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】

【商标声明】

【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

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**。

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**。

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。

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**。

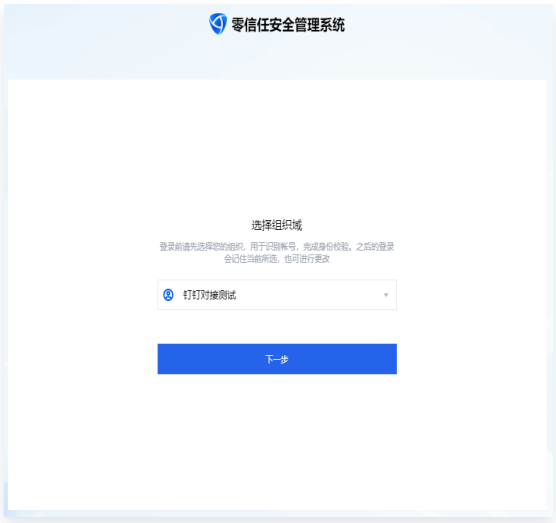
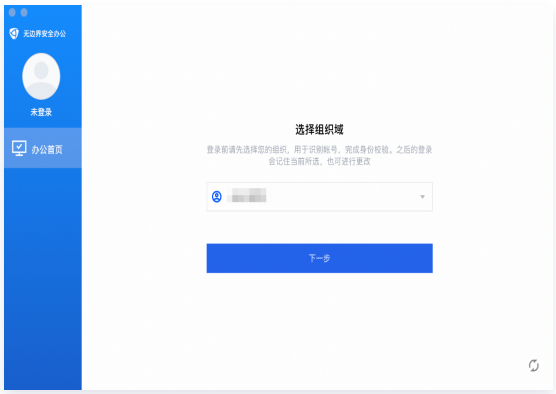
登录客户端

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**。

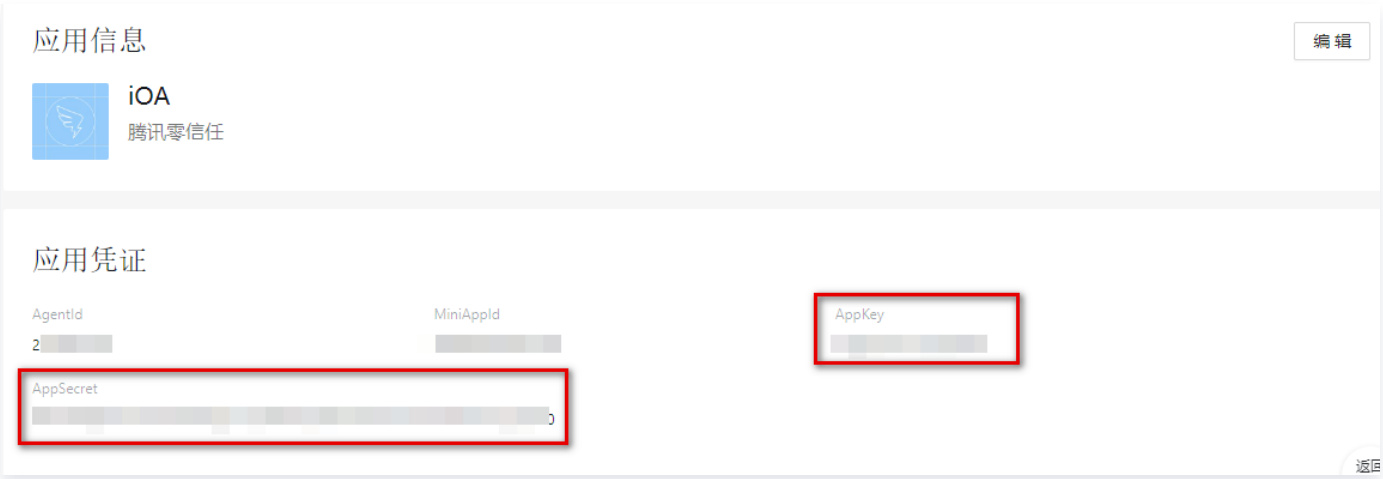
3. 在创建企业内部应用窗口中，配置相关参数，单击**确定创建**即可完成创建。

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 时需要具备的权限、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。

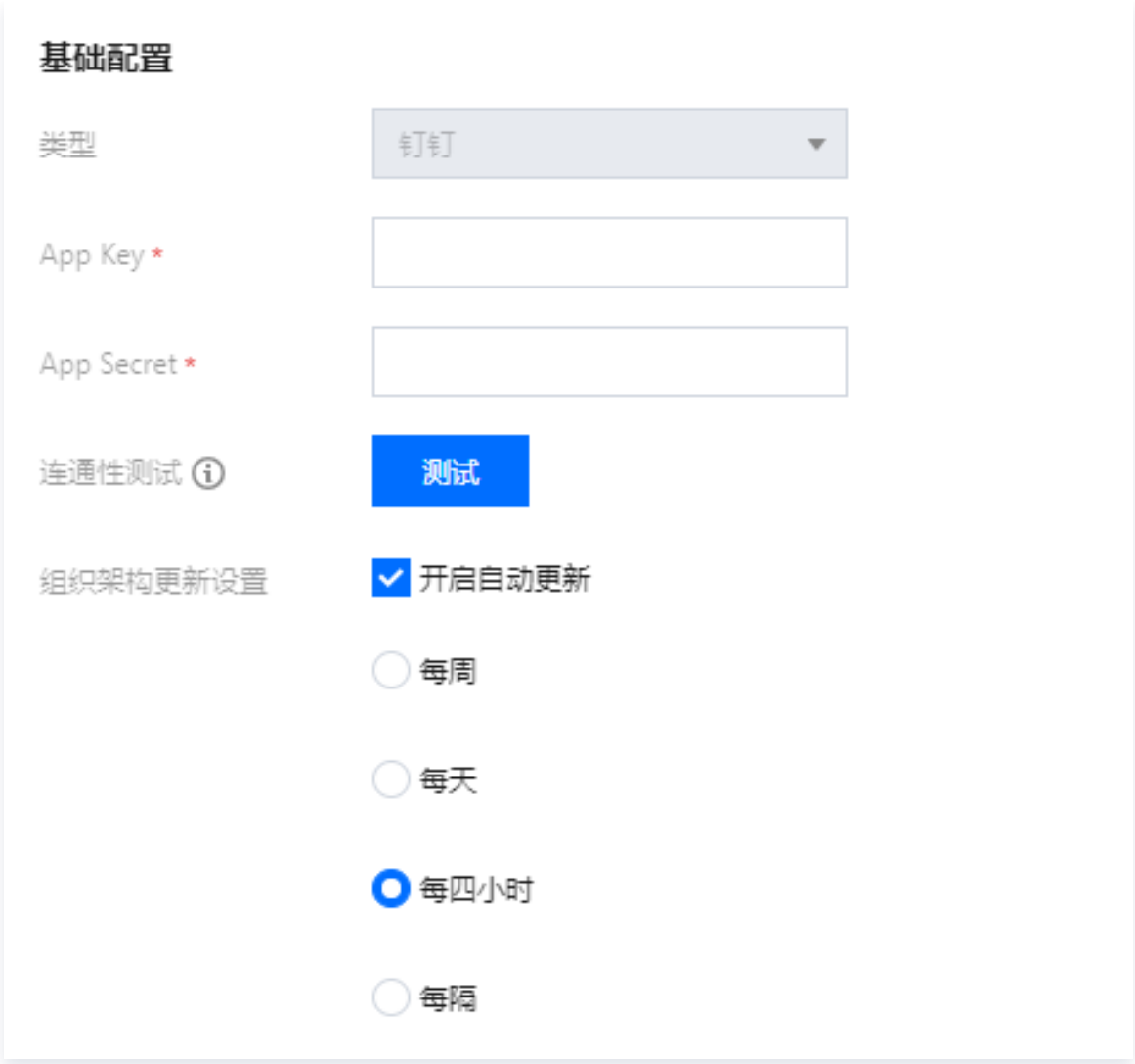
3. 选中目标权限后，单击操作列的**申请权限**，即可为该应用选中所需权限。

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**钉钉**，单击**下一步**。

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



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**。

2. 配置认证源

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，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：

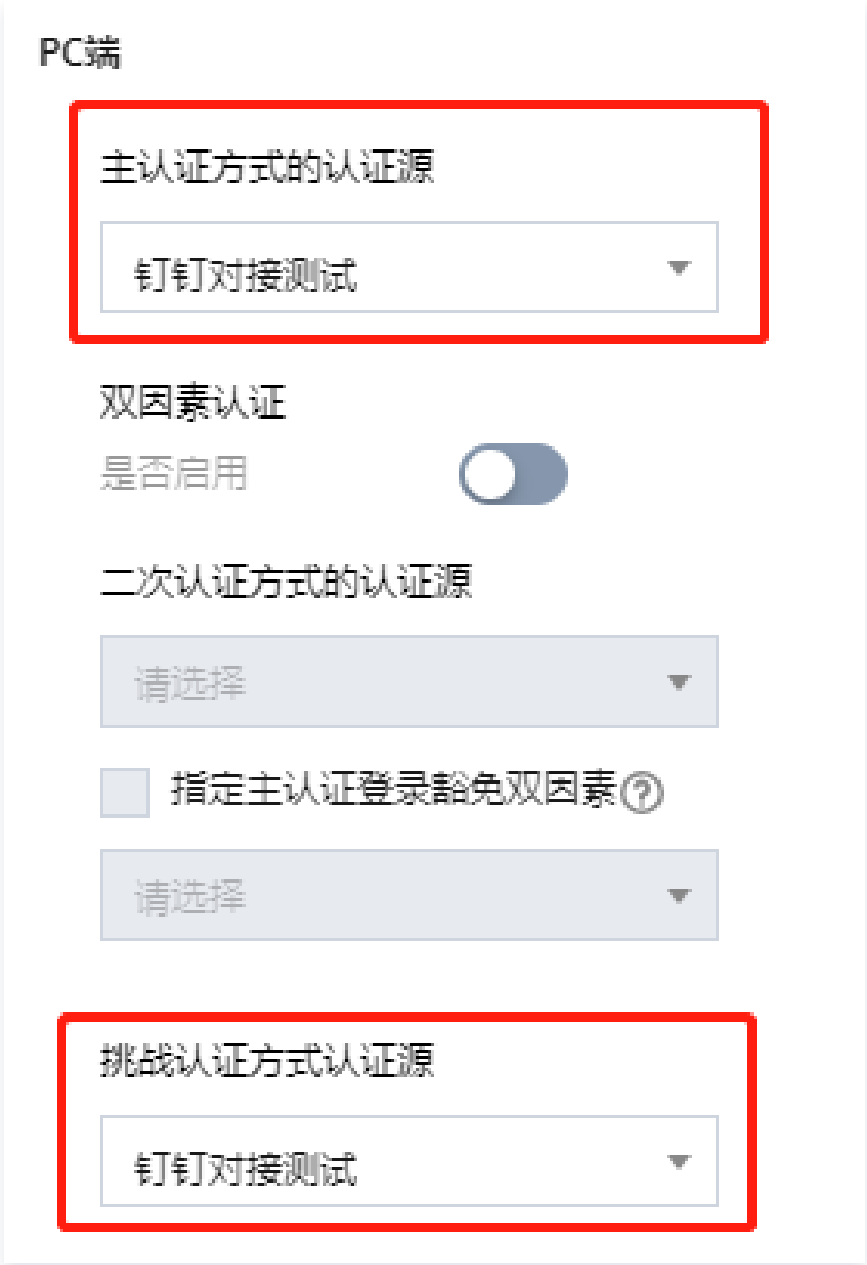
- App ID：为钉钉的 AppKey。
- App Secret：为钉钉的 AppSecret。

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

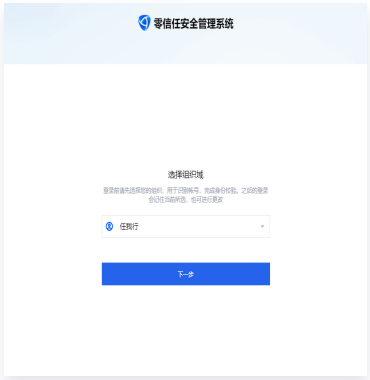
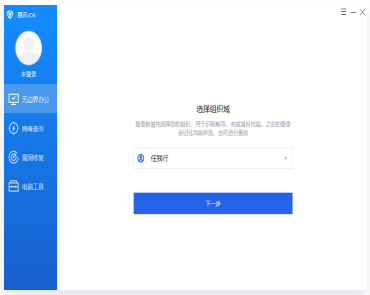
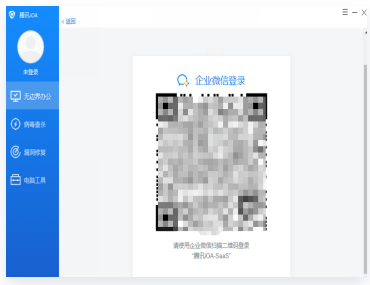
3. 单击**添加**，完成编辑。

