

iOA 零信任安全管理系统 操作指南（私有化版）



腾讯云

【 版权声明 】

©2013–2024 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

操作指南（私有化版）

认证对接

- 用户源同步

- iOA 私有化钉钉对接

- iOA 私有化企业微信对接

- iOA 私有化飞书对接

 - 方案1：飞书认证

 - 方案2：OAuth2 认证

- iOA 私有化 SCIM2.0 用户同步

数据安全中心

- 终端数据安全策略

 - 管控范围

 - 审批流配置

- 数据存储设置

操作指南（私有化版）

认证对接

用户源同步

最近更新时间：2024-06-08 06:14:41

本文将介绍如何在本地自建账户，来进行用户源同步。

新增目录

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**用户与授权管理**。
2. 在用户与授权管理页面，单击**新建**，输入相关参数，单击**确认**。

新增目录

* 名称

描述

* 是否导入架构 是 否

添加分组

1. 在用户与授权管理页面，选择所需目录，单击**目录名称**。

[新建](#)

目录名称	描述	关联的用户源	操作
[目录名称]	-	自建账户	目录管理 编辑 删除 资源授权
[目录名称]	-	自建账户	目录管理 编辑 删除 资源授权

2. 在组织架构页面，展示目录组织架构下的账户分组以及账户情况。单击 **...** > **添加分组**，可以在此分组下新增次级分组。

组织架构 自定义分组

搜索 Q

组织架构 +

webtest ...

添加分组

姓名 所在部门 职位 已绑定设备① 活 操作

新增账号 批量操作 批量导入账号

账号 Q

活跃用户设置

共 1 项

10 条/页 1 / 1 页

3. 在新增分组弹窗中，输入分组名称，选择上级分级，单击确定。

新增分组

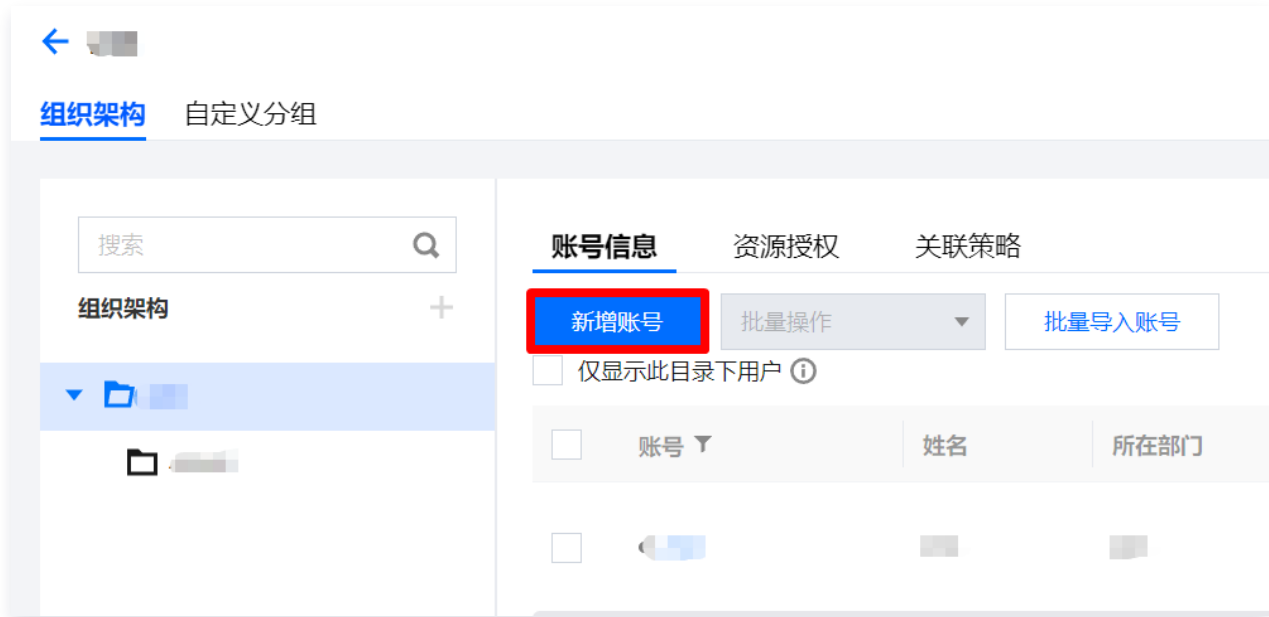
* 分组名称 请输入分组名称

* 上级分组

确定

新建单个账户

1. 在用户与授权管理页面，单击新增账号。



2. 在账户管理页面，配置相关参数，单击**确定**。

账户管理

基本信息

* 状态: 启用 禁用

* 账号:

* 姓名:

* 密码:

* 确认密码:

* 账号有效期: 永不过期 在这之后

* 所属部门:

职位:

身份证:

手机:

邮箱:

保存

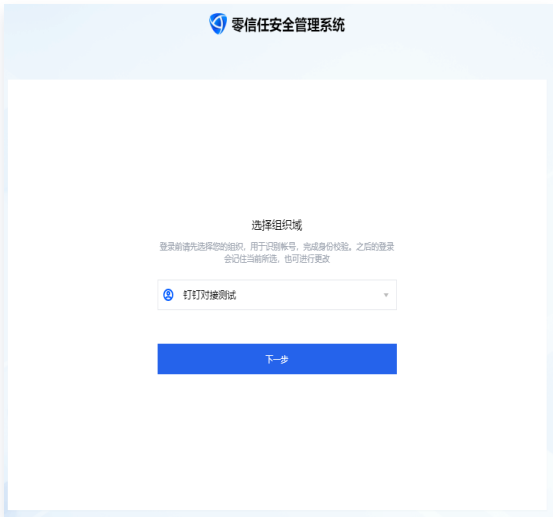

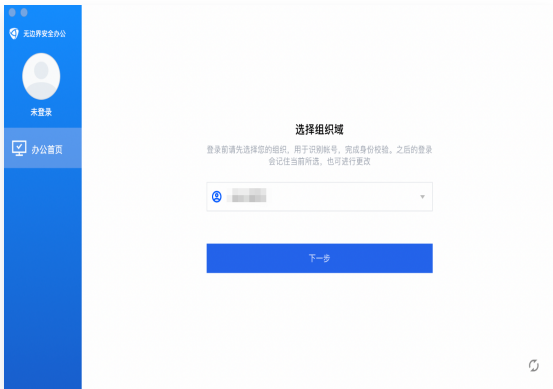

登录客户端

打开客户端，输入账户密码，即可完成登录。

iOA 私有化钉钉对接

最近更新时间：2024-06-08 06:14:41

实现效果

类型\操作步骤	选择组织域	登录效果
浏览器		
客户端		

步骤一：钉钉认证准备

1. 配置钉钉自建应用

1. 登录 [钉钉管理后台](#)，在左侧导览中，单击**钉钉应用**。
2. 在钉钉应用页面，单击**创建应用**。

3. 在创建企业内部应用窗口中，配置相关参数，单击**确定创建**即可完成创建。

创建企业内部应用
✕

应用类型: H5微应用 小程序

* 应用名称:

* 应用描述:

应用图标: 

请上传JPG/PNG格式、240*240px以上、1:1、2MB 以内的无圆角图标

[查看图标规范 >](#)

* 开发方式: 企业自主开发 委托服务商开发

取消
确定创建

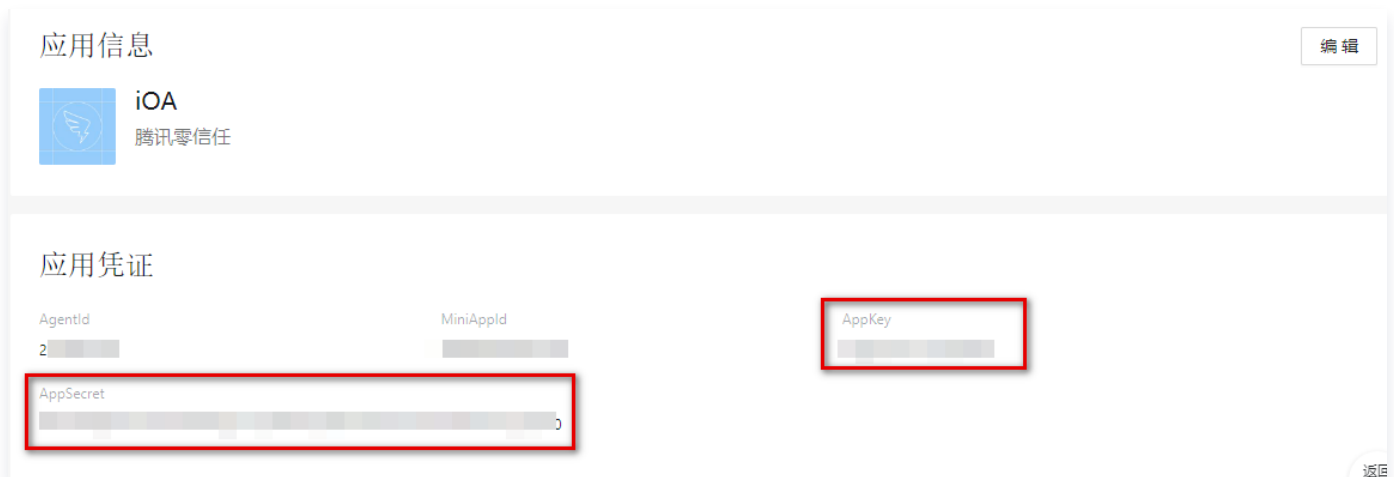
参数名称	说明
应用类型	小程序
应用名称	腾讯 iOA
应用描述	根据实际需填写
开发方式	企业自主开发

2. 获取该应用的 AppKey 和 AppSecret

1. 在应用开发页面，单击选择刚刚创建的自建应用。



2. 在应用信息页面，复制 AppKey 和 AppSecret，其中钉钉的 Appkey 对应 iOA 控制台上的 App ID，钉钉的 AppSecret 对应 iOA 控制台的 AppSecret。



3. 取回调域名

1. 在应用信息页面，单击应用功能 > 登录与分享。

2. 在登录与分享页面，输入 iOA 的网关回调域名

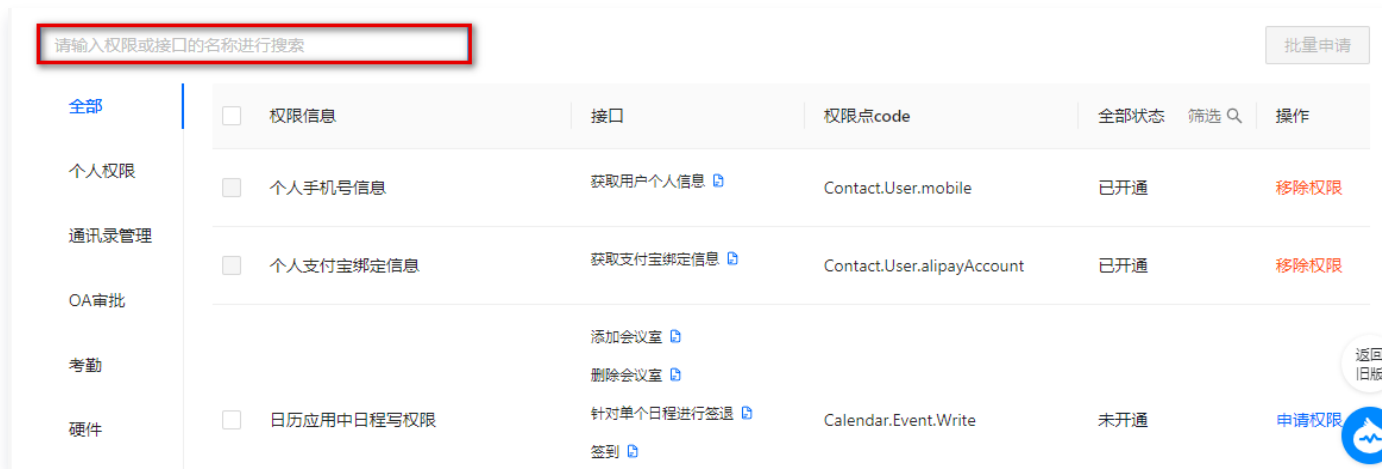
`https://scs.gateway.tencent.com/akpage/qrcode/redirect`。



3. 单击添加，即可将 iOA 的网关回调域名添加到钉钉的回调域名列表中。

4. 配置权限管理

1. 应用信息页面，单击**权限管理**。
2. 在权限管理页面，支持通过搜索框选择权限，如：调用企业 API 基础权限、调用 OpenApp 专有 API 时需要的权限、调用 SNS API 时需要具备的基本权限、企业员工手机号信息、邮箱等个人信息、通讯录部门信息读权限、成员信息读权限、根据手机号姓名获取成员信息的接口访问权限、通讯录部门成员读权限。



3. 选中目标权限后，单击操作列的**申请权限**，即可为该应用选中所需权限。

步骤二：配置 iOA 私有化 控制台

1. 新建目录

1. 登录 iOA 零信任管理平台控制台，在左侧导航中，单击**管理中心 > 用户与授权管理**。
2. 在用户与授权管理页面，单击**新建**。
3. 在新增目录页面，输入名称和描述，是否导入架构选择**是**，导入类型选择**钉钉**，单击**下一步**。

新增目录

* 名称

描述

* 是否导入架构 是 否

* 导入类型

4. 在新增目录页面，输入 **App ID**和**App Secret**，以及其他参数。

基础配置

类型 钉钉 ▼

App Key *

App Secret *

连通性测试 ⓘ 测试

组织架构更新设置 开启自动更新

每周
 每天
 每四小时
 每隔

5. 单击**测试**，测试通过后单击**保存**。

6. 在用户与授权管理页面，找到刚刚创建的目录，单击**用户同步**。

新建

目录名称	描述	关联的用户源	操作
飞-	-	飞书	目录管理 编辑 删除 用户同步
钉-	-	钉钉	目录管理 编辑 删除 用户同步
cor-	-	钉钉	目录管理 编辑 删除 用户同步

2. 配置认证源

1. 登录 iOA 零信任管理平台控制台，在左侧导航中，单击**身份安全策略 > 认证安全 > 认证源配置**。

2. 在认证源配置页面，单击**新增认证源实例**。

3. 在新增认证源实例页面，类型选择**钉钉**，并配置其他参数，单击**保存**。

说明:

- App ID: 为钉钉的 AppKey。
- App Secret: 为钉钉的 AppSecret。

新增认证源实例

i 配置说明

展开 ▶

类型

钉钉

认证方式

扫码认证 授权认证

名称 *

钉钉对接测试



客户端登录标题 **i**

客户端登录标题(英文)

客户端登录提示

客户端登录提示(英文)

AppKey *

AppSecret *

.....

CorpId

3. 设置认证策略

1. 在策略中心 > 身份安全策略 > 认证安全 > 认证策略页面，选择目标目录，单击编辑。



2. 在编辑认证策略页面，可根据自身需要设置 PC 端的主认证方式认证源和挑战认证方式认证源，认证源可设置多种。

⚠ 注意:

如您要使用钉钉 App 内的应用免登录，您还需要设置移动端的主认证方式认证源和挑战认证方式认证源，设置方式与 PC 端相同。

PC端

主认证方式的认证源

钉钉对接测试

双因素认证

是否启用



二次认证方式的认证源

请选择

指定主认证登录豁免双因素?

