身份管理服务 IDaaS

操作指南

产品文档

腾讯云

【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。

文档目录

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

> 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。

1. 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

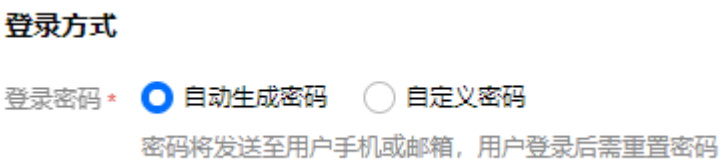
本文将为您分别介绍“在线创建”和“从本地表格创建”2种用户的添加方式。

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。

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。

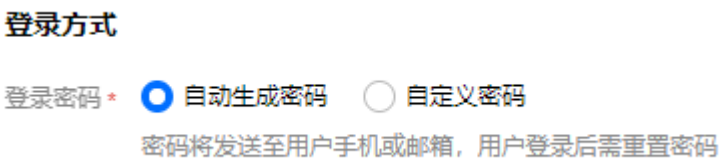


3. 单击【 下一步 】，为用户设置用户组，一个用户可以所属多个组。若需要新增组可以单击 【 + 快速创建组 】，进行组的创建。
   初始状态下默认存在一个根目录，所有新增的用户组都是根目录的所属组。
4. 单击【 完成 】，完成用户添加。

从本地表格创建

1. 单击【导入模版】，下载 excel 模板。

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。



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。

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。

3. 单击【 安全信息 】，进入“安全信息”模块。

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”。

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 】。

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】。

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。

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。

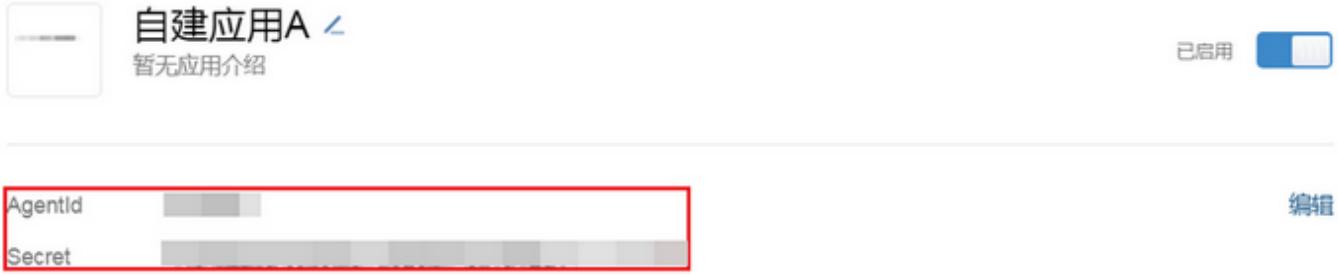
- 通讯录 Secret：可前往【企业微信管理后台】>【管理工具】>【通讯录同步】，开启 API 接口同步后，获取 Secret。

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】。

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】。

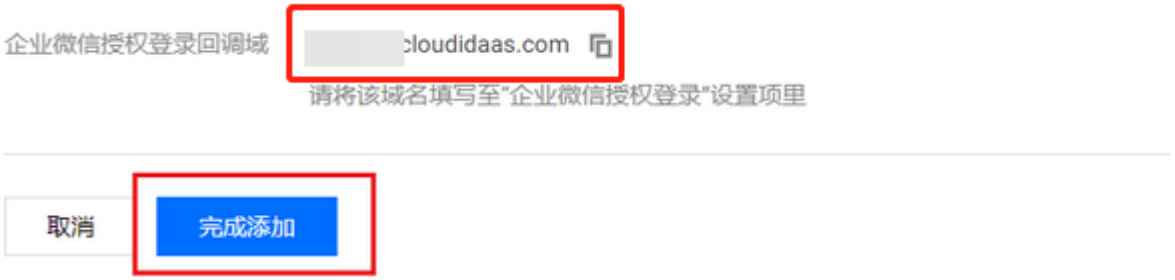
> ⚠ 注意：
> 应用可见范围设置时，请设置全员或需要通过企业微信扫码登录 IDaaS 门户的用户。不在可见范围内的用户也将无法通过企业微信扫码登录。

iii. 获取自建应用的 AgentId 和 Secret。



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。

8. 复制 IDaaS 提供的“企业微信授权登录回调域”，单击【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】。

