

# 身份管理服务 IDaaS 操作指南 产品文档





【版权声明】

◎2013-2020 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】

## 🕗 腾讯云

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。



操作指南

## 文档目录

控制台操作指引 开通服务 用户管理 添加用户 修改登录密码 删除用户 认证源管理 企业微信认证源配置 LDAP 认证源配置 数据源管理 LDAP/AD 数据源配置 应用管理 创建应用 创建 OAuth2 应用 配置应用 配置 AWS 应用 配置 Weekdone 配置腾讯企业邮 配置腾讯云控制台 配置 Dropbox 管理应用权限 查看企业信息 企业门户操作指引



## 操作指南 控制台操作指引 开通服务

最近更新时间: 2020-07-10 15:22:26

## 前提条件

目前腾讯云身份管理服务(IDaaS)处于公测阶段。

### 操作步骤

⑦ 说明: 管理员是指主账号或拥有 IDaaS 管理权限的腾讯云账号。

本文为您介绍如何开通身份管理服务(IDaaS),具体步骤如下。

管理员登录 IDaaS 控制台,首次登录需输入"门户 URL"和"企业名称"用于开通服务。
 门户 URL: 仅支持小写英文,下划线,且不能以下划线开头结尾,长度 64 字符内。
 企业名称: 仅支持字母、数字、中文及部分符号,如.()()《》.空格,长度 64 字符内。
 门户 URL 和企业名称都不能有重名。

#### ▲ 注意:

门户 URL 将作为您企业用户访问应用程序的唯一路径,设置后将不支持修改,请您仔细填写。

2. 单击【确认】开通服务。



## 用户管理 添加用户

最近更新时间: 2020-12-24 15:38:40

本文将为您分别介绍"在线创建"和"从本地表格创建"2种用户的添加方式。

### 操作步骤

- 1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【用户管理】。
- 2. 单击【添加用户】,选择对应的方式添加用户。

				添加用户	置用户组
用户ID	姓名	所属组	手机	在线创建	用户来
		测试一组	+86	风本地获惜的建 @qq.com	系统

#### 在线创建

- 1. 填写用户 ID、姓名、手机等基本信息。
  - 。 用户 ID 仅支持数字、小写英文字母、符号(@.\_-),且不能以符号开头。
  - 。 姓名仅支持字母、数字、中文及部分符号,如 @.-()()《》空格,长度64字符内。
  - 。 手机和邮箱不能同时为空。
  - 。 单次最多创建10个用户。
- 2. 为用户设置微信登录,登录密码。
  - 登录密码:管理员可选择"自动生成密码"或"自定义密码"为用户设置密码,密码将发送至用户手机或邮箱,用户首次登录都需要重置密码。

#### 登录方式

#### 登录密码 🔹 🔾 自动生成密码 🔹 自定义密码

密码将发送至用户手机或邮箱,用户登录后需重置密码

3. 单击【下一步】,为用户设置用户组,一个用户可以所属多个组。若需要新增组可以单击【+快速创建组】,进行组的创建。

初始状态下默认存在一个根目录,所有新增的用户组都是根目录的所属组。

4. 单击【完成】,完成用户添加。

#### 从本地表格创建



1. 单击【导入模版】,下载 excel 模板。

#### ← 从本地表格创建

导入用户(	言息	
请下载	模版 , 根据模版格式填写用户信息后上	传
上传表格 <b>*</b>		选择文件
	请上传 excel 文件 , 大小在 5M 以内	

- 2. 按照模板上的规则填写 excel 文件并保存。
- 3. 单击【选择文件】,上传符合要求的 excel 文件。
- 4. 为用户设置微信登录,登录密码。
  - 登录密码:管理员可选择"自动生成密码"或"自定义密码"为用户设置密码,密码将发送至用户手机或邮箱,用户首次登录都需要重置密码。

#### 登录方式

登录密码 *	🔾 自动生成密码		《密码
	密码将发送至用户手	=机或邮箱,	用户登录后需重置密码

5. 单击【提交】,将开始导入用户。

若导入成功,则完成用户添加。若导入失败,可单击【下载失败列表】,查看失败原因。

(!)	导入用户失败			
	未导入有效用户 , 请按	照表格标准填写并	重新上传。	「载失败列表
		重新导入	关闭	



## 修改登录密码

最近更新时间: 2020-06-29 16:43:37

本文为您介绍管理员如何为用户修改登录密码。仅管理员可为用户修改密码,用户无法自行修改。

## 操作步骤

- 1. 管理员登录 IDaaS 控制台 ,单击左侧菜单中的【用户管理】。
- 2. 单击用户 ID, 进入"用户详情"页面。

					添加用户
	用户ID	姓名	所屋组	手机	
			测试一组	+86	
	test		测试一组	+86	
3. 4	单击【安全信息】,读	进入"安全信息"模	块。		
	应用程序	用户组	安全信息		
	微信登录	已关闭			
	登录密码 ****	**** 重置密码			

4.单击【重置密码】,弹出"重置密码"对话框,管理员可选择"自动生成密码"或"自定义密码"。



### 重置密码

 $\times$ 



5.单击【确定】,即可修改用户登录密码。



## 删除用户

最近更新时间: 2020-06-29 16:44:03

本文为您介绍管理员如何删除用户。

#### △ 注意:

- 如果用户仅属于一个组,删除用户后,用户和其应用授权关系将被完全清除。
- 如果用户属于多个组,删除用户后,仅将用户从当前组移除。
- 如果直接从根目录下删除用户,用户和其应用授权关系将被完全清除。

### 操作步骤

1. 管理员登录 IDaaS 控制台 ,单击左侧菜单中的【用户管理】。

2. 在"用户管理"页面,管理员可进行"单用户删除"和"多用户删除"操作。

#### 单用户删除

1.在"用户管理"页面,对应用户右侧操作栏下选择【更多】>【删除用户】。

			漆加用户 设置	身份验证 设置用户组	删除用户
用户ID	姓名	所屋组	手机	邮箱	操作
		测试一组	+86		更多 ▼
		测试二组	+86	设置身份	验证
		测试二组	+86	謝除用户	更多 ▼

2. 系统将弹出确认删除的对话框,单击【确定】完成用户删除。

多用户删除



1.在"用户管理"页面,勾选需要删除的用户,单击用户右侧操作栏上方的【删除用户】。

			添加用户 说	设置身份验证 设置用户组	删除用户
<mark>一</mark> 用户ID	姓名	所屋组	手机	邮箱	操作
		测试一组	+86		更多 ▼
		测试二组	+86		更多 ▼
		测试二组	+86		更多 ▼

2. 系统将弹出确认删除的对话框,单击【确定】完成用户删除。



## 认证源管理 企业微信认证源配置

最近更新时间: 2020-07-16 11:39:34

## 操作场景

IDaaS 支持企业成员通过企业微信扫码登录门户,设置企业微信认证源有两种方法:

1. 首次添加企业微信数据源时,可以设置开启企业微信认证源。

2. 已经添加企业微信数据源,但是尚未设置企业微信认证源时,可以后续单独开启并设置企业微信认证源。

本文将为您详细介绍这两种方法。

### 操作步骤

#### 方法一:首次添加企业微信数据源

- 1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【数据源管理】。
- 2. 单击【添加数据源】,选择【企业微信】,单击【创建】后即可进入企业微信数据源设置页面。

Х

#### 添加数据源

Ø	腾讯云账号 同步您在腾讯云访问管理(CAM)管理的用户及用户信息至IDaaS
$\bigcap$	企业微信 同步您在企业微信管理的成员及成员信息至IDaaS
	创建取消

3. 填写数据源描述(选填),企业 ID 和通讯录 Secret,单击【下一步】。



。 企业 ID: 可前往【企业微信管理后台】	>	【我的企业】	,	获取企业 ID。
------------------------	---	--------	---	----------

行业类型	IT服务-其他 修改
人员规模	1-50人 修改
创建时间	2017年6月9日
企业ID	
	已成为企业微信服务商,前往服务商平台

通讯录 Secret:可前往【企业微信管理后台】>【管理工具】>【通讯录同步】,开启 API 接口同步后,获取 Secret。

	通讯录同步 可通过API接口或第三方应用同步通讯录
同步方式	API接口
权限	API只读通讯录 编辑 可通过API接口读取企业微信通讯录
Secret	重新获取

- 4. 设置数据同步规则:
  - 自动同步:如果选择开启,IDaaS可根据用户自定义的时间从企业微信同步用户信息。如果不开启,也可以手动进行数据同步。
  - 。 自动同步时间: 支持4、12、24个小时。
  - 。同步规则:当同步的用户和 IDaaS 系统里的用户重复,可以选择不同步或覆盖。
- 5. 可以选择为用户设置密码登录和企业微信扫码登录。
- 6. 企业微信扫码登录设置。设置企业微信扫码登录需要企业自建应用,详细操作如下:

i. 前往【企业微信管理后台】	>	【 应用管理 】	,	自建应用模块下单击	(创建应用)	0
-----------------	---	----------	---	-----------	--------	---

自建





ii. 填写应用名称和应用介绍(选填),设置应用可见范围,单击【创建应用】。

#### ▲ 注意:

应用可见范围设置时,请设置全员或需要通过企业微信扫码登录 IDaaS 门户的用户。不在可见范围内 的用户也将无法通过企业微信扫码登录。

#### iii. 获取自建应用的 AgentId 和 Secret。

	自建应用A ~ 暂无应用介绍	已启用	
Agentid Secret			编辑

#### 7. 回到 IDaaS 控制台将应用的 AgentId 和 Secret 填写至企业微信扫码登录的表单里。

自建应用 AgentId *	请输入自建应用 AgentId
	可前往企业微信管理后台-应用管理自建应用,在应用信息中获取 AgentID
自建应用 Secret *	请输入自建应用 Secret
	可前往企业微信管理后台-应用管理自建应用,在应用信息中获取 Secret

8. 复制 IDaaS 提供的"企业微信授权登录回调域",单击【完成添加】。

请将该域名填写至"企业微信授权登录"设置项里
取消 完成添加

9. 前往【企业微信管理后台】>【自建应用】的开发者接口模块,单击"企业微信授权登录"下的【设置】。

开发者接口





#### 0. 单击【设置授权回调域】。

请配置所需的类别		获取帮助
Web网页 使用企业微信扫一扫登录	iOS 嵌入登录分享SDK,实现一键登录、内容分享	Android 嵌入登录分享SDK,实现一键登录、内容分享
设置授权回调域 ②	设置 Bundle ID ⑦	设置该应用签名和包名 ⑦

1. 将 IDaaS 提供的"企业微信授权登录回调域"填入,单击【保存】,完成企业微信认证源配置。



### Web网页

使用企业微信扫-	一扫登录
----------	------

授权回调域	?



取消

保存

## 方法二:已经添加企业微信数据源

#### ? 说明:

此方式适用于已经添加企业微信数据源,但是尚未设置企业微信认证源。

1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【认证源管理】。



3.

4.

2. 单击【添加认证源】,选择【企业微信扫码认证】,单击【创建】后即可进入企业微信数据源设置页面。

添加认证源		×	
创建认证源需添 对应方式的数据	加对应方式的数据源。如果您还未同步用户,请前往数据调 源并同步用户。	原管理添加	
上 時間 通过	入云账号授权认证 腾讯云账号同步的用户可使用腾讯云账号授权登录进行身份	分认证	
	2. 微信扫码认证 企业微信同步的用户可使用企业微信扫码登录进行身份认证	E	
填写企业 ID ,可育	创建 取消 前往【企业微信管理后台】>【 <mark>我的企业</mark> 】,获取	企业 ID。	
行业类型 人员规模	IT服务-其他 修改 1-50人 修改		
创建时间 企业ID	2017年6月9日 1 已成为企业微信服务商,前往服务商平台		
⑦ 注意: 认证源填写的 过企业微信	的企业 ID 需和数据源的企业 ID 保持一致,如果不 ∃码登录。	一致,通过企业微信同步的用户将无法道	<u>آ</u>
企业微信扫码登录i i. 前往【企业微信 自建	殳置。设置企业微信扫码登录需要企业自建应用,i 管理后台 】>【 <mark>应用管理</mark> 】,自建应用模块下单击	详细操作如下: <del>.</del> 【创建应用】。	
● 机器	人 企业小助手	十 创建应用	



ii. 填写应用名称和应用介绍(选填),设置应用可见范围,单击【创建应用】。

#### ▲ 注意:

应用可见范围设置时,请设置全员或需要通过企业微信扫码登录 IDaaS 门户的用户。不在可见范围内 的用户也将无法通过企业微信扫码登录。

#### iii. 获取自建应用的 AgentId 和 Secret。

	自建应用A ~ <sup>暂无应用介绍</sup>	已启用	
Agentid Secret			编辑

#### 5. 回到 IDaaS 控制台将应用的 AgentId 和 Secret 填写至企业微信扫码登录的表单里。

自建应用 AgentId *	请输入自建应用 AgentId
	可前往企业微信管理后台-应用管理自建应用,在应用信息中获取 AgentID
自建应用 Secret *	请输入自建应用 Secret
	可前往企业微信管理后台-应用管理自建应用,在应用信息中获取 Secret
6. 复制 IDaaS 提供的	"企业微信授权登录回调域",单击【完成添加】。

