账号连接器

产品简介

腾讯云

文档目录

产品简介

产品概述

最近更新时间：2023-09-19 15:02:01

什么是账号连接器

账号连接器（TencentCloud IDaaS）致力于为企业提供身份认证和数据管理服务，作为新一代企业身份连接平台，可针对多身份源进行数据清洗和数据聚合，适配复杂多样的企业既有应用和认证系统，实现企业应用身份的打通和连接。

产品功能

统一目录（UD）

实现对人员、组织架构及人员组等多维度身份数据的储存及权限规则管理。

功能描述	详细说明
企业统一目录管理	• 存储企业最基本的人员和组织架构信息。 • 支持人员的生命周期管理。 • 提供激活、离职、停用等多个状态。
对象管理	• 基础对象配置：除人员、用户组等基础对象外，还可自定义对象，例如客户、财务等。 • 对象属性管理：除基础属性外，还可以根据自己的业务需求设置自定义属性。
认证源管理	• 支持外部认证源的账号密码或凭证信息登录。 • 允许用户自定义认证源。 • 支持多认证源同时存在，登录时可灵活切换。
密码策略	• 密码强度：支持配置密码长度、复杂度和黑名单等内容。 • 密码重置：支持配置密码有效期和过期重置等内容。 • 密码安全：支持配置验证方式、账号锁定和解锁规则等内容。 • 生效范围：支持根据人员或部门分配密码策略。

账号生命周期管理（LCM）

功能描述	详细说明
同步工作流	• 将不同服务之间的账号打通，有效追踪各个系统之间的账户关联关系。 • 通过灵活制定特殊规则，根据属性来设置使用应用系统的权限范围。

同步数据流	• 对每一个对象同步关系进行同步数据流配置。 • 数据流由不同的节点构成，每个节点负责不同的对数据的处理能力。 • 转换：转换节点提供数据转换和映射功能。 • 删除：对删除节点不同行为的配置。 • 通知：节点动作完成后，进行外部通知。 • 更新/创建：调用目标系统的对应 API 进行数据新建和更新。 • 匹配：将目标应用与数据源的数据进行匹配。 • 同步预览：可根据同步状态筛选，展示每一条数据要进行的同步操作，完成在同步之前的数据校准。 • 同步日志：记录了同步成功及失败的数据，同时展示出失败的原因，也能根据报错信息调整数据。

安全审计（SA）

功能描述	详细说明
日志审计	员工登录门户日志、员工登录应用日志、员工登出应用日志、管理员分配应用日志、数据同步日志。
管理员分级分权	• 安全合规：管理授权、业务操作、审计监察均可独立授权。 • 精细分权：各级授权均可编辑、查看。 • 分级管理：给分类权限均可分级授权。 • 批量授权：通过管理员组批量管理同类授权。

多因素认证（MFA）

账号连接器提供多种二次验证方式，包括扫码、OTP（一次性密码认证）、推送通知等。

登录策略：分别包括全局以及应用登录策略：

- 全局登录策略是对用户登录账号连接器 portal 行为的管控。
- 应用登录策略是对用户通过账号连接器 portal 单点登录具体应用系统行为的管控。

统一管理企业身份账号及应用

- 预集成大量市场主流的 SaaS 和本地部署应用，同时支持 SDK 及标准协议快速适配多样的企业既有应用。
- 作为认证中台，上游集成企业各类第三方认证系统，实现企业应用认证的互联互通。

产品优势

最近更新时间：2023-09-19 15:02:02

与传统的身份管理系统相比，账号连接器具有以下优势：

对比项	传统身份管理	账号连接器
认证	身份信息存储分散、存在两个“无法”	统一安全高效的身份信息管理机制
密码管理	缺乏自动化账号增删和密码管理机制	自动化账号增删和密码管理机制
应用	云及本地应用并存，形成“三高”威胁	安全快速集成各类应用
审计	缺少有效的合规审计手段	完备的安全管理机制