请选择

挑战认证方式认证源

钉钉对接测试

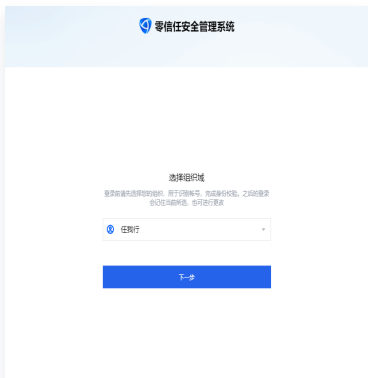


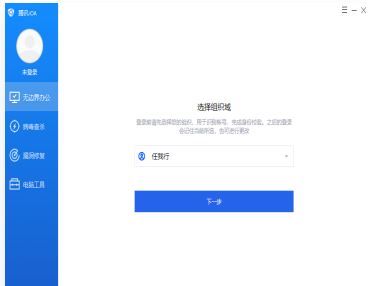

3. 单击添加，完成编辑。

iOA 私有化企业微信对接

最近更新时间：2024-06-11 14:31:31

- **身份源**：您导入组织架构的企业微信会和使用的 iOA 产品进行绑定，您可以给已导入的企业微信身份源创建多个身份目录进行同步。暂时不支持同一个 iOA 绑定多个企业微信主体的身份源。
- **认证源**：您创建的企业微信认证源需要和您导入企业微信身份源保持一致。相同企业微信的认证源可以创建多个，不受此影响。
- 如果您之前的企业微信后台安装过**腾讯零信任 iOA**的应用，请删除原有应用，重新安装。

实现效果

类型 \ 操作步骤	选择组织域	选择登录方式	登录效果
浏览器			
客户端			

步骤一：企业微信认证准备

1. 域名验证

由于企业微信需要通过受信域名才能进行对接，所以需要您提前准备：

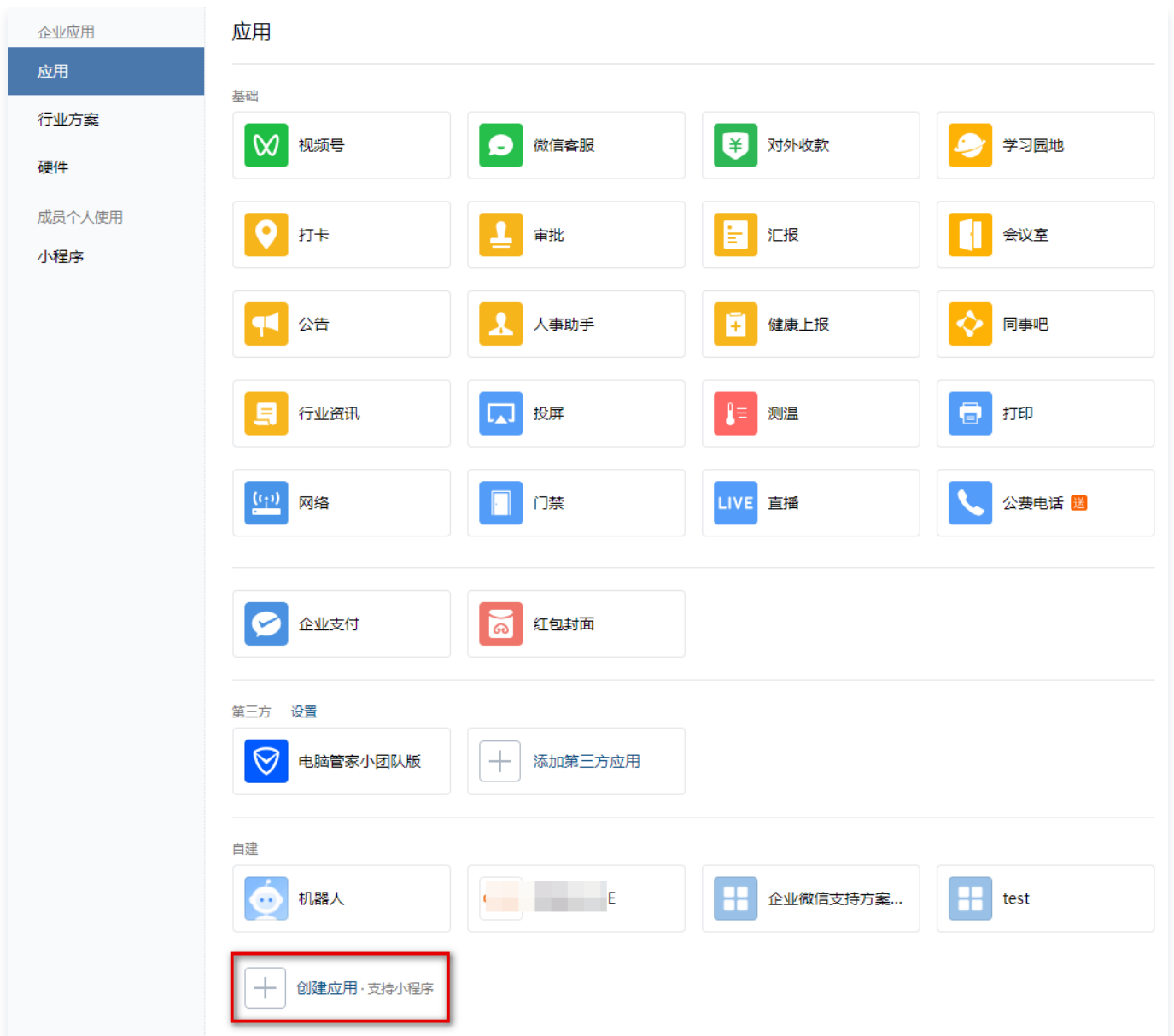
① 说明：

- 需配置备案主体与当前企业主体相同或有关联关系的域名，详情请参见 [企业内部开发配置域名指引](#)。
- 如果已有域名且通过了备案，可跳过步骤1和2。

1. [申请一个域名](#)。
2. [域名备案](#)。
3. [将可信域名指向企微代理服务器 IP](#)。

2. 配置企业微信自建应用

1. 登录 [企业微信管理后台](#)，单击上方的[应用管理](#)，默认进入应用页面。
2. 在应用页面，单击自建 > [创建应用](#)。



3. 在创建应用页面，配置相关参数，单击**创建应用**。

说明：

可见范围务必包含需要同步的组织范围，否则无法同步组织；建议设置为根目录。

应用logo

 建议使用750*750, 1M以内的jpg、png图片

应用名称

应用介绍 (选填)

可见范围

[已有小程序快速创建](#)

3. 设置可信域名

1. 在应用页面，单击刚刚创建的**自建应用**。
2. 在应用详情页面，选择开发者接口，单击**设置可信域名**。

开发者接口

网页授权及JS-SDK

可信域名下的网页可使用网页授权及JS-SDK

设置可信域名

企业微信授权登录

使用企业微信帐号登录已有的Web网页或移动APP

设置

审批接口

使用企业微信审批能力，在非审批应用内设置流程、发起审批。还能订阅通知消息，接收审批状态变化情况。

设置

企业可信IP

仅所配IP可通过接口获取企业数据

配置

3. 在设置可信域名窗口中，输入 [域名验证](#) 中要求的可信任域名，单击 [申请校验域名](#)。

设置可信域名
×

可作为应用OAuth2.0网页授权功能的回调域名

可信域名

为保障企业数据安全，需配置备案主体与当前企业主体相同或有关联关系的域名。[配置指引](#)

可调用JS-SDK、跳转小程序的可信域名（最多10个，需完成域名校验）

可信域名

[+ 添加更多域名](#)

配置可信域名需完成域名归属认证

[申请校验域名](#)

确定

取消

4. 在设置可信域名窗口中，单击**下载文件**，并将该文件发送给腾讯项目对接人。

配置可信域名需完成域名归属认证

1. 请下载文件“WW_verify_b4N6lbCzLusJYQH7.txt” 下载文件

2. 将下载的文件上传至填写域名根目录下
 例如 http://wx.qq.com/WW_verify_b4N6lbCzLusJYQH7.txt，并确保可以访问

5. 待腾讯项目对接人上传文件至企微代理服务器后，单击**确定**，完成可信域名配置。

设置可信域名
✕

可作为应用OAuth2.0网页授权功能的回调域名

可信域名

为保障企业数据安全，需配置备案主体与当前企业主体相同或有关联关系的域名。[配置指引](#)

可调用JS-SDK、跳转小程序的可信域名（最多10个，需完成域名校验）

可信域名

[+ 添加更多域名](#)

配置可信域名需完成域名归属认证 已验证

确定
取消

4. 设置企业可信 IP

1. 在应用页面，单击刚刚创建的自建应用。
2. 在应用详情页面，选择开发者接口，单击企业可信 IP 中的配置。



3. 在企业可信 IP 窗口中，输入 IP 地址。



5. 获取企业 ID 和自建应用 Secret

1. 登录 [企业微信管理后台](#)，单击上方的我的企业，默认进入企业信息页面。

2. 在企业信息页面的下方，获取企业 ID。

企业信息

权限管理

聊天管理

通讯录管理

工作台管理

微信插件

申请加入设置

外部沟通管理

安全与保密

设置

企业信息

企业logo [前往认证](#)

推荐尺寸702*180

企业简称 [修改](#) 认证后可提高使用人数等

企业地址 [添加](#)

联系电话 [添加](#)

企业域名 [添加](#)

企业成员 统计

企业部门

已使用/人数上限

发票抬头 [添加](#) 为企业成员配置增值税发票抬头

行业类型 [修改](#) 计算机软件/硬件/信息服务

员工规模 [修改](#) 51-100人

创建时间 20


企业ID w

3. 单击上方的应用管理，并选中刚刚创建好的自建应用。

4. 在应用详情页面，单击 Secret 右侧的查看，将 Secret 内容复制并保存。

⚠ 注意：

为确保数据安全，请确认为企业内部使用，切勿将 Secret 泄漏给第三方。



首元应用介绍

已启用


AgentId

[编辑](#)

Secret

查看

可见范围



步骤二：配置 iOA 私有化 控制台

1. 设置身份源

1. 登录 iOA 零信任管理平台控制台，在左侧导航中，单击**管理中心** > **用户与授权管理**。
2. 在用户与授权管理页面，单击**新建**。
3. 在新建目录页面，输入名称和描述，是否导入架构选择**是**，导入类型选择**企业微信**，单击**下一步**。

新增目录

* 名称	<input type="text" value="任我行"/>
描述	<input type="text" value="请输入描述"/>
* 是否导入架构	<input checked="" type="radio"/> 是 <input type="radio"/> 否
* 导入类型 	<input type="text" value="企业微信"/>

4. 在新增目录页面，配置相关参数。

基础配置

类型 企业微信 ▼

企业ID * [模糊处理]

应用Secret ⓘ * [模糊处理]

代理地址 ⓘ * [输入框]

连通性测试 ⓘ 测试

组织架构更新设置
 开启自动更新
 每周
 每天
 每四小时
 每隔

高级配置

根部门ID ⓘ * [1]

是否同步标签 ⓘ

用户属性字段映射 ⓘ

姓名 * [name]

手机号 * [mobile]

邮箱 * [email]

头像 * [avatar]

状态 ⓘ
String类型 ▼
表示状态的属性字段
表示正常状态的值

参数名称	说明
------	----

企业 ID	获取方式请参见 获取企业 ID 和自建应用 Secret 。
应用 Secret	获取方式请参见 获取企业 ID 和自建应用 Secret 。
代理地址	填写方式为： <code>http://ip:13732</code> ，具体 IP 请联系腾讯项目对接人获取。
连通性测试	输入企业 ID、企业自建应用 Secret 和代理服务器地址后可进行连通性测试，会同时检查基础配置是否有效。
组织架构更新设置	根据实际需求设置。
根部门 ID	如无必要，请勿修改。如果只需要特定部门，请输入正确的部门 ID。
是否同步标签	同步的标签数据会写入自定义分组。
用户属性字段映射	<p>如无特殊需求，请勿修改。</p> <p>其中字段如果不映射，将会用系统定义的状态，其中0表示用户异常状态，1表示用户正常状态。</p> <p>映射支持三种数据类型，且必须填写正常状态的值：</p> <ol style="list-style-type: none"> 对于 Bool 类型和 String 类型，相同的值会关联到状态 1，不相同的统一到 0； 对于 Int 类型，相同的值会关联到状态 1，其他值会默认保留。 <p>属性映射中，若映射字段不存在或不想同步相应字段，则输入任意不存在的属性名即可，同步时会将对应用属性置为空。</p>

5. 单击**测试**，测试通过后单击**保存**。

6. 在用户与授权管理页面，找到刚刚创建的目录，单击**用户同步**，同步组织架构。

目录名称	描述	关联的用户源	操作
	-	自建账户	目录管理 编辑 删除 资源授权
	-	企业微信	目录管理 编辑 删除 资源授权 用户同步 会话存档配置

7. 在用户与授权管理页面，找到刚刚创建的目录，单击**目录管理**，查看组织架构信息。



2. 配置认证源

1. 登录 iOA 零信任管理平台控制台，在左侧导航中，单击**身份安全策略 > 认证安全 > 认证源配置**。
2. 在认证源配置页面，单击**新增认证源实例**。
3. 在新增认证源实例页面，类型选择**企业微信**，并配置其他参数，单击**保存**。

⚠ 注意：

- 必须点击安装连接完成企业微信的第三方应用安装（使用企微管理员账号扫码安装、如果网页已登录企微管理后台则自动添加），否则无法保存认证源。
- 如果您之前的企业微信后台安装过**腾讯零信任 iOA**的应用，请删除原有应用，重新安装。
- 若已经完成了应用安装，但是认证源无法保存，提示未检测到授权结果，则稍等片刻再单击**保存**。
- 若一直报错提示无法保存，请联系腾讯项目对接人。

新增认证源实例
✕

配置说明 ✕
展开 ▶

类型 ▼
企业微信

认证方式 ▼
扫码认证 授权认证

名称 * ✔
任我行

客户端登录标题 ⓘ

客户端登录标题(英文)

客户端登录提示

客户端登录提示(英文)

安装链接 ⓘ
点击跳转

3. 设置认证策略

说明：

- 企业微信认证源需要和您导入企业微信身份源（目录）保持一致。
- 可以为不同身份源(目录)配置不同的认证策略，互不影响。
- 如果针对单个身份源(目录)添加主认证源，需要在该身份源(目录)的**基础策略**中增加认证源。

1. 在**策略中心 > 身份安全策略 > 认证安全 > 认证策略**页面，选择目标目录，单击**编辑**。

执行优...	策略名称	描述	适用用户	主认证	二次认证	动态挑战认证	操作
	基础策略		组织架构: [模糊]	PC: [模糊] 移动端: [模糊]	-	PC: [模糊] 移动端: [模糊]	编辑