0. 单击【设置授权回调域】。

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。

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】。

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。

3. 填写企业 ID，可前往【企业微信管理后台】>【我的企业】，获取企业 ID。

> **注意：**
> 认证源填写的企业 ID 需和数据源的企业 ID 保持一致，如果不一致，通过企业微信同步的用户将无法通过企业微信扫码登录。

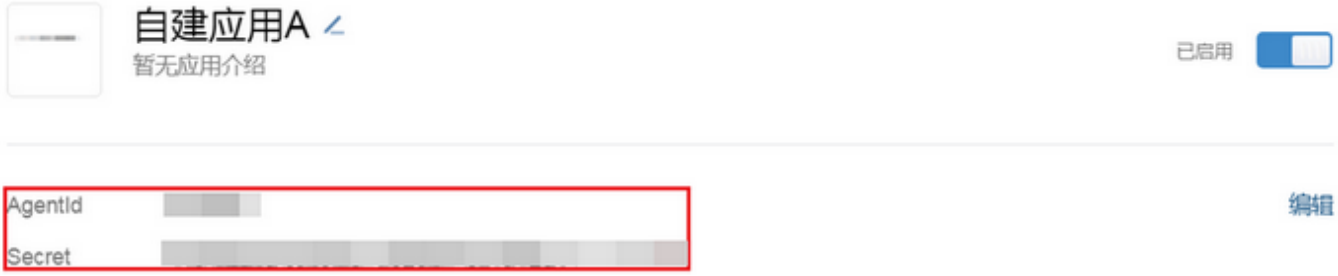
4. 企业微信扫码登录设置。设置企业微信扫码登录需要企业自建应用，详细操作如下：

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】。

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】。

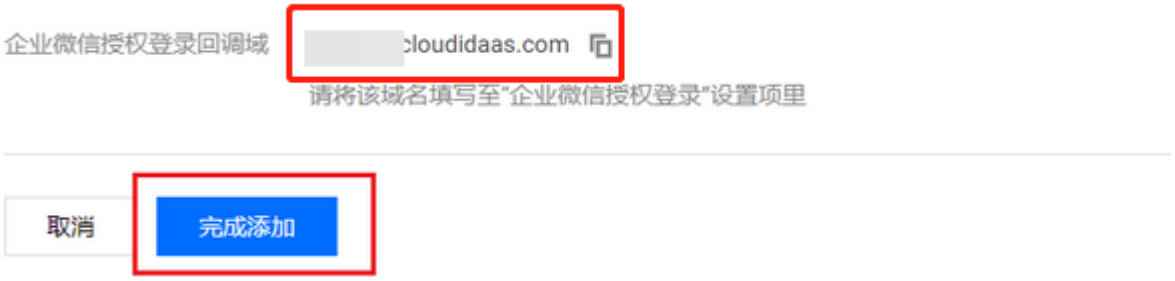
> ⚠ 注意：
> 应用可见范围设置时，请设置全员或需要通过企业微信扫码登录 IDaaS 门户的用户。不在可见范围内的用户也将无法通过企业微信扫码登录。

iii. 获取自建应用的 AgentId 和 Secret。



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。

6. 复制 IDaaS 提供的“企业微信授权登录回调域”，单击【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】。

8. 单击【设置授权回调域】。

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。

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 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。

