

WorkBuddy Enterprise

WorkBuddy Managed Agents



腾讯云

【 版权声明 】

©2013–2026 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

WorkBuddy Managed Agents

产品介绍

快速开始

WorkBuddy Managed Agents

产品介绍

最近更新时间：2026-07-20 21:29:00

WorkBuddy Managed Agents（简称 WMA），提供云端托管的智能体运行服务。底层基于 WorkBuddy Harness 内核构建，无需自建基础设施，轻松调用即可在云端运行复杂任务并接收结果，让企业的每个 Agent 都跑在生产级底座上。WMA 与 WorkBuddy 原生互联，让企业智能体无缝接入 WorkBuddy 管理工作台。



说明：

1. WorkBuddy Managed Agents 在 WorkBuddy 企业管理端已提供服务，腾讯云侧将于近期上线，敬请期待。需要体验的用户可先前往 [WorkBuddy 企业版管理端](#)。
2. 访问 WorkBuddy 企业管理端需先购买 WorkBuddy 企业版座席，前往 [购买](#)。

核心概念

Agent

Agent 定义了一个 AI 助手的完整配置：使用什么模型、扮演什么角色（系统提示词）、拥有哪些技能和工具。

Runtime

Runtime 是企业智能体的核心资源，代表一个独立的 Agent 运行环境，是 Session 背后真正运行的云端沙箱环境。

每个 Runtime 包含：

- 一个云端沙箱实例（完整的 Linux 文件系统和终端）。
- Agent 的配置信息（Manifest），是声明式配置文件（JSON），定义了 Agent 的身份、能力、工作空间和运行环境。
- 一个或多个 Session（会话）。

说明：

创建 Runtime 时会自动创建一个初始 Session。

Session

Session 代表一个用户与 Agent 之间的完整会话过程。一个 Runtime 下可以有多个 Session，每个 Session 维护独立的对话历史和 Agent 上下文。

产品优势

7×24 小时云端运行

WMA 的 Agent 均在云端沙箱运行，可 7×24 小时不间断服务和运行，特别适合长程任务、在线客服、自动触发任务等场景。同时支持自动休眠和毫秒级恢复能力，大幅节省使用成本。

Agent 一键下发 WorkBuddy 端

在 WMA 控制台创建的 Agent 可一键下发至当前账号绑定的 WorkBuddy 端侧企业智能体列表，无缝连接 Agent 从创建到使用环节。支持多种权限管理，用户可灵活管理 Agent 的可见范围和可管理权限。

企业级安全合规，保障数据不出域

WMA 从配置到运行，均在云端执行，基于统一身份实现 Agent 对各个业务系统的安全访问。所有敏感数据，无论是 Skill 配置还是 MCP 调用结果，敏感产出物均实现云端驻留不经过本地，从根源上杜绝企业资产和数据的外泄风险。

WorkBuddy Harness 内核驱动

基于 WorkBuddy Harness 内核构建，内置 Agent 编排、记忆、行动与管控四层能力，释放大模型在长任务场景中的全部潜力，提供更快的执行、更精准的推理与更可靠的任务引导

全流程 Agent 生命周期治理

覆盖 Agent 从上线到运营的全流程治理——统一身份、独立运行环境、全链路 Trace、效果评测与持续优化，为每个 Agent 建立确定性的运行边界与可量化的质量基线

一体化交付的 Agent Runtime

业界领先的 Agent 原生 Runtime 完备沙箱环境，具备数据持久化、跨节点恢复、秒级 Cow Fork、端口转发与预热池一体交付等能力。向下直连腾讯云全栈底座与弹性算力，规模可平滑扩展至万级集群

快速开始

最近更新时间：2026-07-17 19:38:00

1. **登录企业账号**：使用分配了企业坐席的个人账号登录企业后台。
2. **创建 Agent**：点击右上角**企业智能体**进入企业后台，填写基础配置后点击**发布**。
3. **接入渠道**：在**渠道接入**中配置企微 AIBot、QQ 机器人、飞书或钉钉，即可开始使用。

说明：

创建 Agent 后，建议在左侧对话框切换 **Test Run** 模式测试 Agent 的响应效果，确认配置无误后再发布。

创建 Agent

在 **WorkBuddy 企业管理后台**，点击**企业智能体**的**快速开始**，创建 Agent。填写以下配置项后点击右上角**发布**完成 Agent 创建。