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

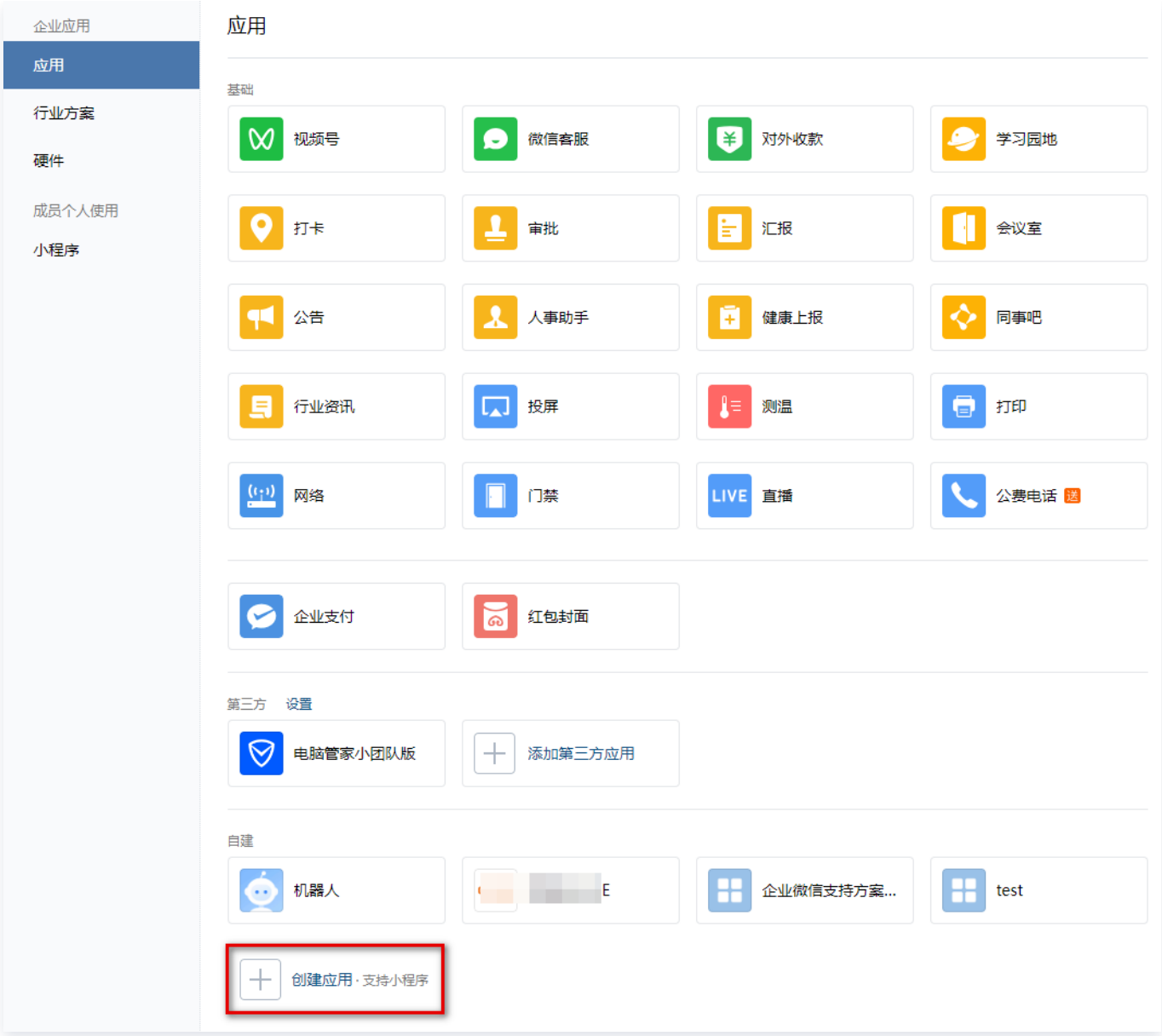
由于企业微信需要通过受信域名才能进行对接，所以需要您提前准备：

> **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**。

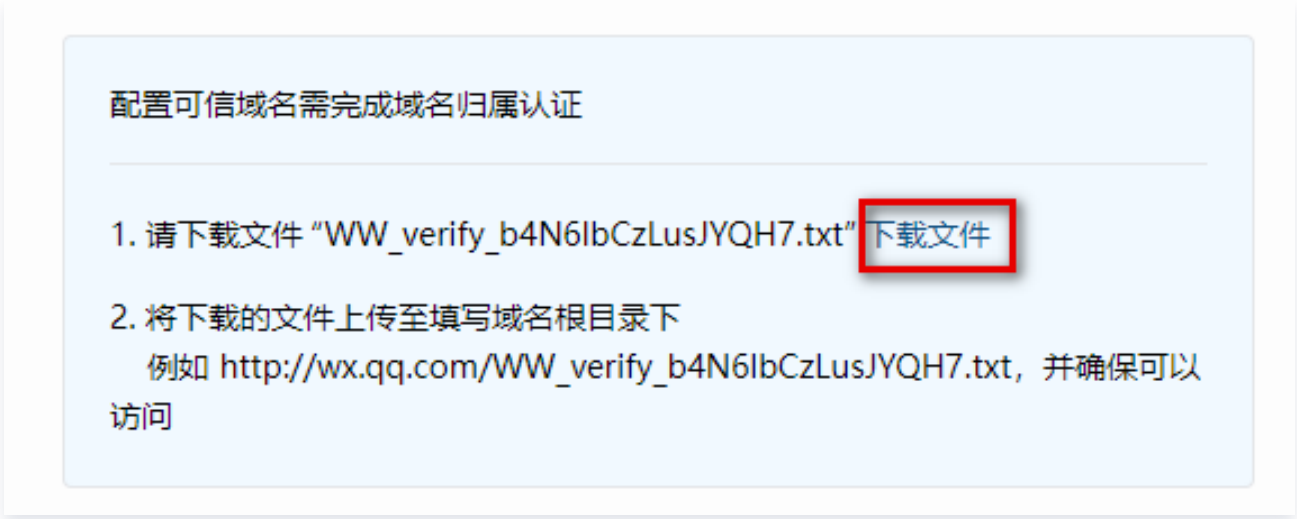
> **说明：**
> 可见范围务必包含需要同步的组织范围，否则无法同步组织；建议设置为根目录。

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**。

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**。

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。



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。

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。

> **说明：**
> IP 地址为企微代理服务器 IP，请联系腾讯项目对接人获取。

5. 获取企业 ID 和自建应用 Secret

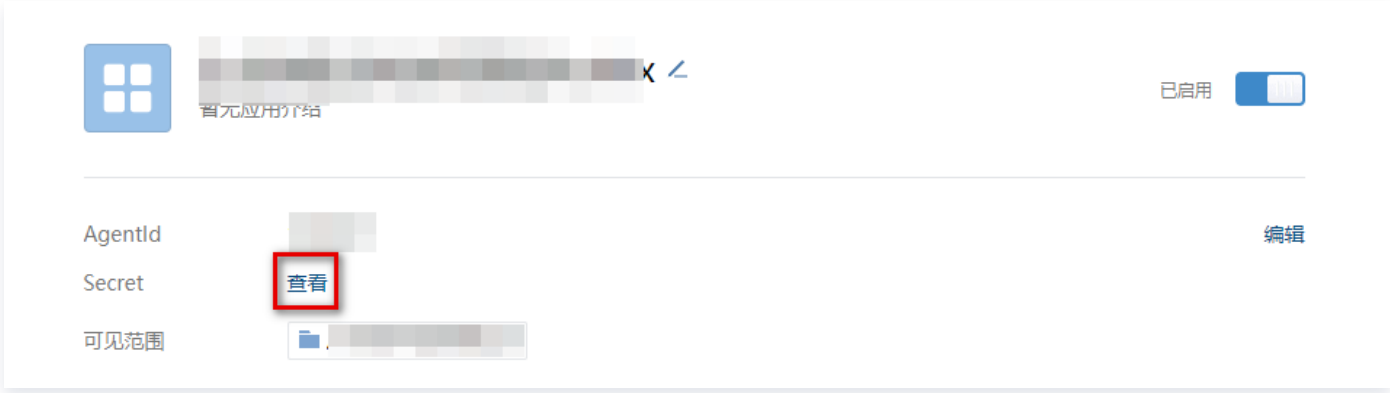
1. 登录 企业微信管理后台 ，单击上方的**我的企业**，默认进入企业信息页面。

2. 在企业信息页面的下方，获取企业 ID。

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。

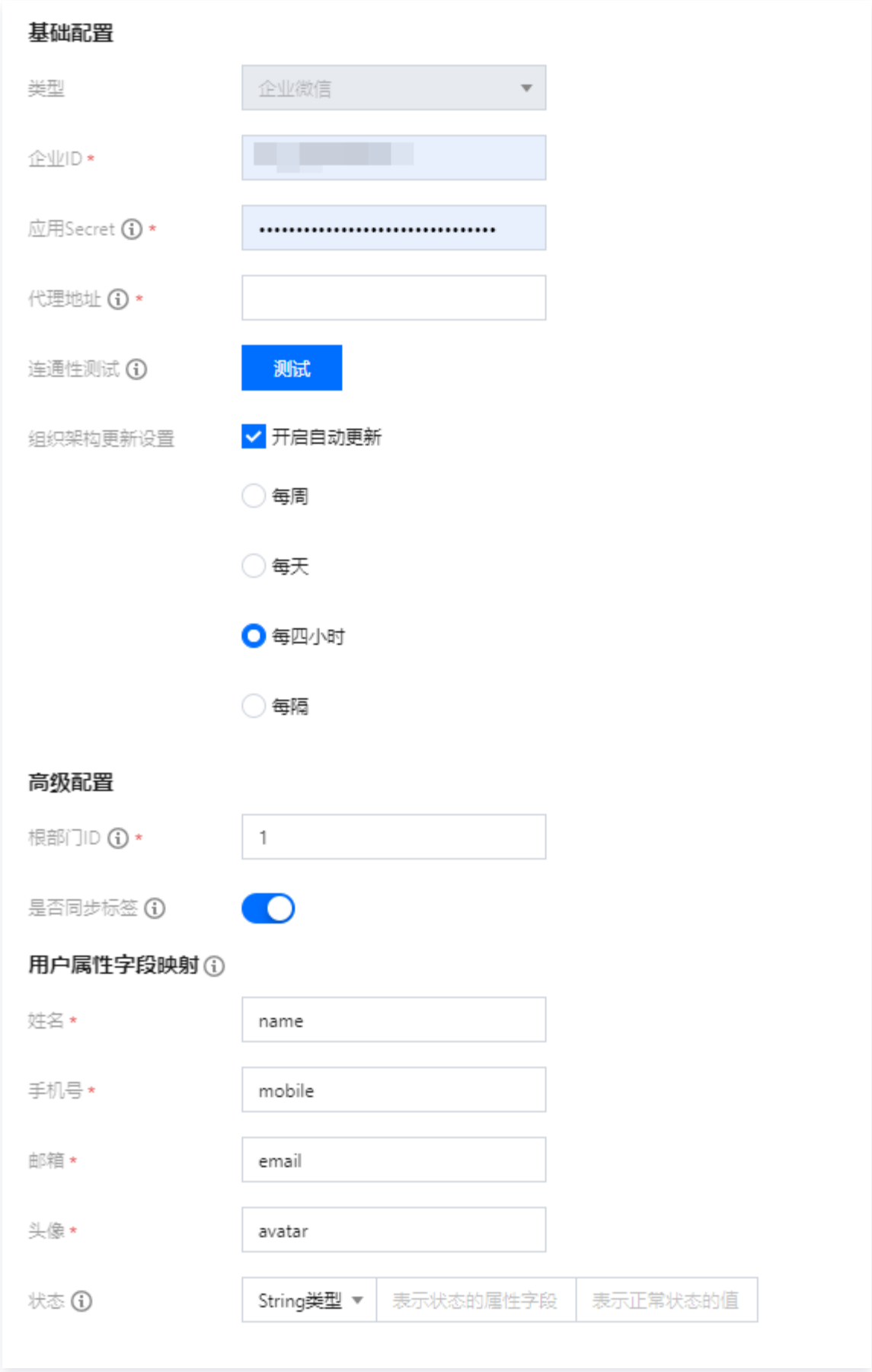


步骤二：配置 iOA 私有化 控制台

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**。

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 *
应用Secret *
代理地址 *
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： `http://ip:13732` ，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	如无特殊需求，请勿修改。 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。 映射支持三种数据类型，且必须填写正常状态的值： 1. 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； 2. 对于 Int 类型，相同的值会关联到状态 1，其他值会默认保留。 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，同步时会将对应属性置为空。

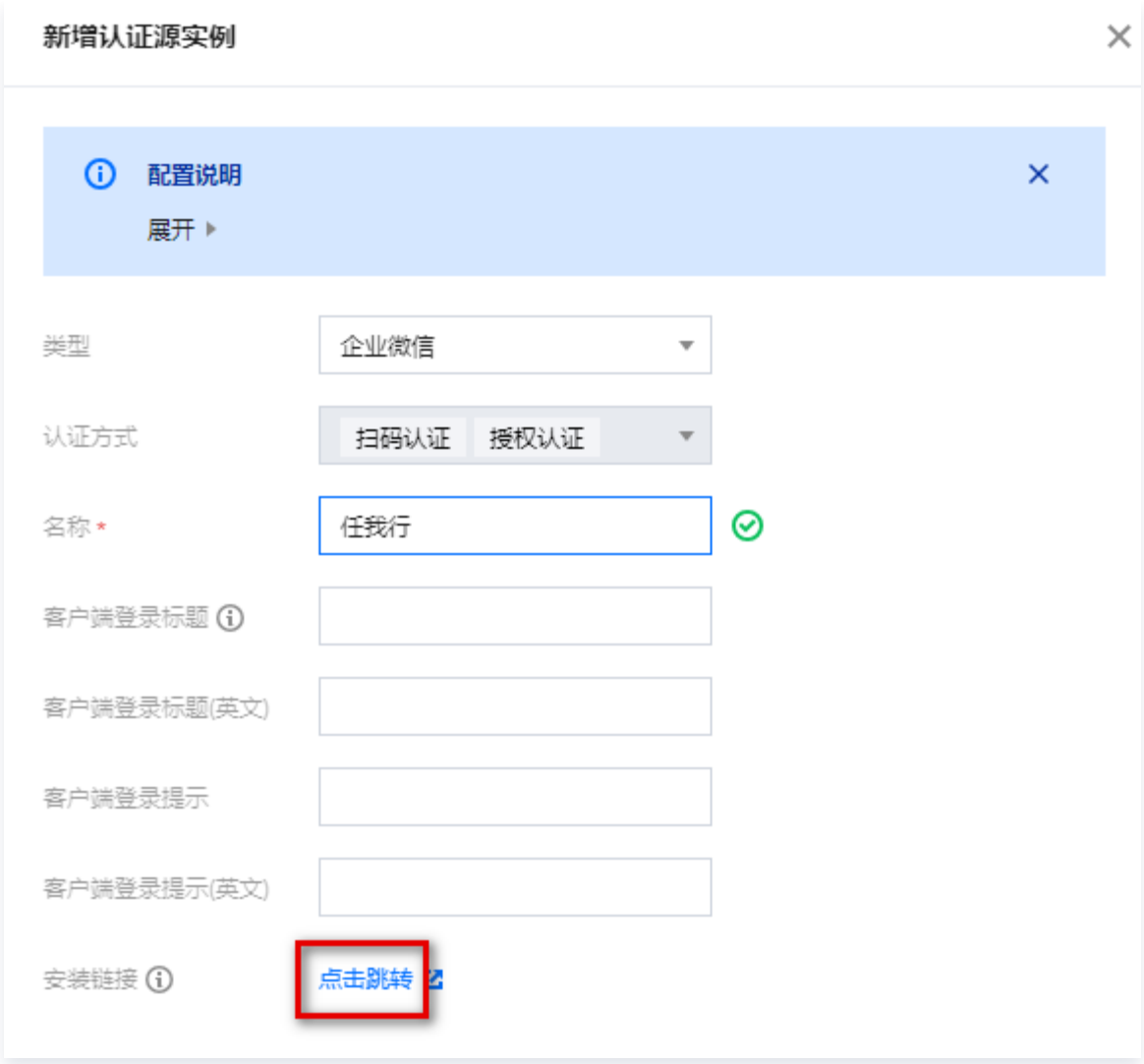
5. 单击**测试**，测试通过后单击**保存**。
6. 在用户与授权管理页面，找到刚刚创建的目录，单击**用户同步**，同步组织架构。