企业微信授权登录回调域	loudidaas.com ┗ 请将该域名填写至"企业微信授权登录"设置项里	
取消 完成添加		

7. 前往【企业微信管理后台】>【自建应用】的开发者接口模块,单击"企业微信授权登录"下的【设置】。

开发者接口





#### 8. 单击【设置授权回调域】。

请配置所需的类别		获取帮助
	iOS	Android
	駅八豆米刀字3DK,头现 <sup>™</sup> 健豆米、内谷刀字	取八豆水刀子3DK,头现一谜豆水、闪谷刀子
设置授权回调域 ⑦	设置 Bundle ID ⑦	设置该应用签名和包名 ⑦

9. 将 IDaaS 提供的"企业微信授权登录回调域"填入,单击【保存】,完成企业微信认证源配置。



### Web网页

使用企业微信扫一扫登录

授权回调域 🕐



保存

取消



## LDAP 认证源配置

最近更新时间: 2020-08-28 16:07:25

## 操作场景

IDaaS 支持企业成员通过 LDAP/AD 用户名密码登录门户,本文将为您详细介绍如何进行 LDAP 认证源配置。

### 配置步骤

- 1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【认证源管理】。
- 2. 选择【启用】LDAP 认证源,即进入 LDAP 认证源设置页面。
- 3. 填写认证源配置信息。



LDAP
Idap://196.0.0.0:389/ I Idap://196.0.0.0:389/,暂不支持 Ipv6
dc=users,dc=com 译会在所埴节点下认证用户,如:dc=users,dc=com
cn=administrator,dc=users,dc=coi j填写有上述 Base 管理权限的节点,如: cn=administrator,dc=users,dc=corr
sAMAccountName=\$userId\$ ]: sAMAccountName=\$userId\$



- LDAP URL: 请填写 LDAP 服务器 IP 与端口号。若服务器 IP 为196.0.0.0,端口号为389,则填写 ldap://196.0.0.0:389/,目前暂不支持 IPv6。
- 。 LDAP Base: LDAP 中的节点,认证时将会从该节点下匹配用户节点进行认证,如: dc=users,dc=com。
- LDAP 账户:请填写有上述 LDAP Base 管理权限的节点,认证过程需有管理权限才能进行,如: cn=administrator,dc=users,dc=com。
- 。 LDAP 账户密码:请填写上述 LDAP 账户对应的密码。
- ・ 用户过滤条件:请填写 LDAP 匹配腾讯云 IDaaS 用户 ID 的过滤条件,如: sAMAccountName=\$userId\$,
   \$userId\$ 为本系统用户 ID 参数,是目录用户唯一标识符。具体规则可参考 LDAP 官方文档。
- 4. 单击【提交】,LDAP 认证源配置成功!



## 数据源管理 LDAP/AD 数据源配置

最近更新时间: 2020-09-25 16:55:10

本文将为您详细介绍 LDAP/AD 数据源配置。

## 操作场景

腾讯云 IDaaS 支持通过 LDAP 从 AD 中拉取组织机构和账户信息至 IDaaS 用户目录,本文将为您详细介绍 LDAP/AD 数据源配置与同步方法。目前仅支持 Windows AD。

### 操作步骤

- 1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【数据源管理】。
- 2. 单击【启用】LDAP/AD 数据源,即可进入 LDAP/AD 数据源设置页面。

#### 数据源管理

() 腾讯云IDaaS支持企业微信。	LDAP/AD、腾讯云访问管理(CAM)3种数据源,您可设置将	数据源的用户导入至IDaaS平台		
数据源名称	数据源描述	数据源状态	启用时间	操作
▶ 腾讯云账号		已开启	2020-08-03 14:32:34	禁用 同步 查看日志
○ 企业微信		已开启	2020-08-14 16:22:21	禁用 同步 查看日志
ldap LDAP/AD	同步您在AD管理的成员及成员信息至IDaaS	未开启	-	<b>启用</b> 同步 查看日志

3. 配置 LDAP/AD 数据源。



#### i. 填写 LDAP 服务器配置信息。

LDAP服务器配置	
服务器地址★	
端□号★	389
Base DN *	OU=testcompany,DC=taotest,DC:
连接方式	使用SSL连接
管理员 DN *	CN=administrator,CN=Users,DC=
密码 *	••••••

- 服务器地址:请填写 LDAP 服务器 IP。例如100.0.0.1,目前暂不支持 IPv6。
- 端口号: 请填写 LDAP 服务器端口号。例如389。
- Base DN: 请填写 LDAP 服务器的 Base DN。例如 OU=testcompany, DC=test。
- 连接方式:请选择是否使用 SSL 连接。
- 管理员 DN: 请填写 LDAP 服务器的管理员 DN。例如 CN=administrator,CN=Users,DC=test,DC=com。
- 密码: 请填写 LDAP 服务器的管理员密码。
- ii. 填写字段匹配信息,即 IDaaS 中字段与 LDAP/AD 中字段的匹配关系。

字段匹配	
用户ID・	CN -
	此字段将作为用户登录IDaaS时的用户名,一般选择 CN,若您的 CN 字段值为中文,建议您使用 sAMAccountName
姓名•	Name -
	此字段将是IDaaS用户目录中的姓名,一般选择Name
手机字段	TelephoneNumber 👻
	此字段将是IDaaS用户目录中的手机号,一般选择TelephoneNumber
邮箱字段	Mail -
	此字段将是IDaaS用户目录中的邮箱,一般选择Mail

- 用户 ID:此字段将对应 IDaaS 用户目录中的用户名字段,一般选择 CN。注意:若您的 CN 字段值为中 文,将无法同步 AD 数据源信息至 IDaaS,此时建议您选择 sAMAccountName 字段。
- 姓名:此字段将对应 IDaaS 用户目录中的姓名字段,一般选择 Name。



- 手机字段:此字段将对应 IDaaS 用户目录中的手机字段,一般选择 TelephoneNumber。
- 邮箱字段:此字段将对应 IDaaS 用户目录中的邮箱字段,一般选择 Mail。

iii. 进行密码设置,可选自动生成密码或自定义密码。

密码设置	
初始登录密码 *	○ 自动生成密码 ○ 自定义密码 密码将发送至用户手机或邮箱,用户登录后需重置密码

iv. 进行数据同步设置,目前支持手动同步和自动定时同步。若选择定时同步,可选同步频率。

数据同步设置	
同步方式 *	● 手动同步   ○ 定时同步
同步规则 *	● 若用户 ID 重复,该用户不同步 ○ 若用户 ID 重复,该用户覆盖 IDaaS 中的用户

v. 配置完成后,单击【保存并启用】完成。之后下载并安装 Qcloud AD Agent。

(!)	注意:
Ū	您必须成功安装AD Agent,IDaaS才能通过 LDAP 从 AD 中拉取到组织和账户信息,数 据源才能同步。 您可以在LDAP/AD数据源详情页下载Agent并获取安装所需的配置信息。
	确定

