分页记录。

2 逐项查看执行、结算与保存状态。成功生成但未保存时，先选择目标工作区，再使用原任务的保存重试。

3 账务待核对时保留任务 ID、调用时间和可见错误，等待管理员核对供应商结果。超时、取消或断网不能直接当作免费。

4 在结果恢复期限内保存文件并打开验证。链接或临时资产可能提前失效，遇到失效先查询原任务，不盲目再次生成。

正确的恢复选择

“仅重试保存”复用已有结果及计费身份，不重新生成或计费；重新发起生成属于新任务，可能再次收费。补款、恢复成员或扩容不会自动重放原付费任务，需要重新检查原任务状态后决定。

图中的 Fixture video、金额与恢复日期均为测试值，不是生产保留期限。实际模型任务的可恢复时间、价格和支持操作以当前记录为准。

12 查看账单与分配预算



图 11 个人用量 调用记录与钱包流水分别查看

1 进入“设置 → 账单”，选择近 3、7、30 天或自定义日期；按账期查看对应汇总。管理团队资金需要 billing.read 等相应权限。

2 到“调用记录”检查模型、时间、token、结算状态与金额；“钱包流水”核对充值、调整、结算和退款。导出时保存筛选条件与账期。

3 管理员进入“团队资源与管理 → 成员预算”，选择成员及预算方式，填写金额和操作原因，保存后重新读取确认。

预算如何生效

新增付费请求检查团队正余额与成员当月已结算消费；最终按实际费用完整扣款。并发任务可能造成超预算或负余额。Owner 当前豁免个人预算，但仍受团队资金、状态和容量限制。预算是准入控制，不能当作绝不超支的硬封顶。

核账口径

以服务端结算记录与账本为准，预估费用不是最终金额。请求接纳时固定价格及归属月份；跨月结算仍计入原接纳月份。钱包退款表示平台账务处理，不等于外部支付渠道原路退款。

13 邀请成员与维护部门



图 12 通讯录的成员 部门与待接受邀请

1 以有权限的身份进入“设置 → 通讯录”，点击“邀请成员”，填写对方邮箱和允许授予的角色，发送邀请。

2 在“待接受邀请”跟踪接纳状态。邮件投递与邀请记录分开；邮件失败按支持入口重发，过期或撤销的链接不能加入。

3 选择成员查看资料与状态；调用记录位于受权限控制的独立标签，不应把能看名册等同于能看会话正文。

4 进入“部门”，创建或编辑名称与上级，再为活跃成员分配一个或多个部门。删除前移除下级、成员归属和部门角色。

操作结果

邀请接受后出现有效成员关系，席位不超限；部门树与成员归属符合组织结构。根部门受保护，不能删除。部门组织成员和分享范围，不会自动授予全团队管理权。

对已停用成员，使用授权恢复流程；不要新建账号或重复邀请替代恢复。邮箱纠正、全局账号恢复等高权限操作由平台管理员完成并留存原因。

14 设置角色与团队资源



图 13 自定义角色与授权角色绑定入口

1 进入“团队权限与身份 → 自定义角色”，选择已有角色或新建名称，勾选工作所需权限并保存。先定义职责，再选权限。

2 到“现有角色绑定”，选择成员及角色；若界面提供继承或范围选项，按企业规则显式选择并保存。重新登录或刷新验证实际入口和可操作范围。

3 在“团队资源与管理”维护团队默认、成员预算、成员状态和存储政策。切换标签可保留未提交草稿，修改完成仍需明确保存。

4 从“团队审计”按时间和对象核对授权、预算及状态变化。并发编辑被拒绝时先读取当前版本，再决定保留哪些修改。

职责分开配置

财务查看可围绕 billing.read 授权；插件管理使用 plugin.manage，购买使用 plugin.purchase；身份管理和目录同步分别使用 identity.manage 与 directory.sync。具体可授予权限以当前目录和委托规则为准。