The screenshot displays the 'New Agent' creation interface in the WorkBuddy management console. On the left, a sidebar lists navigation items, with 'Enterprise AI' and 'Quick Start' highlighted. The main workspace is divided into a central configuration area and a right-hand settings panel. The central area, titled 'New Agent', offers a 'Build Mode' tab and a prompt to describe requirements or select from pre-built templates such as 'Blank Agent', 'CRM Sales', 'ERP Reporting', and 'Code Review Assistant'. The right-hand panel, under the 'Basic Configuration' tab, contains input fields for 'Agent Name', 'Agent Title', and 'Welcome Message', each with a character count. It also features a 'Select Model' dropdown set to 'Auto' and a 'System Prompt' section with a text area for defining the agent's role and constraints.

基础配置

完成以下配置：

- Agent 名称
- Agent 标题
- 欢迎语

- **选择模型：**支持采用 Auto 模式自动选择或选择**模型管理 > 模型列表**中的内置模型。
- **System Prompt：**在输入框中定义 Agent 的角色、行为规范和约束条件。
- **追问：**预设引导问题

System Prompt

✓ 已配置

定义 Agent 的角色、行为规范和约束条件

你是一名专业的销售运营助手，服务于 B2B 销售团队。你的核心职责：

1. ****客户跟进管理**：**根据提供的客户信息和沟通记录，整理结构化的跟进纪要，标注关键决策点和下一步行动项。

2. ****邮件起草**：**根据客户画像（行业、规模、痛点）和沟通历史，起草个性化的回访/跟进邮件。

305 字符

追问

预设引导问题，最多 5 条，每条不超过 20 字

请输入一个引导问题

0/20

×

追问内容不能为空

+ 添加问题

技能/专家/MCP/连接器

可以为 Agent 添加技能/专家/MCP/连接器，这些配置项会自动同步到 Agent 的 Manifest 中。

- **技能：**为 Agent 挂载技能包，扩充特定领域能力。
- **专家：**为 Agent 绑定专家，扩展领域能力。
- **连接器：**为 Agent 接入第三方平台（腾讯文档、QQ 邮箱等），运行时通过统一网关访问 MCP 工具。
- **MCP：**填写 MCP Server 配置，发布时与连接器合并生效。

基础配置

技能 / 专家

高级配置

Manifest

技能

已选 0 项

为 Agent 挂载技能包，扩充特定领域能力

预设

自定义

Q 搜索技能名称 / 描述 / ID



NeoData金融搜索服务

市场

自然语言查询股票、基金、宏观、外汇、大宗商品等金融数据



wechat-article-search

市场

搜索微信公众号文章（标题、摘要、发布时间、来源账号、链接）



专家

已选 0 项

为 Agent 绑定专家，扩展领域能力

预设

自定义

Q 搜索专家名称 / 专业 / ID



鹏城信息AI专家

内置

会议纪要提取专家 · 项目质量



腾讯云安全运营专家

内置

腾讯云安全运营专家 · 腾讯专家



基础配置

技能 / 专家

高级配置

Manifest

连接器

已选 0 项

为 Agent 接入第三方平台（腾讯文档、QQ 邮箱等），运行时通过统一网关访问 MCP 工具

Q 搜索连接器名称 / 描述

微云

官方



查看、下载、删除微云文件，并且提供上传文件到微云、生成分享链接能力，帮你管理微云文件

授权

Notion

官方



Notion 知识库与项目管理 MCP 连接器，支持读取、搜索和管理 Notion 页面与数据库

授权

Supabase

官方



Supabase MCP，支持数据库与项目管理相关能力。

授权

GitHub MCP

官方



GitHub Copilot MCP Server

授权

日历

企业



授权

共 6 项

上一页12下一页

共 6 项

上一页12下一页

MCP 工具

已选 0 项

填写 MCP Server 配置，发布时与连接器合并生效

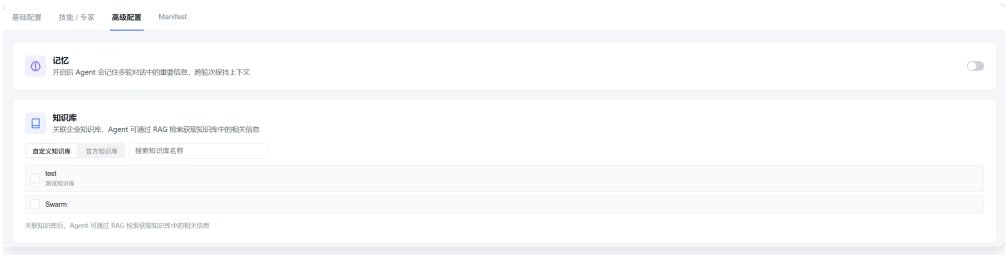
```
{
  "mcpServers": {
    "my-server": {
      "url": "https://mcp.example.com/sse",
      "type": "sse"
    }
  }
}
```