4. 下载并安装 Qcloud AD Agent。



#### i. 在 LDAP/AD 数据源详情页下载 AD Agent。

- LDAP/AD

<ol> <li>腾讯云 IDaas</li> </ol>	S 支持通过 LDAP 从 AD 中拉取组织机构和账户信息,支持手动同步与定时同步。目前仅支持Windows AD。您必须成功安装AD Agent,LDAP/AD数据源才能同步成功。不知道如何配置? <u>点击这里</u>
数据源信息	
数据源名称	LDAP/AD
数据源描述	演示验证
Agent 配置信息	Agent安装成功,IDaaS才能通过 LDAP 从 AD 中拉取到组织和账户信息。安装时需填入以下信息。
Agent 下载地址	点击下载
同步 ID	5f0ef93 383c 🗖
同步 Token	90dbdf c6 T
同步加密 Key	NTZjMm DhjNjQ5N2VhMTk5YjI0NmRkNzQ I
同步 URL	https://evt.service.cloudidaas.com/release/proxy_kafka/ldap/a51f9d2c58f0a15e244 3c5d3d42c91127ec57e665f88a 🛅

- ii. 下载好安装文件后,安装 AD Agent。过程中需输入 Agent 配置信息中的同步 ID、同步 Token、同步加密 Key 和同步 URL。
  - LDAP/AD

<ol> <li>         ·</li></ol>	支持通过 LDAP 从 AD 中拉取组织机构和账户信息,支持手	加同步与定时同步。目前仅支持Windows AD。您必须成功安装AD Agent,LDAP/AD数据源才能同步成功。不知道如何配置? <u>点击这里</u>
数据源信息		
数据源名称	LDAP/AD	请输入Agent電置信息
数据源描述	演示验证	
Agent 配置信息	Agent安装成功,IDaaS才能通过 LDAP 从 AD 中	同步 ID: 5£0°£935 383°
同步 ID	5f0ef935: 3a383c F	■ 同步加密 Key:
同步 Token	90dbd 7c6 Г	kal≩⊾ nxr:
同步加密 Key	NTZjMmYyMWZmYTBjM 2VhMTk5YjI0NmRkN	QCloudADAgent installer
同步 URL	https://evt.service.cloudidaas.com/release/proxy_kafka/ld	< 上一步 (B)

5. 至此,您已完成 LDAP/AD 数据源的配置。

注意:
若想使用 AD 账号登录 IDaaS 门户,还需将 LDAP/AD 数据源同步至 IDaaS 并配置 LDAP 认证
源。



## 应用管理 创建应用

最近更新时间: 2020-06-29 16:45:40

本文为您介绍管理员如何创建应用。

### 操作步骤

1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【应用管理】。

- 2. 单击【新建应用】,进入"新建应用"页面。
- 3. 选择应用程序类型,并填写应用名称和应用详情。
  - 。 应用名称: 仅支持字母、数字、中文及部分符号,如.()()《》.空格,长度64字符内。
  - 。 库应用程序: 应用程序的基本信息已预设,仅需补充少量特有信息。
  - 。 自定义 SAML2.0 应用程序:可以自定义添加支持SAML2.0的应用程序。

🗲 新建应用

	<b>库应用程序</b> 添加已配置预设模版的库应用程序	自定义 SAML2.0 应用程序 创建支持SAML2.0的应用程序
应用名称 *		
应田详信		

4. 单击【提交】,完成应用的创建。



## 创建 OAuth2 应用

最近更新时间: 2020-10-16 17:45:00

此篇文档将向您介绍 Web 网页应用如何使用 IDaaS OAuth API 实现自建应用对 IDaaS 目录用户进行身份鉴权 并获取用户授权的身份信息。

## 步骤一: 创建 Oauth 应用

登录 IDaaS 控制台,选择【应用管理】>【新建应用】。在新建应用页面,选择【自定义 OAuth2 应用程序】, 创建应用。

#### 🗲 新建应用

应用程序类型	* 库应用程序 添加已配置预设模版的库应用程序	<b>自定义 SAML2.0 应用程序</b> 创建支持SAML2.0的应用程序	<b>自定义 OAuth2 应用程序</b> 创建支持OAuth2的应用程序		
应用名称 *	Oauth2应用				
应用详情	企业内部自建Oauth2应用				
提交	取消				

## 步骤二:开启应用授权登录

进入已创建的 OAuth2 应用的详情中,在"配置内容"面板中的"OAuth 应用协议配置"卡片中,单击【编辑】,补充可信域名和回调 URI。

#### △ 注意:

回调 URI 应在可信域名下。



#### ← Oauth2应用

配置内容	详情信息	关联用户	关联用户组		
	OAuth 应用协议	化配置			编辑
	您需要配置以下信	息才能实现 OAuth [	应用的单点登录		
	可信域名	请完善信息			
	回调 URI	请完善信息			
	展示授权页				
	登录操作发起方	应用			

完成补充信息并提交后,将自动分配 client\_id 和 client\_secret,如下图:

← Oauth2应用

置内容	详情信息	关联用户	关联用户组	
1				
	OAuth 应用协i	义配置		编辑
	您需要配置以下信	息才能实现 OAuth 应	用的单点登录	
	可信域名	http://cloud.tencen	com	
	回调 URI	http://cloud.tencen	com/oauth2/ca	
	展示授权页			
	登录操作发起方	应用		
	Client Id	585	ła4ee 🗖	
	Client Secret		61222e3fc2e7697eeb4a6f40c43732d14759584d3e	

## 步骤三:构造网页授权链接

用户授权的地址为 https://<IDaaS域名>/oauth2/authorize。完整的授权地址格式如下:

https://mycorp.cloudidaas.com/open/oauth2/authorize?client\_id=<client\_id>&redirect\_u
ri=<redirect\_uri>&repsonse\_type=code&scope=basic&state=m7NTlQV1qc8MbCU

#### 参数说明:

参数	必选	说明
client_id	是	客户端 ID, 可以在应用"详情信息"面板中"授权登录"卡片可以查询到



参数	必选	说明
redirect_uri	是	用户授权后的回调链接,请遵循 URL 规范作 URL Encode
response_type	是	返回类型,此时固定为: code
scope	是	授权范围,支持 basic 或 userinfo
state	否	推荐传入,用于校验授权发起方和接收方为同一终端,该参数交将在追加在 redirect_uri <b>的 query 参数中</b>

用户登录后,默认静默授权,页面将跳转至 redirect\_uri?code=<code>&state=<state>。

## 相关接口

#### 获取 access\_token

请求方式: POST

请求地址:https://api.open.cloudidaas.com/oauth2/v1/token 参数说明:

参数	必选	说明
code	是	授权码,从 redirect_uri 的 query 参数可以获得
client_id	是	客户端 ID, 可以在应用"详情信息"面板中"授权登录"卡片可以查询到
client_secret	是	客户端密钥,可以在应用"详情信息"面板中"授权登录"卡片可以查询到
redirect_uri	是	用户授权后的回调链接
grant_type	是	此时固定为: authorization_code

#### 响应示例如下:





#### 获取用户信息

请求方式: GET

请求地址: https://api.open.cloudidaas.com/oauth2/v1/userinfo

参数	必选	说明
access_token	是	通过用户授权码获得,参考上一小节

响应示例如下:

{ "user id"• "zhangshan"		
"name": "张三",		
}		

#### 错误码

调用接口时,接口失败会返回相应的 HTTP 状态码,常见的状态码,如:

- 400 Bad Request 无效请求
- 401 Unauthorized 请求未通过鉴权
- 403 Forbidden 请求无权限
- 404 Not Found 资源不存在
- 500 Internal Server Error 内部服务异常
- 503 Service Unavailable 服务不可用

body 中还会返回 error 对象,格式形如:

```
{
   "error": {
   "message": "",
   "type": "OAuthException",
   "code": 11000002,
   "trace_id": ""
}
}
```

企业可以根据 error 对象中的 code 信息调试接口,排查错误。



错误码	含义
9003	参数错误
11000002	授权码 code 或 access_token 无效
1800000	授权码 code 已过期
18000001	access_token 已过期
18000002	redirect_uri 不匹配



## 配置应用 配置 AWS 应用

最近更新时间: 2020-06-29 16:31:45

### 操作场景

当企业需要管理 AWS 资源时,管理员可以在 IDaaS 控制台的"应用管理"模块添加 AWS 控制台应用。本文将 介绍 AWS 控制台的配置方法及相关注意事项。配置成功后,您的企业用户即可以角色身份登录 AWS 控制台,管 理 AWS 资源。(AWS 角色描述请参见 角色术语和概念)

## 前提条件

- 您的腾讯云账号已开通 IDaaS 服务。详情请参见 开通服务。
- 您已有 AWS 账号,并有权限管理 IAM。

### 操作步骤

#### 创建 AWS 控制台应用

- 1. 管理员登录 IDaaS 控制台。
- 2. 在左侧导航栏中,单击【应用管理】,进入应用管理页面。
- 3. 单击【新建应用】,选择【库应用程序】>【Amazon Web Service】,并填写应用名称和应用详情。单击 【提交】,完成 AWS 控制台应用的创建。
- 4. 单击【下载】,下载元数据文件。

SAML元数据文件URL	https://	pudidaas.com/app/saml_metadat	a/	复制 URL	下载
登录URL	https://	oudidaas.com/app/	复制URL		
注销URL	https://	oudidaas.com/logout 复制 URL			
发布者URL	https:/	oudidaas.com/saml/	复制URL		
证书	下载证书				

#### 配置身份提供商和角色

1. 登录 AWS,前往 IAM 控制台。在左侧导航栏中,单击【身份提供商】,进入身份提供商页面。



2. 单击【新建提供商】,填写提供商基本信息,在元数据文档处上传已下载的元数据文件。单击【下一步】,确认信息并单击【完成】。

配置提供程序		
选择提供商类型。		
提供商类型*	SAML •	
提供商名称*	<b>tencentIDaaS</b> 最长 128 个字符。请使用字母数字和"	-"字符.
元数据文档*	C:\ 726c.xml	选择文件

- 3. 在左侧导航栏中,单击【角色】,进入角色页面。单击【创建角色】,选择【SAML2.0 身份联合】。
- 4. 选择第2步创建的身份提供商,并勾选【允许编程访问和AWS管理控制台访问】。您可以根据实际需要添加使用 条件。

创建角色				1 2 3 4
选择受信任实体的类型				• • • •
AWS 产品 EC2、Lambda 和其他	<b>其他 AWS 账户</b> 量于您或第三方	Web 身份 Cognito 或任何 Open 商	D 提供	SAML 2.0 身份联合 您的企业目录
光许与 SAML 2.0 联合的用户担任此角色以在您的 选择 SAML 2.0 提供商	账户中执行操作。 了解更多	3		
如果要为 API 访问创建角色,请选择一个属性,然	后键入要包含在角色中的值	直。这将限制对具有指定属性的	用户的访问	).
SAML 提供商	tencentIDaaS	▼ 创建新提供商 🖸	刷新	
	<ul><li>只允许编程访问</li><li>允许编程访问和 AI</li></ul>	WS管理控制台访问		
属性	SAML:aud	•		
值*	https://signin.aws.am	azon.com/saml		
条件	● 添加条件 (可选)			
*必填				取消 下一步:权限



- 5. 单击【下一步】,为角色设置预设策略。
- 6. 单击【下一步】,添加标签(可选)。
- 7. 单击【下一步】,设置角色名称,并完成创建。

#### 配置腾讯云应用属性值

1. 返回 AWS 应用配置页面,配置属性。腾讯云 IDaaS 已基本预设好属性和属性值,您只需补充如下图中红框部 分的内容:

#### 配置属性

属性信息将成为发送到应用程序的SAML断言的一部分

属性	值	操作
NamelD	\${user:UserId}	编辑删除
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam:: <accountid>:role/<rolename>,arn:aws:iam::<accountid>:saml</accountid></rolename></accountid>	编辑 删除
https://aws.amazon.com/SAML/Attributes/RoleSessionName	TencentIDaaS	编辑 删除
新增字段		

- **2.** 替换https://aws.amazon.com/SAML/Attributes/Role属性的值,替换规则如下:
  - 。 <AccountID>替换为 AWS 账号 ID, 可前往 IAM 控制台 查看。
  - 。 <RoleName>替换为您在角色页面创建的角色名,可前往 角色控制台 查看。
  - 。 <ProviderName>替换为您在身份提供商页面创建的角色名,可前往身份提供商控制台查看。

#### 测试并分配权限

- 1. 为应用关联一个用于测试的用户,详情请参见 管理应用权限。
- 2. 测试用户登录 IDaaS 企业门户,尝试访问 AWS 应用。
- 3. 若访问成功即可关联其他用户,设置应用访问权限。

? 说明:

如果访问不成功,请检查您是否按照文档步骤填写正确的信息。



## 配置 Weekdone

最近更新时间: 2020-06-29 16:32:13

## 操作场景

当企业需要管理 Weekdone 资源时,管理员可以在 IDaaS 控制台的"应用管理"模块添加 Weekdone 应用。 本文将介绍 Weekdone 的配置方法及相关注意事项。配置成功后,您的企业用户即可登录 Weekdone 进行操 作。

