火山引擎 Volcano Engine

飞连-飞书身份源导入&认证源登录配置指导

北京火山引擎科技有限公司

2022 年 09 月

目录

第一章 飞书作为身份源

飞连支持企业以多种身份源渠道导入用户和组织架构信息至飞连管理后台，本文将为您介绍如何在飞连平台中配置飞书身份源，实现组织架构和用户数据的同步。

1.1 前提条件

(1) 企业拥有在飞连管理后台的配置权限。

(2) 企业在飞书开放平台注册完成，并在飞书管理后台完善好本企业的组织体系。

1.2 快捷步骤

请先创建一个 飞书应用，以下是快捷步骤说明：

(1) 在飞书开放平台 https://open.feishu.cn/ 中创建应用

(2) 飞书权限配置：进入【权限管理】页面，在【权限配置】-【通讯录】选择所需要的权限“更新通讯录”、“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”、“获取角色权限”、“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”、“获取用户受雇信息”、“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”、“搜索用户”权

(3) 事件订阅配置请求地址 URL（选填，在飞书配置完成后从飞连管理后台获取）：http://飞连门户域名:端口/webhook/lark/{占位符}

(4) 发布应用版本：进入应用详情【版本管理与发布】页面，点击“创建版本”，基于实际情况输入应用信息，“可用性状态”选择需要导入飞连系统的部门范围，点击“保存”后并点击“申请发布”。发布应用需等待有权限的管理员进行应用审核，审核完成后，版本状态变为“已上架”即可。

(5) 获取 APP ID 与 App Secret：进入应用详情【凭证与基础信息】页面，复制“App ID” 与 “App Secret” 的信息至飞连

(6) 配置完成，可以去飞连后台继续配置。

以下是回填至飞连的信息说明：

(1) App ID、App Secret：进入飞书开放平台的应用详情【凭证与基础信息】页面获取 App ID（应用 ID）、App Secret（应用密钥）

(2) Lark Host（选填）：如果为中国版飞书，无需填写；如果为海外版 Lark，那么地址为 https://open.larksuite.com，其他私有化版本可根据具体情况修改

(3) 获取 Encrypt_key 与 Verification_Token（选填）：进入应用详情【事件订阅】页面，复制 Encrypt_key” 与 “Verification_Token” 的信息至飞连