团队管理、存储交接与内容读取分别授权。管理员不要通过扩大文件分享来解决预算或目录权限问题。至少使用一个普通成员和一个受限管理员验证最终权限。

15 停用成员与资料交接



图 14 离职资料的管理交接与内容权限分别处理

离职或调岗的处理顺序

1. 管理员先核对待执行任务、未结算费用与需要保留的文件，再按权限停用来源成员，防止新增工作。
2. 在“存储与回收站 → 交接给我管理的文件”及团队交接入口处理资料。来源成员必须停用，接收成员必须有效。
3. 核对交接结果、明确需要的内容分享，保留审计。交接本身只授予元数据管理与清理，不自动授予下载或分享权。

团队暂停或关闭

先核对任务、资金、资产和必要导出，再由授权人员提交状态变更。关闭保留余额、账单与数据；永久清理文件是另一项明确操作。到期、缩容或减席限制新增，不自动删除历史。恢复后先复核原任务状态，再决定是否重新执行。

交接后分别验证接收人的管理权限与内容权限，保留交接范围和审计 ID。需要读取正文时由有权分享的人另行授权。

16 创建并验证触发器

1 条件 2 目标 3 指令



测试界面截图 示例数据 实际界面以交付版本为准

图 15 触发器分别设置条件 目标与指令

1 打开触发器并新建规则，设置名称、事件来源与计划；循环规则填写正间隔和时间单位，核对开始时间及时区。

2 选择界面实际支持的执行目标，填写 Agent 指令，按需使用“可用变量”，保存后核对规则详情。

3 先用低成本任务测试，在运行历史确认实际触发、输入和成果，再启用正式规则；停用后检查后续监听状态。

规则启用与 Runtime 正在监听是两个状态；本地 Host 必须运行。月年间隔遵循界面说明的日历规则。触发器不等于通用云调度；会话内提醒另受 Schedule 组合和 Session 激活条件限制。

17 桌面软件更新与设备管理



图 16 通用设置中的软件更新状态与操作

1 先保存草稿并核对运行中任务。进入“设置 → 通用设置 → 软件更新”，按当前入口检查已发布版本。

2 下载过程中查看字节数、百分比、速度和校验状态；可按界面取消。设置与启动通知显示同一原生更新状态。

3 等到安装就绪，按原生确认流程安装或重启。下载完成不是安装成功；重启后核对版本、账号和原有工作区。

4 到“企业账户 → 设备”检查云端登录授权。撤销前确认设备；当前页面要求再次确认。丢失设备由管理员按组织流程处理。

失败处理

桥接不可用时更新操作会禁用，按恢复提示启动正确的桌面客户端。签名、哈希或下载失败保留原安装，不使用来源不明的替代包。设备授权有效不代表设备在线；撤销云端授权不等于远程擦除本地文件。

18 平台管理员开通企业

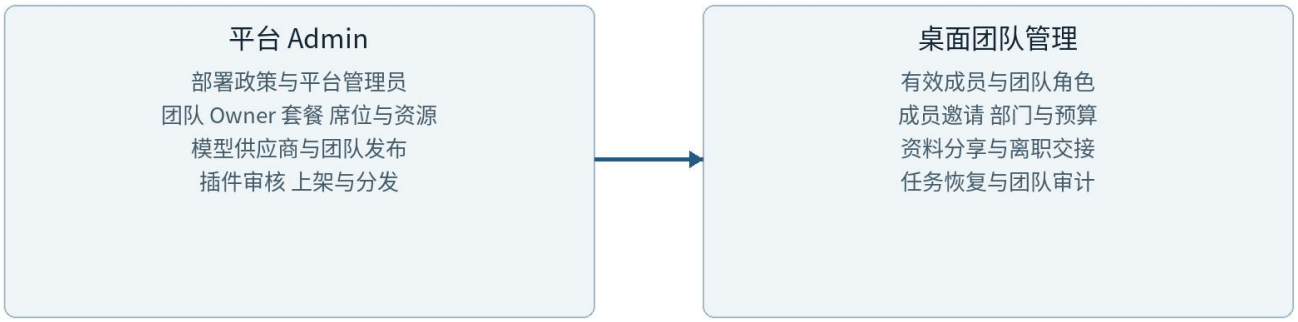


图 17 平台开通与桌面团队管理的职责 示意图

1. 在 Admin 地址以平台管理员登录，先确认部署模式、注册政策和当前环境。平台管理身份本身不授予客户团队内容访问。
2. 在团队管理搜索或创建目标团队，明确 Owner、套餐、席位、资源和余额。对带版本的操作填写原因，确认对象和当前修订后提交。
3. 在套餐目录创建或选择可用套餐，设置团队到期时间与席位覆盖值。分配套餐应用资源默认值，不充值、不清零消费；后续编辑目录不改写已分配团队。
4. 让 Owner 在桌面登录并选择团队，配置角色、成员、预算与文件分享。由实际成员执行一次低成本测试，核对费用和审计。