## 前提条件

- 您的腾讯云账号已开通 IDaaS 服务。详情请参见 开通服务。
- 您已有 Weekdone 管理员,并有权限管理 Weekdone。

## 操作步骤

#### 创建 Weekdone 应用

- 1. 管理员登录 IDaaS 控制台。
- 2. 在左侧导航栏中,单击【应用管理】,进入应用管理页面。
- 3. 单击【新建应用】,选择【自定义 SAML2.0 应用程序】,并填写应用名称和应用详情。单击【提交】。完成 Weekdone 应用的创建。
  - 🗲 新建应用

应用程序类型★	库应田程度	白完义 SAMI 2 0 应田程度
	添加已配置预设模版的库应用程序	创建支持SAML2.0的应用程序
应用名称 * W	eekdone	
应用详情		



#### 4. 记录登录 URL 和注销 URL,并单击【下载证书】。

#### 腾讯云单点登录元数据

您需要集成的应用程序可能需要以下证书和元数据信息,才能认可腾讯云单点登录身份提供商

SAML元数据文件URL	https://	loudidaas.com/app/saml_metadat	a,	复制 URL   下载
登录URL	https://	oudidaas.com/app.	复制 URL	
注销URL	https://	loudidaas.com/logout 复制 URL		
发布者URL	https://	:loudidaas.com/saml/	复制 URL	
证书	下载证书			

#### 配置 Weekdone 单点登录设置

- 1. 新开页前往 Weekdone 官网,登录您的管理员账号。
- 2. 顶部导航右上角个人头像下拉菜单里,单击设置一栏。
- 3. 单击【Single-sign-on (SAML2)】。
- 4. 填写在腾讯云 IDaaS 创建的 Weekdone 应用信息:

SAML名称	https://weekdone.com/a/ tencent-idaas
SAML登录网址	https:// oudidaas.com/app/
SAML登出网址	https:// loudidaas.com/logout
X509认证	BEGIN CERTIFICATE MIIEATCCAumgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBmjELMAkGA

- 。 SAML 名称:您可以随意设置您的 SAML 名称,例如 IDaaS。
- 。 SAML 登录网址: 您在【创建Weekdone应用】第4步里准备的登录 URL,如下图所示。
- 。 SAML 登出网址:您在【创建Weekdone应用】第4步里准备的注销 URL,如下图所示。
- X509认证: 输入您在【创建 Weekdone 应用】下载的证书,打开证书内容并复制在 X509 认证文本框内。



#### 腾讯云单点登录元数据

您需要集成的应用程序可能需要以下证书和元数据信息,才能认可腾讯云单点登录身份提供商

SAML元数据文件URL	https://	:loudidaas.com/app/saml_metada	ta,	复制 URL	下载
登录URL	https://	budidaas.com/app,	复制 URL		
注销URL	https://	loudidaas.com/logout 复制 URL			
发布者URL	https://	:loudidaas.com/saml/	复制 URL		
证书	下载证书				

#### 配置 Weekdone 应用信息

- 1. 返回 Weekdone 配置页面,配置应用程序 SAML 配置。
  - · 应用程序 ACS URL: 您在【配置Weekdone单点登录设置】第4步里填写的SAML名称,本案例即为:
     https://weekdone.com/a/tencent-idaas
  - 。应用程序 SAML 受众:您在【配置Weekdone单点登录设置】第4步里填写的SAML名称,本案例即为:
     https://weekdone.com/a/tencent-idaas

#### 应用程序SAML配置

腾讯云单点登录需要应用程序提供具体元数据才能信任该应用程序

应用程序启动URL	
中继状态	
会话持续时间 ★	5分钟 🔹
应用程序ACS URL *	https://weekdone.com/a/tencent-idaas
应用程序SAML受众*	https://weekdone.com/a/tencent-idaas

#### 2. 配置应用程序属性值

由于 Weekdone 使用邮箱作为用户标识,您需要修改属性 NameID 的值为 \${user:Email}。如下图所示:



#### 配置属性

属性信息将成为发送到应用程序的SAML断言的一部分

属性	值	操作
NameID	\${user:Email}	编辑删除
新增字段		

#### 测试并分配权限

- 1. 为应用关联一个用于测试的用户,且该用户的邮箱需和 Weekdone 应用里用户邮箱匹配。关联用户步骤可参见 管理应用权限。
- 2. 测试用户登录 IDaaS 企业门户,尝试访问 Weekdone 应用。
- 3. 若访问成功即可关联其他用户,设置应用访问权限。

Λ	注音:
È	に思・

IDaaS 门户的用户邮箱必须和 Weekdone 应用的用户邮箱匹配。



## 配置腾讯企业邮

最近更新时间: 2020-06-29 16:32:39

## 操作场景

当企业需要管理腾讯企业邮资源时,管理员可以在 IDaaS 控制台的"应用管理"模块添加腾讯企业邮应用。本文档 将介绍腾讯云企业邮的配置方法及相关注意事项。配置成功后,您的企业用户即可以登录腾讯企业邮。

## 前提条件

- 您的腾讯云账号已开通 IDaaS 服务。详情请参见 开通服务。
- 您已开通腾讯企业邮服务,能够以管理员身份登录腾讯企业邮。

#### 操作步骤

#### 创建腾讯企业邮应用

- 1. 管理员登录 IDaaS 控制台。
- 2. 在左侧导航栏中,单击【应用管理】,进入应用管理页面。
- 3. 单击【新建应用】,选择【库应用程序】>【腾讯企业邮】,并填写应用名称和应用详情。单击【提交】,完成腾 讯企业邮应用创建。

#### 获取应用所需信息

- 1. 新开页登录 腾讯企业邮,以管理员身份进入管理后台。
- 2. 在顶部菜单中单击【我的企业】,在"企业信息"页面获取企业 ID。
- 3. 在顶部菜单中单击【管理工具】,进入"管理工具"页面单击【应用中心】。
- 4. 进入"应用中心"模块,单击【单点登录】。
- 5. 获取 Secret。



## 单点登录

可以从公司OA系统,网站一键进入企业邮箱,免去登录过程。帮助

Secret

配置应用属性值

重新获取



#### 返回腾讯云应用配置页面,配置企业 ID 和 Secret。

#### 应用程序配置信息

企业邮 corpld *	v 3	
企业邮 通讯录秘钥 *	ał	2

? 说明:

腾讯云 IDaaS 已为您预设属性值为 \${user:Email},若您的 IDaaS 系统用户的邮箱为企业邮的邮箱地 址,即可使用 \${user:Email} 作为属性值。若您的企业邮箱前缀和 IDaaS 系统用户的 Userld 一致,则 配置属性值为 \${user:Userld}@domain,domain 需替换为您的企业邮域名。

#### 测试并分配权限

- 1. 为应用关联一个用于测试的用户,详情请参见 管理应用权限。
- 2. 测试用户登录 IDaaS 企业门户,尝试访问腾讯企业邮应用。
- 3. 若访问成功即可关联其他用户,设置应用访问权限。