3. 配置 LDAP/AD 数据源。

i. 填写 LDAP 服务器配置信息。

- 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。

- 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。

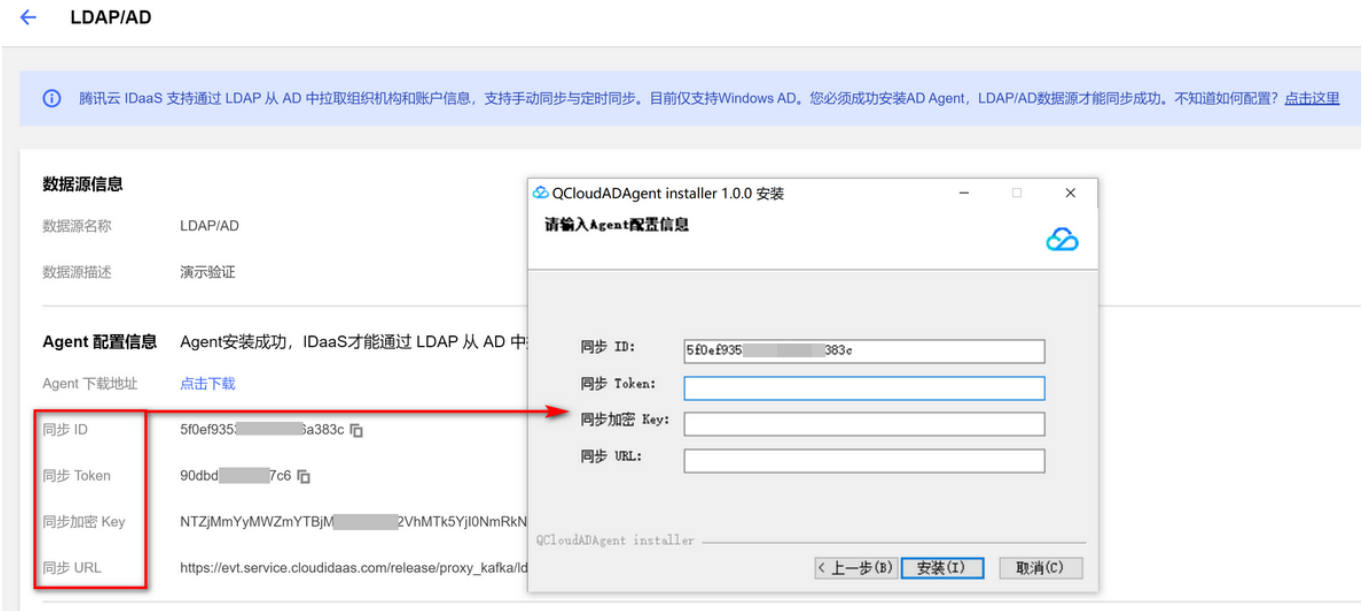
iv. 进行数据同步设置，目前支持手动同步和自动定时同步。若选择定时同步，可选同步频率。

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。

4. 下载并安装 Qcloud AD Agent。

i. 在 LDAP/AD 数据源详情页下载 AD Agent。

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。



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。

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。

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。

完成补充信息并提交后，将自动分配 `client_id` 和 `client_secret`，如下图：

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_uri=<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 的 query 参数中

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：

```
{
"token_type": "Bearer",
"expires_in": 600,
"access_token": "94abc92867c1fc4ddbc22b1d3060e40d78746f95f1f8e7120306437e352825bf",
"refresh_token": ""
}
```

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
18000000	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）