开通完成的判据

至少有一个有效 Owner；员工能选中团队；模型和插件发布范围正确；资金、容量和席位符合约定。平台后台负责全局开通与恢复，团队角色及部门日常管理主要在桌面完成。

余额调整、Owner 恢复和账号恢复应明确对象、版本与原因。恢复账号可能撤销已有登录凭据，通知用户重新登录；不能用重新初始化部署修复个别账号。

19 发布模型与接入企业身份

配置模型供应商并向团队发布

1. 在 Admin 的模型与供应商资源中创建连接，填写真实供应商地址与密钥，并配置操作版本、输入能力、限制和价格。密钥进入服务端管理，不写入员工文档或聊天。
2. 使用平台模型 ID 管理对外目录，启用模型并选择全部或指定团队发布。普通成员只看到展示信息与能力，不取得上游连接凭据。
3. 用目标团队的实际成员验证一次文本或媒体请求，核对输入支持、返回结果、最终用量与费用；媒体同时验证原结果保存重试。

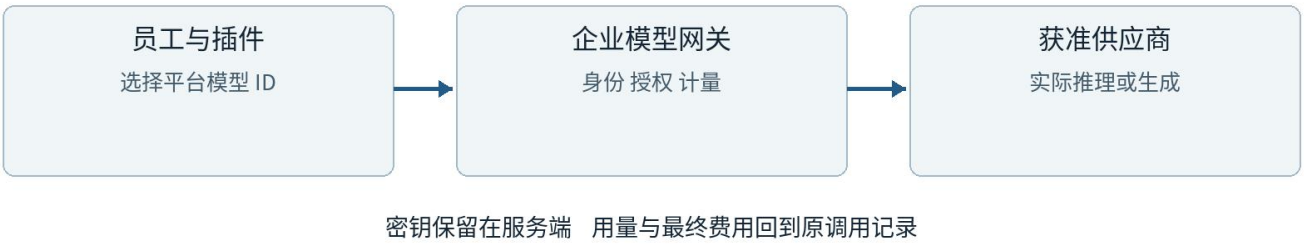


图 18 员工选择平台模型并经网关调用供应商 示意图

私有化身份与目录同步

按项目约定在桌面身份入口维护提供方，在私有部署的 Admin 企业工作区完成字段映射、登录失败诊断、同步脚本、预览和差异审批。Admin 访问还要求有效团队成员关系及 identity.manage 或 directory.sync。

OIDC 与 OAuth2 已有网页登录支持；保存 SAML 或 LDAP 配置不代表登录已联通。目录同步先预览、人工确认再应用，控制台不提供定时或 Webhook 管理。上线前验证停用、恢复、字段冲突与补偿回滚。