1.3 详细操作步骤

1.3.1 飞书开放平台配置

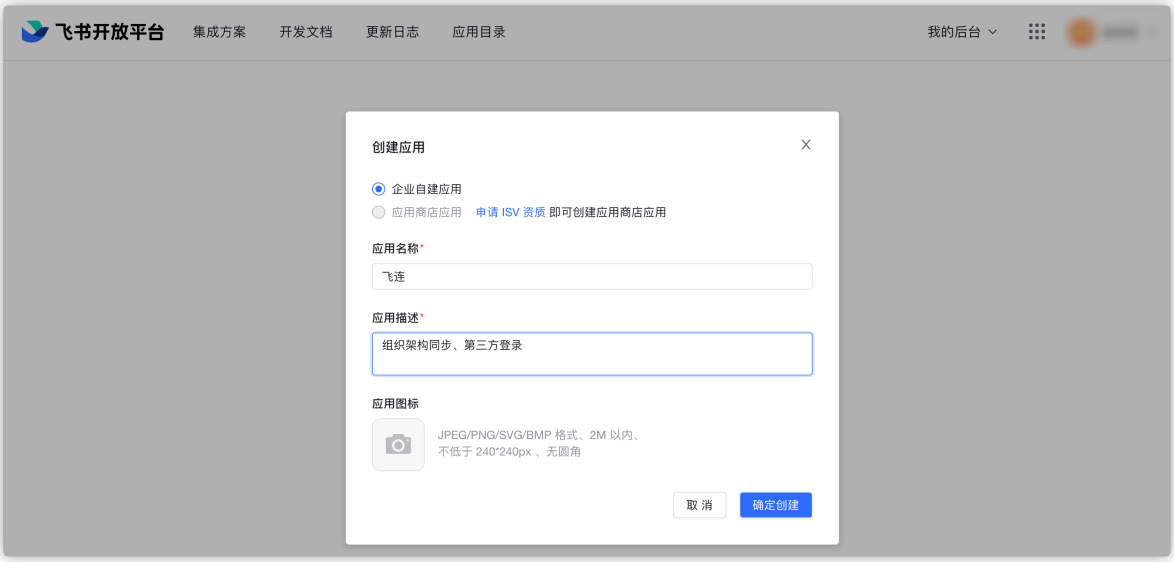
1. 登录飞书开放平台

飞书开放平台首页(https://open.feishu.cn/)，使用企业管理员账号登录。

2. 创建企业自建应用

若第一次创建应用，进入页面后，点击【创建应用】，选择【企业自建应用】，【应用名称】和【应用描述】按照企业实际需要填写。

注意：请务必上传应用图标，否则无法发布该应用（版本）。



3. 查看企业自建应用的详情，获取以及配置相关信息

在【企业自建应用】板块点击新创建的应用所在行，进入详情页。

4. 开通应用权限以及通讯录范围

（1）设置通讯录权限范围

进入【权限管理】页面，配置【设置通讯录权限范围】，通讯录权限范围即同步至飞

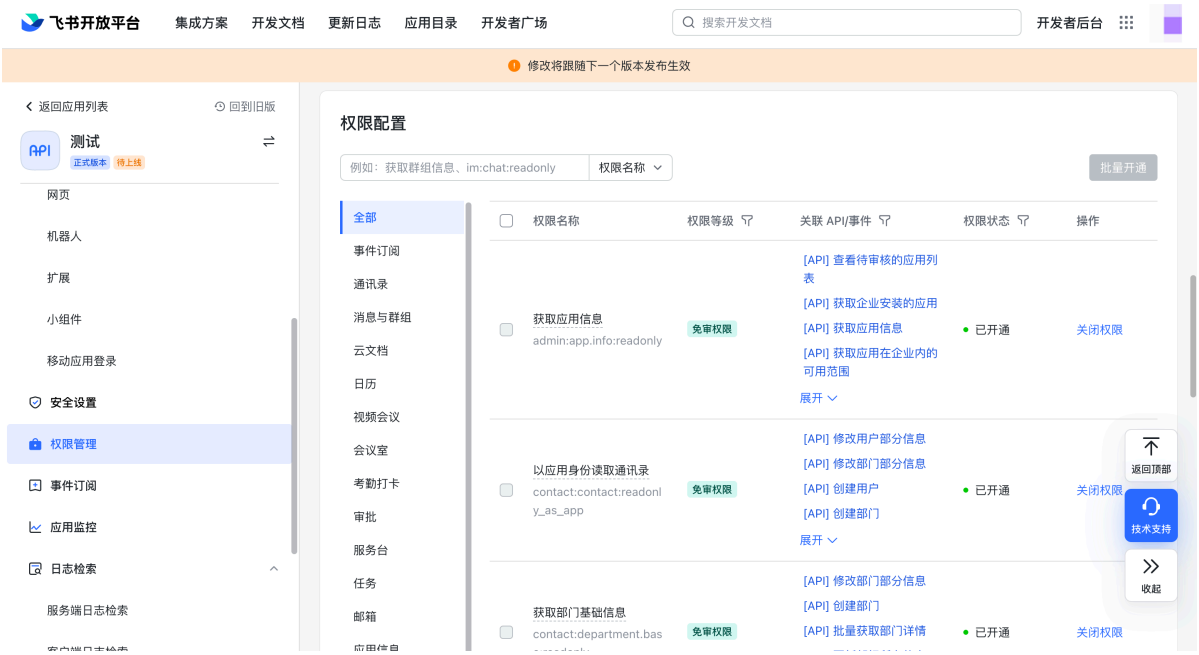
连的组织架构的范围。

（2）开通应用权限

进入【权限管理】页面，在【权限配置】-【通讯录】选择所需要的权限。

- 开通应用权限：“更新通讯录”、“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”、“获取角色权限”、“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”、“获取用户受雇信息”、“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”、“搜索用户”权限。

- 快捷开通方式：复制权限名称，勾选所有的应用权限再选择批量开通。



5. 获取应用凭证

飞书开放平台-【凭证与基础信息】页面，获取或者复制【App ID】与【AppSecret】信息至飞连管理后台。

6. 配置事件订阅

当飞书组织数据发生变更时，飞连为企业提供三种同步方式可供选择，包括手动同步、定时同步和实时同步。若企业选择实时同步的方式需要获取“Encrypt Key 与

Verification Token”

- 手动同步：人工主动去触发同步操作，点击同步即执行同步任务。适用于企业管理员配置完成后，当下不想立即执行同步任务，待调试准备完成后，再进行手动同步的工作。

- 定时同步：指定时间同步上游白名单数据源。适用于企业运维人员无需关注何时去同步组织数据，指定特定时间去定时同步。

- 实时同步【推荐】：根据组织机构或者人员实时变化的信息，进行差量同步，实时同步的特点是同步速度快、响应及时、无需排队等待。适用于企业员工每日有较大的员工、部门数据信息调整，需要在飞连侧及时获取到变更情况。

参数说明：

- Encrypt Key 与 Verification Token：在【飞书开放平台】-【事件订阅】-点击“刷新获取“或者“自定义编辑”，复制 Encrypt_key” 与 “Verification_Token” 的信息至飞连

- 请求地址：数据变更通知地址，此为 http://飞连门户域名:端口/webhook/lark/{占位符}

注意：请求地址为飞连门户域名，而非飞连管理后台域名。

7. 应用发布

进入【版本管理与发布】页面，点击【创建版本】按钮。

配置【应用版本号】建议与当前部署飞连版本一致，便于维护。设置【可用性状态】，可用性状态指能够使用该应用的用户范围，如果全员需要使用飞连中的飞书第三方登录，则选择【所有员工】。完成配置后，点击【保存】。

创建完版本后，点击【申请发布】

8. 已完成飞书开放平台配置，开启在飞连管理后台配置获取应用“Secret”