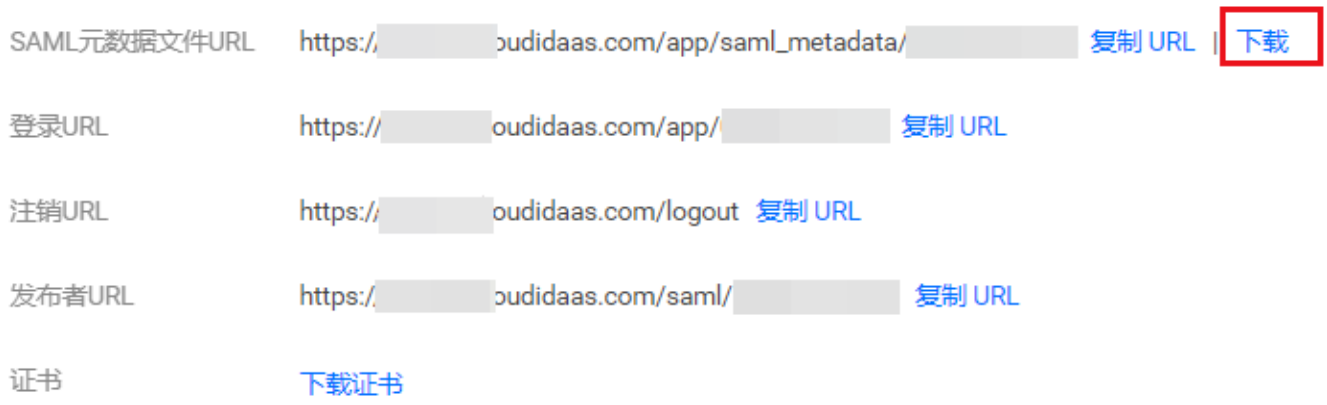
前提条件

- 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。



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。

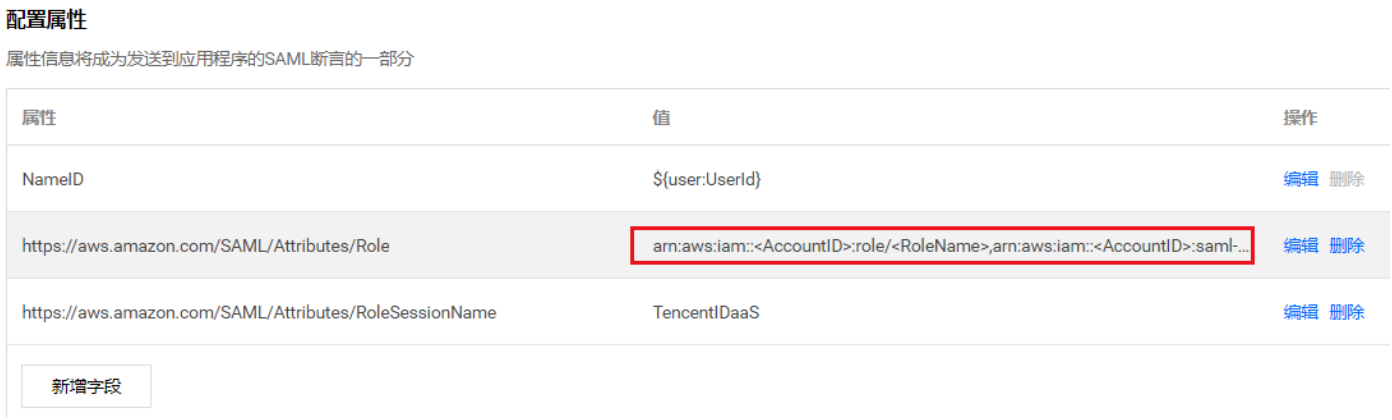
2. 单击【新建提供商】，填写提供商基本信息，在元数据文档处上传已下载的元数据文件。单击【下一步】，确认信息并单击【完成】。