2. 在编辑认证策略页面，PC 端将刚刚添加的企业微信认证源作为主认证方式。

PC端

主认证方式的认证源

北京任我行

- [模糊] [模糊]
- 北京任我行
- 钉钉 [模糊]
- iOA本地账密
- TOTP认证
- 设备认证

确定 重置

3. 单击添加，完成编辑。

PC端

主认证方式的认证源

北京任我行

双因素认证

是否启用

二次认证方式的认证源

请选择

指定主认证登录豁免双因素

请选择

挑战认证方式认证源

iOA本地账密

添加 取消

iOA 私有化飞书对接



方案1：飞书认证

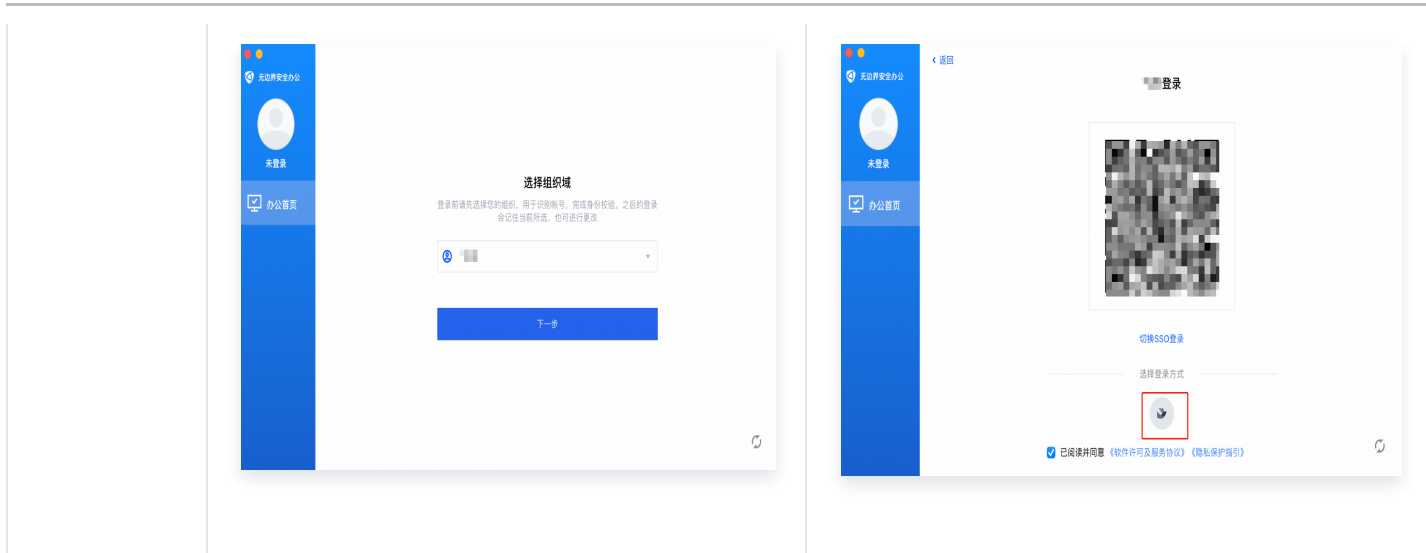
最近更新时间：2024-06-08 06:14:42

说明：

- iOS 端如需使用“飞书认证”，请联系腾讯项目对接人，我们需要在后台配置登录参数，可以提供 iOS 端的登录 Demo。
- 方案1 后续可能会不兼容 Mac，无法支持 Mac 的扫码登录。飞书支持 OAuth2 方式登录，建议使用 Mac 的用户配置飞书的 [OAuth2 登录方式](#)。

登录效果

类型	选择组织域	登录效果
浏览器		
客户端		



步骤一：飞书认证准备

1. 配置飞书信息

如您是首次使用，需要创建一个企业自建应用；如您还没有开通飞书开发者账号，请前往 [飞书开放平台](#) 创建一个开发者账号。

1. 登录 [飞书开放平台](#)，选择企业自建应用，单击创建企业自建应用。



2. 在创建企业自建应用窗口中，配置相关参数，单击创建。

创建企业自建应用
✕

该应用仅可在“扬基科技”内部使用，应用发布需经过企业管理员审核，请仔细阅读[应用审核规则](#)。

名称*

5/32

应用描述*

应用图标*

JPEG/PNG/SVG/BMP 格式，2 MB 以内，大于 240*240 px，无圆角



上传图标

选择背景色

✓

选择图标

































取消

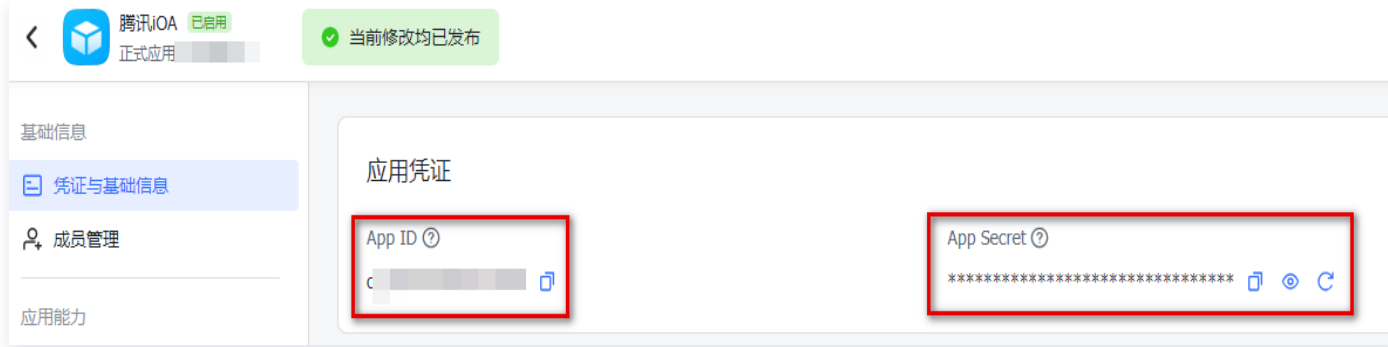
创建

2. 获取 App ID 和 App Secret

1. 在企业自建应用页面，单击刚刚创建的**自建应用**。
2. 在凭证与基础信息页面，选择应用凭证，获取 App ID 和 AppSecret。其中：飞书的 App ID 对应 iOA 控制台上的 App ID，飞书的 App Secret 对应 iOA 控制台的 App Secret。

版权所有：腾讯云计算（北京）有限责任公司

第32 共97页



3. 配置重定向 URL

1. 在凭证与基础信息页面，单击**安全设置**。
2. 在重定向 URL 页面，输入以下 iOA 的网关回调域名，单击**添加**，即可添加到重定向 URL 列表中。
 - SSO 的回调域名：`https://scs.gateway.tencent.com/akpage/sso/redirect`。
 - 二维码的回调域名：`https://scs.gateway.tencent.com/akpage/qrcode/redirect`。



4. 配置权限管理

1. 在安全设置页面，单击**权限管理**。
2. 在权限管理页面，支持通过搜索框选择权限，如：以应用身份读取通讯录；获取部门基础信息；获取部门组织架构信息；获取用户组信息；获取用户基本信息；获取用户组织架构信息；获取用户邮箱信息；获取用户 user ID；通过手机号或邮箱获取用户 ID；获取用户手机号；获取企业信息。



3. 选中目标权限后，单击操作列的**开通权限**，即可为该应用选中所需权限。

说明：

配置权限后，需要重新发布应用才能生效。

5. 发布应用

1. 在权限管理页面，单击**版本管理与发布**。
2. 在版本管理与发布页面，单击右上角的**创建版本**。



3. 在版本详情页面，填写应用版本号（格式如 1.0.0）和更新说明，设置可用性状态，单击**保存**。

注意：

可用范围：选择所有员工（除非只同步指定部门）。

[< 返回](#)

版本详情

! 为保障企业数据安全及应用质量，本次发布需要“扬基科技”企业管理员审核，详情参见 [应用审核规则](#)

应用版本号*

对用户展示的正式版本号，上一个版本号为 1.1.1

更新说明*

此内容将于应用的更新日志中显示

0/500

应用能力

暂无

权限变更

暂无

可用范围

所有员工 [编辑](#)

申请理由

帮助审核人员了解此应用的附加信息，例如：1. 为什么需要开通这些高级权限；2. 为什么需要申请相关可用范围。

[保存](#) [取消](#)

4. 保存完成后，单击[申请线上发布](#)。

i 确认提交发布申请？

发布前请仔细阅读 [应用审核规则](#)

[取消](#) [申请线上发布](#)

! 说明：

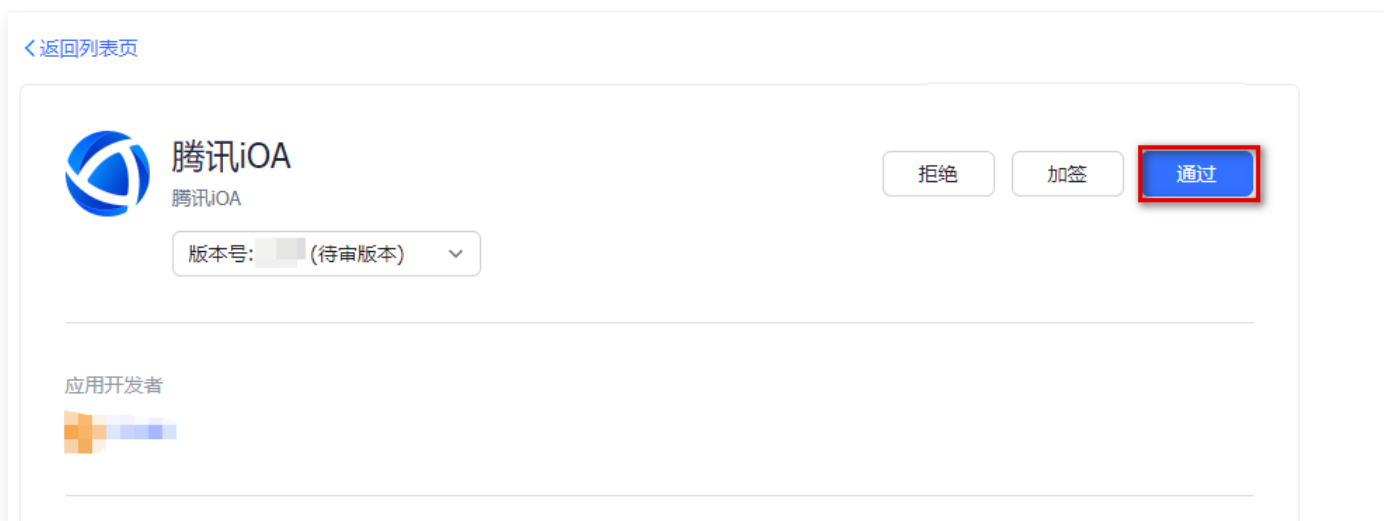
- 提交申请后，企业管理员会进行审核。
- 审核结果会通过飞书和开发者后台发送给您。
- 更多详情请见 [飞书文档 - 开发企业自建应用](#)。

6. 应用审核（如无需审核，请跳过）

1. 在 [应用审核页面](#)，选择目标应用，单击审核。



2. 在审核详情页面，单击通过。



7. 开启飞书移动应用登录功能（选配）

1. 登录 [飞书开放平台](#)，选择企业自建应用，并单击需要开启移动登录功能的自建应用。

2. 在应用详情页面，单击添加应用能力 > 按能力添加。

3. 找到移动应用登录，单击添加。



4. 在移动应用登录页面，配置相关参数，单击保存。

移动应用登录 ● 未完成必填项配置

用户可使用飞书账号登录移动应用 [如何开发](#)

[查看能力介绍](#)

飞书登录配置

用户登录协议 *

OAuth2.0 OIDC

应用类型 *

iOS应用 Android 应用

iOS 市场地址

请输入 iOS 市场地址

请输入 iOS Bundle ID *

请输入 iOS Bundle ID

Android 市场地址

请输入 Android 市场地址

Android 包名称 *

请输入 Android 包名称

Android 签名 *

请输入 Android 签名

[如何生成 Android 签名](#)

保存

取消

参数类型	参数名称	参数详情	备注
用户登录协议	OAuth2.0	根据实际需求选择。	-
	OIDC	根据实际需求选择。	-
应用类型	iOS 应用	iOS Bundle ID: 正式版 <code>com.tencent.ioa</code> ; 其他体验版或测试请联系腾讯项目对接人。	如不需要移动端授权, 无需填写
	Android	正式版是固定的, 其他体验版或测试请联系	

应用	腾讯项目对接人。 Android 包名称: <code>com.tencent.ioa</code> 。 Android 签名: <code>9xxxx594cd6xxxxcxxxxe3xxxx88dd5a</code> 。
----	---

8. 开启邮箱/手机号账号身份关联功能（选配）

说明:

如果需要开启手机验证码或邮箱验证码作为二次认证/挑战认证的实例，则建议从飞书同步字段时，开通手机号或邮箱的同步权限。在 iOA 控制台添加短信验证码或邮箱验证码时，将通过飞书同步过来的手机号/邮箱作为字段映射和身份认证的依据。

1. 登录 [飞书开放平台](#)，选择企业自建应用，并单击目标自建应用。
2. 在应用详情页面，单击权限管理，下滑至权限配置。
3. 在权限配置模块，分别开启以下两个功能：
 - 开启手机号账号身份关联功能：搜索获取用户手机号，单击开通权限。



权限配置

获取用户手机号 权限名称 批量开通

全部 (1)	权限名称	权限等级	关联 API/事件	权限状态	操作
通讯录 (1)			[API] 使用手机号或邮箱获取用户 ID		
	获取用户手机号 contact:user.phone:readonly	需审核权限	[API] 修改用户部分信息 [API] 创建用户 [API] 刷新 user_access_token 展开	未开通	开通权限

- 开启邮箱账号身份关联功能：搜索获取用户邮箱信息，单击开通权限。

权限配置

获取用户邮箱信息

权限名称 ▾

批量开通

全部 (1)	权限名称	权限等级 ▾	关联 API/事件 ▾	权限状态 ▾	操作
通讯录 (1)			[API] 使用手机号或邮箱获取用户 ID		
	<input type="checkbox"/> 获取用户邮箱信息 contact:user.email:readonly	需审核权限	[API] 修改用户部分信息 [API] 创建用户 [API] 刷新 user_access_token 展开 ▾	• 未开通	开通权限

↑ 返回顶部
↻ 技术支持
➡ 收起

4. 配置上述权限后，需要重新 [发布应用版本](#) 才能生效。

步骤二：iOA 控制台配置

1. 新建目录

1. 登录 iOA 零信任管理平台控制台，在左侧导航中，单击 **管理中心 > 用户与授权管理**。
2. 在用户与授权管理页面，单击 **新建**。
3. 在新增目录页面，输入名称和描述，是否导入架构选择 **是**，导入类型选择 **飞书**，单击 **下一步**。

新增目录

* 名称

描述

* 是否导入架构 是 否

* 导入类型 !

4. 在新增目录页面，输入 [App ID](#) 和 [App Secret](#)，以及其他参数。

基础配置

类型 ▼
飞书

App ID *

App Secret *

连通性测试 ⓘ 测试

组织架构更新设置 开启自动更新

每周

每天

每四小时

每隔

5. 单击**测试**，测试通过后检查根部门 ID 与应用可见范围是否一致，核对无误后单击**保存**。

说明：

- 当根部门 ID 为 0 时，则代表根部门 ID 与可见范围一致，都是所有员工。
- 当应用可见范围同步指定部门时，需核对根部门 ID 与指定可见范围是否一致。

高级配置

根部门ID ⓘ * 0

是否同步用户组 ⓘ

6. 在用户与授权管理页面，找到刚刚创建的目录，单击**用户同步**，即可同步组织架构。

2. 配置认证源

1. 登录 [iOA 零信任管理平台控制台](#)，在左侧导航中，单击[身份安全策略](#) > [认证安全](#) > [认证源配置](#)。
2. 在认证源配置页面，单击[新增认证源实例](#)。
3. 在新增认证源实例页面，类型选择[飞书](#)，并配置其他参数，单击[保存](#)。

说明：

- App ID：为飞书的 App ID。
- App Secret：为飞书的 App Secret。

类型：飞书

认证方式：扫码认证 授权认证

名称 *：飞书对接测试

客户端登录标题 ⓘ

客户端登录标题(英文)

客户端登录提示

客户端登录提示(英文)

App ID *

App Secret *

3. 设置认证策略

1. 在[策略中心](#) > [身份安全策略](#) > [认证安全](#) > [认证策略](#)页面，选择目标目录，单击[编辑](#)。

执行优...	策略名称	描述	适用用户	主认证	二次认证	动态挑战认证	操作
	基础策略		组织架构: ...	PC: ... 移动端: ...	-	PC: ... 移动端: ...	编辑

2. 在编辑认证策略页面，设置 PC 端的主认证方式认证源和挑战认证方式认证源。

说明：

如您要使用飞书 App 内的应用免登录，您还需要设置移动端的主认证方式认证源和挑战认证方式认证源，设置方式与 PC 端相同。

PC端

主认证方式的认证源

飞书对接测试

双因素认证

是否启用



二次认证方式的认证源

请选择

 指定主认证登录豁免双因素?