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，在左侧导览中，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。



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**。

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
北京任我行
钉钉
iOA本地账密
TOTP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

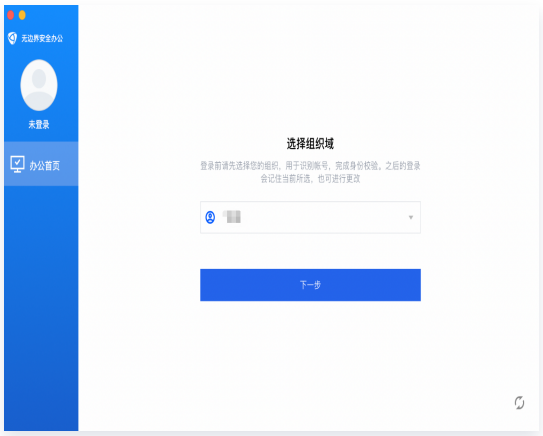
最近更新时间：2024-06-08 06:14:42

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

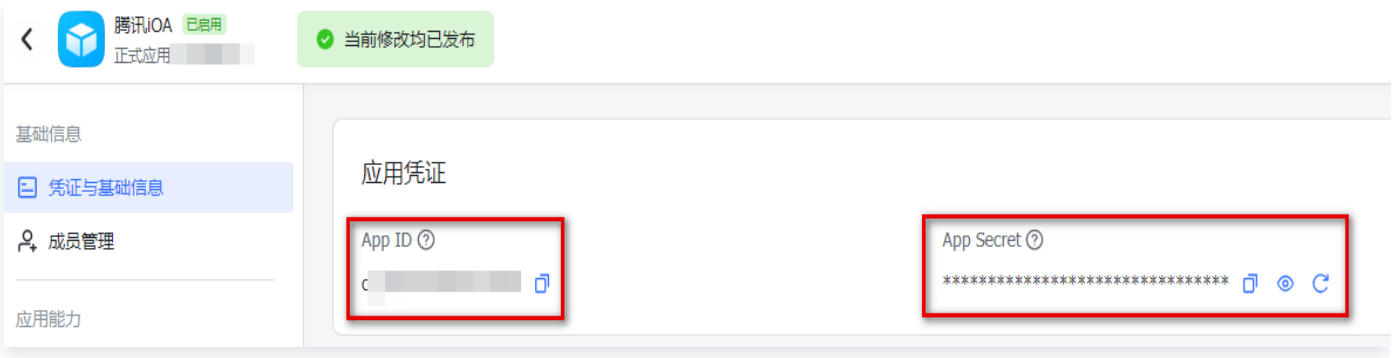
如您是首次使用，需要创建一个企业自建应用；如您还没有开通飞书开发者账号，请先前往 飞书开放平台 创建一个开发者账号。

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**。

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）。

4. 保存完成后，单击**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**。

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 `com.tencent.ioa`；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：`com.tencent.ioa` 。 Android 签名： `9xxxx594cd6xxxxcxxxxe3xxxx88dd5a` 。	

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**。

   - 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**。

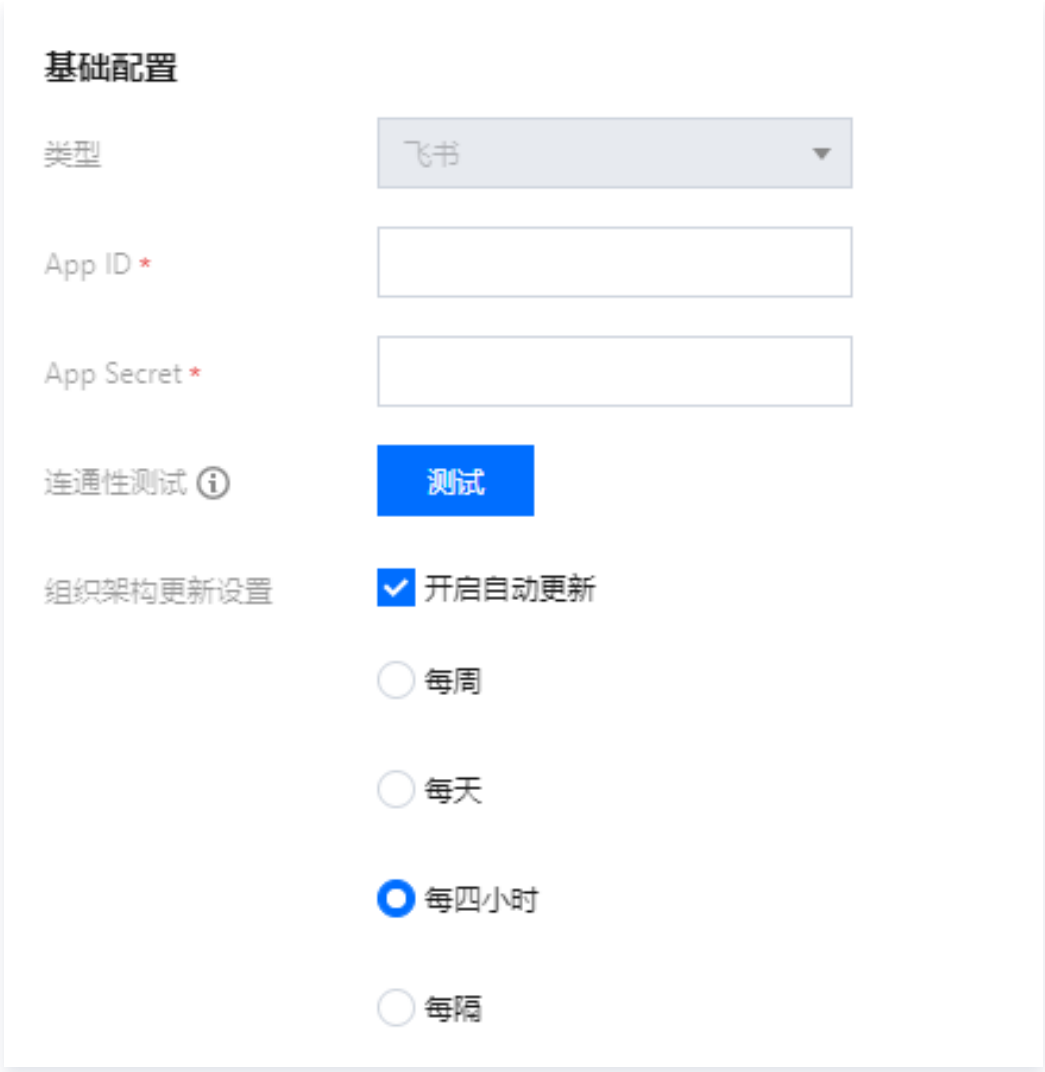
4. 配置上述权限后，需要重新发布应用版本 才能生效。

步骤二：iOA 控制台配置

1. 新建目录

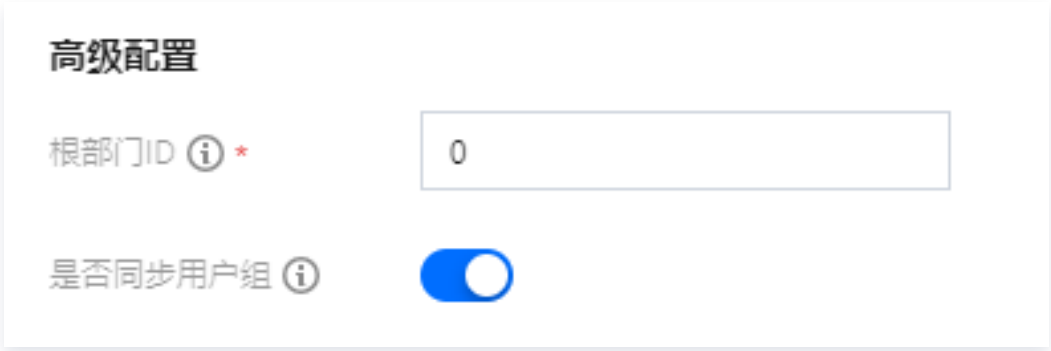
1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**管理中心** > **用户与授权管理**。
2. 在用户与授权管理页面，单击**新建**。
3. 在新增目录页面，输入名称和描述，是否导入架构选择**是**，导入类型选择**飞书**，单击**下一步**。

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



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。

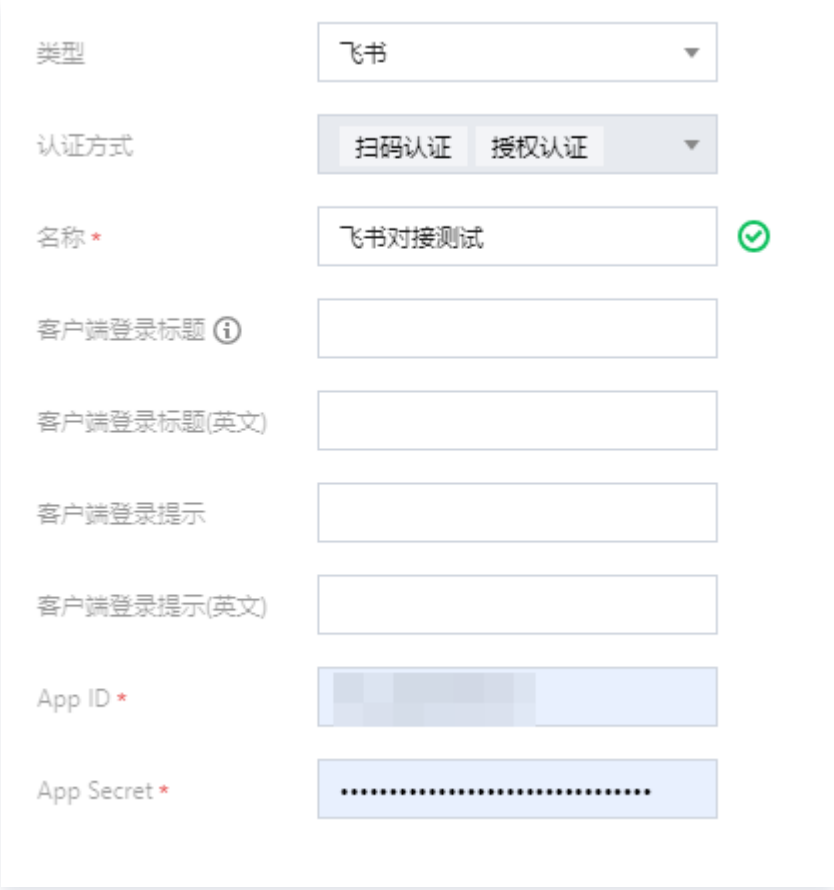


6. 在用户与授权管理页面，找到刚刚创建的目录，单击**用户同步**，即可同步组织架构。

2. 配置认证源

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，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。

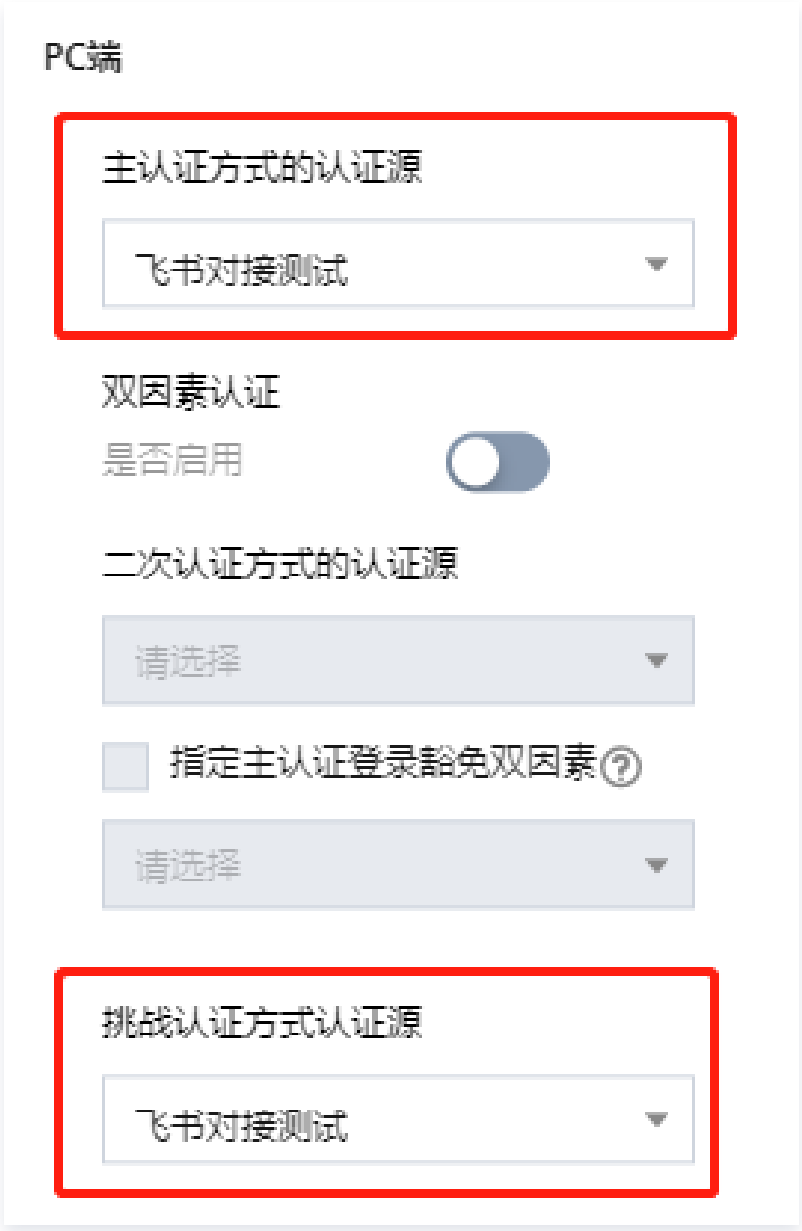


3. 设置认证策略

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，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。