高级配置

- 记忆：开启后 Agent 会记住多轮对话中的重要信息，跨轮次保持上下文。
- 知识库：关联官方知识库和企业后台配置的自定义知识库，Agent 可通过 RAG 检索获取知识库中的相关信息。

版权所有：腾讯云计算（北京）有限责任公司

第9 共18页



Manifest

Manifest 是 Agent 的声明式配置，在创建 Agent 时传入，可在企业后台编辑管理。

最小配置

```
{
  "id": "my-agent",
  "name": "My Agent",
  "manifestVersion": "1.0"
}
```

配置项说明

基础配置

字段	类型	必需	说明
id	string	是	Agent 唯一标识符
name	string	是	Agent 显示名称
manifestVersion	string	是	Manifest 版本（当前 1.0）
system_prompt	string	否	系统提示词（与 system_prompt_file 互斥）
system_prompt_file	string	否	系统提示词文件 URL
useWorkspaceRoot	boolean	否	是否直接以工作空间根目录作为 Agent 的工作目录。为 true 时，Agent 直接在工作空间根目录读写文件，无需再声明 workspaces[]；缺省或 false 时，需通过 workspaces[] 显式声明工作空间。适用于文档/办公型 Agent。

能力配置

字段	类型	必需	说明
----	----	----	----

rules	Rule[]	否	行为规则文件列表
skills	Skill[]	否	预定义技能（pdf, xlsx 等）
plugins	Plugin[]	否	扩展插件
mcp	MCPConfig[]	否	MCP 服务配置
subagents	Subagent[]	否	可调用的子 Agent

工作空间配置

字段	类型	必需	说明
workspaces[].name	string	是	工作空间名（映射到 /workspace/<name>/）
workspaces[].repository	string	否	Git 仓库 URL
workspaces[].downloadUrl	string	否	源码包 URL
workspaces[].ref	string	否	Git 分支 / 标签 / Commit SHA
workspaces[].initShellCommand	string	否	初始化 Shell 命令
workspaces[].initCommand	string	否	CodeBuddy 初始化命令

环境配置

字段	类型	必需	说明
secrets	Secret[]	否	敏感信息（通过安全通道注入，不写入沙箱文件）
envs	EnvVar[]	否	环境变量（写入 manifest 并同步到运行环境）

 注意：

secrets 支持 `${VAR_NAME}` 引用环境变量，避免硬编码密钥。系统会自动注入 `AGENTOS_RUNTIME_ID` 环境变量。

Test Run

在左侧对话框切换 **Test Run** 模式，使用当前配置对话测试 Agent 的响应效果。

渠道接入

支持接入企微 AIBot、QQ 机器人、飞书和钉钉接收和回复 Agent 消息。在企业后台可以管理 Agent 的即时通讯渠道，每条接入记录对应一个 Bot → Session 的绑定关系。

1. 选择类型

例如选择企微 AIBot 接入：

新增渠道接入

1 选择类型

2 填写配置

3 绑定 Session

4 完成

选择接入渠道

选择要接入的即时通讯渠道类型

企

企微 AIBot

注册企微 AIBot，接收企业微信消息

☒

QQ

QQ 机器人

注册 QQ 机器人，接收 QQ 消息

☐

飞

飞书

注册飞书应用，通过飞书接收和回复消息

☐

钉

钉钉

注册钉钉机器人，通过钉钉接收和回复消息

☐

取消

下一步

2. 填写配置

在创建的企微 AIBot 中选择使用 **URL 回调** 的连接方式，点击 Token 和 EncodingAESKey 输入框右侧的**随机获取**。将获取到的 Token 和 EncodingAESKey 填入对应位置：

新增渠道接入

✓ 选择类型

2 填写配置

3 绑定 Session

4 完成

企 企微 AIBot [查看配置指南](#)

连接模式

☒ Webhook

Token *

EncodingAESKey *

取消

上一步

下一步

3. 绑定 Session

选择一个 Session 与此渠道绑定，消息将路由到该 Session：

新增渠道接入

×

✓ 选择类型

—

✓ 填写配置

—

3 绑定 Session

—

4 完成

绑定 Session

选择一个 Session 与此渠道绑定，消息将路由到该 Session

Q 搜索 Session...