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。

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：



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

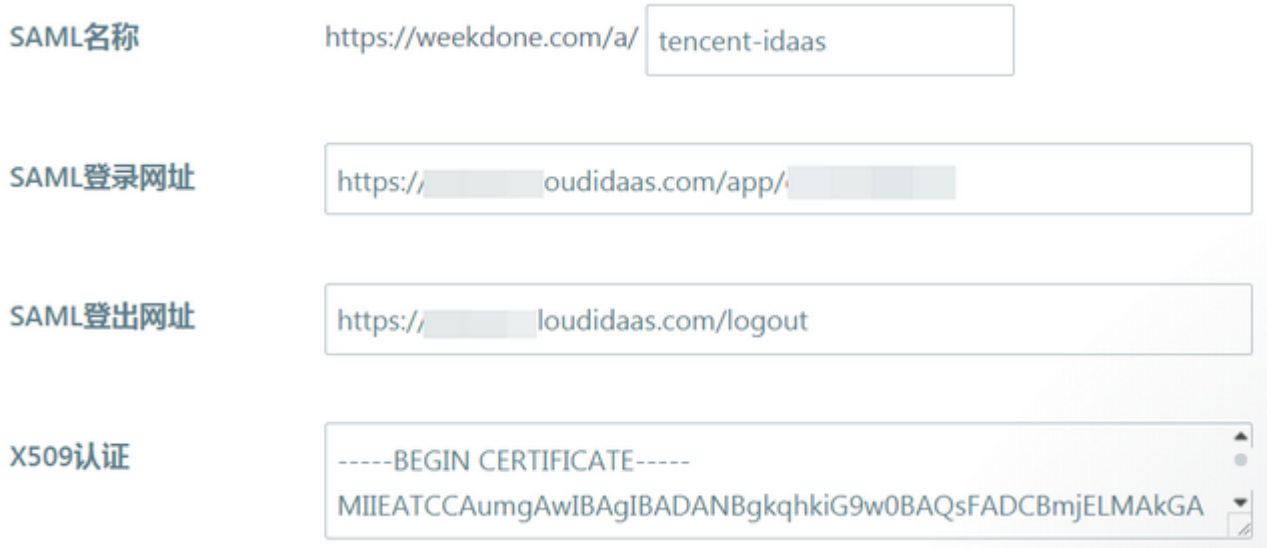
创建 Weekdone 应用

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。

4. 记录登录 URL 和注销 URL，并单击【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：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。

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`

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：

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。

> ⚠ 注意：
> 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。

配置应用属性值

返回腾讯云应用配置页面，配置企业 ID 和 Secret。

> 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 UserId 一致，则配置属性值为 ${user:UserId}@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 角色概述）