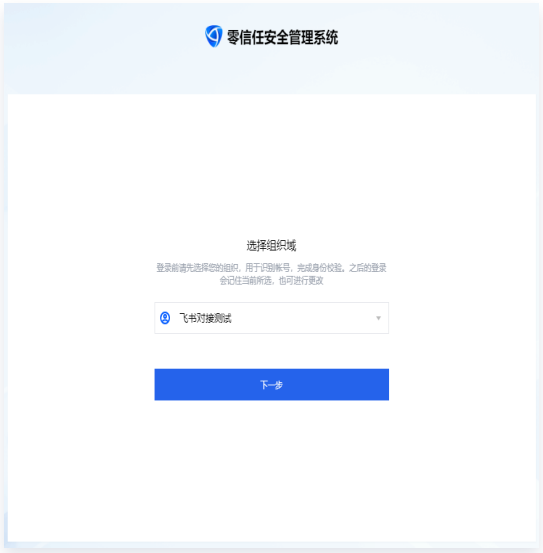
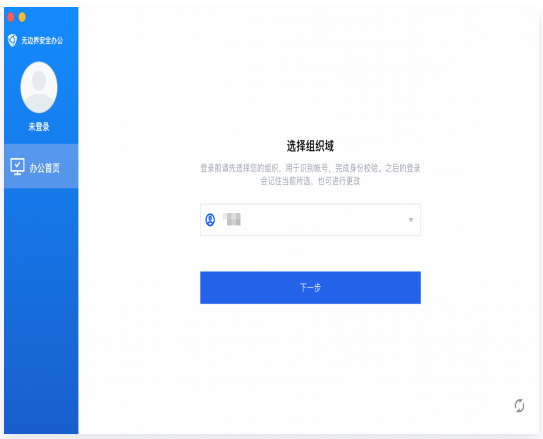
3. 单击**添加**，完成编辑。

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

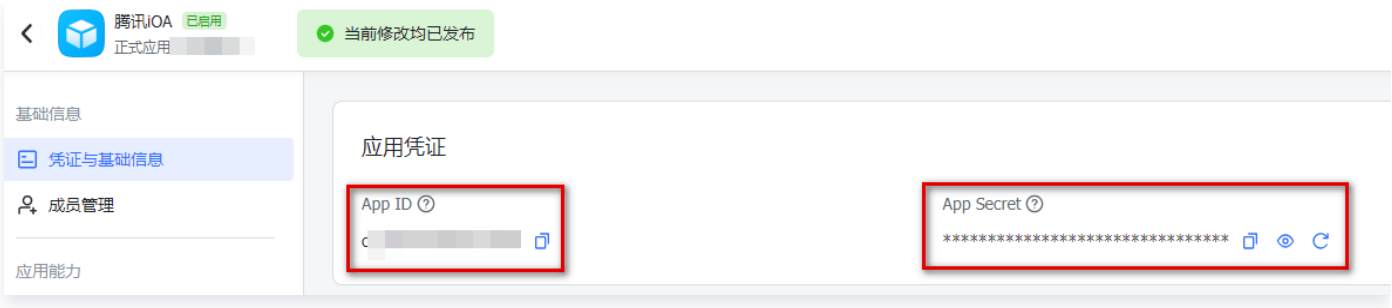
如您是首次使用，需要创建一个企业自建应用；如您还没有开通飞书开发者账号，请先前往 飞书开放平台 创建一个开发者账号。

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**。

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。

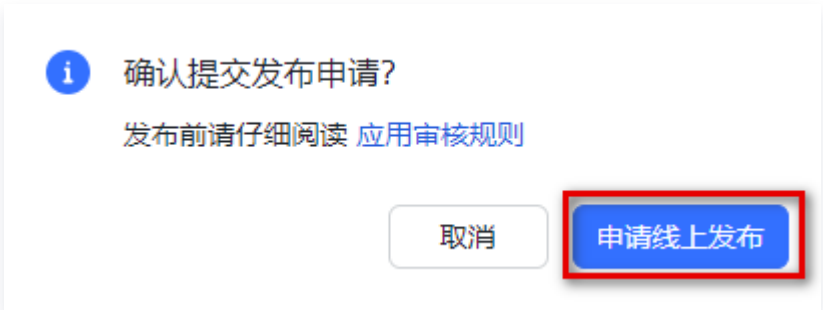
5. 发布应用

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**。

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）。

4. 保存完成后，单击**申请线上发布**。



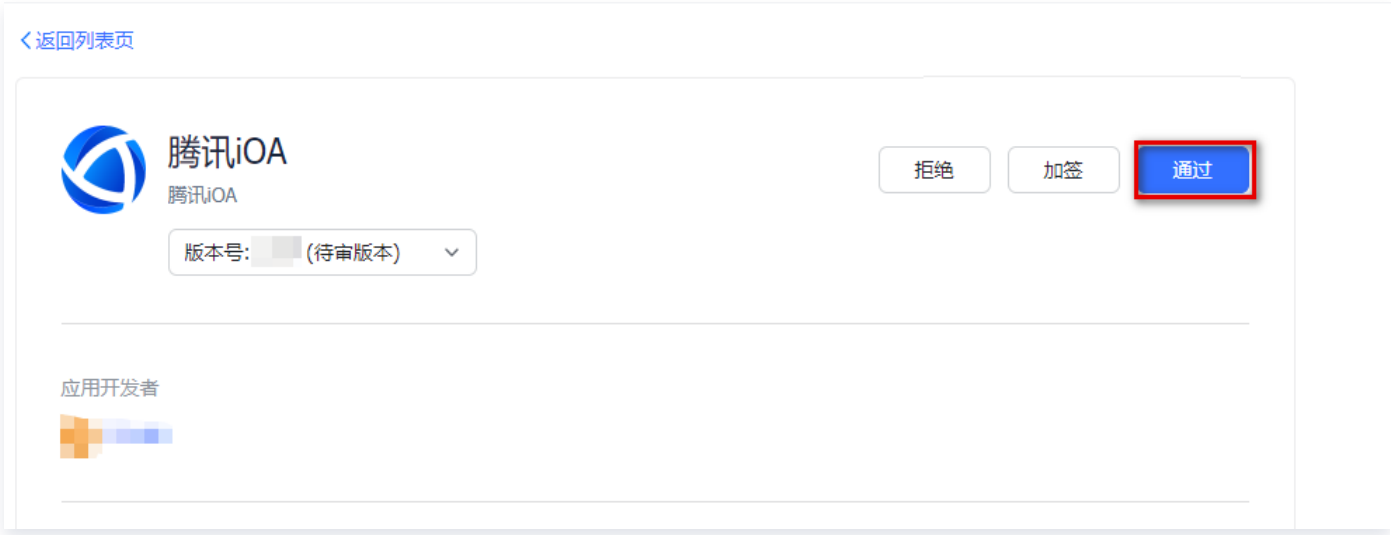
说明：

- 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**。

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 `com.tencent.ioa`；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：`com.tencent.ioa` 。 Android 签名： `9xxxx594cd6xxxxcxxxxe3xxxx88dd5a` 。	

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**。

   - 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，在左侧导览中，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":[

        ],
```

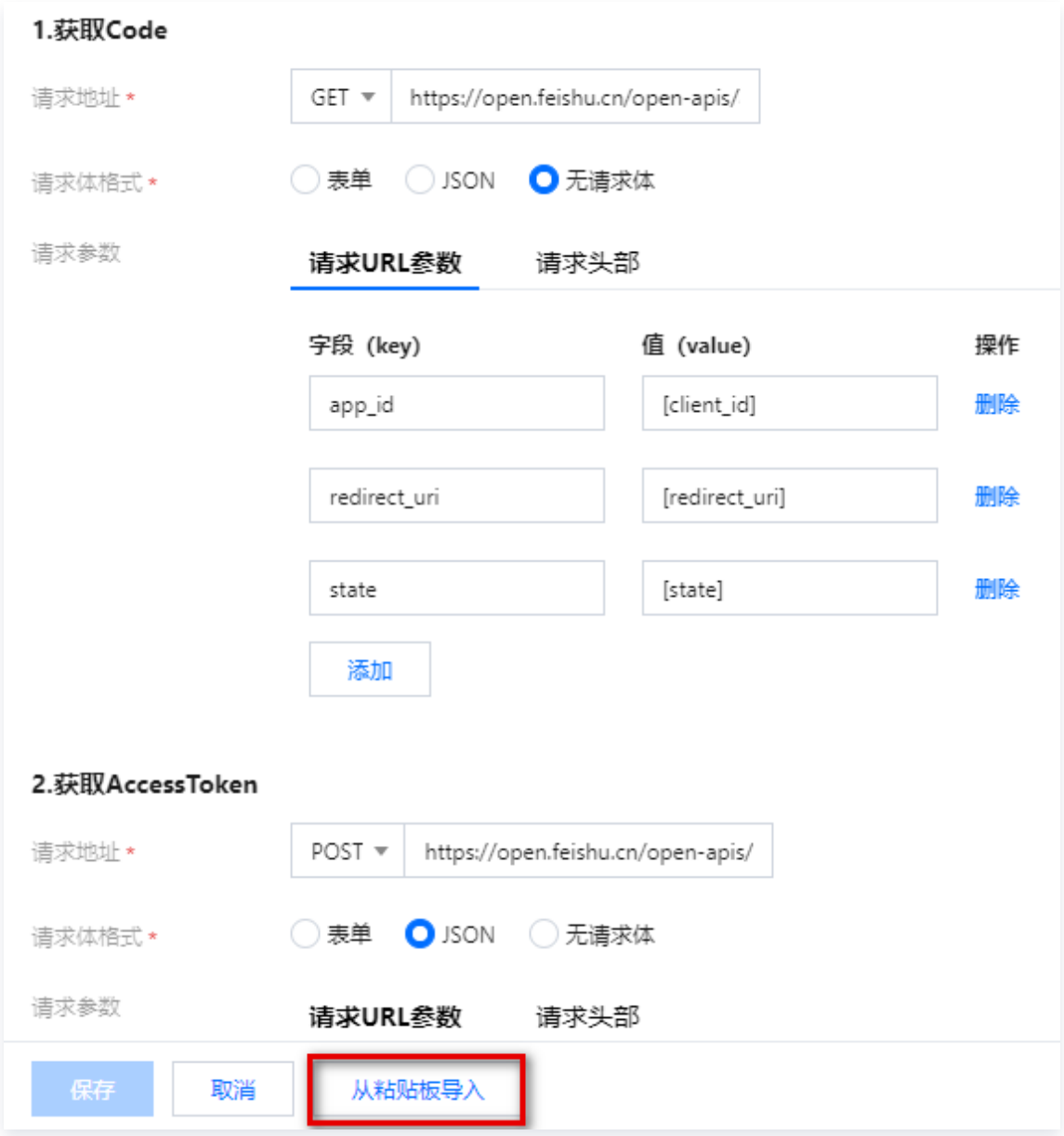
```
    "header_parameters":[

    ],
    "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。



6. 在新增认证源实例页面，填写基本信息，单击**保存**。

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。 • 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**。

4. 在新增目录页面，配置基础信息。

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	• 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。

参数类型	参数名称	说明
组织架构接口配置	接口 URI	默认 `/scim/v2/Organizations`，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	• 开启分页后会进行分页拉取；分页只支持标准的参数，startIndex 表示开始项的位置，count 表示一页的数量。 • 不开启分页则默认 count=-1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 `/scim/v2/Groups` ，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	• 开启分页后会进行分页拉取；分页只支持标准的参数，startIndex 表示开始项的位置，count 表示一页的数量。 • 不开启分页则默认 count=-1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 `/scim/v2/Users` ，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	• 开启分页后会进行分页拉取；分页只支持标准的参数，startIndex 表示开始项的位置，count 表示一页的数量。 • 不开启分页则默认 count=-1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。