1.3.2 飞连管理后台配置

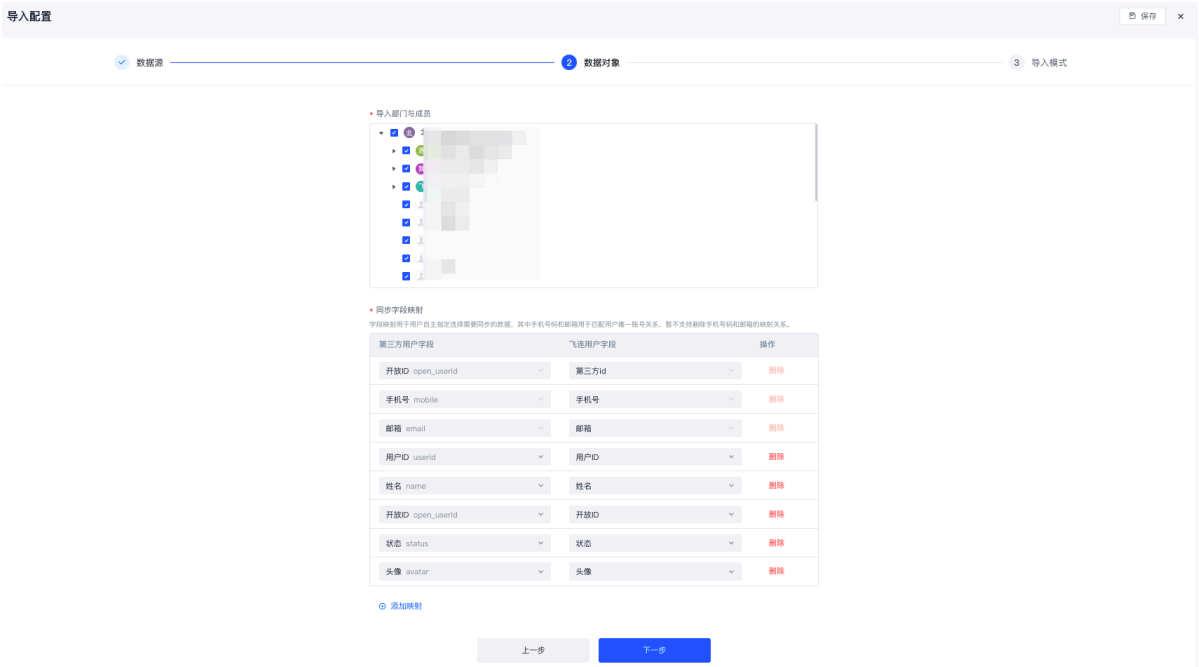
1. 登录飞连管理后台

在飞连管理后台，找到【组织架构-账号配置-数据同步】，点击“添加配置”，选择“企飞书”作为身份源接入。

2. 填写“App ID、App Secret”以及“权限探测”

- App ID、App Secret：飞书开放平台的应用详情【凭证与基础信息】页面获取 App ID、App Secret
- 权限探测指通过连通性探测功能，帮助管理员有效检查“是否已配置好第三方平台的权限”，避免配置完成导入后，无法正常使用。对于飞书而言，将检测“飞连与飞书”数据之间的通信以及应用权限开通情况。

3. 选择“同步对象”以及“同步字段映射”



- 同步对象：飞连从飞书获取本企业的组织数据，企业管理员在“同步对象树”选择需要同步至飞连的组织对象。
- 同步字段映射：同步字段映射用于企业将第三方的成员信息中的字段映射到飞连。其中手机号码和邮箱用于匹配用户唯一账号关系，暂不支持删除手机号码和邮箱的映射关系（除 LDAP）。
  - 左侧为第三方用户字段：选择第三方用户字段
    - 核心字段：
      - 第三方 ID、手机号、邮箱：不允许修改，用于匹配用户唯一账号关系
      - 状态：飞连需要获取第三方成员的身份状态的变更
    - 非核心字段：选择需要同步至飞连的基础数据
  - 右侧为飞连用户字段
    - 选择映射至飞连的用户字段，若没有指定的字段，支持添加“自定义属性”，填写说明如下：

字段KEY	字段名称	字段类型	字段值	是否必填	操作
定义字段唯一值	字段显示名称	选择字段类型 1. String：字符串 2. Number：数字 3. Boolean：布尔值 4. Expression：表达式	当选择“Expression”，输入表达式	选择该字段是否为必填项	1. 删除：删除此字段 2. 编辑：重新编辑字段信息

- 当自定义字段创建完成后，支持在“飞连用户字段”列表中选择“该扩展字段”。例如“创建企业邮箱字段”，可以在“飞连用户字段”列表中选择“企业邮箱”扩展字段

4. 选择“导入模式”，推荐实时同步方式

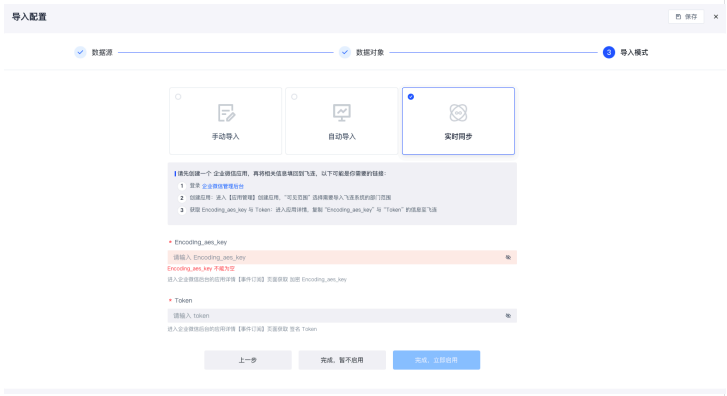
当飞书数据发生变更时，飞连为用户提供三种同步方式可供选择，包括手动同步、定时同步和实时同步。

- 导入模式说明

同步方式	概念 & 场景	策略
手动同步	人工主动去触发同步操作，点击同步即执行同步任务。适用于企业管理员配置完成后，当下不想立即执行同步任务，待调试准备完成后，再进行手动同步的工作。	手动全量同步
定时同步	指定时间同步上游白名单数据源。适用于企业运维人员无需关注何时去同步组织数据，指定特定时间去定时同步。	定时全量同步
实时同步	细粒度的同步方式，实时同步会根据组织机构或者人员实时变化的信息，进行差量同步，实时同步的特点是同步速度快、响应及时、无需排队等待。适用于企业员工每日有较大的员工、部门数据信息调整，需要在飞连侧及时获取到变更情况。	增量同步（仅同步变更的部门与员工，需要在开启实时同步之前先手动同步一次全量数据）