请选择

挑战认证方式认证源

飞书对接测试

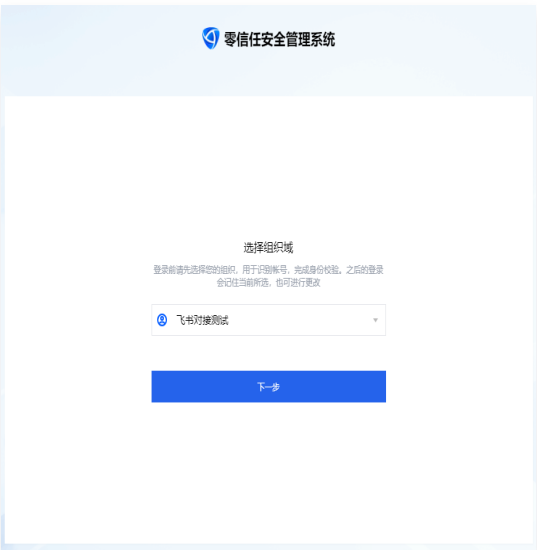

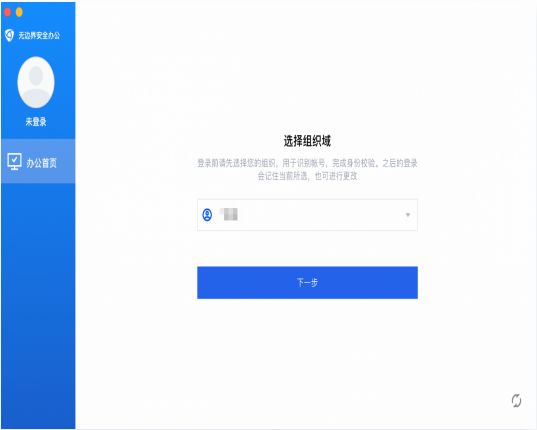

3. 单击**添加**，完成编辑。

方案2: OAuth2 认证

最近更新时间: 2024-06-08 06:14:42

说明:
建议使用 Mac 的用户配置飞书的 OAuth2 登录方式。

登录效果

类型	选择组织域	登录效果
浏览器		
客户端		

步骤一：飞书认证准备

1. 配置飞书信息

如您是首次使用，需要创建一个企业自建应用；如您还没有开通飞书开发者账号，请前往 [飞书开放平台](#) 创建一个开发者账号。

1. 登录 [飞书开放平台](#)，选择**企业自建应用**，单击**创建企业自建应用**。



2. 在创建企业自建应用窗口中，配置相关参数，单击**创建**。

创建企业自建应用 ✕

该应用仅可在“扬基科技”内部使用，应用发布需经过企业管理员审核，请仔细阅读[应用审核规则](#)。

名称*
腾讯iOA 5/32

应用描述*
腾讯零信任 5/120

应用图标*
JPEG/PNG/SVG/BMP 格式，2 MB 以内，大于 240*240 px，无圆角



上传图标

选择背景色

<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	-------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

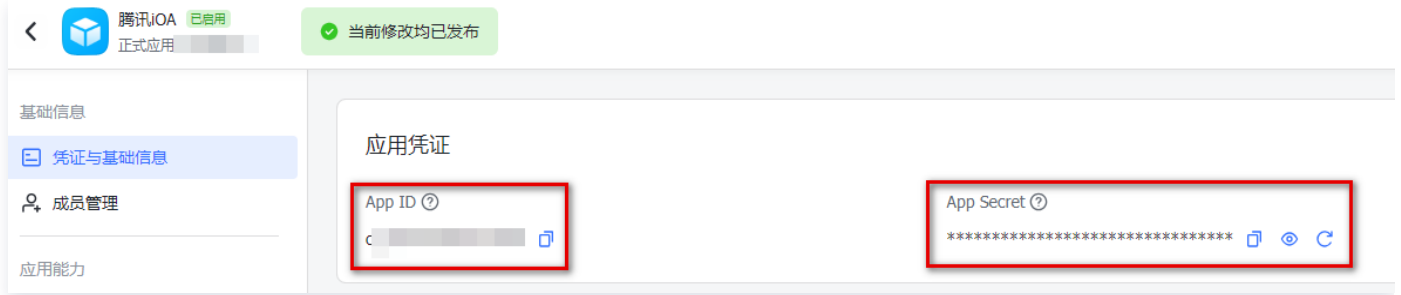
选择图标

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

取消 创建

2. 获取 App ID 和 App Secret

1. 在企业自建应用页面，单击刚刚创建的**自建应用**。
2. 在凭证与基础信息页面，选择应用凭证，获取 App ID 和 AppSecret。其中：飞书的 App ID 对应 iOA 控制台上的 App ID，飞书的 App Secret 对应 iOA 控制台的 App Secret。



3. 配置重定向 URL

1. 在凭证与基础信息页面，单击**安全设置**。
2. 在重定向 URL 页面，输入 iOA 的网关回调域名 `https://scs.gateway.tencent.com/akpage/sso/redirect`，单击**添加**，即可添加到重定向 URL 列表中。

⚠ 注意：

OAuth2 认证方案的飞书认证准备步骤中，其他步骤都与飞书认证方案一样，唯有重定向URL与飞书认证方案的重定向 URL 不同。



4. 配置权限管理

1. 在安全设置页面，单击**权限管理**。
2. 在权限管理页面，支持通过搜索框选择权限，如：以应用身份读取通讯录；获取部门基础信息；获取部门组织架构信息；获取用户组信息；获取用户基本信息；获取用户组织架构信息；获取用户邮箱信息；获取用户 user ID；通过手机号或邮箱获取用户 ID；获取用户手机号；获取企业信息。



3. 选中目标权限后，单击操作列的**开通权限**，即可为该应用选中所需权限。

说明：

配置权限后，需要重新发布应用才能生效。

5. 发布应用

1. 在权限管理页面，单击**版本管理与发布**。
2. 在版本管理与发布页面，单击右上角的**创建版本**。

版本管理与发布

若企业自建应用需要供企业内其他用户使用，或商店应用需要上架飞书应用目录，都必须发布一个版本。

[创建版本](#)

版本号	版本状态	发布人	发布通过时间	操作
1.1.1	已发布		2023-6-7 19:21	-

3. 在版本详情页面，填写应用版本号（格式如 1.0.0）和更新说明，设置可用性状态，单击**保存**。

注意：

可用范围：选择所有员工（除非只同步指定部门）。

[< 返回](#)

版本详情

i 为保障企业数据安全及应用质量，本次发布需要“扬基科技”企业管理员审核，详情参见 [应用审核规则](#)

应用版本号 *

对用户展示的正式版本号，上一个版本号为 1.1.1

更新说明 *

此内容将于应用的更新日志中显示

0/500

应用能力

暂无

权限变更

暂无

可用范围

所有员工 [编辑](#)

申请理由

帮助审核人员了解此应用的附加信息，例如：1. 为什么需要开通这些高级权限；2. 为什么需要申请相关可用范围。

保存

取消

4. 保存完成后，单击申请线上发布。

i 确认提交发布申请？

发布前请仔细阅读 [应用审核规则](#)

取消

申请线上发布

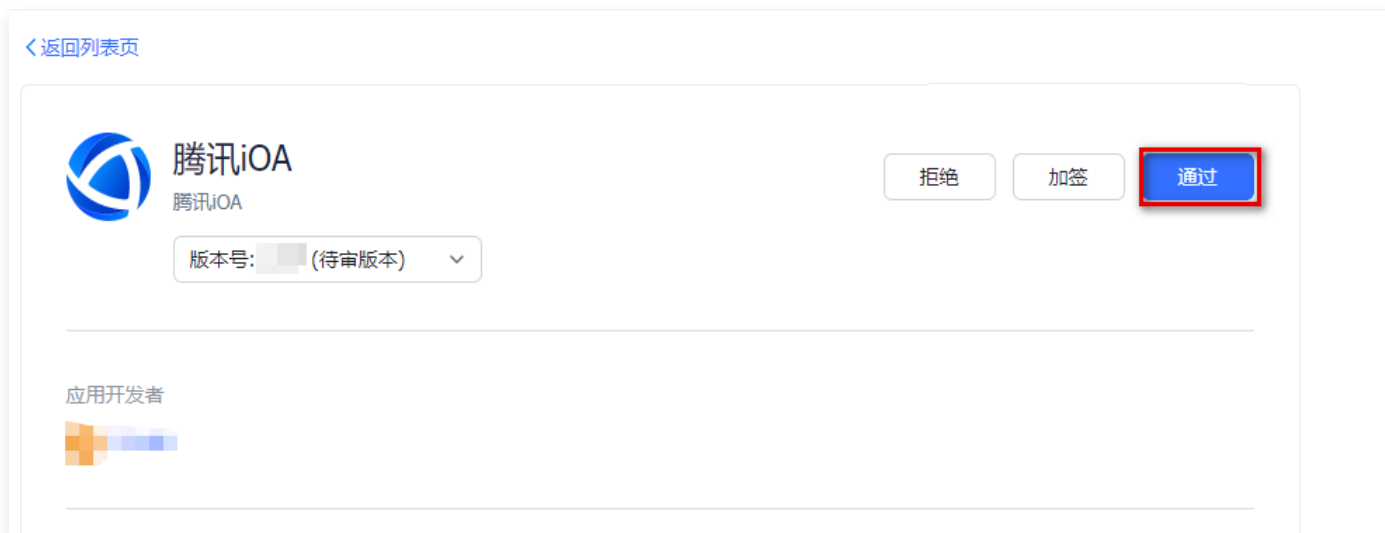
i 说明：

- 提交申请后，企业管理员会进行审核。

- 审核结果会通过飞书和开发者后台发送给您。
- 更多详情请见 [飞书文档 - 开发企业自建应用](#)。

6. 应用审核（如无需审核，请跳过）

1. 在 [应用审核页面](#)，选择目标应用，单击审核。
2. 在审核详情页面，单击**通过**。



7. 开启飞书移动应用登录功能（选配）

1. 登录 [飞书开放平台](#)，选择**企业自建应用**，并单击需要开启移动登录功能的**自建应用**。
2. 在应用详情页面，单击**添加应用能力 > 按能力添加**。
3. 找到**移动应用登录**，单击**添加**。



4. 在移动应用登录页面，配置相关参数，单击**保存**。

移动应用登录 ● 未完成必填项配置

用户可使用飞书账号登录移动应用 [如何开发](#)

[查看能力介绍](#)

飞书登录配置

用户登录协议 *

OAuth2.0 OIDC

应用类型 *

iOS应用 Android 应用

iOS 市场地址

请输入 iOS 市场地址

请输入 iOS Bundle ID *

请输入 iOS Bundle ID

Android 市场地址

请输入 Android 市场地址

Android 包名称 *

请输入 Android 包名称

Android 签名 *

请输入 Android 签名

[如何生成 Android 签名](#)

保存

取消

参数类型	参数名称	参数详情	备注
用户登录协议	OAuth2.0	根据实际需求选择。	-
	OIDC	根据实际需求选择。	-
应用类型	iOS 应用	iOS Bundle ID: 正式版 <code>com.tencent.ioa</code> ; 其他体验版或测试请联系	如不需要移动端授

	腾讯项目对接人。	权, 无需填写
Android 应用	正式版是固定的, 其他体验版或测试请联系腾讯项目对接人。 Android 包名称: <code>com.tencent.ioa</code> 。 Android 签名: <code>9xxxx594cd6xxxxcxxxxe3xxxx88dd5a</code> 。	

8. 开启邮箱/手机号账号身份关联功能 (选配)

说明:

如果需要开启手机验证码或邮箱验证码作为二次认证/挑战认证的实例, 则建议从飞书同步字段时, 开通手机号或邮箱的同步权限。在 iOA 控制台添加短信验证码或邮箱验证码时, 将通过飞书同步过来的手机号/邮箱作为字段映射和身份认证的依据。

1. 登录 [飞书开放平台](#), 选择企业自建应用, 并单击目标自建应用。
2. 在应用详情页面, 单击权限管理, 下滑至权限配置。
3. 在权限配置模块, 分别开启以下两个功能:
 - 开启手机号账号身份关联功能: 搜索获取用户手机号, 单击开通权限。

权限配置

获取用户手机号 权限名称 批量开通

全部 (1)	权限名称	权限等级	关联 API/事件	权限状态	操作
通讯录 (1)			[API] 使用手机号或邮箱获取用户 ID		
	获取用户手机号 contact:user.phone:readonly	需审核权限	[API] 修改用户部分信息 [API] 创建用户 [API] 刷新 user_access_token	未开通	开通权限

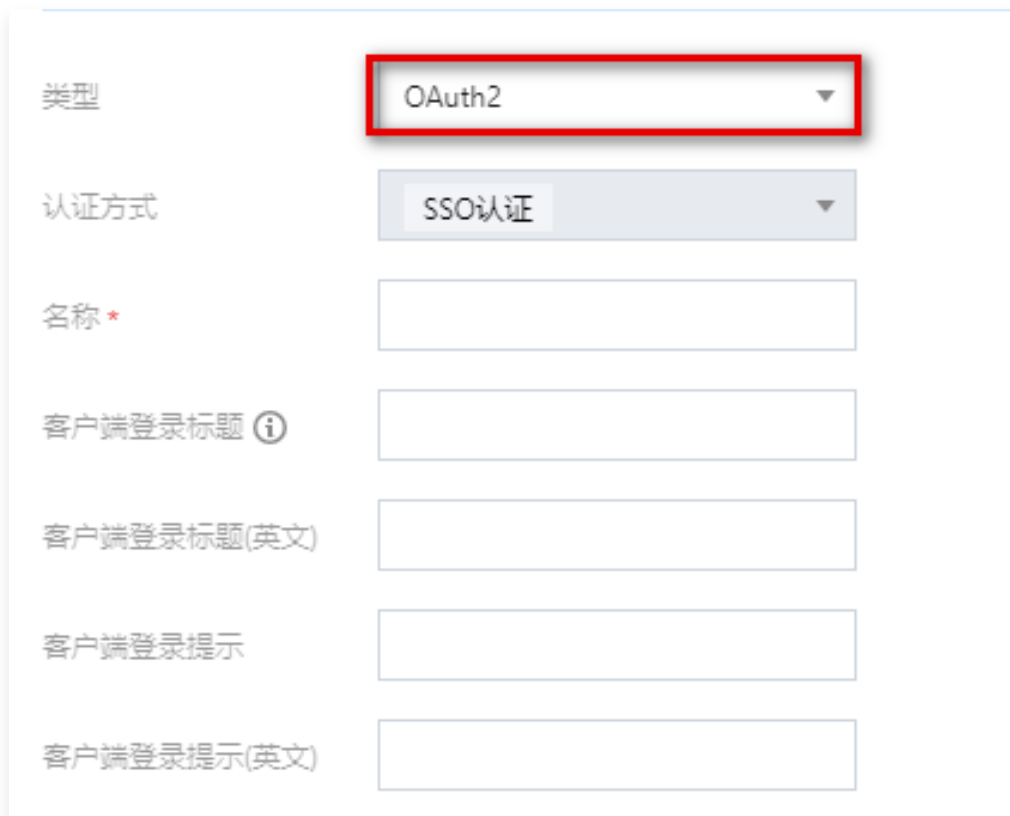
- 开启邮箱账号身份关联功能: 搜索获取用户邮箱信息, 单击开通权限。



4. 配置上述权限后，需要重新 **发布应用版本** 才能生效。

步骤二：iOA 控制台配置

1. 登录 iOA 零信任管理平台控制台，在左侧导航中，单击**身份安全策略 > 认证安全 > 认证源配置**。
2. 在认证源配置页面，单击**新增认证源实例**。
3. 在新增认证源实例页面，类型选择 **OAuth2**。