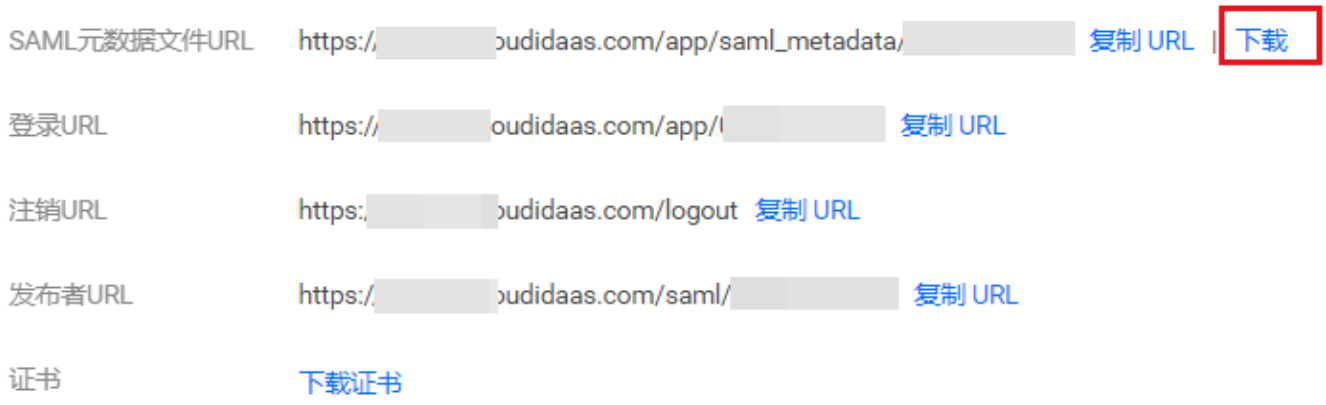
前提条件

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

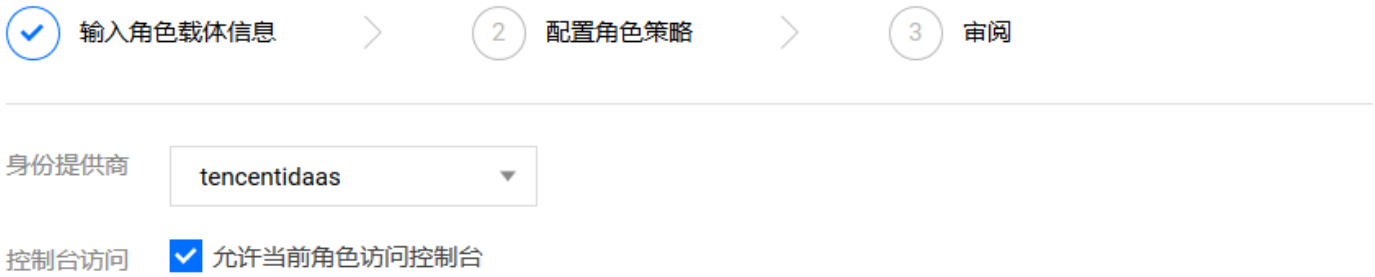


配置身份提供商和角色

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。

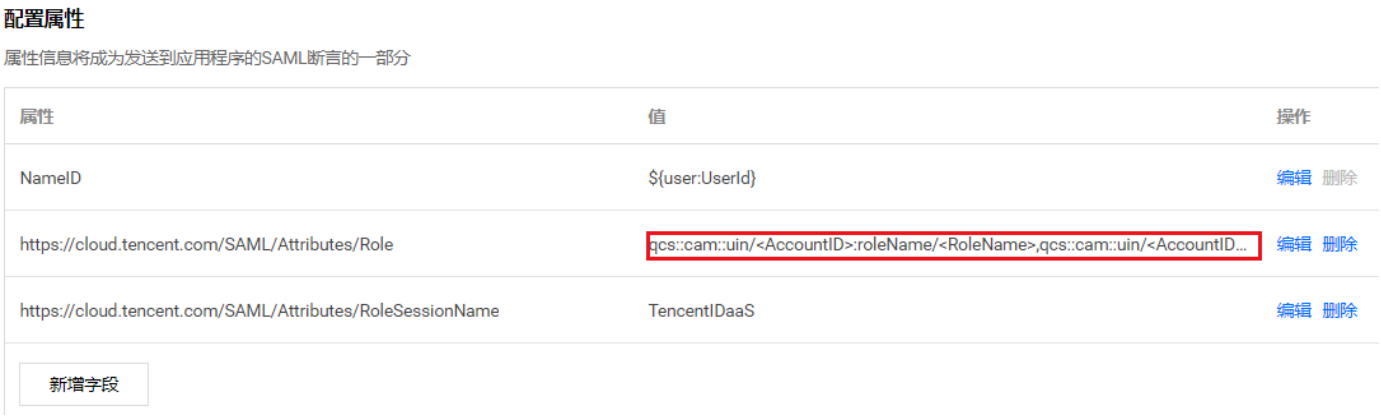
4. 单击【下一步】，审阅信息并单击【完成】。
5. 在左侧导航栏中，单击【角色】，进入角色页面。
6. 单击【新建角色】，选择【身份提供商】。
7. 选择第2步创建的身份提供商，并勾选“允许当前角色访问控制台”。
   您可以根据实际需要添加使用条件，详情可参见 创建角色。