- 导入操作说明

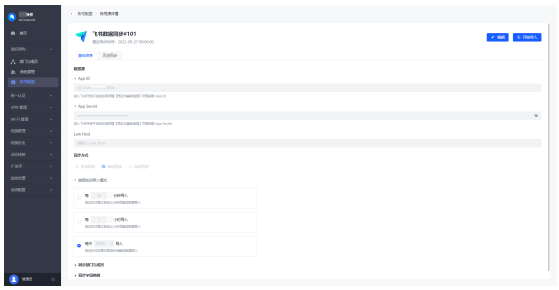
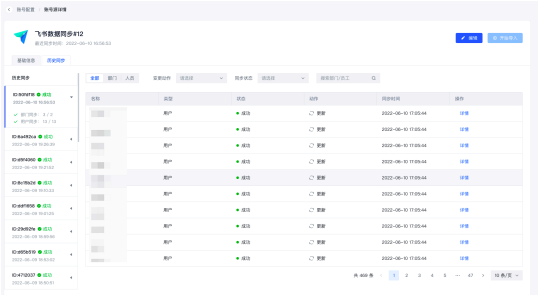
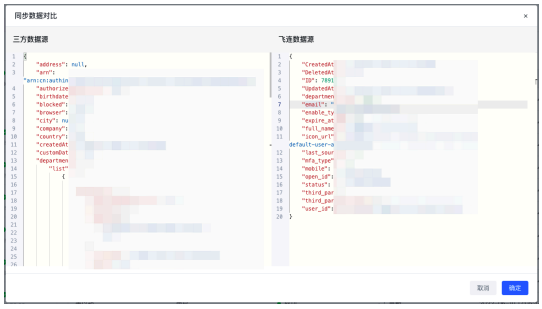
同步方式	产品配图	操作说明
手动同步		选择“手动导入”，一键手工同步。
定时同步		选择“自动导入”，按照分钟、小时、天的间隔进行自动导入。

实时同步		选择“实时同步”，输入“Encrypt_key与Verification_Token” • Encrypt_key:飞书开放平台的应用详情【事件订阅】页面获取 加密Encrypt_key • Verification_Token:进入飞书开放平台的应用详情【事件订阅】页面获取 签名Verification_Token

5. 保存配置，查看同步任务

支持在飞连管理后台查看数据源同步信息以及任务日志，日志包含单次任务下同步对象的变更情况以及详细同步数据信息对比。

• 账号源信息	查看企业微信相关配置信息

	
• 历史同步任务查询日志 	• 左侧：可以按照时间选择历史同步任务 • 右侧：每次任务下同步对象变更情况
• 点击“详情”，可以查看该对象上游同步至飞连数据源信息对比，方便查看同步前后的数据，用于日志审计以及排查用户数据相关的问题。 	• 左侧：员工或者部门在上游数据源的详情信息 • 右侧：根据字段映射情况，查看同步到飞连的员工或者部门的详情信息

第二章 飞书作为认证源

飞连支持企业以多种认证源渠道登录至飞连，本文将为您介绍如何在飞连平台中配置飞书认证源，实现企业用户登录飞连。

2.1 前提条件

(1) 企业拥有在飞连管理后台的配置权限。

(2) 企业在飞书开放平台注册完成，完善好本企业的组织体系。

2.2 快捷步骤

请先创建一个飞书应用，再将相关信息回填到飞连，以下是快捷步骤说明：

(1) 在飞书开放平台中创建应用 https://open.feishu.cn/

(2) 飞书权限配置：进入【权限管理】页面，在【权限配置】-【通讯录】选择所需要的权限“更新通讯录”、“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”、“获取角色权限”、“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”、“获取用户受雇信息”、“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”、“搜索用户”权限

(3) 网页配置：进入【应用功能】-【网页】，将【网页】按钮置为开启状态，进行桌面端主页地址、移动端主页地址配置

注：桌面端主页地址、移动端主页地址为“https://飞连门户域名”

(4) 安全设置：进入【安全设置】中添加重定向 URL
重定向 URL 为：

https://飞连门户域名:端口/multiple-pages/third-login.html（必填）

https://飞连门户域名:端口/api/tpslogin/callback/lark（必填）

飞书内免登访问配置 https://飞连门户域名:端口/login（选填）

(5) 发布应用版本：进入应用详情【版本管理与发布】页面，点击“创建版本”，基于实际情况输入应用信息，“可用性状态”选择需要导入飞连系统的部门范围，点击“保存”后并点击“申请发布”。发布应用需等待有权限的管理员进行应用审核，审核完成后，版本状态变为“已上架”即可。