供应商连接受公网 HTTPS 与 DNS 安全校验约束，私网地址不能直接假定可接入。身份和模型接入都需要按目标服务完成联调。

20 上传审核与分发插件

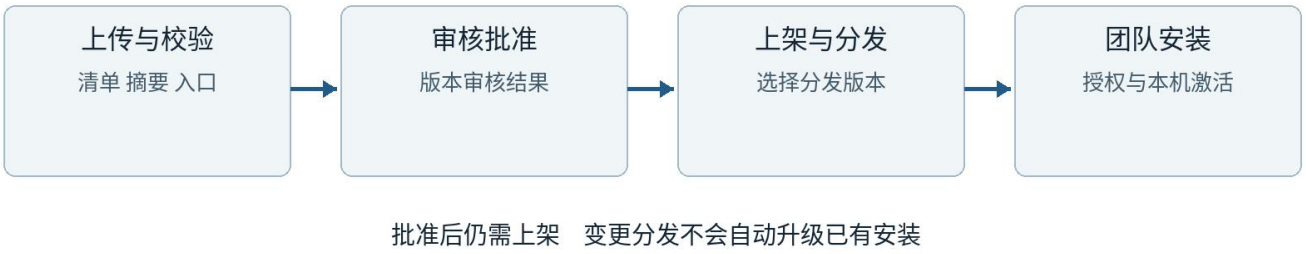


图 19 插件版本审核与分发是独立阶段 示意图

1. 准备标准 .dsh-plugin.zip，核对发布方、商品 ID、版本、目标、权限和不可变摘要。Client 与 Host bundle、资源及预设入口必须与清单一致。
2. 在 Admin /platform/plugins 上传一个或多个包，检查逐项校验与审核结果。平台代理批准失败时，保留版本并使用人工恢复；不要通过更换文件内容覆盖同一版本。
3. 审核批准后执行上架，选择分发版本。配置分类、排序与推荐；批准、上架和切换分发不是同一个操作。
4. 使用目标团队在市场发现、安装、配置并启用，验证工具、Skill、预设及 Client 贡献，再演练升级、停用与卸载。

版本恢复与下架

下架当前分发版本时，需要选择已上架替代版本或明确暂停分发；重新上架不会自动切换分发。下架保留已有安装，撤销发布属于独立的运行权限决策。回退要求有效团队成员关系、plugin.manage、未变化的安装版本及数据兼容性。

当前协议支持 Host、Client 及 v3 仅预设包，不提供 Cloud target。销售开关默认关闭；启用前需另行验收权益、准入、续费和退款规则。

21 本地开发与联调启动

本章用于源码开发环境，生产环境使用已验证的部署产物与发布流程。

准备环境

在仓库根目录使用 Node ^22.19 或 >=24、仓库约定的 pnpm 与可用 Docker。桌面开发另需目标平台的 Electrobun 与原生构建依赖。准备受保护的初始化账号环境变量；密码至少 12 字符，不提交、不打印。

```
pnpm install
# 先在受保护环境设置 ENTERPRISE_BOOTSTRAP_EMAIL
# 和 ENTERPRISE_BOOTSTRAP_PASSWORD，再执行
pnpm run enterprise:start
```

命令会构建 Host 与 Client、初始化项目基础设施、执行迁移与幂等开通，再启动 API 与 Admin。添加 --desktop 会构建并启动桌面开发客户端；首次构建需要等待。已有部署不会重新创建授权。

```
# 需要桌面联调时使用
pnpm run enterprise:start -- --desktop
# 只查看本项目基础设施状态
pnpm run enterprise:infra status
# API 基础连通性检查
curl --fail http://127.0.0.1:8787/health
```

检查与停止

默认 API 为 http://127.0.0.1:8787，Admin 为 http://127.0.0.1:4000。检查登录、明确团队选择、模型目录和一项真实调用；健康接口正常不等于模型或存储验收通过。Ctrl-C 停应用但保留项目基础设施。

8787 或 4000 被占用时，先识别并停止旧的本项目进程再重试。不要删除数据卷处理端口问题，也不要从 package bin 绕过 dsh profile 启动应用。