说明

- 两个无法：无法在一个系统中看到所有人的账号，HR、AD 或 OA 系统不统一；无法在一个系统中看到同一个人的所有字段。
- 三高：云及本地应用并存，导致应用集成连接成本高，维护难度高，身份数据泄露风险高。

快速

快速对接各类云端、本地及自研应用，适配各种标准协议及自定义协议，并给无接口应用提供账号连接器 SDK，确保应用的快速对接，对于有标准接口的应用，账号连接器最快只需要2个小时即可完成对接开通。

灵活

不同于项目制的工程方式强行写死同步映射关系，企业所有的同步依靠账号连接器强大的同步流中的转化编辑器来随时编辑修改，不论是组织架构的变化，还是应用的上新或接口调整，或者特殊同步规则的设定，都可以自由配置，随时可控。

可视化

针对于身份管理的专项可视化安全审计服务，所有登录及授权行为全部记录并进行智能分析，优化账号连接器系统内身份管理安全策略。

服务

不同于竞品的项目制发展，账号连接器提供 SaaS/本地部署两种服务类型，所有的项目借助账号连接器高度产品化方案，需求响应速度快，企业随时可以享用不断更新迭代的新功能、新技术，并不断的有售后部门提供专职服务。

专业

国内部分友商基本是从其他行业转型而来，主要提供传统方案，例如堡垒机、企业数据总线等等，账号连接器真正专注做身份信息治理服务，产品的专业度、稳定性和迭代速度为业界领先。

应用场景

最近更新时间：2023-09-19 15:02:02

场景一

国内知名消费级电子雾化器品牌公司，在全国多地成立分公司，员工达千人规模。

场景痛点：

- 多应用多密码管理不便：采用数套 SaaS 应用，多应用多密码的存在给员工日常工作和 IT 管理员带来很大不便。
- IT手动维护账号信息：未建立身份信息同步机制，需要手动在各系统中进行人员账号信息的增删改查，效率低、易出错。

解决方案：

- 构建统一门户：预集成大量主流 SaaS 应用，统一的门户，实现访问权限和安全策略的统一管理。
- 自动化账号增删改查：预集成国内外主流 SaaS 应用，简单配置即可构建所有应用之间的账号同步集成。

方案亮点：

- 只需1人/天配置，快速建立国内外 SaaS 应用之间的账号同步机制。
- 提供 LDAP 拓展能力，实现 VPN 与其他应用的统一身份认证集成。

场景二

全国排名前十的大型券商机构，内部拥有大量自研系统，因业务发展需要不断采用新应用。客户内部员工达数万人规模，分为正式工、临时工、经纪人等多种身份和角色。

场景痛点：

- 应用集成难：自研系统接口参差不齐，很难实现所有应用的快速单点登录和账号同步集成。
- 遗留身份信息改造难：采用 AD/LDAP 对部分应用系统的人员身份信息进行管理，但是难以实现统一的身份信息管理和认证机制。
- 存在较高的安全隐患：IT 手动管理海量人员的账号权限和密码，工作效率低，引发不必要的安全隐患，缺少账号行为审计功能。

解决方案：

- 完备的应用集成：提供多语言超轻量级 SDK 和 SCIM 集成套件，轻松实现云端及本地部署应用的单点登录和账号同步。
- 现代化身份信息管理：无缝对接已有 AD/LDAP 身份信息管理系统，实现对云应用和其他非微软系应用身份信息的统一管理。
- 完备的安全管理策略：自动化的人员信息增删改查机制，确保正确的人有权限访问正确的应用。
- 完备的账号审计功能：集中管理所有用户和 IT 操作日志，确保所有人员操作行为有迹可循，有效防范安全隐患。

方案亮点：

- 快速实现自研系统的单点登录集成。

- 实现所有人员信息和账号权限的集中安全管理。