(6) 获取 APP ID 与 App Secret：进入应用详情【凭证与基础信息】页面，复制“App ID” 与 “App Secret” 的信息至飞连

以下是回填至飞连的信息说明：

(1) App ID、App Secret：进入飞书开放平台的应用详情【凭证与基础信息】页面获取 App ID（应用 ID）、App Secret（应用密钥）

(2) 发布登录位置：移动端、桌面端、WEB 端

2.3 操作步骤

2.3.1 在飞书开放平台配置

1. 登录飞书开放平台

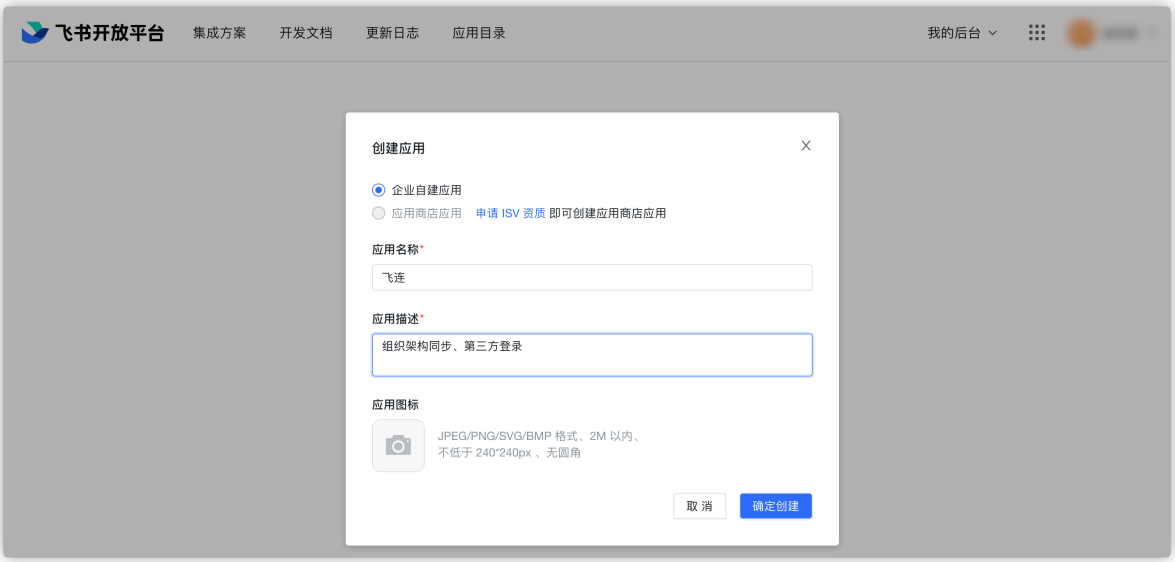
飞书开放平台首页(https://open.feishu.cn/)，使用企业管理员账号登录。

2.创建企业自建应用

若第一次创建应用，进入页面后，点击【创建应用】，选择【企业自建应用】，【应

用名称】和【应用描述】按照企业实际需要填写。

注意：请务必上传应用图标，否则无法发布该应用（版本）。



3. 查看企业自建应用的详情，获取以及配置相关信息

在【企业自建应用】板块点击新创建的应用所在行，进入详情页。

4. 开通应用权限以及通讯录范围

（1）设置通讯录权限范围

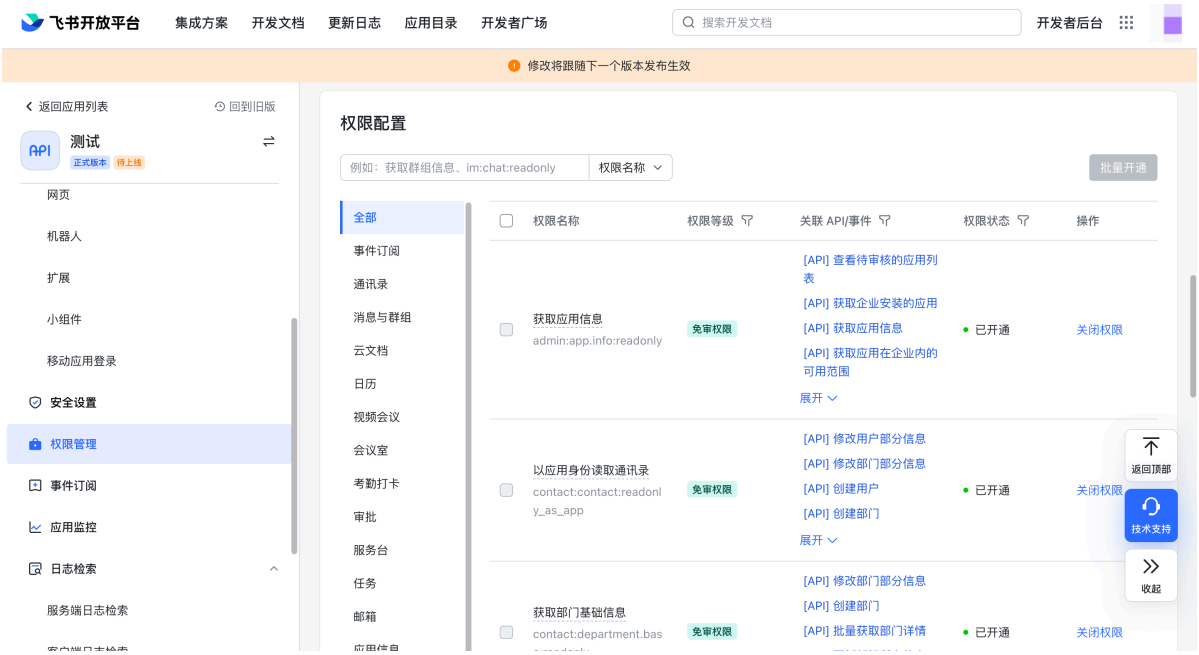
进入【权限管理】页面，配置【设置通讯录权限范围】，通讯录权限范围即同步至飞连的组织架构的范围。

（2）开通应用权限

进入【权限管理】页面，在【权限配置】-【通讯录】选择所需要的权限。

- 开通应用权限：“更新通讯录”、“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”、“获取角色权限”、“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”、“获取用户受雇信息”、“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”、“搜索用户”权限。

- 快捷开通方式：复制权限名称，勾选所有的应用权限再选择批量开通。



5. 网页配置（与身份源不同的配置之处）

进入【应用功能】-【网页】页面，将【启用网页】按钮置为开启状态，并在【网页配置】板块中，将桌面端主页和移动端主页设置为“https://飞连门户域名”（必填），点击【保存】。

注意：桌面端主页和移动端主页都需要填写：“https://飞连门户域名”，“飞连门户域名”是飞连后台【系统配置】/【企业配置】中的门户域名，不是管理后台域名，请仔细检查。

6. 安全设置（与身份源不同的配置之处）

进入【安全设置】页面，在“重定向 URL”配置项中，添加以下三个重定向 URL:

https://飞连门户域名:端口/multiple-pages/third-login.html（必填）

https://飞连门户域名:端口/api/tpslogin/callback/lark（必填）

飞书内免登飞连访问配置：https://飞连门户域名:端口/login（选填）

注意：

- 实现 APP 内免登访问飞连系统，无需进行手动登录。现在可提供在飞书工作台内查看飞连 OTP 口令，配置详情请查看《飞连_第三方 IM 查看飞连 OTP 口令》。
- “飞连门户域名：端口”是飞连后台【系统配置】/【企业配置】中的门户域名，不是管理后台域名，请仔细检查。