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	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/Boot/String，这里关联状态的值必须是正常状态的值。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。
	• 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：
	`{ "name":{ "name256":"xxx" } }`
	• 指定 name256 为头像，那么可以输入 name.name256。
	`{ "name":[`

```
    {
        "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

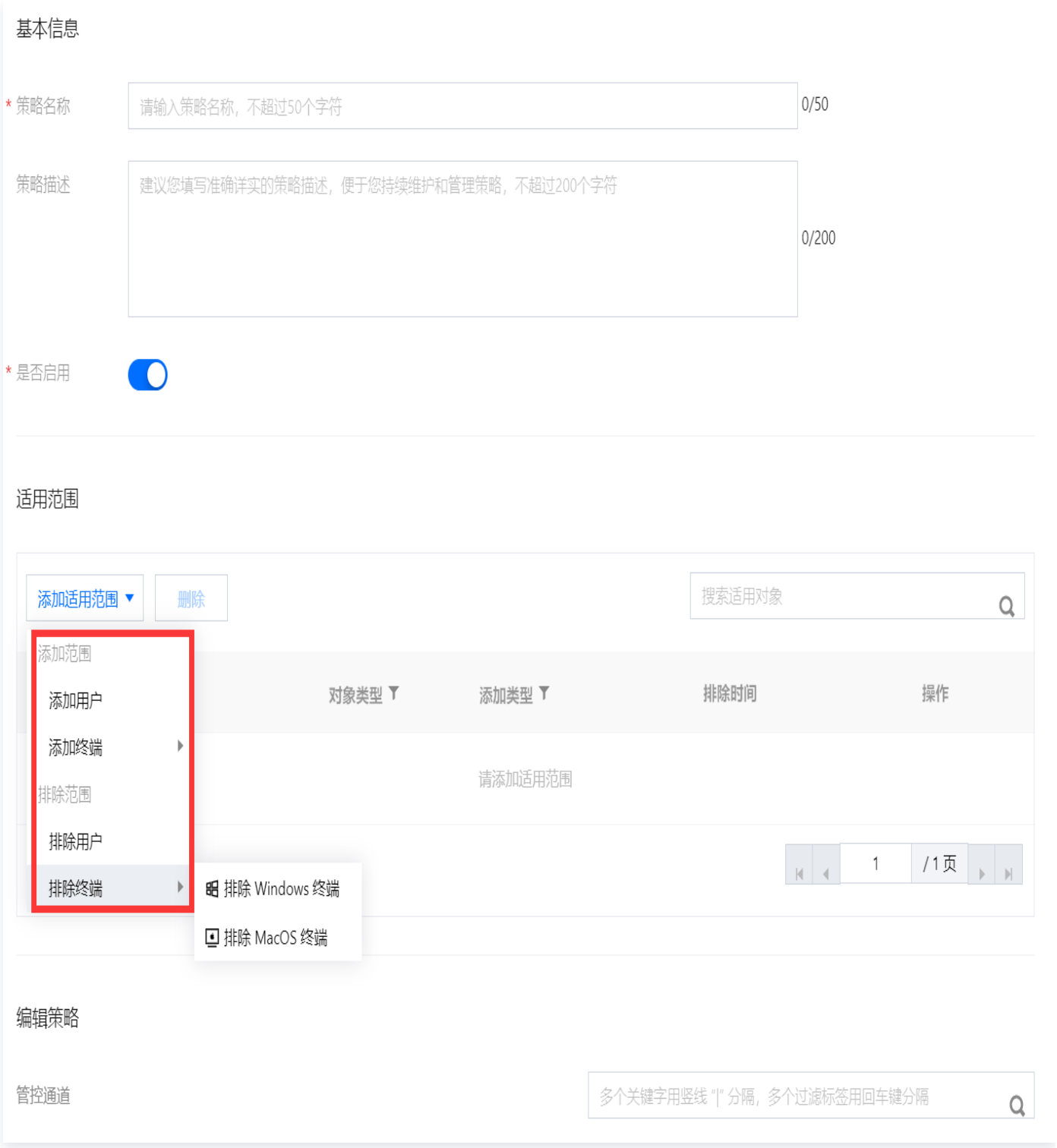
最近更新时间：2024-06-08 06:14:42

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。

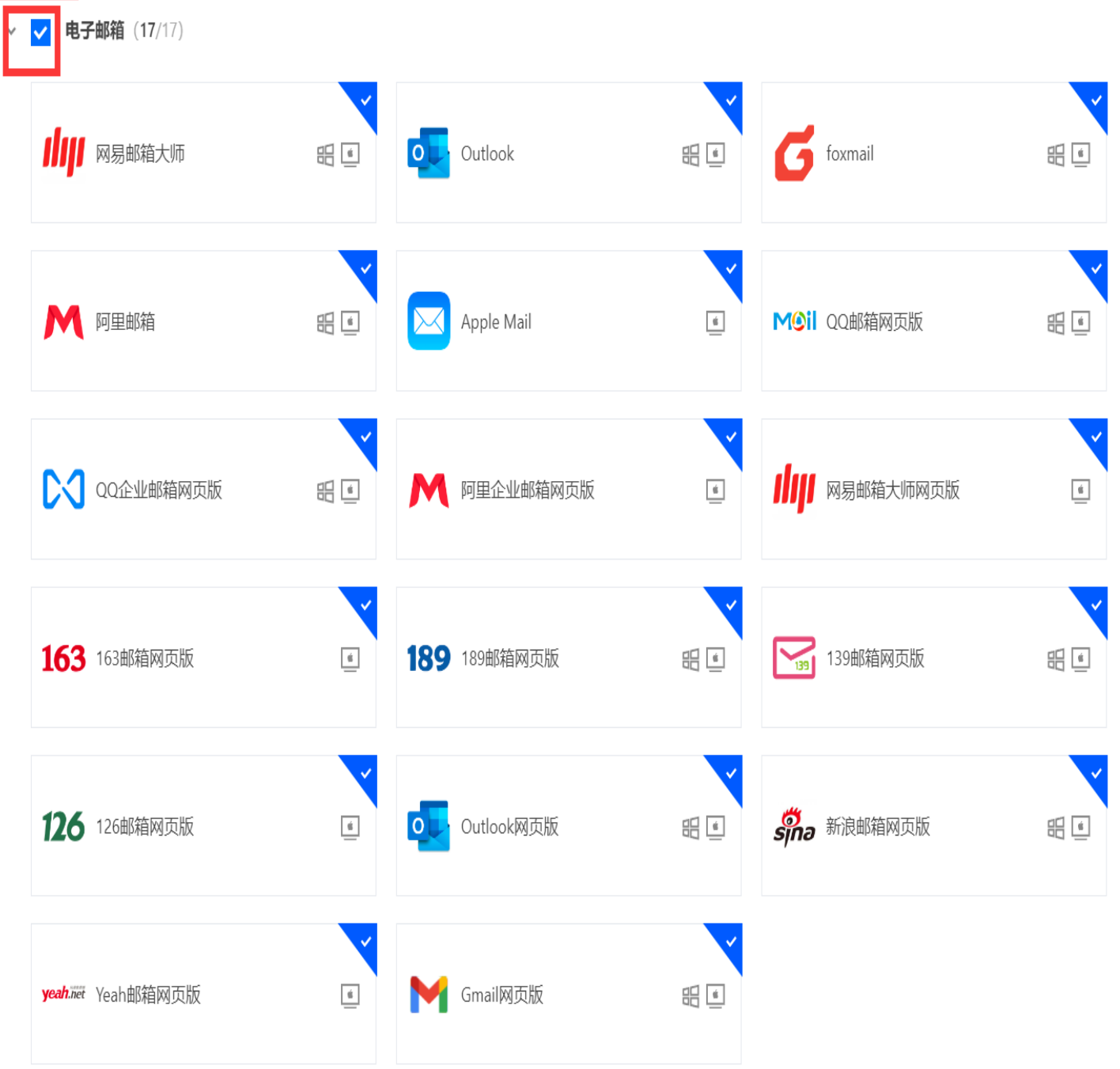


管控通道

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



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：

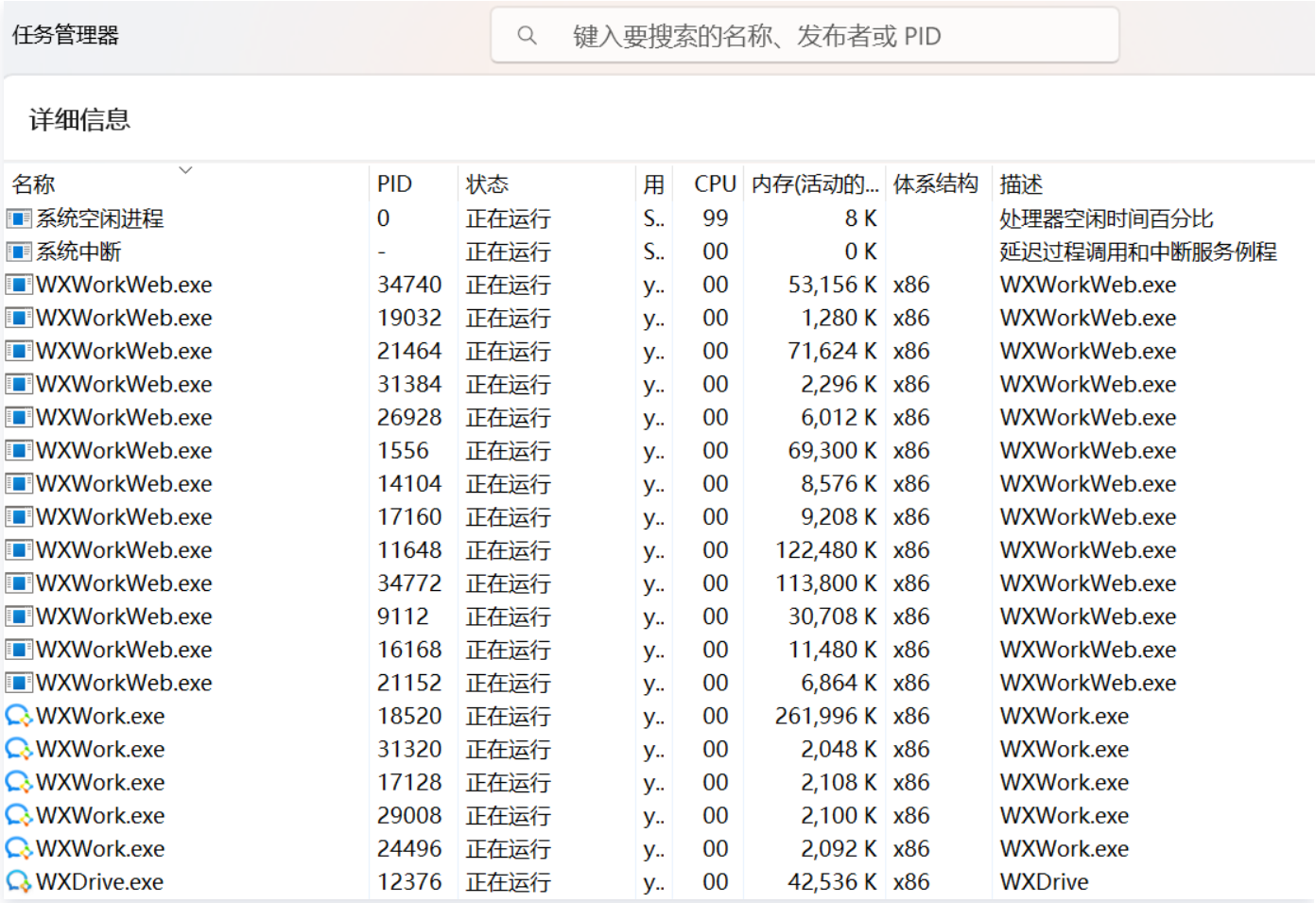
参数名称	说明
通道名称	自定义管控通道的名称。
通道类型	选择该管控通道的类别。
通道图标	上传36x36像素至150x150像素大小的正方形通道图标，图片宽高比例为1：1，支持PNG、JPG 格式。
是否启用	默认开启。

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。

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

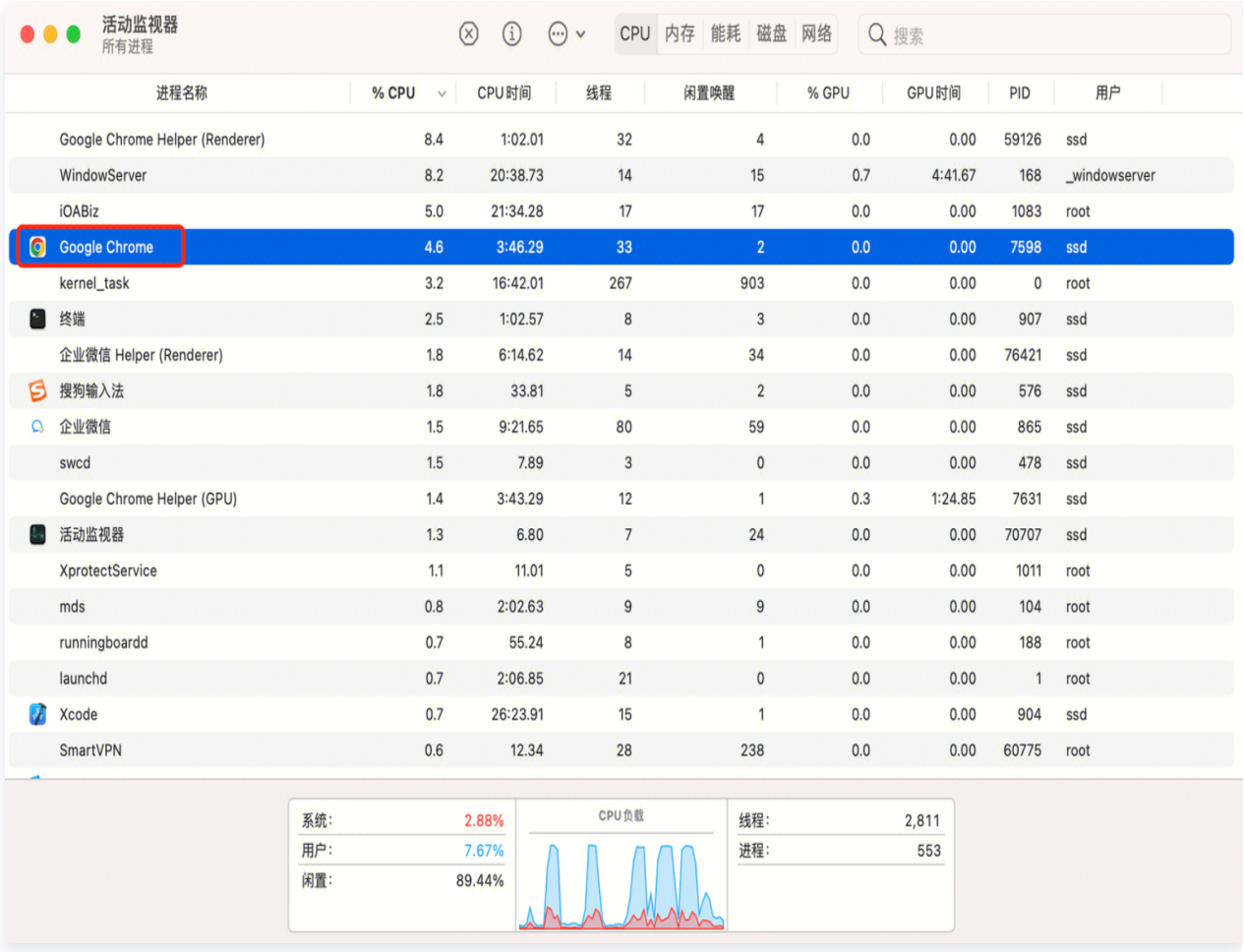
名称	PID	状态	用	CPU	内存(活动的...	体系结构	描述