22 部署配置与网络接入

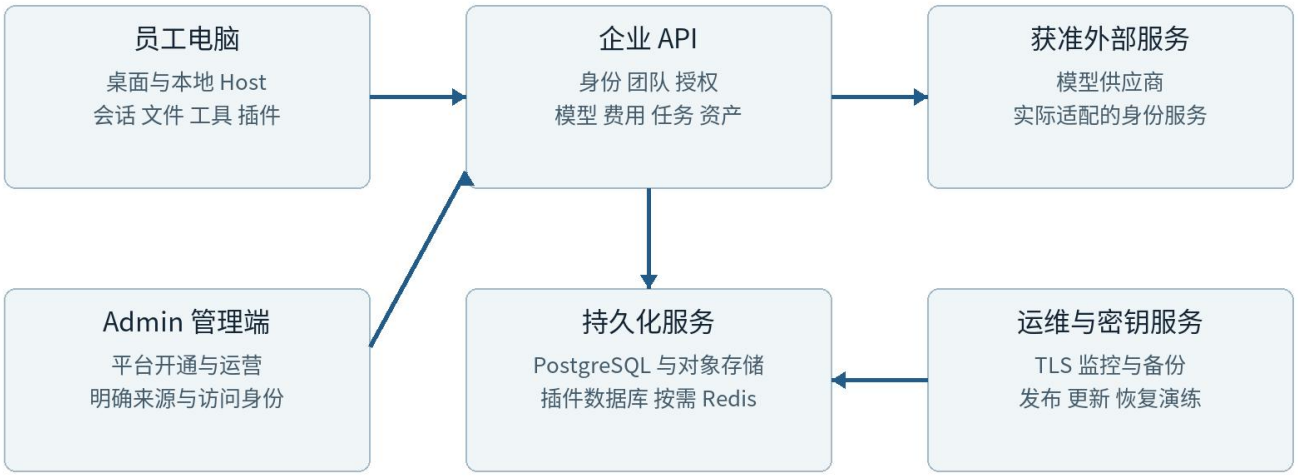


图 20 桌面执行与企业服务的部署关系 示意图

配置组	实际变量或对象	配置要点
数据库	ENTERPRISE_DATABASE_URL ENTERPRISE_MIGRATION_URL	独立数据库；可分迁移与应用凭据
插件数据	ENTERPRISE_PLUGIN_DATABASE_URL	启用插件 SQL 时配置独立数据服务
认证与加密	ENTERPRISE_AUTH_SECRET ENTERPRISE_ENCRYPTION_KEY	前者至少 32 字符；后者为 64 位十六进制
公开来源	ENTERPRISE_API_URL ENTERPRISE_ADMIN_ORIGIN ENTERPRISE_PORTAL_ORIGIN	填写实际公开来源，核对 Cookie 写请求来源
管理端	ADMIN_API_URL	浏览器可访问的 API 地址，不是密钥
对象存储	ENTERPRISE_MINIO_ENDPOINT ENTERPRISE_MINIO_ACCESS_KEY ENTERPRISE_MINIO_APP_PASSWORD	端点和凭据成组配置；另核对 bucket 与 region
协调与模式	ENTERPRISE_REDIS_URL ENTERPRISE_MODE	Redis 按环境配置；mode 为 open 或 private

API 默认只监听 127.0.0.1；容器需 ENTERPRISE_API_HOST=0.0.0.0 并置于安全入口后。服务端配置独立 TLS、受限来源和网络策略。模型网关只接受满足安全校验的公网 HTTPS 供应商地址。

23 初始化上线与验收

容器启动与数据库

使用版本固定的 Backend 和 Admin 产物。Backend 在受支持的 dsh enterprise-api profile 启动前执行初始化与待应用迁移；新部署才需要初始化账号变量。用已验证的部署编排提供参数，不把开发栈默认值直接当成生产配置。

```
ENTERPRISE_DATABASE_URL=postgres://APP_USER:URL_ENCODED_PASSWORD@DB_HOST:5432/dsh_enterprise
ENTERPRISE_BOOTSTRAP_EMAIL=owner@example.com
ENTERPRISE_BOOTSTRAP_PASSWORD=REPLACE_WITH_SECURE_PASSWORD
ENTERPRISE_API_HOST=0.0.0.0
```

上面是占位模板，真实凭据通过秘密管理服务注入。可用 ENTERPRISE_MIGRATION_URL 指向同主机、端口和库的迁移账号。应用与迁移角色分权；超级用户或 BYPASSRLS 会绕过数据库行级保护，不作为隔离验收依据。

首次上线操作

1. 创建独立数据库、对象存储与受控密钥，设置真实来源、部署模式和邮件政策；数据库无安装标记且存在冲突表时应核对目标库，不删除未知关系。
2. 启动 API 与 Admin，检查迁移日志及健康接口。初始化仅在部署不存在时创建管理员；重复启动保留已有账号、政策和成员关系。
3. 通过 Admin 登录，完成团队、套餐、Owner、模型与插件开通；普通成员登录验证跨团队拒绝、预算准入、文件分享及任务保存。
4. 完成备份恢复、断网重连、设备撤销和插件升级演练，记录版本、结果、责任人和恢复步骤后再扩大使用。