7. 获取应用凭证

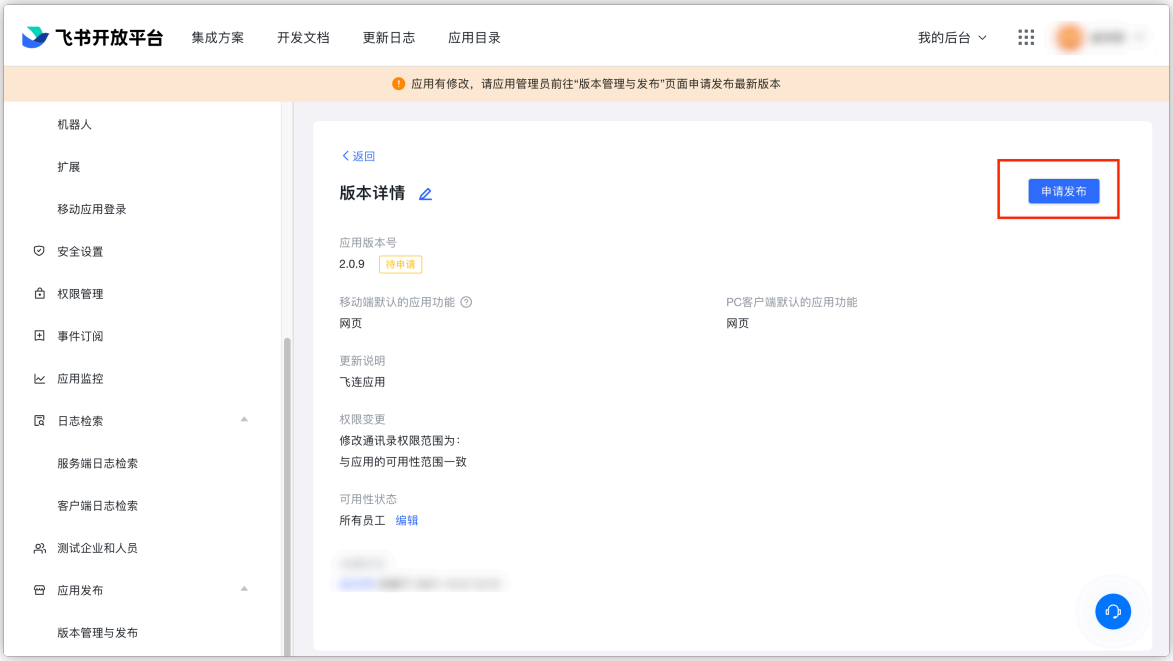
飞书开放平台-【凭证与基础信息】页面，获取或者复制【App ID】与【AppSecret】信息至飞连管理后台。

8. 应用发布

进入【版本管理与发布】页面，点击【创建版本】按钮。

配置【应用版本号】建议与当前部署飞连版本一致，便于维护。设置【可用性状态】，可用性状态指能够使用该应用的用户范围，如果全员需要使用飞连中的飞书第三方登录，则选择【所有员工】。完成配置后，点击【保存】。