系统空闲进程	0	正在运行	S..	99	8 K		处理器空闲时间百分比
系统中断	-	正在运行	S..	00	0 K		延迟过程调用和中断服务例程
WXWorkWeb.exe	34740	正在运行	y..	00	53,156 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	19032	正在运行	y..	00	1,280 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	21464	正在运行	y..	00	71,624 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	31384	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。

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。

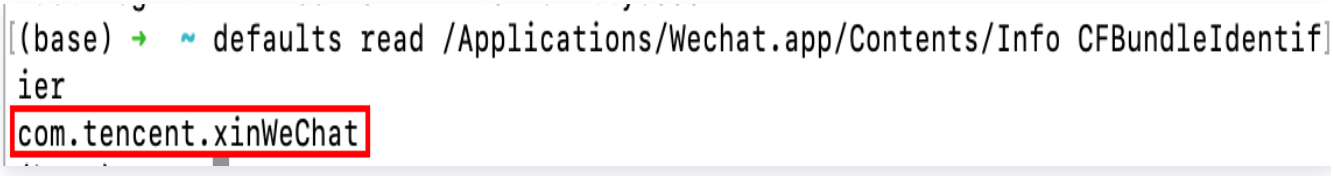
5.2 获取 Bundle ID

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` 。



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

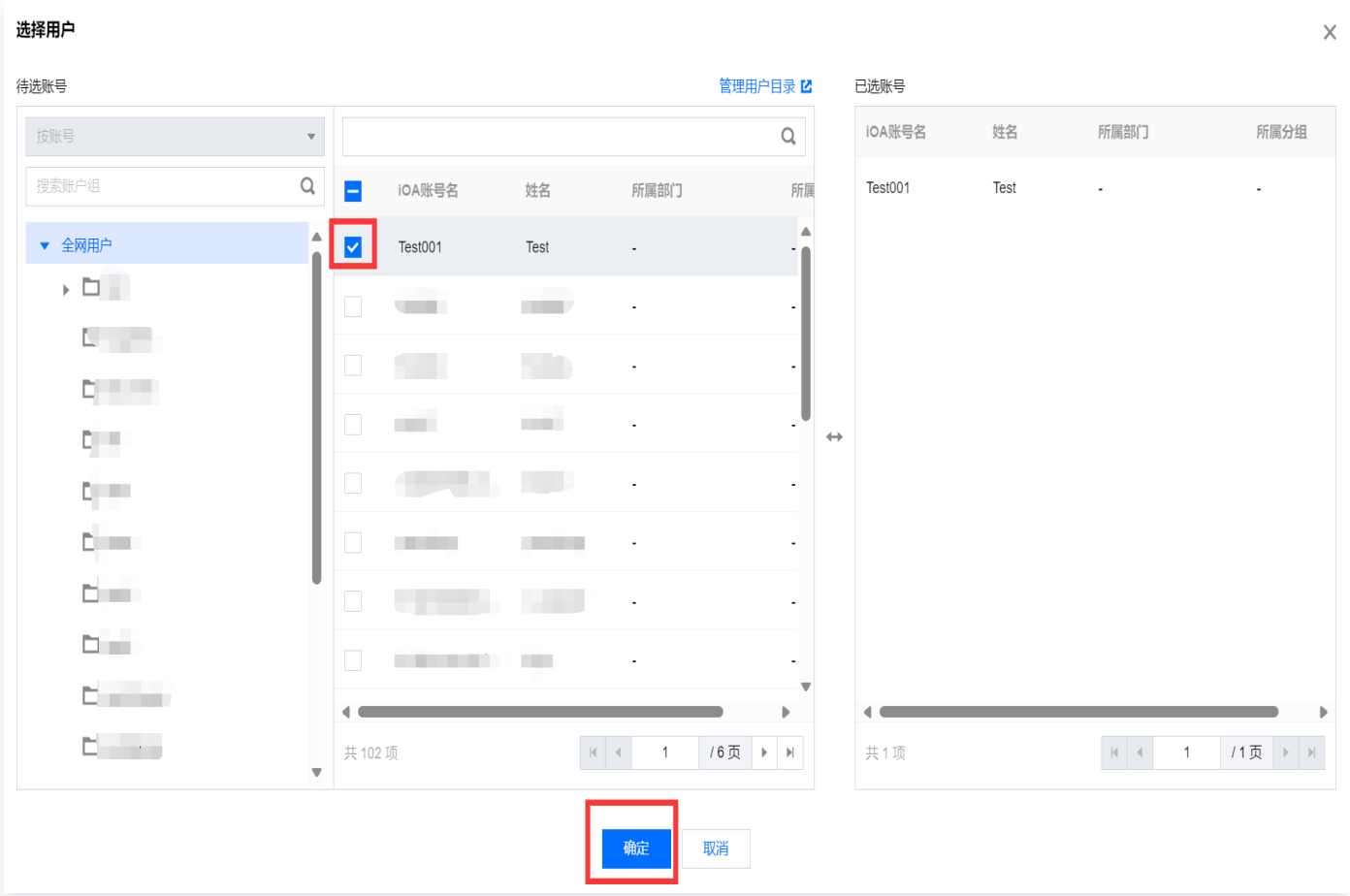
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据安全中心** > **数据安全策略** > **终端数据安全策略**。
2. 在终端数据安全策略页面，选择**审批流配置**，单击**添加审批流**，进入审批流配置页面。

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**。

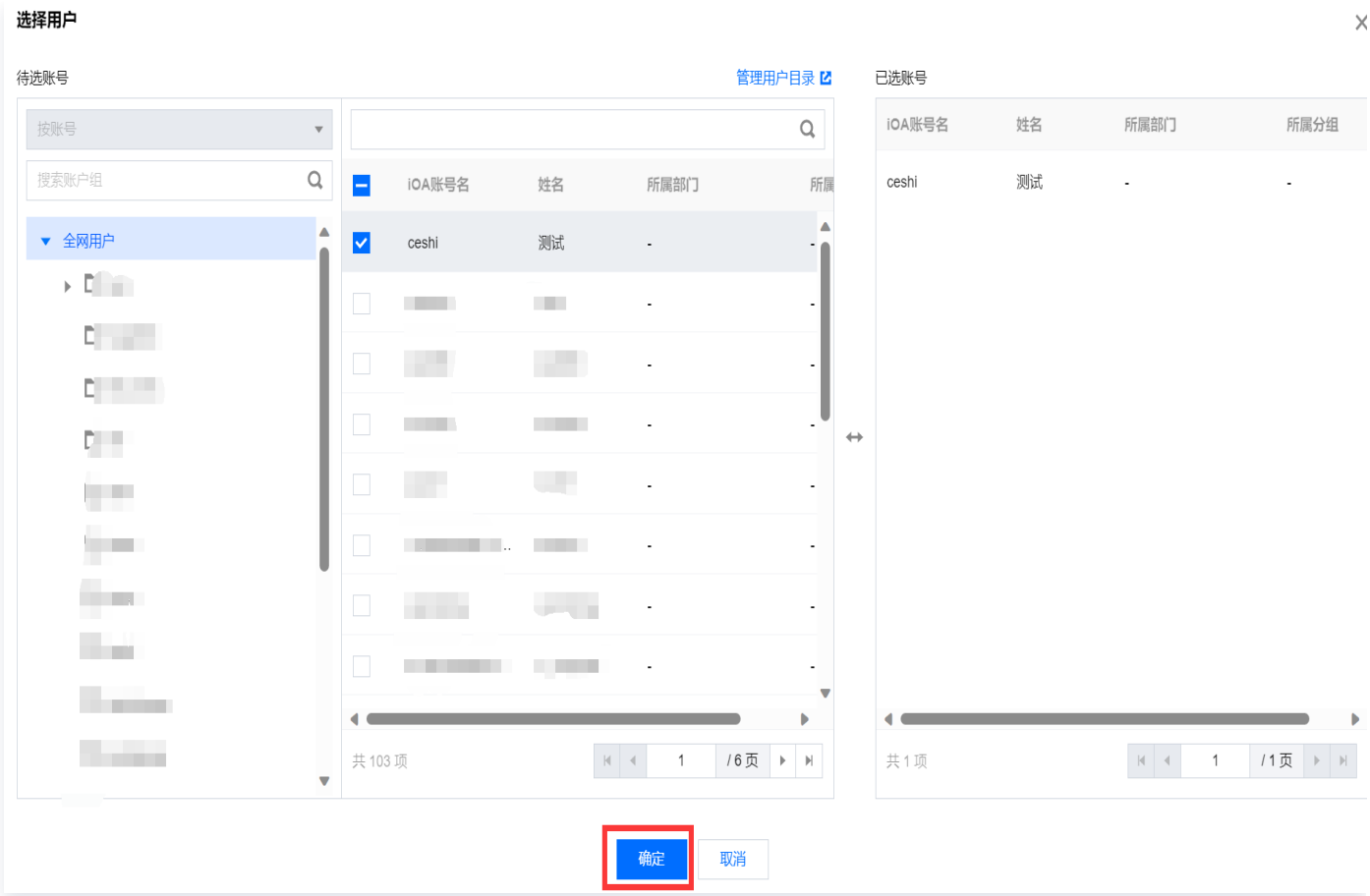
   示例：指定用户，单击**选择用户**，勾选账号名，单击**确定**保存。

> **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。

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。