邮箱验证启用时配置 ENTERPRISE_SMTP_URL 和 ENTERPRISE_MAIL_FROM。生产容量、并发、可用性及完整安全审计按目标环境验收，配置项存在不代表已通过验收。

24 业务插件开发与能力接入

选择正确的扩展方式

Cordis 提供服务、事件和生命周期；DeepSeek Harness 提供 Agent、工具、Skill、MCP 与会话基础。智域 OS 在其上增加受管理的插件包、安装实例、激活授权、平台 SDK、资源归属与升级协调。新业务行为优先通过这些扩展点实现。

开发步骤	具体工作	验证重点
定义清单	发布方 产品 版本 package target 权限与预设	入口存在、摘要一致、依赖完整
实现业务能力	Host 工具或服务；Client slot 或 window	注册可释放、界面与工具输出一致
使用平台 SDK	models identity objects SQL cache 等获准能力	当前安装与团队归属，错误可诊断
设计持久数据	迁移编号与兼容性声明	中断恢复、旧代码读取兼容
发布与验证	构建标准 ZIP，在目标团队安装	启用、撤销、升级、卸载及数据保留

模型任务调用顺序

以下为调用顺序示意，不是可直接运行的代码
models.list({ operation }) → 选择平台模型 ID
previewTask → 向用户说明报价与参数
createTask → 保存原任务标识
queryTask / listTaskPage → 查询执行与结算
assetAccess / retryTaskSave → 授权读取或保存结果

SDK 绑定当前激活安装，不能选择其他团队、用户或数据空间；撤销后旧句柄失效。Client 不取得平台或供应商 token。Host 属于受信任同进程 Node 代码，SDK 作用域隔离不构成进程沙箱。

外部系统接入另行验证接口、凭据、读写范围与审批。不能因支持 MCP 或网络接口就承诺现成 CRM、ERP 或 OA 连接器。

25 日常运维备份与版本升级

频率或触发	检查对象	需要保留的记录
日常值守	API 与依赖、错误率、容量、任务积压	错误分类、任务 ID、处理结果
每日或按业务 RPO	数据库、插件数据库与对象存储备份	备份时间、保留期、加密与校验
变更前后	模型连接、角色、套餐、版本与迁移	变更原因、审批、差异和验收结果
定期演练	恢复、撤销、交接、升级中断与待核账	实际恢复用时、缺口及修复动作

备份范围

覆盖企业 PostgreSQL、插件数据、对象及版本、部署配置与恢复所需密钥。数据库与对象存储需要一致性策略。另行保护员工电脑会话、附件和工作目录；云端对话存档不是完整终端备份。密钥单独受控，避免与公开备份清单放在一起。

升级操作顺序

1. 记录当前 API、Admin、桌面、插件及数据库版本；做可恢复备份，在演练环境执行相同迁移。
2. 停止或限制新增任务接纳，检查已接纳任务、用量待核对和插件升级维护状态，按任务类别排空处理。
3. 更新经过验证的产物，执行受支持迁移；核对健康、登录、团队权限、模型调用、账务与文件读写，再恢复新增流量。
4. 失败时依据迁移和数据兼容声明决定向前修复或恢复备份，不直接把旧代码覆盖迁移后数据。保留审计与操作记录。

监控应避免收集完整提示词、供应商密钥和文件正文。RPO、RTO、保留期与响应时限由企业约定并通过恢复演练测量，不预设服务等级。

26 常见故障处理

现象	优先排查与处理	升级支持时提供
登录成功但没有团队	核对成员有效性、邀请状态、席位；重新明确选择	账号、目标团队、时间及错误
模型为空或调用被拒绝	核对发布范围、启用状态、成员预算和余额	平台模型 ID 与调用 ID
插件已安装但不可用	核对本机授权、Host/Client 错误与会话可见性	安装 ID、版本、target 和错误
升级长期等待或维护	核对运行中轮次、迁移记录；按原更新重试	升级操作 ID、阶段和时间
已生成但没有文件	查任务保存状态与恢复期；原任务重试保存	任务 ID 与目标工作区
超时却有费用	查看调用结算及待核对状态；不要重复生成	调用记录与对应钱包流水
删除文件容量未减少	检查版本、回收站、上传预占和清理任务	空间、对象 ID 及占用变化
对话下载冲突	停止两端写入、保留数据，交由支持核对分歧	设备、账号团队与冲突信息
浏览器或更新不可用	确认运行正确桌面壳与原生桥接，按提示恢复	客户端版本、系统与桥接错误
API 启动失败	核对配置、数据库角色、迁移与端口；不删库试错	部署版本、脱敏日志与错误分类