8. 单击【下一步】，为角色设置预设策略。
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：



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。

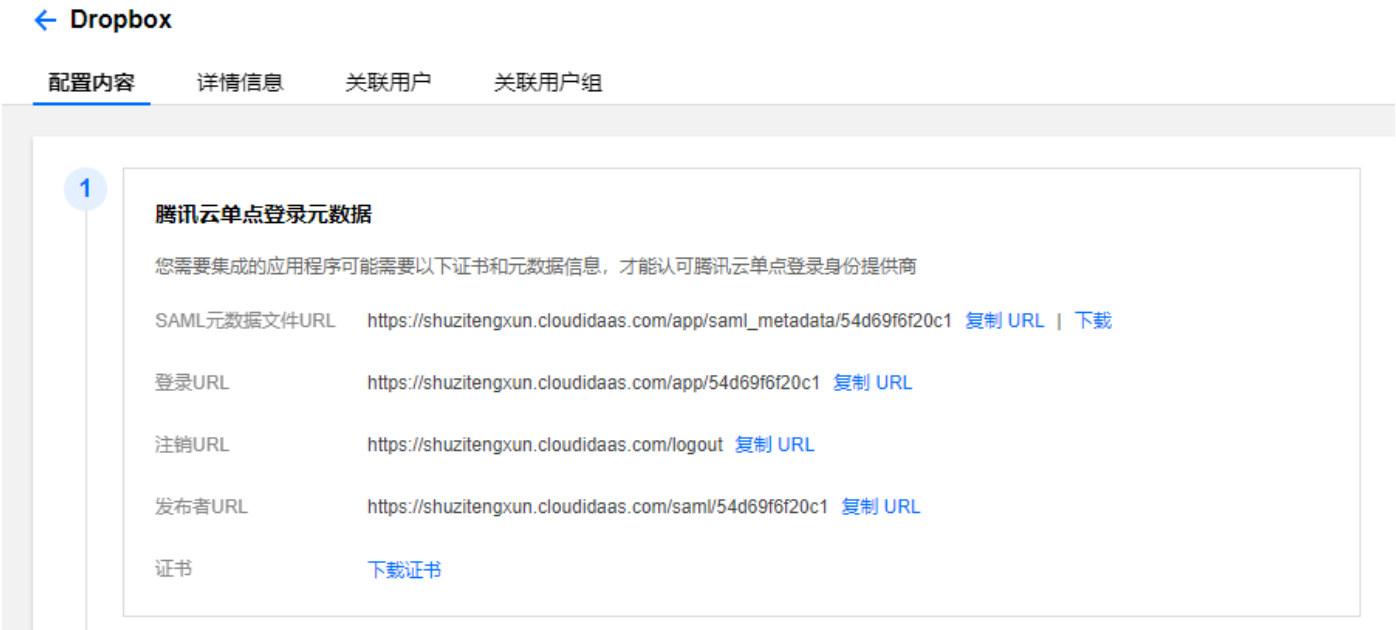
前提条件

- 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

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 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】。