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。

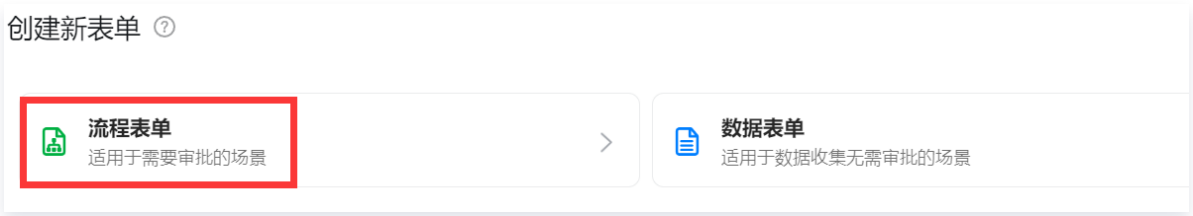
7.2.1 登录钉钉开放平台-开发者后台，进入应用开发，单击**创建应用**，填写应用名称、应用描述后单击**保存**。

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。

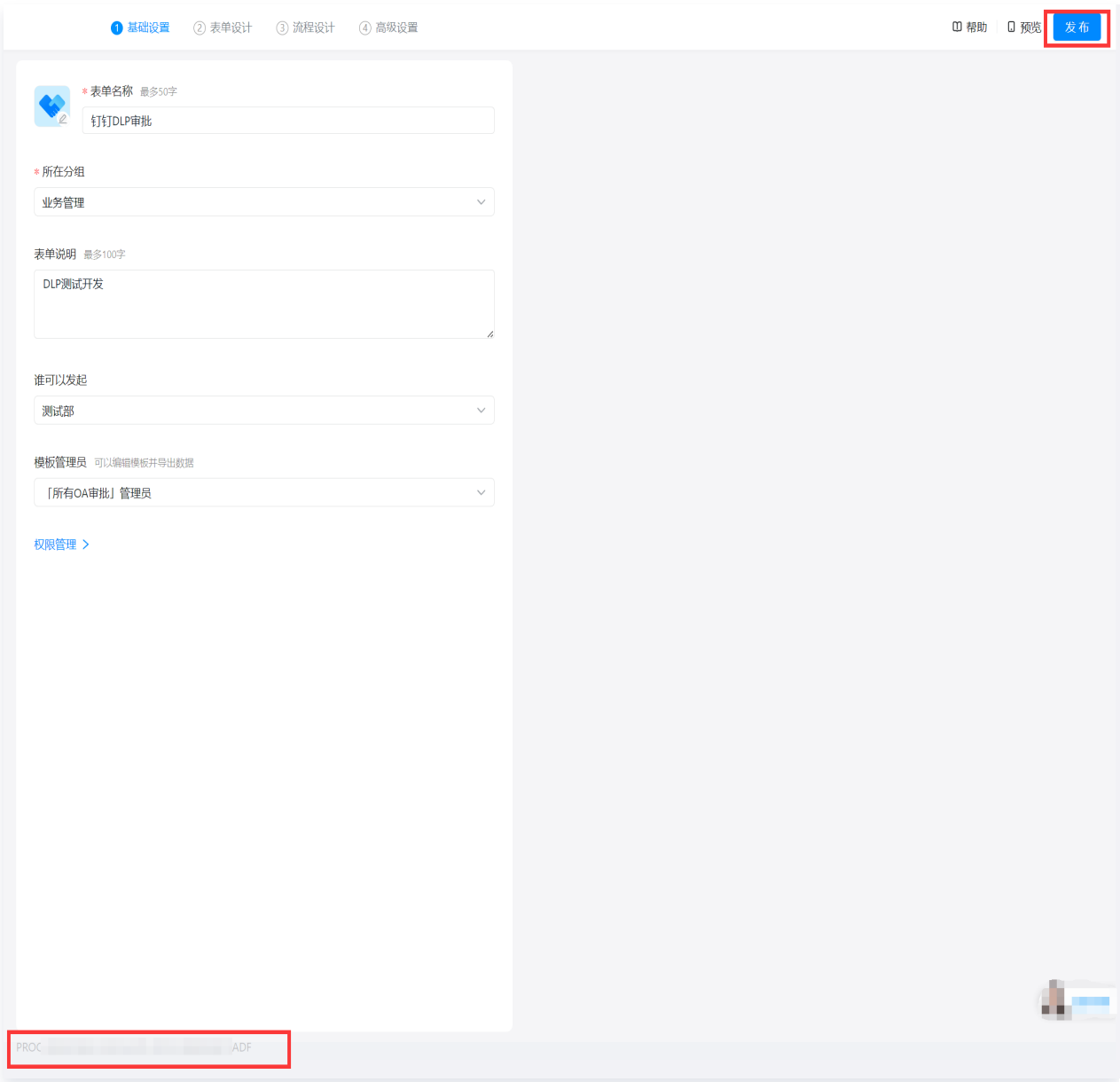
7.2.3 单击**凭证与基础信息**，获取凭证与基础信息，查看 App Key，App Secret。

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**。



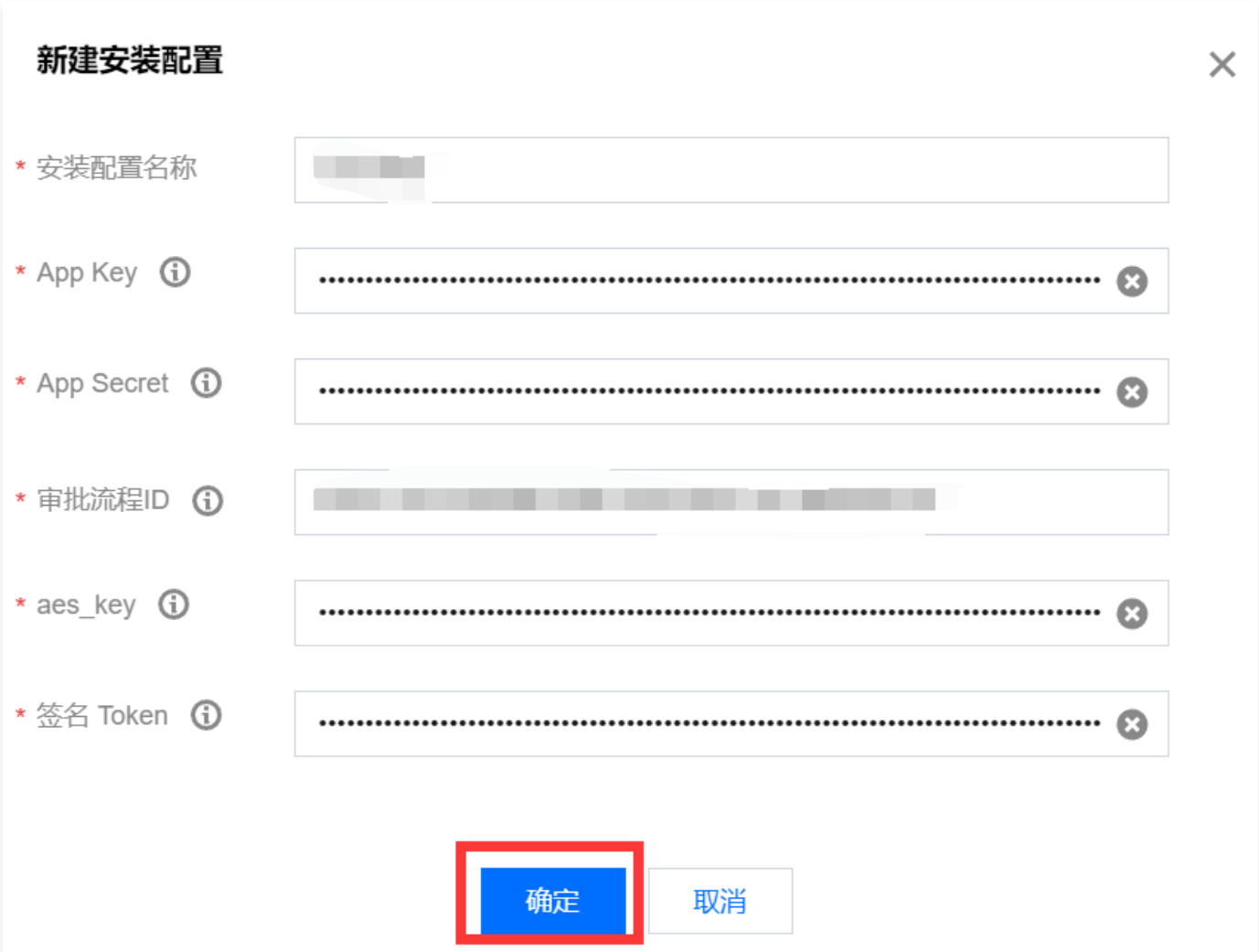
7.4 获取 aes_key 参数。

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。**

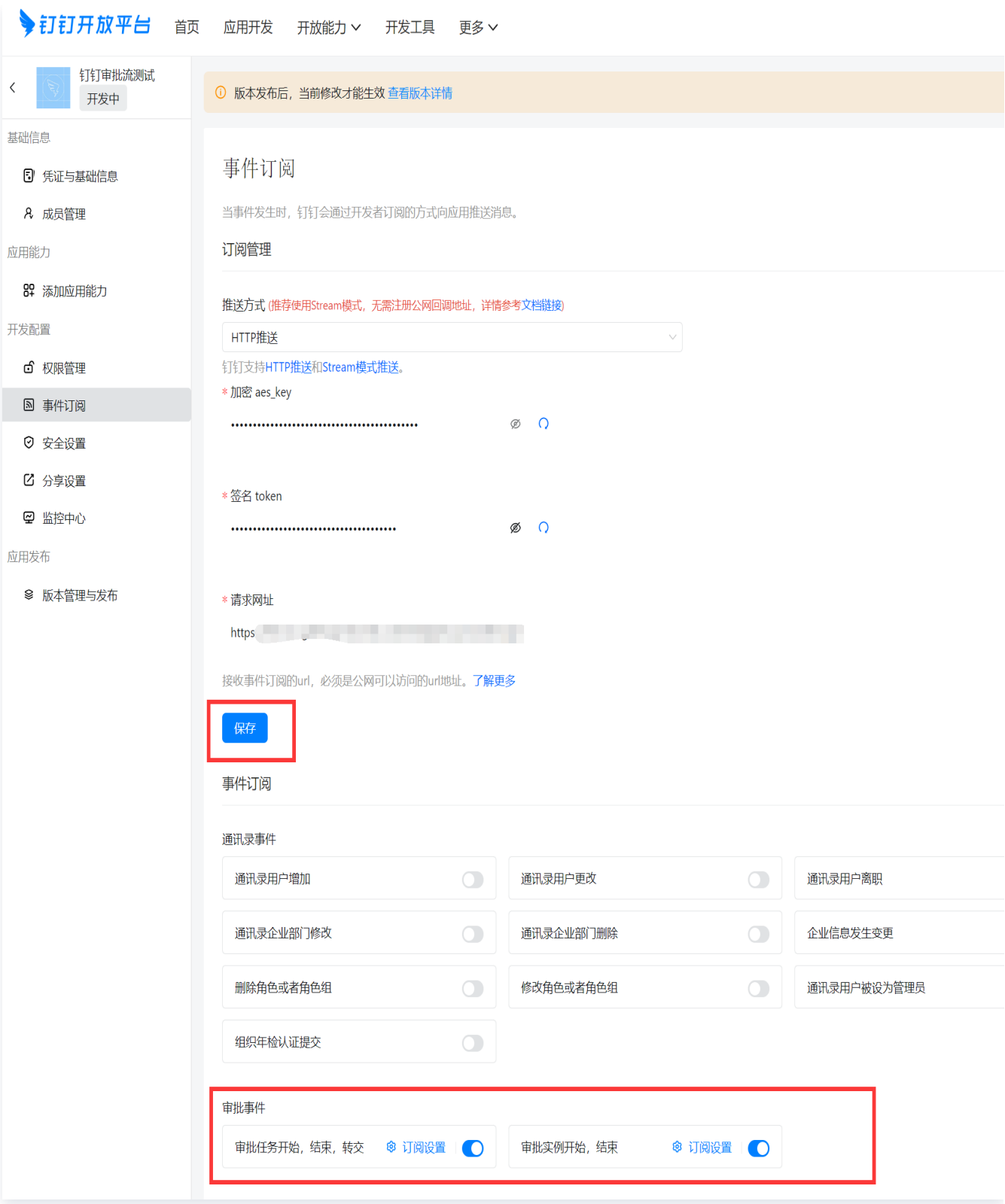
8. 将获取的安装配置信息依次录入，单击确定。



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**。

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）。

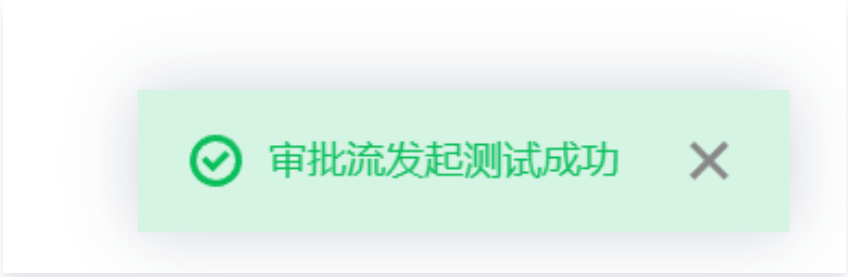


8.4 进入权限管理，勾选个人权限、通讯录管理、OA 审批，单击批量申请。

9. 在添加审批流页面，单击**测试**，发送审批流测试信息。

9.1 单击**确定**，发送审批测试信息。

9.2 钉钉收到审批信息，审批流发起测试成功。



10. 单击**保存**，完成钉钉审批流配置。

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**。

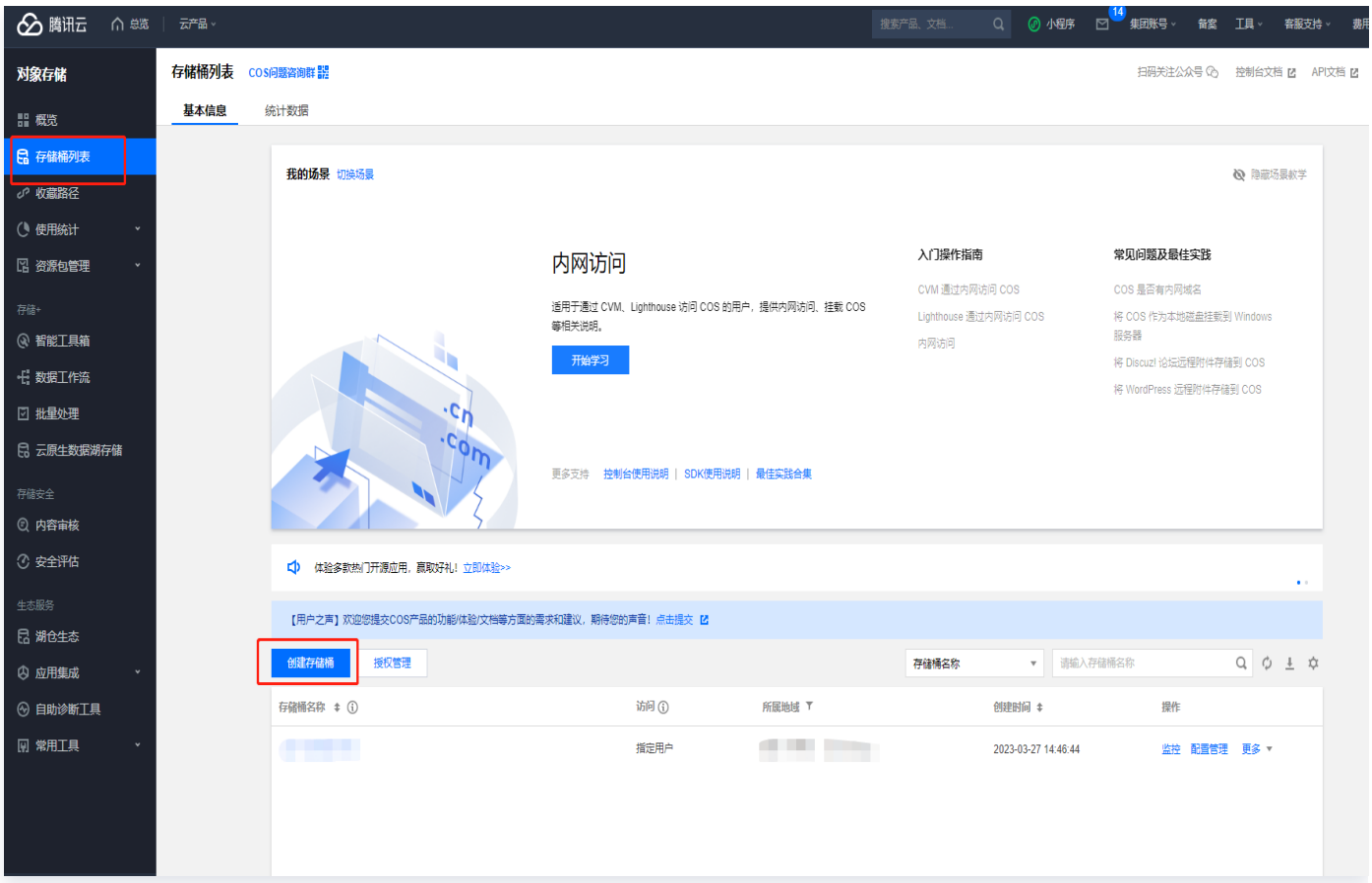
3. 在存储方案设置页面，选择存储目标，获取配置参数请参考 配置腾讯云存储服务 和 配置S3协议存储服务 。

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**。