○

○

○

○

○

取消

上一步

完成配置

4. 完成

复制 Webhook 地址填入企微 AIBot 连接方式中的 URL 位置：

新增渠道接入

×

✓ 选择类型

—

✓ 填写配置

—

✓ 绑定 Session

—

4 完成

✓

接入成功

企微 AIBot 渠道已配置完成，请将以下 Webhook 地址填入平台后台

Webhook 地址

查看配置指南

/webhook/

复制

完成

❗ 说明：

版权所有：腾讯云计算（北京）有限责任公司

第14 共18页

企微 AIBot 后台相关配置参考 [企微助理](#) 中的使用 URL 回调接入板块。

凭据管理

凭据管理为 Agent 提供安全的凭据存储和代理注入能力。当 Agent 调用 **MCP 服务**、**Skill 技能**或**外部 API** 时，系统会自动将对应的认证凭据注入请求中，无需在代码或配置中明文暴露密钥。

说明：
凭据以加密方式存储，仅在 Agent 运行时由代理层解密并注入请求头，确保凭据在传输和存储过程中的安全性。

添加凭据

进入企业后台，在**企业智能体 > 凭据管理**右上角点击**添加凭据**，填写以下信息后点击**下一步**完成凭据添加。

添加凭据

1 基础信息

2 凭据内容

* Connector

选择要配置凭据的 Connector

当前企业暂无可配置凭据的 Connector

* 凭据类型

* 凭据名称

如：生产 GitHub Token

描述

用途说明（可选）

Agent 管理

Agent

进入企业后台的**企业智能体 > Agent** 板块可以查看已创建的 Agent 信息，对 Agent 进行接入、版本管理、编辑、克隆、删除等操作。

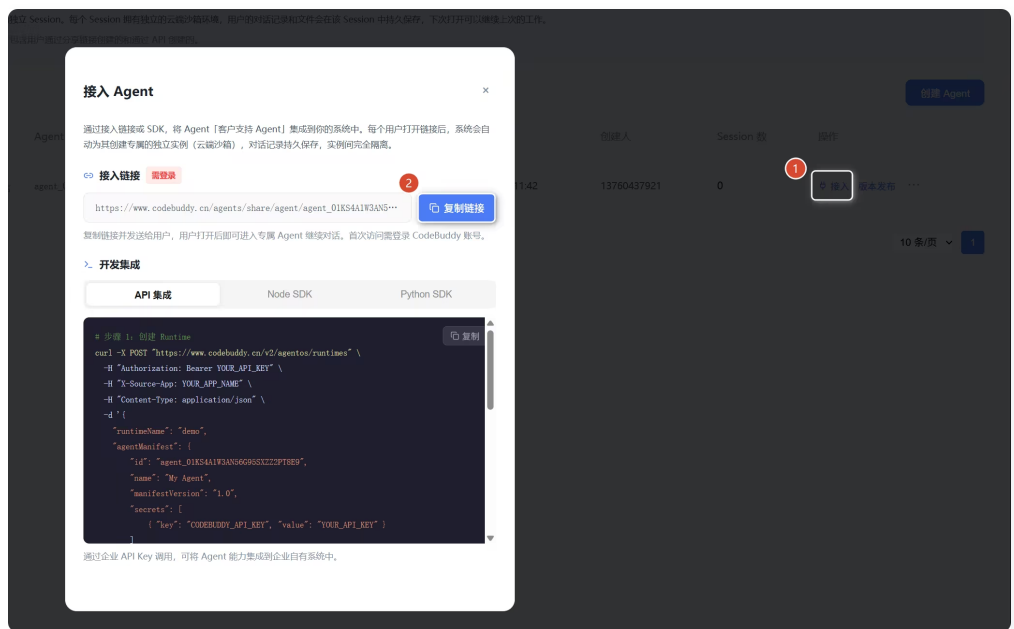


说明：

「Session 数」表示当前基于该 Agent 运行的 Session 总数，包含用户通过分享链接创建的和通过 API 创建的。

团队成员接入

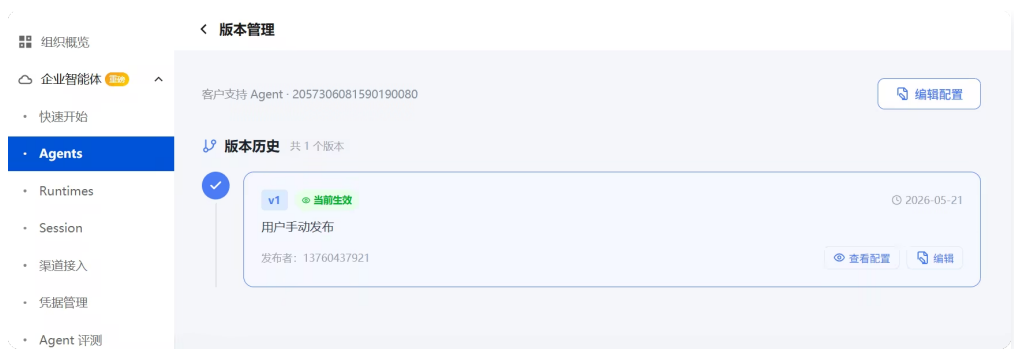
将 Agent 通过**接入**操作，**复制链接**分享给团队成员后，每个人打开链接都会自动获得一个专属的独立 Session。



- **接入链接：**团队成员打开链接可见的独立 Session。
- **开发集成 > API 集成：**通过企业 API Key 调用，可将 Agent 能力集成到企业自有系统中。

版本管理

点击对应 Agent 的**版本发布**操作，进入版本管理页面，查看和编辑版本历史。



Runtime

Runtime 页面面向运维管理，展示沙箱的真实运行状态。

- **创建中**：正在创建沙箱。
- **运行中**：沙箱正在活跃服务。
- **休眠**：空闲超时后自动暂停（再次访问自动唤醒）。
- **已停止**：沙箱停止运行。