身份提供商登入网址：上一步中记录的登录 URL。

身份提供商注销网址：上一步中记录的注销 URL。

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。

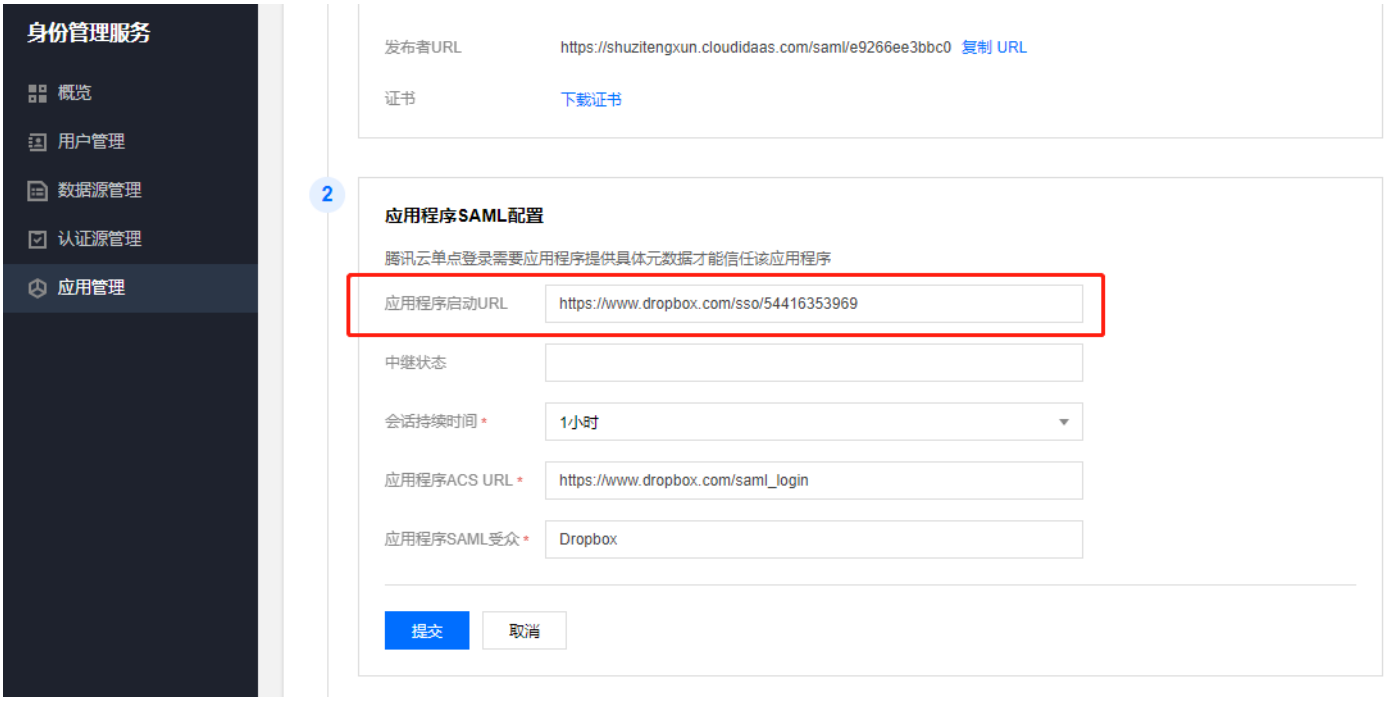
单点登录的登录网址：

5. 开启 Dropbox Business 单一登录 。

配置腾讯云 SSO 单点登录

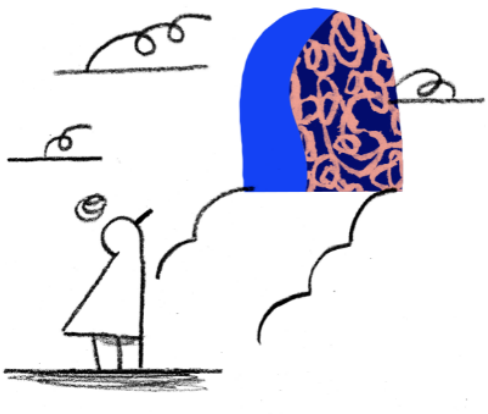
1. 转回 IDaaS 控制台。
2. 进入 Dropbox 应用配置内容页。
3. 配置以下单一登录信息。

   应用程序启动URL： 填入上一步收集的单点登录的登录网址。



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。

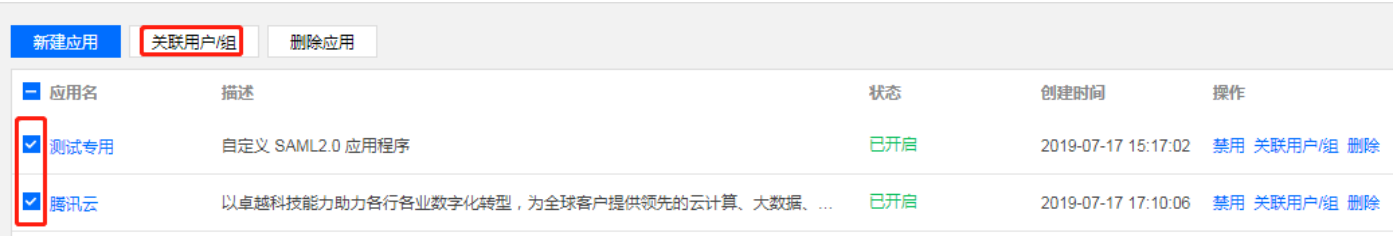
单应用关联

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 】。

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 】。



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。
3. 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
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、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。

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。