4. 复制如下代码，来获取 Code、AccessToken 和 用户信息。

```
{
  "sensitive_fields": [
```

```
"client_secret"
],
"browser":true,
"hide_iam":false,
"hide_back":false,
"start_immediate":false,
"redirect_uri":"https://console.cloud.tencent.com:27800/akpage/sso/redirect",
"get_code":{
  "method":"GET",
  "content_type":"NONE",
  "code_field":"code",
  "url":"https://open.feishu.cn/open-apis/authen/v1/index",
  "url_parameters":[
    {
      "key":"app_id",
      "value":"[client_id]",
      "description":""
    },
    {
      "key":"redirect_uri",
      "value":"[redirect_uri]",
      "description":""
    },
    {
      "key":"state",
      "value":"[state]",
      "description":""
    }
  ],
  "header_parameters":[

],
  "body_parameters":[

]
},
"get_access_token":{
  "method":"POST",
  "content_type":"JSON",
  "url":"https://open.feishu.cn/open-apis/auth/v3/tenant_access_token/internal",
  "error_message_path":"msg",
  "access_token_path":"tenant_access_token",
  "url_parameters":[

],

```

```
"header_parameters":[
],
"body_parameters":[
  {
    "key":"app_id",
    "value":"[client_id]",
    "description":""
  },
  {
    "key":"app_secret",
    "value":"[client_secret]",
    "description":""
  }
]
},
"get_user_info":{
  "method":"POST",
  "content_type":"JSON",
  "url":"https://open.feishu.cn/open-apis/authen/v1/access_token",
  "error_message_path":"msg",
  "user_id_path":"data.user_id",
  "user_avatar_path":"",
  "url_parameters":[

],
"header_parameters":[
  {
    "key":"Authorization",
    "value":"Bearer [access_token]",
    "description":""
  }
],
"body_parameters":[
  {
    "key":"grant_type",
    "value":"authorization_code",
    "description":""
  },
  {
    "key":"code",
    "value":"[code]",
    "description":""
  }
]
]
```

```
},
"client_id": "",
"client_secret": ""
}
```

5. 在新增认证源实例页面，单击从粘贴板导入，即可迅速完成 Code、AccessToken 和用户信息的导入。

1. 获取Code

请求地址 *

请求体格式 * 表单 JSON 无请求体

请求参数

请求URL参数
请求头部

字段 (key)	值 (value)	操作
<input type="text" value="app_id"/>	<input type="text" value="[client_id]"/>	删除
<input type="text" value="redirect_uri"/>	<input type="text" value="[redirect_uri]"/>	删除
<input type="text" value="state"/>	<input type="text" value="[state]"/>	删除
<input type="button" value="添加"/>		

2. 获取AccessToken

请求地址 *

请求体格式 * 表单 JSON 无请求体

请求参数

请求URL参数
请求头部

6. 在新增认证源实例页面，填写基本信息，单击保存。

类型	OAuth2
认证方式	SSO认证
名称 *	<input type="text"/>
客户端登录标题 ⓘ	<input type="text"/>
客户端登录标题(英文)	<input type="text"/>
客户端登录提示	<input type="text"/>
客户端登录提示(英文)	<input type="text"/>
基础配置	
客户端ID *	<input type="text"/>
客户端Secret *	<input type="password"/>
登出地址	<input type="text" value="https://"/>
使用系统浏览器 ⓘ *	<input checked="" type="checkbox"/>
隐藏内网身份系统 ⓘ *	<input type="checkbox"/>

参数名称	说明
名称	填写认证源实例名称。
App ID	为飞书的 App ID。
App Secret	为飞书的 App Secret。

登出地址	可不填，如果填写，可支持从 iOA 跳浏览器清理登录态能力。识别方式：URL 以 logout 结尾。
使用系统浏览器	建议关闭。 <ul style="list-style-type: none">● 如果开启，则会跳到系统浏览器认证，可以共享已经 SSO 登录的状态；● 如果关闭，全程在 iOA 内完成 SSO 认证。
其他参数	根据实际需求选择。

iOA 私有化 SCIM2.0 用户同步

最近更新时间：2024-06-08 06:14:42

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**管理中心** > **用户与授权管理**。
2. 在用户与授权管理页面，单击**新建**。
3. 在新增目录页面，输入名称和描述，是否导入架构选择**是**，导入类型选择 **SCIM2.0**，单击**下一步**。

新增目录

* 名称	<input type="text" value="测试"/>
描述	<input type="text" value="请输入描述"/>
* 是否导入架构	<input checked="" type="radio"/> 是 <input type="radio"/> 否
* 导入类型 	<input type="text" value="SCIM2.0"/>

4. 在新增目录页面，配置基础信息。

基础配置

类型 SCIM2.0标准 ▼

SCIM服务地址 *

接口验证方式 * Basic Auth OAuth2.0

用户名 *

密码 *

组织架构更新设置 开启自动更新

每周

每天

每四小时

每隔

参数名称		说明
SCIM 服务地址		IAM 平台地址。
接口验证方式	Basic Auth	用户名和密码可能是 IAM 平台管理员的账号密码，如不正确，请通过查找 API 请求头字段 Authorization，值是 Basic Base64(用户名:密码)。
	OAuth2.0	<ul style="list-style-type: none"> 获取 token 地址：access_token 的地址必须是完整的 URL。只支持标准的 OAuth2 方式，即请求形如 GET https://xxxx?。 客户端 ID：iOA 在 IAM 平台上注册的应用 ID。 客户端 SECRET：iOA 在 IAM 平台申请时提供的应用 Secret。

5. (可选) 在新增目录页面，配置组织架构接口、用户组接口和用户接口。

组织架构接口配置

接口URI *

是否使用分页 ⓘ *

每页最大数量 ⓘ *

父级组织ID字段 *

用户组接口配置

接口URI *

是否使用分页 ⓘ *

每页最大数量 ⓘ *

用户接口配置

接口URI *

是否使用分页 ⓘ *

每页最大数量 ⓘ *

组织架构列表字段 *

用户组列表字段

参数类型	参数名称	说明
组织架构接口配置	接口 URI	默认 <code>/scim/v2/Organizations</code> ，如果接口特殊，可以参考默认格式填写接口名称。
	是否使用分页	<ul style="list-style-type: none"> 开启分页后会进行分页拉取；分页只支持标准的参数，<code>startIndex</code> 表示开始项的位置，<code>count</code> 表示一页的数量。 不开启分页则默认 <code>count=-1</code> 拉取全量数据。

	每页最大数量	每页数据量最少为10。
	父级组织 ID 字段	组织架构必须包含表示父级目录 ID 的字段，否则无法构建目录树。
用户组接口配置	接口 URI	默认 <code>/scim/v2/Groups</code> ，如果接口特殊，可以参考默认格式填写接口名称。
	是否使用分页	<ul style="list-style-type: none"> 开启分页后会进行分页拉取；分页只支持标准的参数，<code>startIndex</code> 表示开始项的位置，<code>count</code> 表示一页的数量。 不开启分页则默认 <code>count=-1</code> 拉取全量数据。
	每页最大数量	每页数据量最少为10。
用户接口配置	接口 URI	默认 <code>/scim/v2/Users</code> ，如果接口特殊，可以参考默认格式填写接口名称。
	是否使用分页	<ul style="list-style-type: none"> 开启分页后会进行分页拉取；分页只支持标准的参数，<code>startIndex</code> 表示开始项的位置，<code>count</code> 表示一页的数量。 不开启分页则默认 <code>count=-1</code> 拉取全量数据。
	每页最大数量	每页数据量最少为10。
	组织架构列表字段	用户必须包含所属组织架构的 ID 字段，用于将用户放入特定的组织架构目录。
	用户组列表字段	填写默认字段即可，如果字段特殊，可填写自己的列表字段。

6. (可选) 在新增目录页面，配置用户属性字段映射。

注意:

如无特殊需求，请勿修改。

用户属性字段映射 ?

用户ID *	<input type="text" value="userName"/>
姓名 *	<input type="text" value="displayName"/>
手机号 *	<input type="text" value="phoneNumbers.#.value"/>
邮箱 *	<input type="text" value="emails.#.value"/>
头像 *	<input type="text" value="avatar"/>
状态 ?	<input type="button" value="不映射状态"/> <input type="button" value="表示状态的属性字段"/> <input type="button" value="表示正常状态的值得"/>

参数名称	说明
用户 ID	用户在 iOA 用来登录的 ID，可以是用户名/手机号/邮箱等等，但是必须保证唯一。 注意：用户在系统中的其他 ID 无特殊用途。
状态	<p>映射状态是指，将身份源的状态字段关联到 iOA 的锁定/非锁定状态；支持三种类型：Int/Bool/String，这里关联状态的值必须是正常状态的值得。所有星号为必填项目，但是对于无法映射的属性或存在映射关系但不想同步过来的属性，可以赋予一个错误的属性值，那么属性会被赋予空值。</p> <ul style="list-style-type: none"> 如果用户对象是 JSON 格式的，只是语法来获取嵌套属性，以姓名属性为例。例如： <pre style="background-color: #2c3e50; color: white; padding: 10px; margin: 10px 0;">{ "name": { "name256": "xxx" } }</pre> 指定 name256 为头像，那么可以输入 name.name256。 <pre style="background-color: #2c3e50; color: white; padding: 10px; margin: 10px 0;">{ "name": [</pre>

```
{  
  "value": "xxx"  
}  
]  
}
```

- 指定对象数组的元素的值，可以输入 name.#.value。

7. 单击**测试**，测试通过后单击**保存**。
8. 在**用户与授权管理**页面，找到刚刚创建的目录，单击**用户同步**。

数据安全中心

终端数据安全策略

管控范围

最近更新时间：2024-06-08 06:14:42

作为数据安全模块的基础全局配置，请添加需要管控的对象和通道范围。不在管控范围内的用户、终端和通道将不进行数据安全防护。

管控对象

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据安全中心** > **数据安全策略** > **终端数据安全策略**。
2. 在终端数据安全策略页面，选择**管控范围**，您可以通过添加或排除用户、组织架构、自定义用户组和终端，来进行精细化的管控范围设置。配置完成后，iOA 将对被管控的对象下发管控策略，以实现数据安全防护。

ⓘ 说明

当用户处于管控范围内，其登录的终端将自动继承该管控范围。在终端未被其他用户登录之前，它将保持继承该用户的管控范围。

基本信息

* 策略名称 0/50

策略描述 0/200

* 是否启用

适用范围

添加适用范围 ▼
删除

搜索适用对象 Q

	对象类型 ▼	添加类型 ▼	排除时间	操作
请添加适用范围				
排除终端				<div style="border: 1px solid #ccc; padding: 2px; width: fit-content;"> 排除 Windows 终端 排除 MacOS 终端 </div>

1 / 1 页

编辑策略

管控通道 Q

管控通道

iOA 支持对多种外发通道进行管控，包括电子邮箱、即时通讯（IM）、浏览器、网络硬盘和外部设备等。您可以在 **数据安全策略 > 终端数据安全策略 > 管控范围** 页面通过勾选配置管控通道，对用户外发通道进行精细化管理。

管控通道

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔



电子邮箱 (17/17)

网易邮箱大师	Outlook	foxmail
阿里邮箱	Apple Mail	QQ邮箱网页版
QQ企业邮箱网页版	阿里企业邮箱网页版	网易邮箱大师网页版
163邮箱网页版	189邮箱网页版	139邮箱网页版
126邮箱网页版	Outlook网页版	新浪邮箱网页版
Yeah邮箱网页版	Gmail网页版	

> 即时通信 (0/18)

> 浏览器 (0/9)

> 网盘 (0/26)

> 远程控制工具 (0/8)

自定义管控通道

iOA 零信任管理平台提供自定义管控通道来扩大通道覆盖面，您可以按照以下步骤添加自定义通道信息。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据安全中心 > 数据安全策略 > 终端数据安全策略**。
2. 在终端数据安全策略页面，选择**管控范围**，单击**自定义通道**。



3. 单击**添加自定义通道**，在添加自定义通道页面，输入自定义通道的基本信息，具体内容如下：

* 通道名称

* 通道类型

* 通道图标

+

请上传36像素 x 36像素至150像素 x 150像素大小的方形通道图标，图片宽高比例为1:1，支持PNG、JPG格式

* 是否启用

参数名称	说明
通道名称	自定义管控通道的名称。
通道类型	选择该管控通道的类别。
通道图标	上传36x36像素至150x150像素大小的正方形通道图标，图片宽高比例为1: 1，支持PNG、JPG 格式。
是否启用	默认开启。

4. 配置该通道在 Windows 环境下的进程信息，具体包括通道进程名和文件路径白名单。

通道进程

Windows

* 通道进程名

可输入多个进程名，每一行一个进程名

i 若自定义通道的进程名与系统内置通道重复，则优先命中内置通道。参考[帮助文档](#)获取正确的进程名

* 文件路径白名单

请输入路径白名单，用于不管控的系统文件、应用配置文件等非敏感文件，支持"*"、"?"的路径配置，一行数据一行路径。

参数名称	说明
通道进程名	必选，可输入多个进程名，利用换行符分隔，每一行表示一个进程名。
文件路径白名单	文件路径白名单：必选，可用于加白不需要管控的系统文件、应用配置文件路径，支持正则匹配；可输入多个白名单路径，使用换行符分隔，一行表示一个文件路径。例如，需要加白 C:\Windows 路径下的所有文件，可配置为 C:\\Windows\\.*。

进程名获取方法如下：

菜单栏右键打开**任务管理器**，单击**详细信息**。找到需要检测的进程，第 列的名称即为所需**通道进程名**。

任务管理器

键入要搜索的名称、发布者或 PID

详细信息

名称	PID	状态	用	CPU	内存(活动的...	体系结构	描述
系统空闲进程	0	正在运行	S..	99	8 K		处理器空闲时间百分比
系统中断	-	正在运行	S..	00	0 K		延迟过程调用和中断服务例程
WXWorkWeb.exe	34740	正在运行	y..	00	53,156 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	19032	正在运行	y..	00	1,280 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	21464	正在运行	y..	00	71,624 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	31384	正在运行	y..	00	2,296 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	26928	正在运行	y..	00	6,012 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	1556	正在运行	y..	00	69,300 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	14104	正在运行	y..	00	8,576 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	17160	正在运行	y..	00	9,208 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	11648	正在运行	y..	00	122,480 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	34772	正在运行	y..	00	113,800 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	9112	正在运行	y..	00	30,708 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	16168	正在运行	y..	00	11,480 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	21152	正在运行	y..	00	6,864 K	x86	WXWorkWeb.exe
WXWork.exe	18520	正在运行	y..	00	261,996 K	x86	WXWork.exe
WXWork.exe	31320	正在运行	y..	00	2,048 K	x86	WXWork.exe
WXWork.exe	17128	正在运行	y..	00	2,108 K	x86	WXWork.exe
WXWork.exe	29008	正在运行	y..	00	2,100 K	x86	WXWork.exe
WXWork.exe	24496	正在运行	y..	00	2,092 K	x86	WXWork.exe
WXDrive.exe	12376	正在运行	y..	00	42,536 K	x86	WXDrive

5. 配置该通道在 macOS 环境下的进程信息，具体包括通道进程名和 Bundle ID。

macOS

请输入对应的进程名和Bundle ID，需要成对出现并用英文逗号","分割。可输入多个进程，每一行一个进程
例如：WeChat,com.tencent.xinWeChat