- **失败**：沙箱创建或启动异常。

当 Session 出现问题时，可在此排查沙箱模板、状态和错误原因。



说明：
通常 Session 与 Runtime 一一对应。如果 Runtime 没有关联的 Session，可能是 Session 已删除但沙箱资源未回收，建议及时清理以释放资源。

Session

当用户通过分享链接打开 Agent 或通过 API 调用时，系统会自动创建一个专属 Session，承载该用户的所有对话记录和产出文件。

- **对话历史独立**：每个 Session 拥有独立的对话历史和文件存储，用户下次打开可以继续上次的工作。
- **自动休眠机制**：Session 超过 10 分钟无访问会自动休眠以节省资源，再次访问时自动唤醒。

组织概览

企业智能体 最新

快速开始

Agents

Runtimes

Session

渠道接入

凭据管理

自动化任务

Agent 评测

AI 资源管理

Session

Session ID

全部

Runtime ID

用户 ID

查询

重置

Session ID	名称	Runtime ID	状态	创建者	Agent	操作
2077			活跃		CRM 销售助手	查看详情
2077			空闲		CRM 销售助手	查看详情
2077			活跃		AI信息收集助手-t	查看详情
2077			空闲		AI信息收集助手-t	查看详情
2077			活跃		CRM 销售助手00	查看详情
2077			活跃		CRM 销售助手00	查看详情
2077			活跃		代码评审助手	查看详情

列表字段说明

- **名称:** 该 Session 名称，创建时填入。
- **Agent:** 该 Session 中运行的 Agent。
- **Runtime ID:** 该 Session 对应的 Runtime ID。
- **创建者:** 标识该 Session 由谁发起。

Agent 评测

通过标准化的评测任务衡量 Agent 的回答质量。选择目标 Agent 和评测数据集，系统会自动逐条运行测试用例并按照指定的评分方式计算得分，帮助你量化 Agent 的能力表现。

Agent 评测

为什么 Agent 评测?

通过标准化的评测任务衡量 Agent 的回答质量。选择目标 Agent 和评测数据集，系统会自动逐条运行测试用例并按照指定的评分方式计算得分，帮助你量化 Agent 的能力表现。

0

评测数据集

0

评测数据集

0

评测数据集

0

评测数据集

评测数据集

评测数据集

搜索 Agent 名称

全部状态

全部方式

评测数据集

名称	Agent	数据集	评测方式	状态	评测	得分	通过 / 总数	耗时	创建人	创建时间	操作
还没有评测数据，点击创建评测数据集。											

共 0 条数据

10 条/页

1 / 1 页

说明:
启动评测将消耗你的个人积分。