提交支持请求

说明操作入口、复现步骤、预期与实际结果，并附发生时间及时区、系统、客户端/API/插件版本、团队和相关记录 ID。截图先遮盖个人资料、密钥与业务内容；原始数据库、完整会话和凭据只走企业批准的受限渠道。

可能已产生付费或外部写入的任务，先保留原 ID 并查询状态。不要用连续点击、重装、清库或重复生成代替诊断。

27 企业培训与交付验收清单

员工上手

1. 完成安装与团队核对，能解释当前 Bot、模型、工作目录和权限。
2. 用获准示例完成第一个任务，处理一次审批，打开并核对成果。
3. 找到账单、任务历史和文件分享入口，知道保存重试与再次生成的区别。
4. 演练手动对话迁移，说明附件和工作目录需要另行备份。

管理员验收

验收项目	通过条件	记录字段
入职与离职	邀请、停用、恢复和交接符合组织规则	参与人、角色、结果与审计 ID
权限与数据	普通成员及受限管理员无法越权	对象范围、拒绝结果和复核人
模型与账务	真实请求能核对用量、结算和原结果保存	模型、调用、任务与账本 ID
插件生命周期	指定版本可安装、升级、停用和卸载	发布方、版本、target 与状态
恢复与更新	备份可恢复，更新后原工作可继续检查	备份点、版本及恢复时间

形成企业自己的操作附件

正式交付时补充：服务与 Admin 地址、支持联系人、目标系统与安装包、可用模型与插件清单、角色矩阵、资料上传政策、预算规则、备份与保留期、RPO/RTO 目标及验收签署记录。培训使用测试资料，不将截图中的金额和套餐当作企业实际配置。

建议由员工、Owner、受限管理员和技术运维共同完成一次端到端演练，确保正常操作与异常恢复均有明确负责人。

28 术语能力范围与技术索引

术语	在本手册中的含义
Bot 与 Session	Bot 是能力预设；Session 是一份独立对话及其事件记录
Runtime 与 Workbench	Runtime 执行任务；Workbench 展示成果、文件及其他面板
安装与激活	安装绑定版本配置与数据；激活是当前获准运行的目标实例
平台模型 ID	企业网关公开的稳定标识，不是上游模型名称
Owner 与平台管理员	Owner 属于团队；平台管理员负责全局开通与运维
预估 结算 保存	分别对应报价、最终费用记录与成果落盘

当前能力的使用边界

本地任务和触发器依赖桌面 Host 运行；SDK 不提供通用 Cloud target。身份协议、真实供应商、业务连接器及私有部署按目标环境联调。手机微信登录、托管账号与团队码仍属规划，微信支付宝支付需适配；销售开关默认关闭。完整安全审计与行业合规以专门报告为准。

研发维护索引

员工界面：packages/client/ui-enterprise、ui-workspace、ui-workbench、ui-agent-preset、ui-permission-presets。部署与平台管理：apps/api/README.zh.md、apps/api/cordis.patch.yml、apps/admin/README.zh.md、apps/electrobun/README.zh.md。

插件开发：packages/plugin/protocol/README.zh.md、packages/plugin/sdk/README.zh.md、docs/developer/plugin-installation-lifecycle.zh.md。团队与账务：docs/developer/enterprise-team-governance.zh.md、docs/developer/model-platform.zh.md。以上为交付源码中的路径。

技术核对基线为仓库版本 d780c62f04。测试截图来自 apps/web/tests/enterprise-settings.e2e.ts，原始来源与裁剪信息随源文件包保存。底层开源执行与扩展基础来自 DeepSeek Harness 和 Cordis，交付保留适用许可与版权说明。

DeepSeek Harness 项目：https://github.com/deepseek-ai/deepseek-harness