0/1024

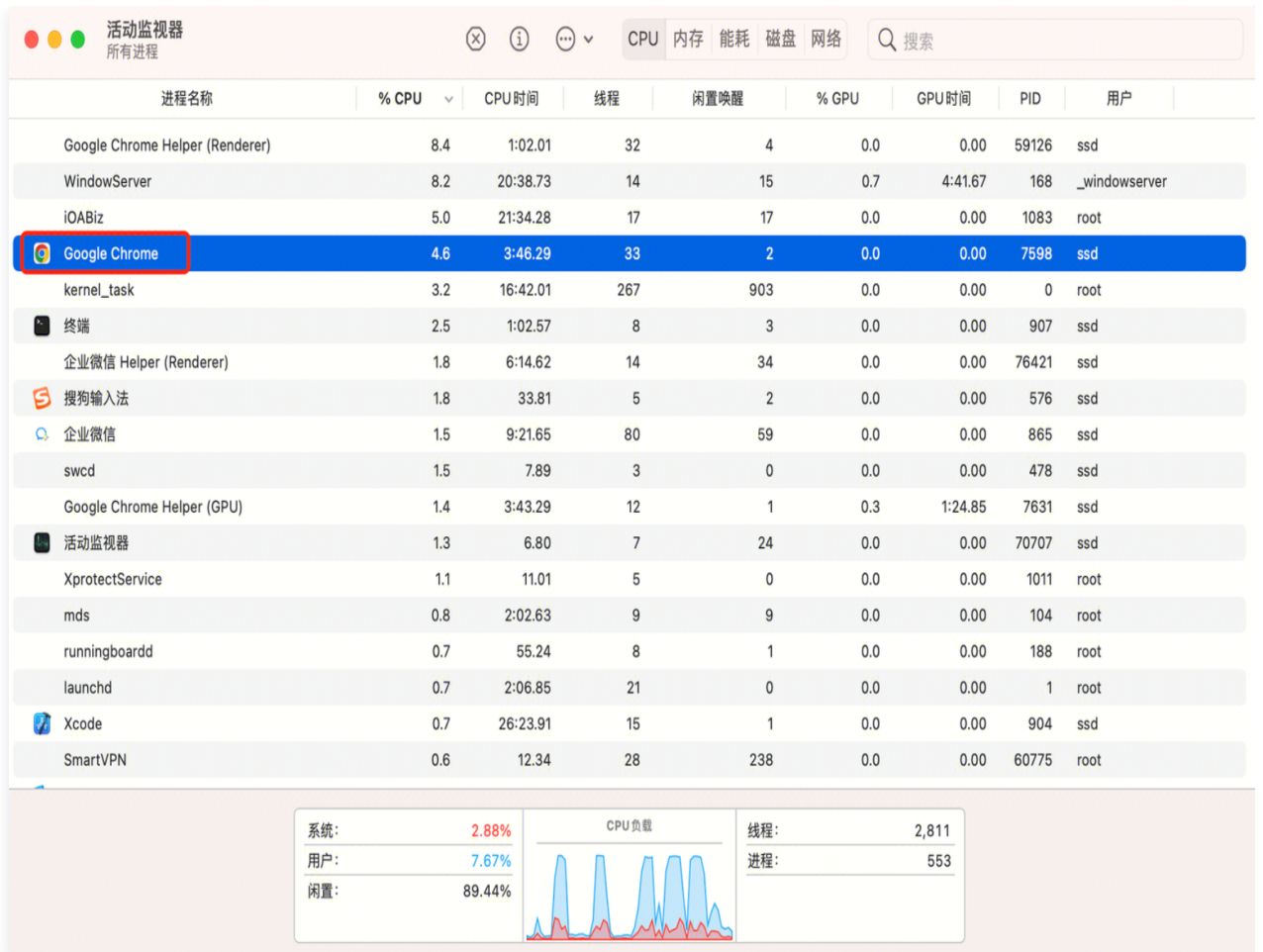
* 进程名和Bundle ID

i 若自定义通道的进程名与系统内置通道重复，则优先命中内置通道。参考[帮助文档](#)获取正确的进程名和应用的Bundle ID

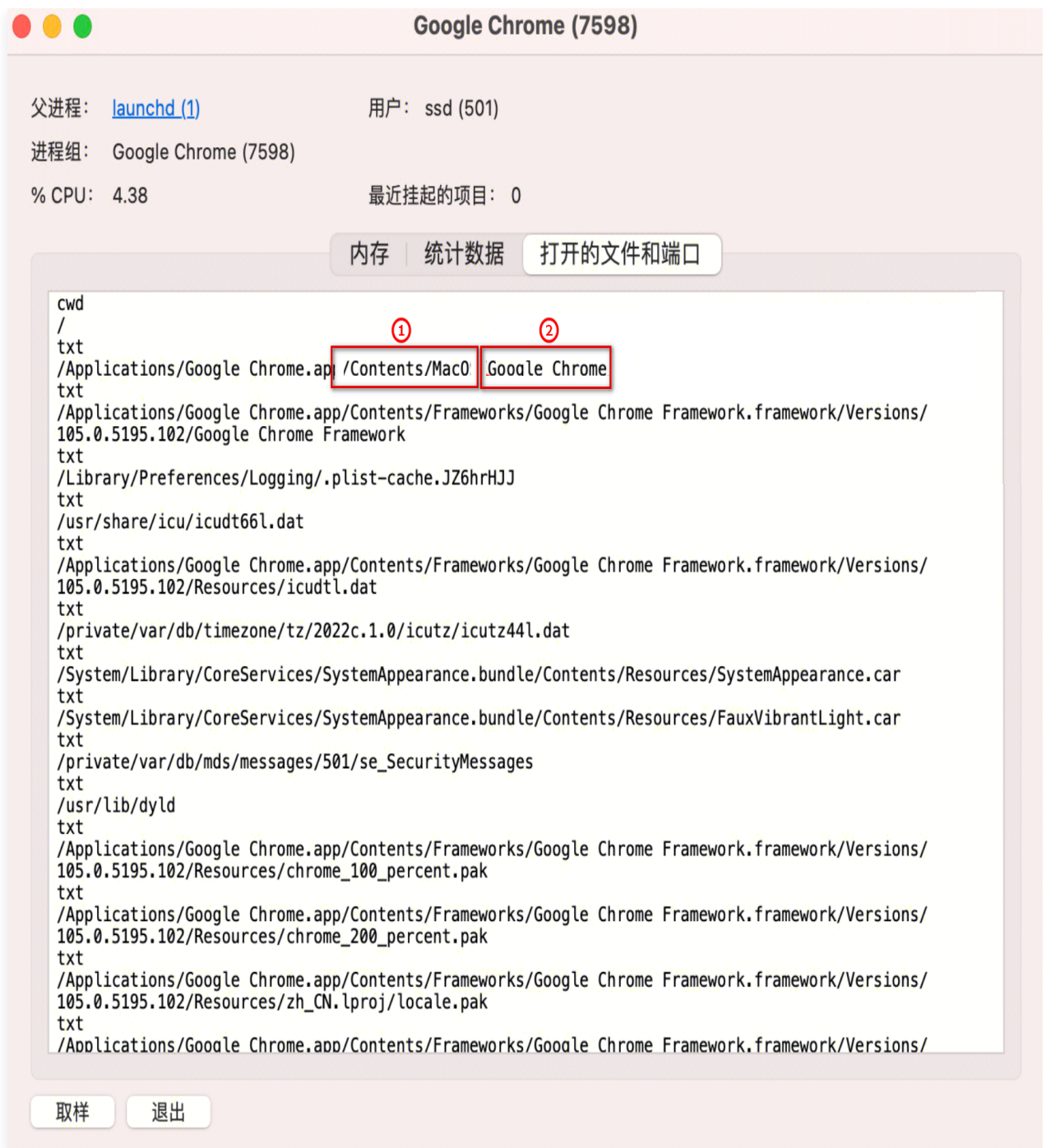
具体获取方法如下：

5.1 获取通道进程名

5.1.1 打开活动监控器（Activity Monitor），找到应用进程信息，双击打开进程的详细信息。



5.1.2 单击打开的文件和端口，找到①处包含 `/Contents/MacOS/` 的字符串，后面的②内容即为所需进程名。



5.2 获取 Bundle ID

打开终端命令（Terminal），在终端命令行中执行：

`defaults read 安装的软件路径/Contents/Info CFBundleIdentifier`，回显即为软件的 Bundle ID。

例如：软件一般安装在 `/Applications/` 目录下，例如需要查看微信（Wechat.app），则微信的路径为 `/Applications/Wechat.app`，即执行命令

`defaults read /Applications/Wechat.app/Contents/Info CFBundleIdentifier`，如下图，得到

Bundle ID: `com.tencent.xinWeChat`。

```
[(base) → ~ defaults read /Applications/Wechat.app/Contents/Info CFBundleIdentif]
ier
com.tencent.xinWeChat
```

6. 配置完上述参数后，单击**确定**保存。

审批流配置

最近更新时间：2024-06-08 06:14:42

将第三方审批应用接入 iOA，快速搭建审批能力。

钉钉

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据安全中心 > 数据安全策略 > 终端数据安全策略**。
2. 在终端数据安全策略页面，选择**审批流配置**，单击**添加审批流**，进入审批流配置页面。

终端数据安全策略

风险告警策略 [拦截策略](#) 管控范围 通道白名单 截屏取证 管控策略设置 **审批流配置**

审批配置

添加审批流

将第三方审批应用接入 iOA，快速搭建审批能力。 [查看文档](#)



编辑 删除

最近更新时间：2024-05-30 16:27:04



钉钉审批

编辑 删除

最近更新时间：2024-05-29 15:22:15

3. 在添加审批流页面，选择**钉钉**，输入示例审批流程名称为**钉钉-Test**，选择**审批管理员**。

示例：指定用户，单击**选择用户**，勾选账号名，单击**确定保存**。

说明：

- 指定用户：选择组织架构中的用户，对应用户名需要与钉钉中的一致，请确保在收到审批测试信息后进行保存。
- 自定义：填写对应审批管理员的钉钉用户名，请确保在收到审批测试信息后进行保存。