创建完版本后，点击【申请发布】

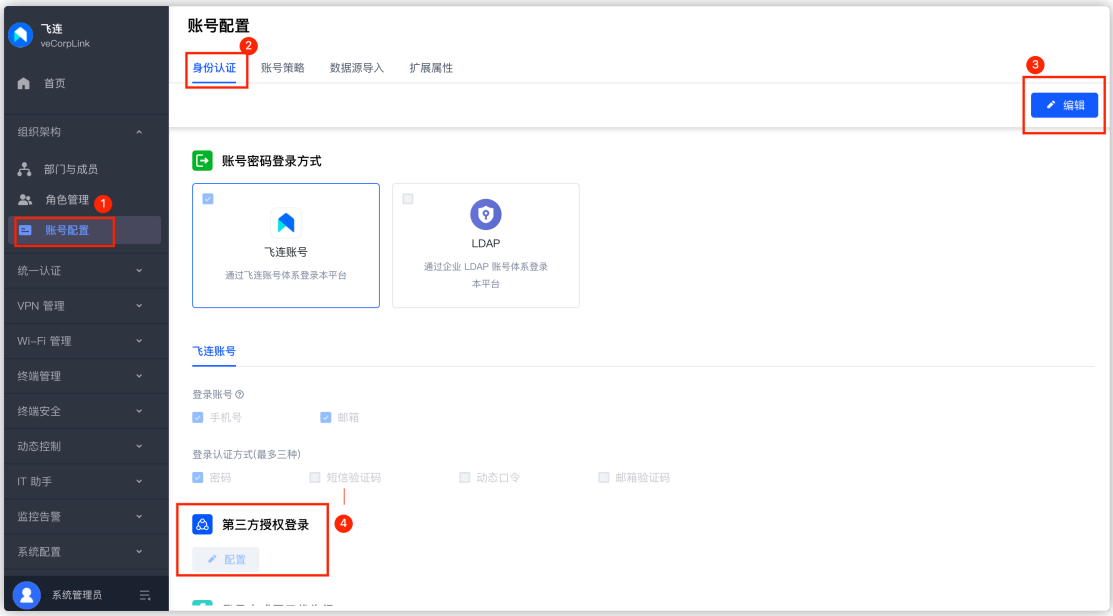


9. 已完成飞书开放平台配置，开启在飞连管理后台配置

2.3.2 在飞连配置飞书认证源

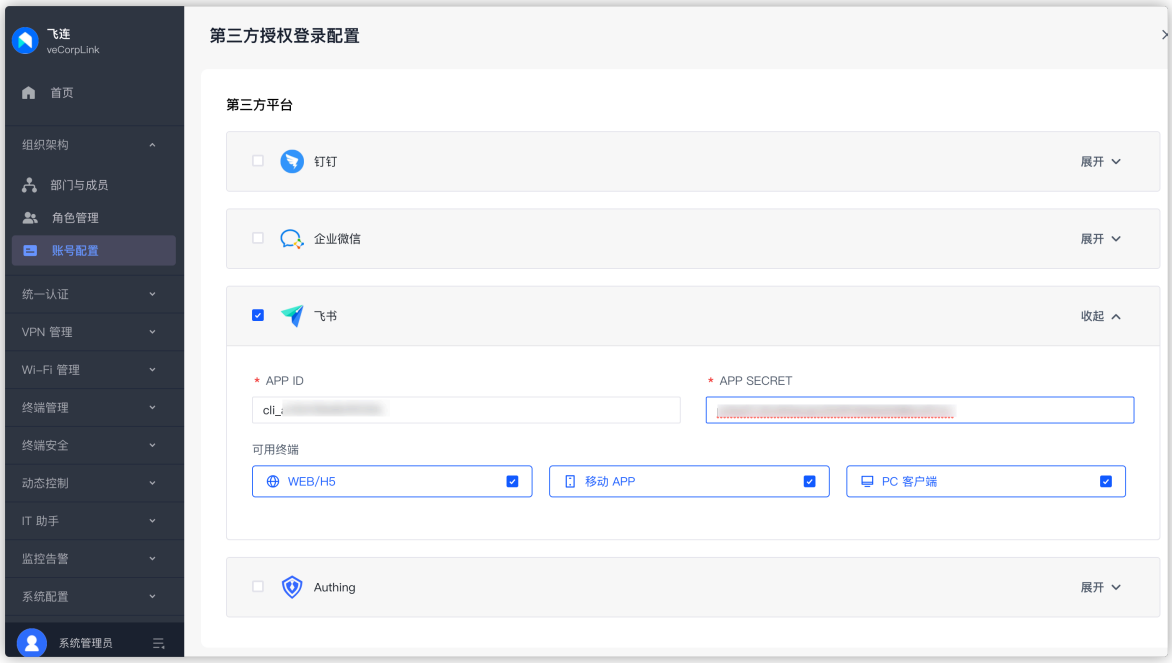
1. 登录飞连管理后台

进入飞连管理后台，点击【组织架构】-【账号配置】-【身份认证】-【第三方授权登录】。



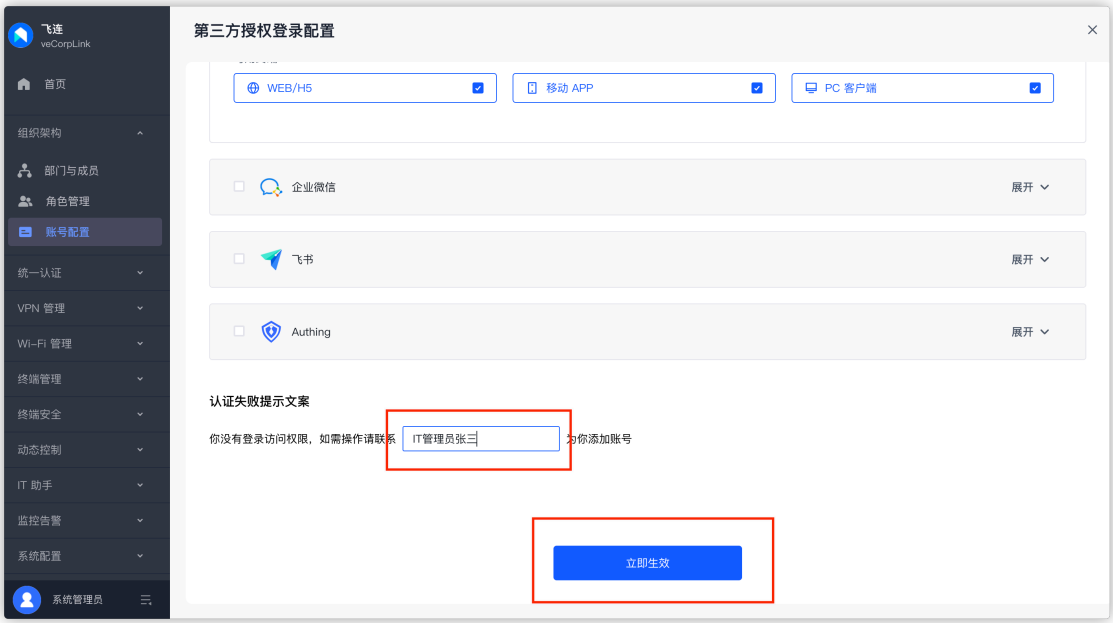
2. 填写登录配置信息

进入“组织架构-账号配置-第三方平台”配置页面，选中【飞书】，【APP ID】、【APP SECRET】。



3. 认证失败提示说明

配置认证失败提示文案，联系人建议填写 IT 管理员，点击【立即生效】，点击【保存】



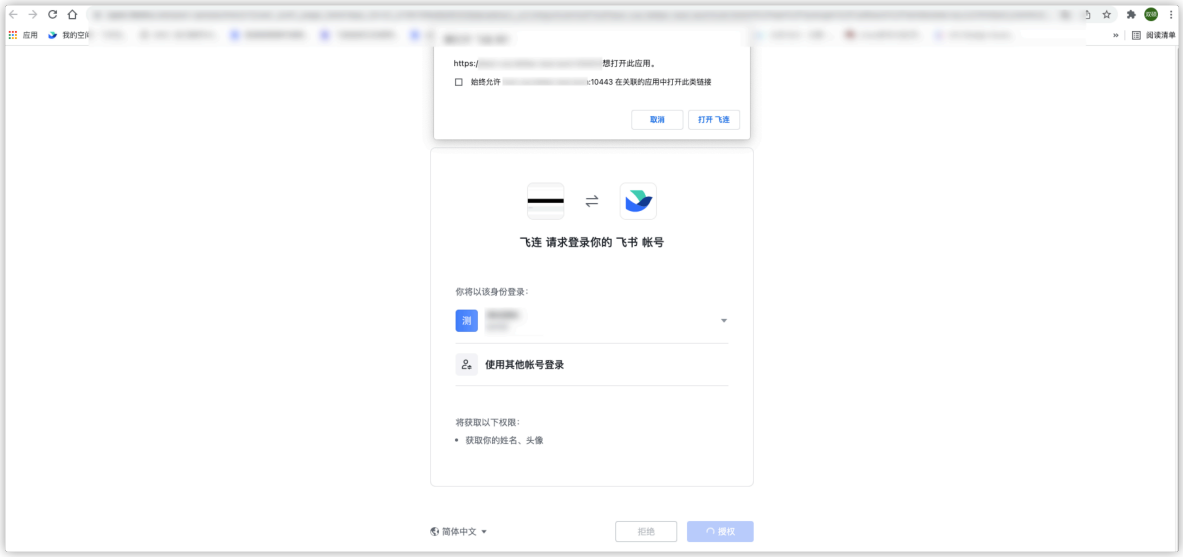
4. 对于第三方数据源新入职用户未及时同步到飞连的场景，推荐开启自动创建账号，解决成员登录问题

在“组织架构-账号配置-自动创建账号”，飞连默认开启此配置，用于解决“当第三方数据源未及时同步入职成员账号时，企业成员登录飞连时将提供自动创建账号”，不打断企业成员登录问题。