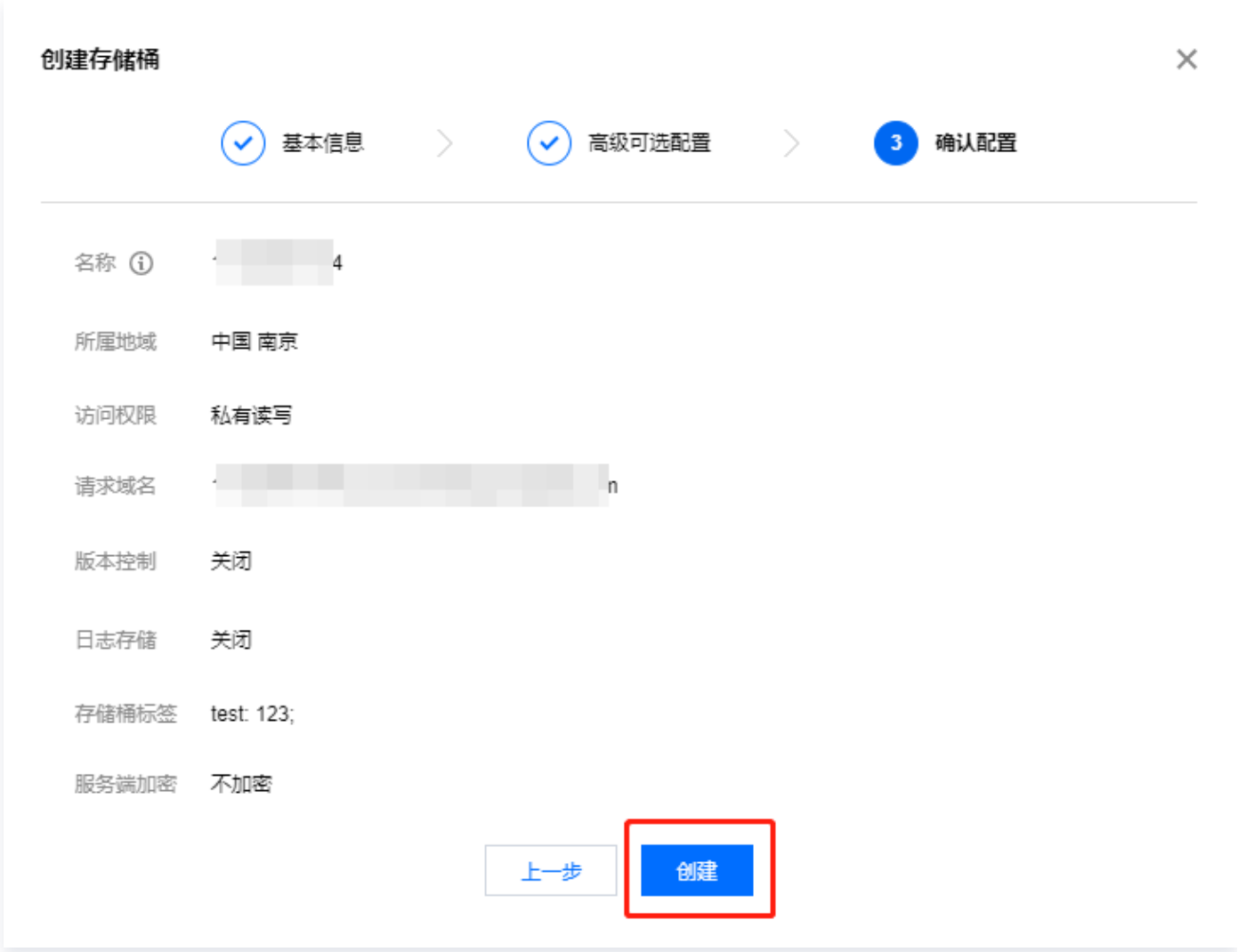
2. 在存储桶列表页面，单击**创建存储桶**，新建一个存储桶。
3. 在创建存储桶窗口中，配置基本信息，单击**下一步**。

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**。

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误删丢失的数据。
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	可选择不加密，或 SSE-COS 加密。

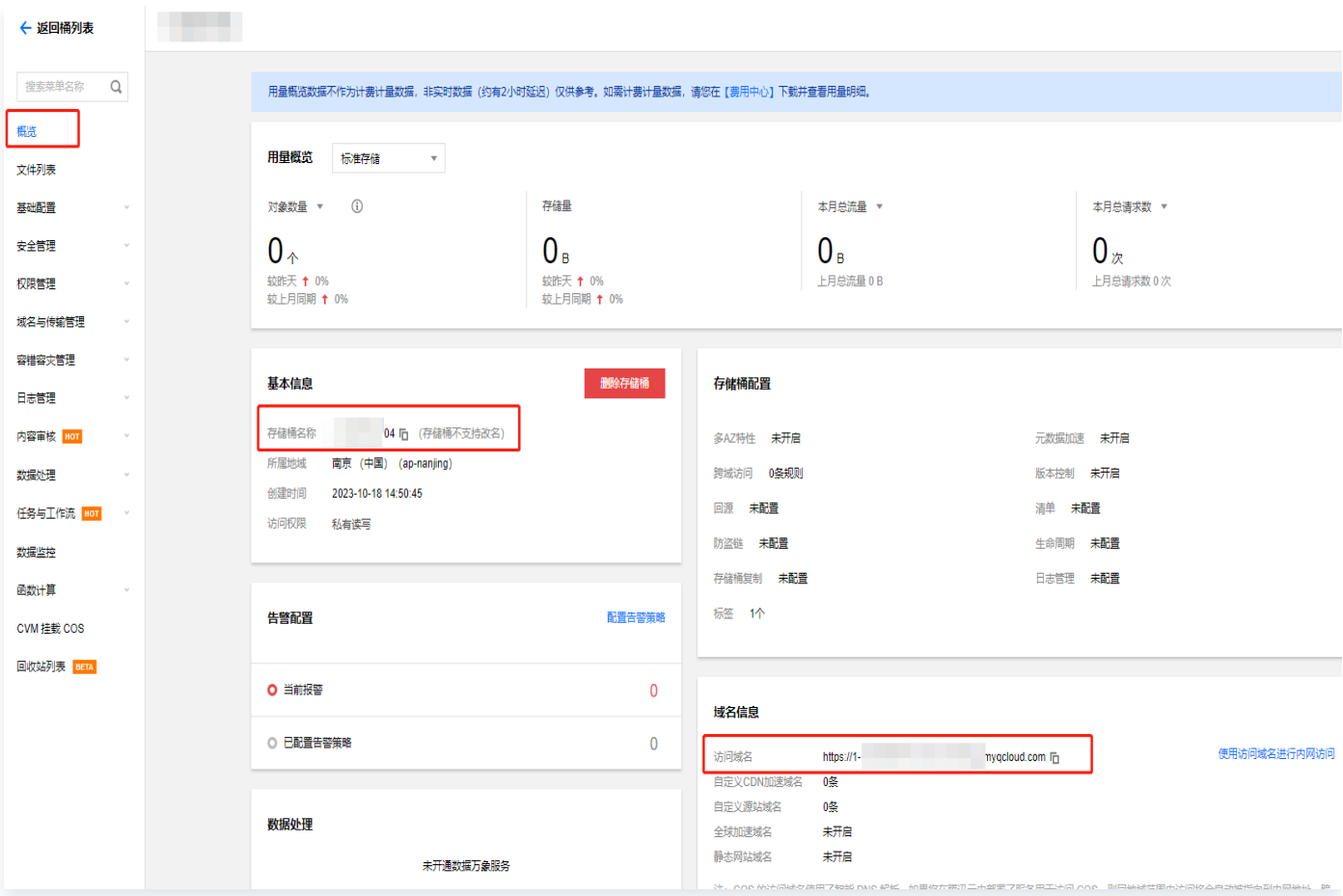
5. 配置信息确认无误后，单击**创建**，完成存储桶的创建。



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。

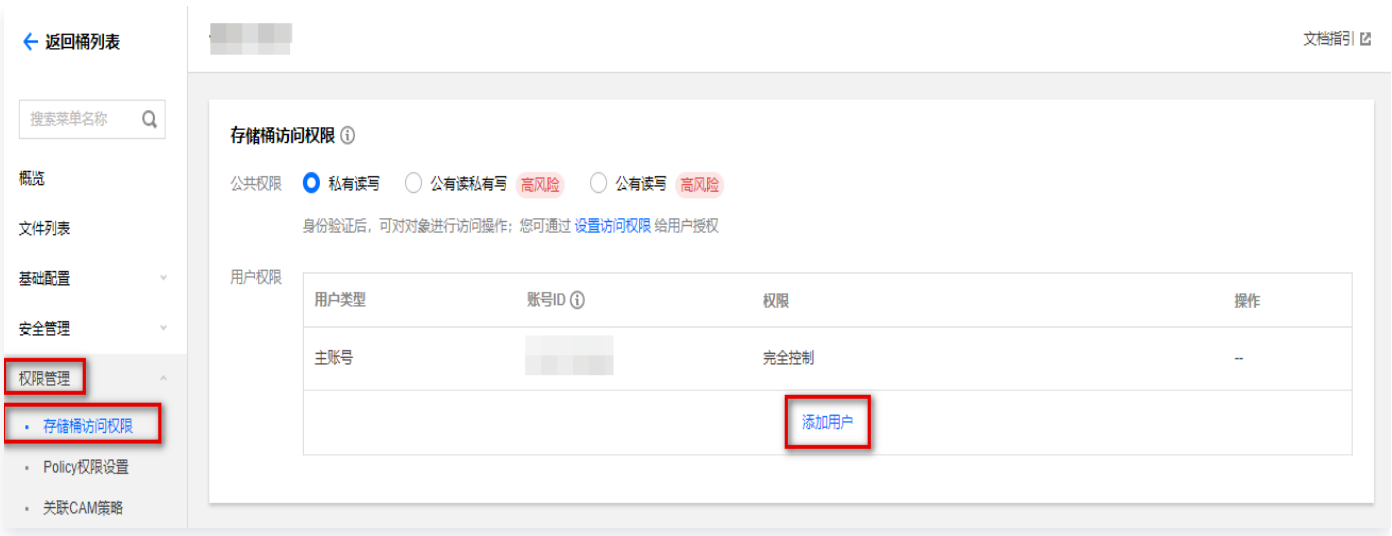
2. 单击**概览**，查看存储桶的概览页。找到**存储桶名称**和**访问域名**，分别作为 Bucket 和 Endpoint 参数。



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**。

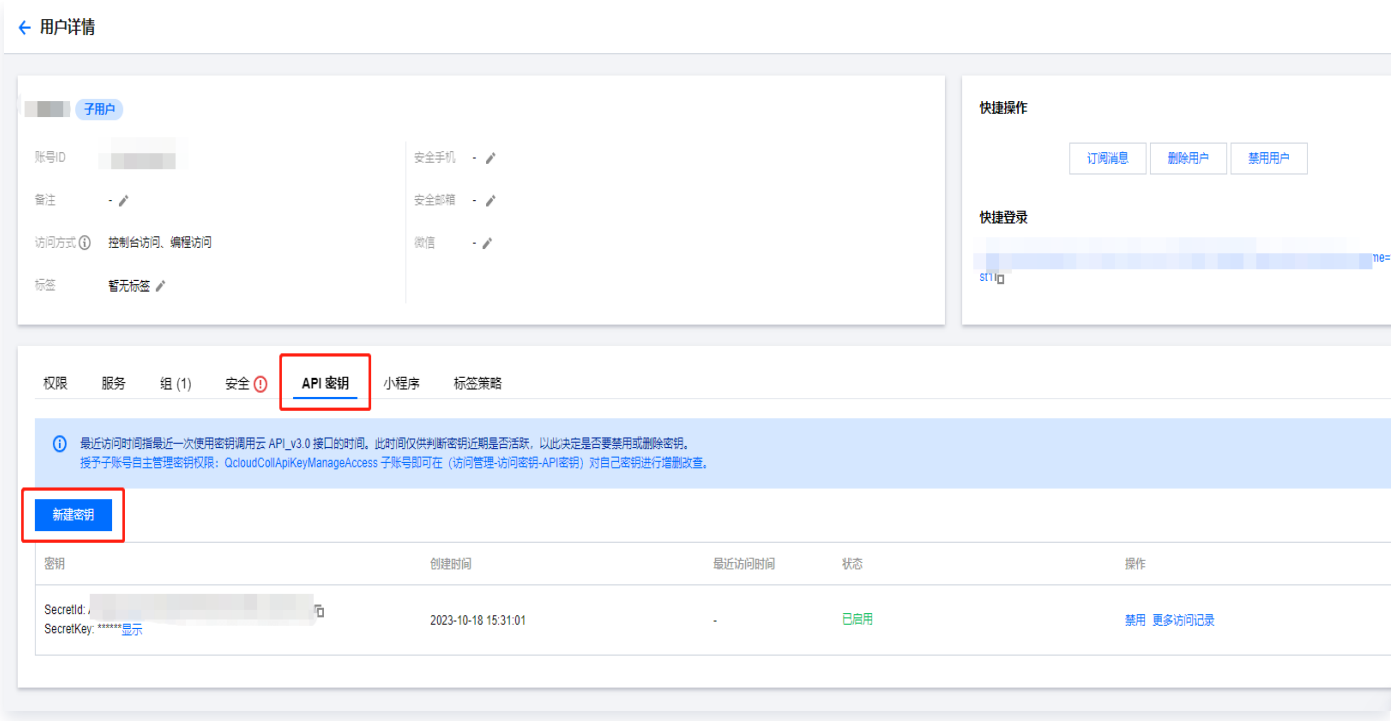


4. 添加用户时选择**子账号**，输入子账号 ID 并选择**数据读取**、**数据写入**两个权限，单击**确定**，即可为此存储桶分配一个具有读写权限（最小权限）的子账号。

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。

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。

> **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 **AccessKeyId** 和 **SecretAccessKey**、**Endpoint**、**Bucket**，单击**测试**

连通性，若提示测试成功，即配置完成。

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。