添加审批流



* 审批应用 钉钉

* 审批流程名称

* 审批管理员 ⓘ 指定用户 自定义

+ 选择用户

* 审批测试发起人 ⓘ 选择发起人 请点击左侧按钮添加审批测试发起人

* 审批测试接收人 ⓘ 选择接收人 请点击左侧按钮添加审批测试接收人

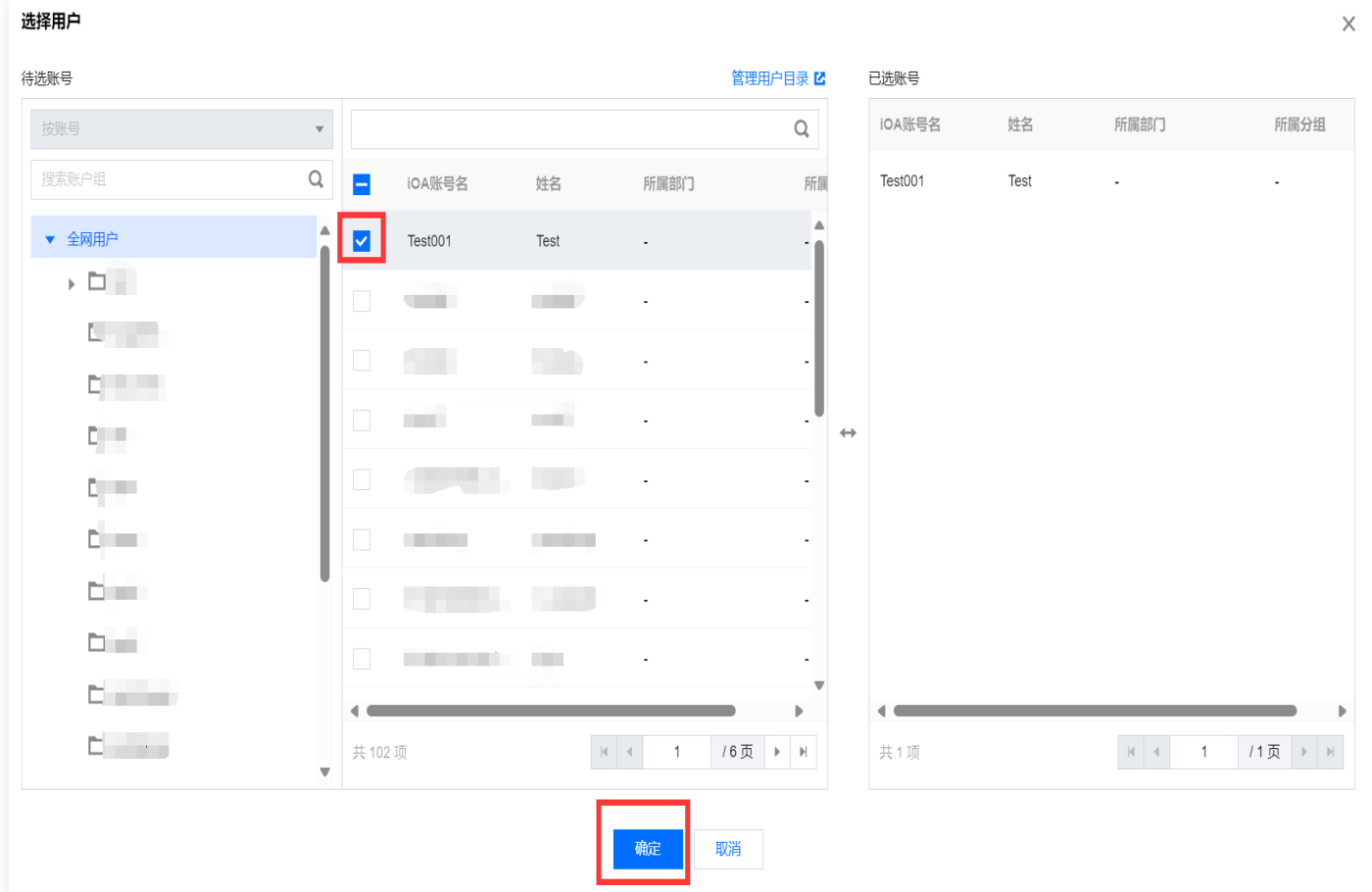
ⓘ 请添加钉钉审批配置，在下方配置一次后可重复使用，无需重新配置。

* 安装配置

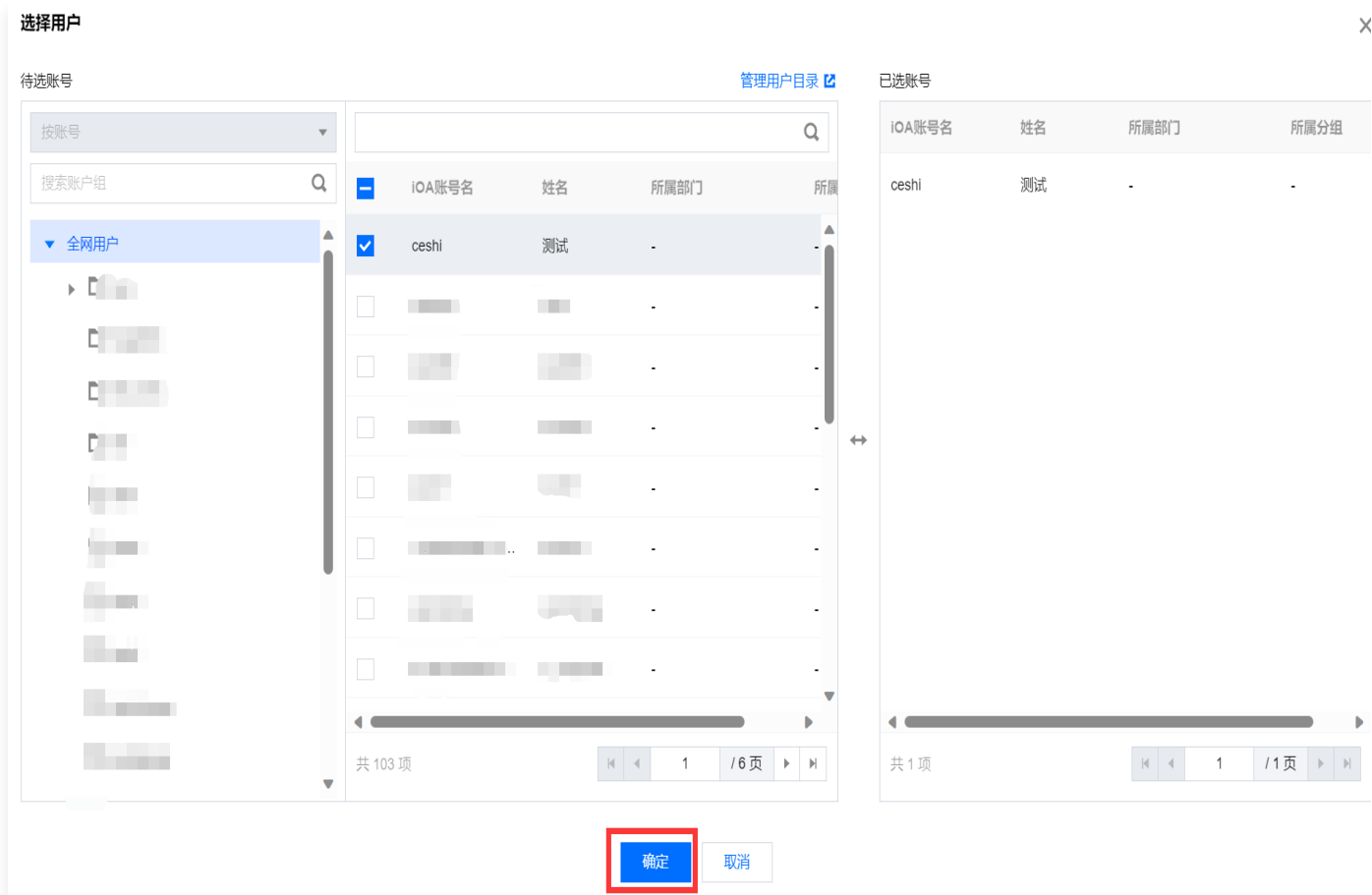
回调地址 复制

请将地址复制到「事件订阅-请求地址配置」处。

4. 审批测试发起人：单击**选择发起人**，单击**确定**保存。



5. 审批测试接收人：单击**选择接收人**，单击**确定**保存。



6. 安装配置：单击下拉框 > 新建配置。



7. 在新建安装配置窗口中，输入安装配置名称，根据如下描述配置相关参数。

* 安装配置名称	请输入
* App Key ⓘ	请输入
* App Secret ⓘ	请输入
* 审批流程ID ⓘ	请输入
* aes_key ⓘ	请输入
* 签名 Token ⓘ	请输入

确定
取消

7.1 安装配置名称：根据实际需求，自定义名称。

7.2 获取 App Key，App Secret 参数。

7.2.1 登录钉钉开放平台- [开发者后台](#)，进入应用开发，单击[创建应用](#)，填写应用名称、应用描述后单击保存。



7.2.2 选择创建的应用，单击[查看版本详情](#)，单击 编辑版本详情信息后保存并发布。

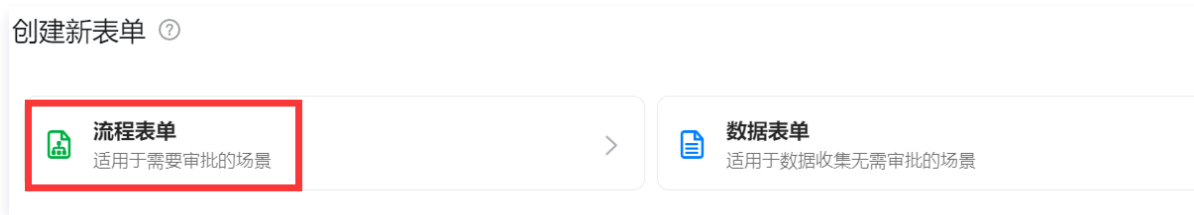


7.2.3 单击凭证与基础信息，获取凭证与基础信息，查看 App Key，App Secret。

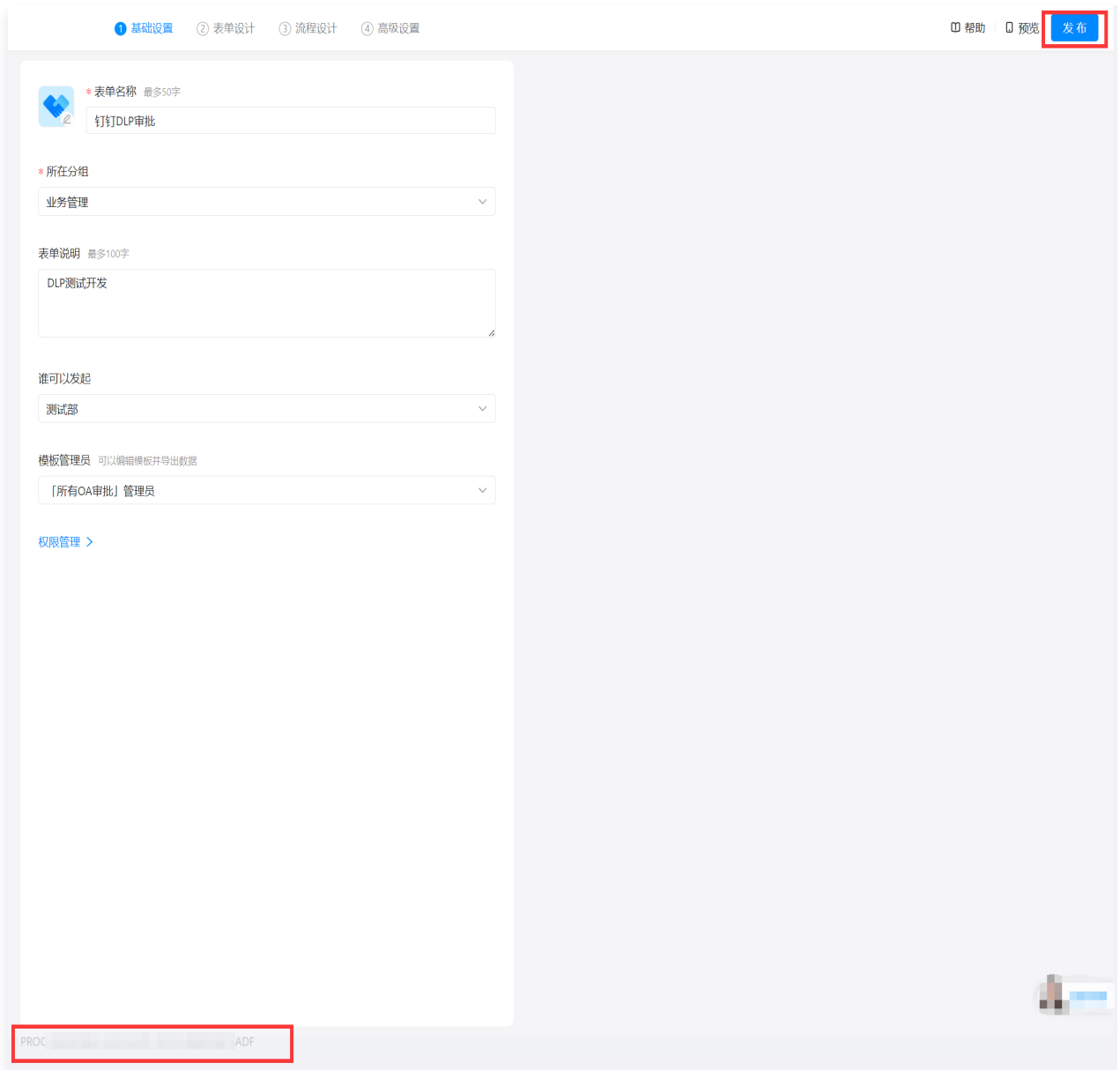


7.3 获取审批流程 ID。

7.3.1 进入 [钉钉审批管理后台](#)，单击 [创建新表单](#) > [流程表单](#)。



7.3.2 配置相关参数，同时页面最下方展示流程 ID，复制流程 ID，单击发布。




7.4 获取 aes_key 参数。

7.4.1 登录钉钉开放平台，在 [开发者后台](#) > [应用开发](#) 页面，单击 [创建的应用](#)。



7.4.2 选择**事件订阅**，配置事件订阅信息，单击**重置**，获取 aes_key、签名 token。

- **推送方式**：选择HTTP推送。
- **加密 aes_key**：单击**重置**，获取 aes_key，单击 ，查看 aes_key。
- **签名 token**：单击**重置**。获取签名 token，单击 ，查看 签名 token。

钉钉审批-Test
已上线

① 版本发布后, 当前修改才能生效 [查看版本详情](#)

事件订阅

当事件发生时, 钉钉会通过开发者订阅的方式向应用推送消息。

订阅管理

推送方式 (推荐使用Stream模式, 无需注册公网回调地址, 详情参考[文档链接](#))

HTTP推送

钉钉支持HTTP推送和Stream模式推送。

* 加密 aes_key [重置]

* 签名 token [重置]

* 请求网址

接收事件订阅的url, 必须是公网可以访问的url地址。 [了解更多](#)

保存

8. 将获取的安装配置信息依次录入, 单击确定。

新建安装配置 ✕

* 安装配置名称

* App Key (i)

* App Secret (i)

* 审批流程ID (i)

* aes_key (i)

* 签名 Token (i)

确定
取消

8.1 下拉选择安装配置名称，后台自动生成回调地址，单击复制。

* 安装配置 ▼

回调地址 复制

请将地址复制到「事件订阅-请求地址配置」处。

8.2 将生成的回调地址，复制到事件订阅 > 请求网址中，单击保存。



8.3 配置审批事件，确认开启审批事件的按钮（审批任务开始、结束、转交；审批实例开始，结束）。

钉钉开放平台 首页 应用开发 开放能力 开发工具 更多

钉钉审批流测试 开发中

基础信息

- 凭证与基础信息
- 成员管理

应用能力

- 添加应用能力

开发配置

- 权限管理
- 事件订阅**
- 安全设置
- 分享设置
- 监控中心

应用发布

- 版本管理与发布

版本发布后, 当前修改才能生效 [查看版本详情](#)

事件订阅

当事件发生时, 钉钉会通过开发者订阅的方式向应用推送消息。

订阅管理

推送方式 (推荐使用Stream模式, 无需注册公网回调地址, 详情参考[文档链接](#))

HTTP推送

钉钉支持HTTP推送和Stream模式推送。

- * 加密 aes_key
- * 签名 token
- * 请求网址

接收事件订阅的url, 必须是公网可以访问的url地址。 [了解更多](#)

保存

事件订阅

通讯录事件

通讯录用户增加	<input type="checkbox"/>	通讯录用户更改	<input type="checkbox"/>	通讯录用户离职	<input type="checkbox"/>
通讯录企业部门修改	<input type="checkbox"/>	通讯录企业部门删除	<input type="checkbox"/>	企业信息发生变更	<input type="checkbox"/>
删除角色或者角色组	<input type="checkbox"/>	修改角色或者角色组	<input type="checkbox"/>	通讯录用户被设为管理员	<input type="checkbox"/>
组织年检认证提交	<input type="checkbox"/>				

审批事件

审批任务开始, 结束, 转交	<input checked="" type="checkbox"/> 订阅设置	审批实例开始, 结束	<input checked="" type="checkbox"/> 订阅设置
----------------	--	------------	--

8.4 进入权限管理, 勾选个人权限、通讯录管理、OA 审批, 单击批量申请。

开发配置

- 权限管理**
- 事件订阅
- 安全设置
- 分享设置
- 监控中心

应用发布

- 版本管理与发布

用，具体参见接口使用指南和调用关系，部分接口需要钉钉专业版专享接口才可使用。
请选择权限范围：(添加通讯录接口权限后生效)

全部员工 部分员工

授权部门：

请输入权限或接口的名称进行搜索 仅看钉钉专业版专享接口 批量申请 (24)

全部	<input checked="" type="checkbox"/> 权限信息	接口	权限点code	全部状态	筛选 Q	操作
个人权限	<input checked="" type="checkbox"/>	查询通过流程中心集成的OA审批任务 🔗				
默认目录	<input checked="" type="checkbox"/>	审批流数据管理权限 🔗	qyapi_flow	未开通		申请权限
通讯录管理		更新流程中心任务状态 🔗				
OA审批		撤销审批实例 🔗				
考勤		同意或拒绝审批任务 🔗				
硬件	<input checked="" type="checkbox"/>	工作流实例写权限 🔗	Workflow.Instance.Write	未开通		申请权限

9. 在添加审批流页面，单击**测试**，发送审批流测试信息。

测试

保存

取消

9.1 单击**确定**，发送审批测试信息。

确定发送审批?

请在成功接收到审批信息后保存审批流配置

确定

取消

9.2 钉钉收到审批信息，审批流发起测试成功。

✔ 审批流发起测试成功 ✕

10. 单击**保存**，完成钉钉审批流配置。

添加审批流

将第三方审批应用接入 iOA，快速搭建审批能力。 [查看文档](#)



钉钉-Test

最近更新时间：2024-03-22 21:56:19

[编辑](#) | [删除](#)

数据存储设置

最近更新时间：2024-06-08 06:14:42

数据存储空间用于存储审计日志中的敏感文件和取证截图。我们为您提供了10G的临时存储空间以进行功能测试，该方式会自动清除符合条件的数据内容，存储容量不超过10G或存储时间超过30天。

注意：

由于涉及敏感数据，**请尽快更改存储方案**，创建自己的数据存储空间。目前，我们的产品支持腾讯云和S3协议的存储服务。

更改存储方案

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据安全中心 > 数据存储设置**。
2. 在数据存储设置页面，单击**更改存储方案**。



3. 在存储方案设置页面，选择存储目标，获取配置参数请参考 [配置腾讯云存储服务](#) 和 [配置S3协议存储服务](#)。

存储方案设置

* 存储目标

腾讯云

S3协议

本地存储

i 请事先分配一个具备当前bucket读写权限的最小权限子账号 [查看帮助文档](#)