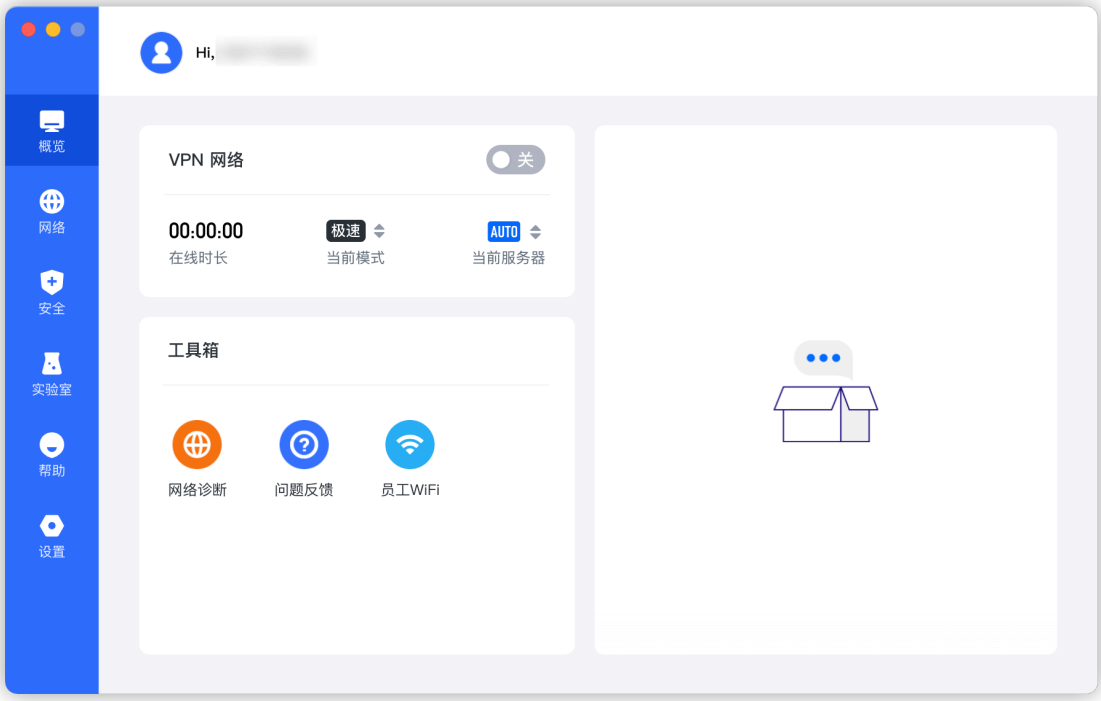
5. 完成登录认证源配置，查看客户端支持情况，开启成员登录

完成导入后，在飞连客户端查看带有飞书图标，同时点击飞书图标能够唤起飞书授权登录。

	Android	iOS	MacOS	Windows	Linux	Web 浏览器
客户端支持情况	支持	支持	支持	支持	支持	支持



扫码并点击【打开飞连】，完成飞连客户端登录。



第三章 FAQ

(1) 问：身份源是什么？

答：身份源存储了所有部门、员工的信息，且是最根本、可信的一个用户目录。

(2) 问：飞连身份源同步能做什么？

答：企业无需在飞连在搭建重复的员工账号身份体系，仅需对接上游数据源，即可实现上游同步变更，飞连及时获取并联动变更。例如：上游入职成员+1，飞连自动授予入职成员相应权限。

(3) 问：飞书支持版本？

答：

版本	飞书国内版	飞书海外版（Larksuite）	飞书私有化
支持情况	支持	支持	请联系飞连供应商

(4) 问：飞连基础信息字段过少，希望增加自定义字段与上游数据源字段做数据映射。

答：已支持，飞连支持自定义字段且支持与上游数据源字段映射。

(5) 问：是否支持同步角色？

答：支持，前置条件需要同步上游用户，但是仅支持同步飞书角色，不支持同步用户组。