? 说明:

- 如果访问不成功,请检查您是否按照文档步骤填写正确的信息。
- 管理员需要先在企业邮添加用户。在顶部菜单中选择【通讯录】>【新增成员】。
- 如果应用属性值为 \${user:Email},那么企业邮用户的邮箱需和 IDaaS 系统里的用户邮箱一一对应。
   如果应用属性值为 \${user:UserId}@domain,那么企业邮用户的邮箱需和 IDaaS 用户的
   ID@domain 一一对应。如果 IDaaS 的用户在企业邮不存在,该用户将无法单点登录企业邮。



## 配置腾讯云控制台

最近更新时间: 2020-06-29 16:41:57

## 操作场景

当企业需要管理腾讯云控制台资源时,管理员可以在 IDaaS 控制台的"应用管理"模块添加腾讯云控制台应用。本 文将介绍腾讯云控制台的配置方法及相关注意事项。配置成功后,您的企业用户即可以角色身份登录腾讯云控制 台,管理腾讯云资源。( 腾讯云角色描述请参见 <mark>角色概述</mark> )

### 前提条件

您的腾讯云账号已开通 IDaaS 服务。详情请参见 开通服务。

#### 操作步骤

#### 创建腾讯云控制台应用

- 1. 管理员登录 IDaaS 控制台。
- 2. 在左侧导航栏中,单击【应用管理】,进入应用管理页面。
- 3. 单击【新建应用】,选择【库应用程序】>【腾讯云】,并填写应用名称和应用详情。单击【提交】,完成腾讯云 控制台应用的创建。
- 4. 单击【下载】,下载元数据文件

SAML元数据文件URL	https://	pudidaas.com/app/saml_metadata	a/	复制 URL	下载
登录URL	https://	oudidaas.com/app/	复制 URL		
注销URL	https:,	oudidaas.com/logout 复制 URL			
发布者URL	https:/	oudidaas.com/saml/	复制 URL		
证书	下载证书				

#### 配置身份提供商和角色

- 1. 登录 访问管理控制台。
- 2. 在左侧导航栏中,单击【身份提供商】,进入身份提供商页面。



3. 单击【新建提供商】,填写提供商基本信息,在元数据文档处上传已下载的元数据文件。

提供商类型	*	O SAML				
提供商名称	*	tencentidaas	S			
备注		请输入备注				
元数据文档	*	0e2	xml	$\odot$	重新选择文件	删除
元数据文档	*	0e2 请上传XML格式	<b>xml</b> 式 , 大小为40	Ø KB以内的	<b>重新选择文件</b> 的文件	删除
元数据文档 单击【下一步 至左侧导航栏 单击【新建角镜 选择第2步创建 您可以根据实际	* ],审阅信息并自 中,单击【角色】 色】,选择【身份 韵的身份提供商, 示需要添加使用务 色载体信息	0e2         请上传XML格式         基【完成】。         ,进入角色页面。         提供商】。         并勾选"允许当前角色说         件,详情可参见 创建角         2         配置角色第	xml 式,大小为40 方问控制台"。 色。	Ø ○ KB以内部	<b>重新选择文件</b> 的文件	

9. 单击【下一步】,设置角色名称,并完成创建。

#### 配置腾讯云应用属性值

1. 返回腾讯云应用配置页面,配置属性。腾讯云 IDaaS 已基本预设好属性和属性值,您只需补充如下部分的内 容:



#### 配置属性

属性信息将成为发送到应用程序的SAML断言的一部分		
属性	值	操作
NamelD	\${user:UserId}	编辑删除
https://cloud.tencent.com/SAML/Attributes/Role	qcs::cam::uin/ <accountid>:roleName/<rolename>,qcs::cam::uin/<accountid< td=""><td>编辑 删除</td></accountid<></rolename></accountid>	编辑 删除
https://cloud.tencent.com/SAML/Attributes/RoleSessionName	TencentIDaaS	编辑 删除

- 新增字段
- **2.** 替换https://cloud.tencent.com/SAML/Attributes/Role属性的值,替换规则如下:
  - 。 <AccountID>替换为腾讯云账号 ID,可前往 账号信息 查看。
  - 。 <RoleName>替换为您在角色控制台创建的角色名,可前往 角色控制台 查看。
  - 。 <IdPName>替换为您在身份提供商页面创建的角色名,可前往 身份提供商控制台 查看。

#### 测试并分配权限

- 1. 为应用关联一个用于测试的用户,详情请参见管理应用权限。
- 2. 测试用户登录 IDaaS 企业门户,尝试访问腾讯云应用。
- 3. 若访问成功即可关联其他用户,设置应用访问权限。

? 说明:

如果访问不成功,请检查您是否按照文档步骤填写正确的信息。



## 配置 Dropbox

最近更新时间: 2020-07-29 17:44:59

## 操作场景

当企业需要管理 Dropbox 资源时,管理员可以在 IDaaS 控制台的"应用管理"模块添加 Dropbox 应用。本文 档将介绍 Dropbox 的配置方法及相关注意事项。配置成功后,您的企业用户即可以登录 Dropbox。

## 前提条件

- 您的腾讯云账号已开通 IDaaS 服务。详情请参见 开通服务。
- 您已开通腾讯企业邮服务,能够以管理员身份登录腾讯企业邮。

### 操作步骤

#### 创建 Dropbox 应用

Contraction of the second s

- 1. 管理员登录 IDaaS 控制台。
- 2. 在左侧导航栏中,单击【应用管理】,进入应用管理页面。
- 3. 单击【新建应用】,选择【库应用程序】>【Dropbox】,并填写应用名称和应用详情。单击【提交】,完成 Dropbox 应用创建。
- 4. 记录登录 URL 和注销 URL,并单击【下载证书】。
  - 配置内容 详情信息 关联用户 关联用户组 1 腾讯云单点登录元数据 您需要集成的应用程序可能需要以下证书和元数据信息,才能认可腾讯云单点登录身份提供商 SAML元数据文件URL https://shuzitengxun.cloudidaas.com/app/saml\_metadata/54d69f6f20c1 复制 URL | 下载 登录URI https://shuzitengxun.cloudidaas.com/app/54d69f6f20c1 复制 URL 注销URL https://shuzitengxun.cloudidaas.com/logout 复制 URL 发布者URL https://shuzitengxun.cloudidaas.com/saml/54d69f6f20c1 复制 URL 证书 下载证书

#### 配置 Dropbox Business 单点登录



- 1. 新开窗口,登录 Dropbox 管理员控制台。
- 2. 选择左侧导航【设置】,选择【验证】>【单一登录】 。
- 3. 配置以下信息,单击【保存】。

設定 > 單一登入



X.509 证书:上一步中下载的证书文件。

4. 收集 Dropbox Business 单点登录配置信息。
 单点登录的登录网址:



#### 設定 > 單一登入

♀ 單一登入 讓團隊成員使用公司的帳號密碼登入 Dropbox。 瞭解詳情	• 必填 -
<b>身分提供者登入網址</b> 由您的身分提供者提供。在成員輸入公司帳密時驗證成員身分。	<u> 登入網址: https://shuzitengxun.cloudidaas.com/app/54d69f6f</u>
身分提供者登出網址(非必要) 由您的身分提供者提供。成員登出後會被重新導引至此頁面。	<u> </u>
X.509 憑證 由您的身分提供者所提供的 .pem 檔案安全憑證	<u>馮諍: shuzitengxun</u> 到期日: 7/28/2022
<b>單一登入的登入網址</b> 若成員已透過您的身分提供者登入,這個自訂連結便能直接將成員導 戶。	引至他們的線上 Dropbox 帳 <u>複製連結</u>

#### 5. 开启 Dropbox Business 单一登录。

♀ 單一登入 讓團隊成員使用公司的帳號密碼登入 Dropbox。 瞭解詳情

#### 配置腾讯云 SSO 单点登录

- 1. 转回 IDaaS 控制台。
- 2. 进入 Dropbox 应用配置内容页。
- 3. 配置以下单一登录信息。

应用程序启动URL: 填入上一步收集的单点登录的登录网址。



身份管理服务	发布者URL	https://shuzitengxun.cloudidaas.com/saml/e9266ee3bbc0 复制 URL
	证书	下载证书
回用户管理		
■ 数据源管理 2	c田铝c 2 MM 원품	2
☑ 认证源管理	西田在13-3AWLLL目 腾讯云单点登录需要应	Ⅰ 用程序提供具体元数据才能信任该应用程序
🖒 应用管理	应用程序启动URL	https://www.dropbox.com/sso/54416353969
	中継状态 会话持续时间。 应用程序ACS URL。 应用程序SAML受众。 提交 取消	1/Jaj       https://www.dropbox.com/saml_login       Dropbox

## 测试并分配权限

- 1. 为应用关联一个用于测试的用户。关联用户步骤可参见 管理应用权限。
- 2. 测试用户登录 IDaaS 企业门户,访问 Dropbox 应用。
- 3. 若访问成功即可关联其他用户,设置应用访问权限





## 管理应用权限

最近更新时间: 2020-06-29 16:33:28

本文为您介绍如何进行应用权限管理,IDaaS 支持为应用程序关联不同的用户/组,被关联的用户/组拥有访问该应 用的权限。

### 操作步骤

1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【应用管理】。

2. 在"应用管理"页面,管理员可进行"单应用关联"、"多应用关联"和"禁用应用"操作。

#### 单应用关联

1. 在"应用管理"页面,找到您需要关联用户/组的应用,在其右侧操作栏下单击【关联用户/组】。

新建应用	关联用户/组 删除应用			
□ 应用名	描述	状态	创建时间	操作
🗌 测试专用	自定义 SAML2.0 应用程序	已开启	2019-07-17 15:17:02	禁用 关联用户/组 删除
□ 腾讯云	以卓越科技能力助力各行各业数字化转型,为全球客户提供领先的云计算、大数据、	已开启	2019-07-17 17:10:06	禁用 关联用户/组 删除

2. 选择关联的用户/组,单击【确定】完成关联。

#### 多应用关联

1. 在"应用管理"页面,勾选您需要关联用户/组的应用,单击上方的【关联用户/组】。

新建应用	关联用户/组 删除应用			
- 应用名	描述	状态	创建时间	操作
✔ 测试专用	自定义 SAML2.0 应用程序	已开启	2019-07-17 15:17:02	禁用 关联用户/组 删除
✓ 腾讯云	以卓越科技能力助力各行各业数字化转型,为全球客户提供领先的云计算、大数据、	已开启	2019-07-17 17:10:06	禁用 关联用户/组 删除

2.选择关联的用户/组,单击【确定】完成关联。

#### 禁用应用

- 1. 找到您需要禁用的应用,在其右侧操作栏下单击【禁用】。
- 2. 系统将弹出确认禁用的对话框,单击【确定】完成应用禁用。
- 禁用应用后,应用状态将变更为"未开启",该状态下应用将不能访问。被禁用的应用,可以单击其右侧操作栏 下的【开启】,重新开启应用。



新建应用 关联用户	组 删除应用			
回 应用名	描述	状态	创建时间	操作
□ 测试专用	自定义 SAML2.0 应用程序	未开启	2019-07-17 15:17:02	开启 关联用户/组 删除
□ 腾汛云	以卓越科技能力助力各行各业数字化转型,为全球客户提供领先的云计算、大数据、人工智能服	已开启	2019-07-17 17:10:06	禁用 关联用户/组 删除



## 查看企业信息

最近更新时间: 2020-06-29 16:33:49

本文为您介绍管理员如何查看企业信息、修改企业名称。

## 操作步骤

1. 管理员登录 IDaaS 控制台,单击左侧菜单中的【企业信息】。

2. 在"企业信息"页面,可查看"登录链接"和"企业信息"。

- 3. 管理员可进行"复制登录链接"和"修改企业名称"操作。
  - 。 复制登录链接

单击"门户 URL"右边的 🔽,可以复制登录链接。

。 修改企业名称

单击"企业名称"右边的 🖍,可以修改企业名称。



## 企业门户操作指引

最近更新时间: 2020-06-29 16:46:12

#### ? 说明:

用户即企业用户是指企业员工、合作伙伴、客户等。

本文为您介绍用户如何登录企业门户,关联微信和访问应用。

### 操作步骤

#### 登录企业门户

管理员在企业下成功创建用户后,将会发送登录信息至用户的手机、邮箱。用户可以通过手机短信或邮箱中的用户 ID、登录密码和登录地址等信息登录企业门户。

#### 关联微信

用户关联微信有"先扫码后登录关联"和"登录后扫码关联"两种方式。

#### 扫码后登录关联

1. 进入登录页面,扫描微信二维码。



#### 2. 扫描二维码后,通过用户 ID 和密码登录即可完成微信关联。

微信未关	<b>联账号</b> , <sub>请登录完成关联</sub>
用户ID	
密码	
汞登录	
< 切换微信登录	忘记账号

3. 若该用户尚未开启微信登录,请联系管理员设置。

#### 登录后扫码关联

- 1. 进入登录页面,单击【切换账号密码登录】。
- 2. 通过用户 ID 和密码登企业门户。
- 3. 若用户尚未关联微信,将跳转微信绑定页面。扫描二维码即可完成微信关联。

#### 访问应用

用户登录后,即可访问管理员授权的应用。