* SecretId

请输入SecretId

* SecretKey

请输入SecretKey

* Endpoint

请输入Endpoint

* Bucket

请输入Bucket

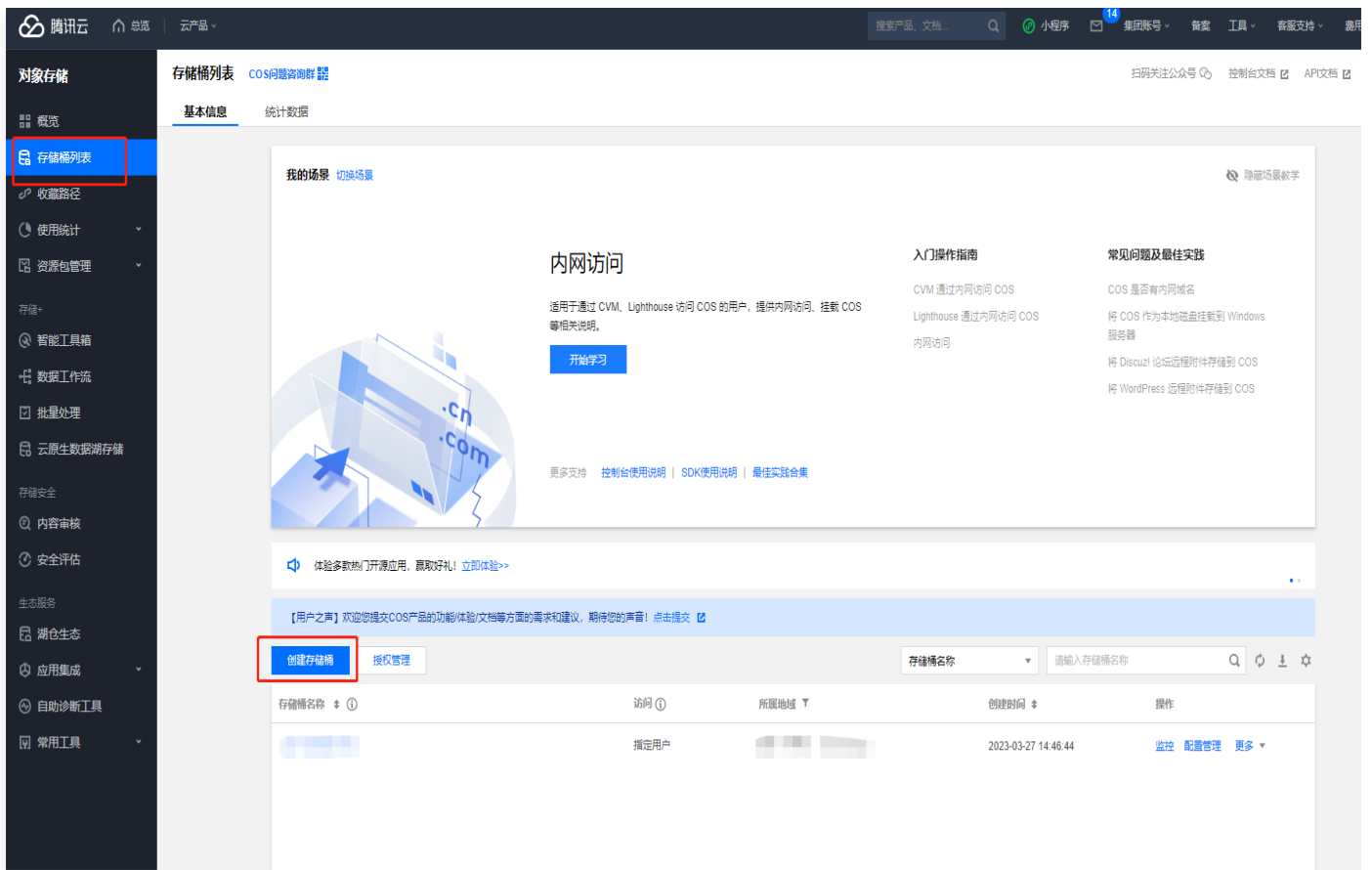
测试连通性

配置腾讯云存储服务

步骤1: 新建存储桶

存储桶用于存储 iOA 审计日志中的敏感文件和取证截图。

1. 登录 [对象存储控制台](#)，在左侧导航栏，选择存储桶列表。



2. 在存储桶列表页面，单击**创建存储桶**，新建一个存储桶。
3. 在创建存储桶窗口中，配置基本信息，单击**下一步**。

创建存储桶
✕

1 基本信息 >
 2 高级可选配置 >
 3 确认配置

所属地域 中国 ▼ 南京 ▼

存储桶与相同地域的其他腾讯云服务内网互通；**创建后地域无法修改**，请您谨慎选择。

名称 * i 存储桶名称创建后无法修改 -1307451704

还能输入 21 个字符，支持小写字母、数字和 -；**创建后名称无法修改**。

访问权限 私有读写 公有读私有写 高风险 公有读写 高风险

身份验证后，可对对象进行访问操作；您可通过 [设置访问权限](#) 给用户授权

请求域名 <名称>-1307451704.cos.ap-nanjing.myqcloud.com

创建完成后，您可以使用该域名对存储桶进行访问

取消
下一步

参数名称	说明
所属地域	选择所属地域，存储桶与相同地域的其他腾讯云服务内网互通，地域一旦选择，无法修改，请谨慎选择。
名称	填写存储桶名称，名称一旦创建，无法修改，请谨慎填写。
访问权限	可在私有读写、公有读私有写、公有读写3种访问权限中进行选择。

4. 在高级可选配置页签中，根据实际需求选择功能，单击下一步。

创建存储桶
✕

1 基本信息 >
 2 高级可选配置 >
 3 确认配置

版本控制

开启版本控制后可以恢复因覆盖或删除丢失的数据。
在相同存储桶中保留对象的多个版本，将产生存储容量费用。[了解更多](#)

多AZ特性

当前地域多AZ特性建设中，暂不支持。建议您设置存储桶跨区域复制，提升业务的容灾能力。[了解更多](#)

日志存储

为您记录跟存储桶操作相关的各种请求日志。[了解更多](#)

存储桶标签

+

您还可以创建49个标签，可通过添加存储桶标签，对存储桶进行分组管理。[了解更多](#)

服务端加密 不加密 SSE-COS ?

上一步
下一步

参数名称	说明
版本控制	可选择是否开启版本控制，开启版本控制后可以恢复因覆盖或删除丢失的数据。
多 AZ 特性	部分地域支持多 AZ 特性，如不支持的地域，可通过设置存储桶跨区域复制，提升业务的容灾能力。
日志存储	可选择是否开启日志存储，开启后可记录跟存储桶操作相关的各种请求日志。
存储桶标签	支持输入标签键和标签值，可创建50个标签。
服务端加密	选择不加密，或 SSE-COS 加密。

5. 配置信息确认无误后，单击**创建**，完成存储桶的创建。

创建存储桶 ×

基本信息 > 高级可选配置 > **3 确认配置**

名称 ⓘ

所属地域 中国 南京

访问权限 私有读写

请求域名

版本控制 关闭

日志存储 关闭

存储桶标签 test: 123;

服务端加密 不加密

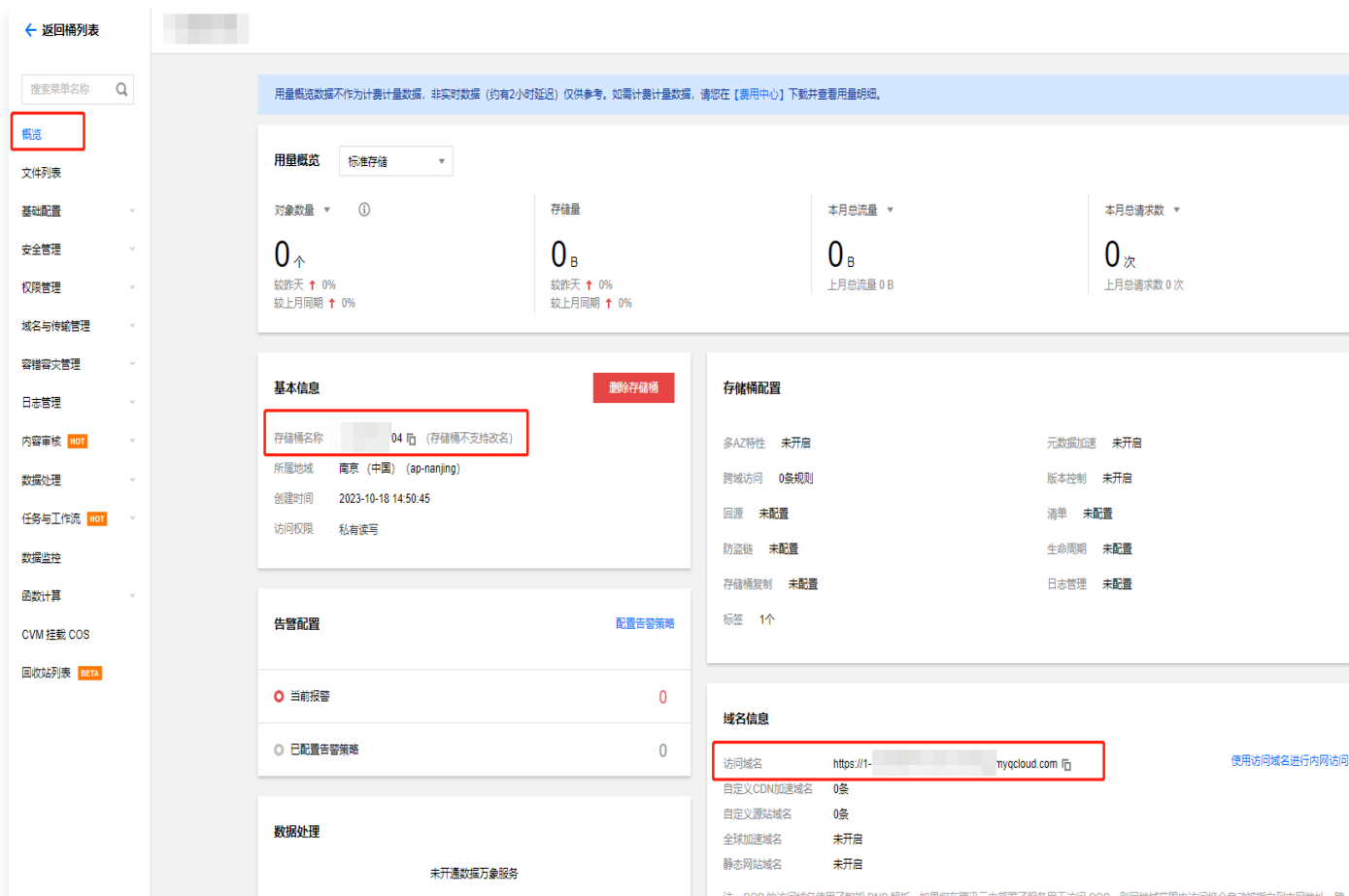
[上一步](#) [创建](#)

步骤2：获取 Bucket 和 Endpoint 参数

1. 完成存储桶的创建后，在 [存储桶列表页面](#)，单击存储桶名称，进入存储桶详情页面。

存储桶名称 ⓘ	访问 ⓘ	所属地域 ▾	创建时间 ⌵	操作
<input type="text" value="18"/>	指定用户	南京 (中国) (ap-nanjing)	2023-10-18 14:50:45	监控 配置管理 更多 ▾

2. 单击概览，查看存储桶的概览页。找到存储桶名称和访问域名，分别作为 Bucket 和 Endpoint 参数。



步骤3：为存储桶分配最小权限的子账号

1. 完成存储桶创建后，在 [存储桶列表页面](#)，单击存储桶名称，进入存储桶详情页面。



2. 在存储桶详情页面，单击 [权限管理](#) > [存储桶访问权限](#)。

3. 在存储桶访问权限页面，单击 [添加用户](#)。

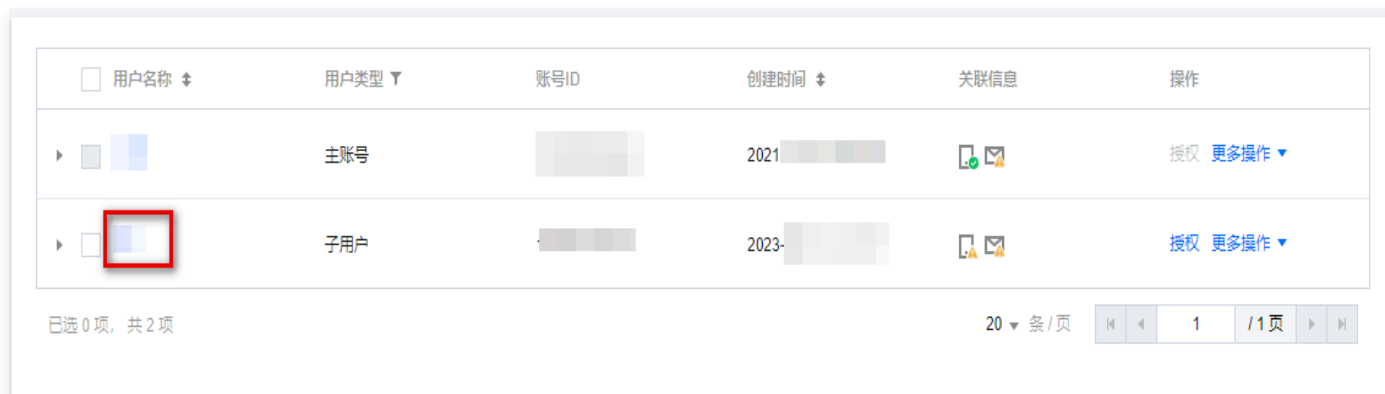


4. 添加用户时选择子账号，输入子账号 ID 并选择数据读取、数据写入两个权限，单击确定，即可为此存储桶分配一个具有读写权限（最小权限）的子账号。



步骤4：获取子账号的 SecretId 和 SecretKey

1. 登录 [访问管理控制台](#)，在左侧导航栏，选择用户 > 用户列表。
2. 在用户列表页面，找到刚刚为存储桶分配的子账号，单击用户名称。



3. 在用户详情页面，单击 [API 密钥](#) > [新建密钥](#)，获取子账号的 **SecretId** 和 **SecretKey**。



步骤5: 回到 iOA 控制台，测试连通性

1. 完成各参数的获取后，返回 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据安全中心 > 数据存储设置**。
2. 在数据存储功能设置页面，单击**更改存储方案**。



3. 存储目标选择**腾讯云**，依次填写上述获取的 **SecretId** 和 **SecretKey**、**访问域名**、**存储桶名称**。填写完成后，单击**测试连通性**，若提示**测试成功**，即配置完成。

* 存储目标 腾讯云 S3协议 本地存储

i 请事先分配一个具备当前bucket读写权限的最小权限子账号 [查看帮助文档](#)

* SecretId

* SecretKey

* Endpoint

* Bucket

↔ 测试连通性

参数名称	说明
存储目标	腾讯云。
SecretId	步骤4 获取的子账号 SecretId。
SecretKey	步骤4 获取的子账号 SecretKey。
Endpoint	步骤2 获取的存储桶访问域名。
Bucket	步骤2 获取的存储桶名称。

配置 S3 协议存储服务

iOA 支持配置 S3协议的存储服务。

i 说明


请事先分配一个具备当前 bucket 读写权限的最小权限子账号。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据安全中心 > 数据存储设置**。
2. 在数据存储设置页面，单击**更改存储方案**。
3. 存储目标选择 **S3协议**，依次填写 **AccessKeyld** 和 **SecretAccessKey**、**Endpoint**、**Bucket**，单击**测试**


连通性，若提示测试成功，即配置完成。

存储方案设置

* 存储目标

 腾讯云

 S3协议

 本地存储

 请事先分配一个具备当前bucket读写权限的最小权限子账号 [查看帮助文档](#) 

* AccessKeyId

请输入AccessKeyId

* SecretAccessKey

请输入SecretAccessKey

* Endpoint

请输入Endpoint

* Bucket

请输入Bucket

 测试连通性

参数名称	说明
存储目标	S3协议。
AccessKeyId	唯一标识符，用于识别访问云存储服务的用户或应用程序。它通常与 SecretAccessKey 配合使用，以便在对云存储服务进行身份验证时提供安全访问。
SecretAccessKey	与 AccessKeyId 配对的私钥，用于对云存储服务进行身份验证。当创建一个新的 AccessKeyId 时，系统会自动生成一个与之关联的 SecretAccessKey。
Endpoint	云存储服务的 API 访问点。它是一个 URL，用于指向服务的特定区域和访问路径。客户端通过这个 URL 与云存储服务进行通信。
Bucket	Bucket 名称。Bucket 是云存储服务中的一个基本容器，用于存储和组织数据。