**Ldap认证管理系统**

**V1.0.-**

**使用说明书**

二○二四年七月

目录

[1 引言 3](#_Toc173244525)

[1.1 编写目的 3](#_Toc173244526)

[1.2 功能简介 3](#_Toc173244527)

[1.3 主要功能 3](#_Toc173244528)

[1.3.1 统一认证中心 3](#_Toc173244529)

[1.3.2 标准协议 4](#_Toc173244530)

[1.3.3 登录支持 4](#_Toc173244531)

[1.3.4 提供标准的接口 4](#_Toc173244532)

[1.3.5 平台扩展行性 4](#_Toc173244533)

[1.4 单点登录的安全性 4](#_Toc173244534)

[1.4.1 二次密码登录 4](#_Toc173244535)

[1.4.2 单点退出 5](#_Toc173244536)

[1.4.3 会话超时设计 5](#_Toc173244537)

[1.4.4 防暴力破解 5](#_Toc173244538)

[1.4.5 连续登陆次失败策略 6](#_Toc173244539)

[1.4.6 静态密码策略 6](#_Toc173244540)

[1.4.7 单点注销-Single Logout 6](#_Toc173244541)

[2 使用说明 6](#_Toc173244542)

[2.1 用户登录 6](#_Toc173244543)

[2.2 登录完成界面 8](#_Toc173244544)

[2.3 忘记密码 8](#_Toc173244545)

[2.4 登录管理 9](#_Toc173244546)

[2.5 我的应用 9](#_Toc173244547)

[2.6 身份管理 10](#_Toc173244548)

[2.6.1 组织管理 10](#_Toc173244549)

[2.6.2 用户管理 10](#_Toc173244550)

[2.6.3 用户组 11](#_Toc173244551)

[2.7 应用管理 11](#_Toc173244552)

[2.7.1 应用列表 11](#_Toc173244553)

[2.7.2 新增应用 12](#_Toc173244554)

[2.8 访问控制 12](#_Toc173244555)

[2.8.1 应用授权 12](#_Toc173244556)

[2.9 同步中心 13](#_Toc173244557)

[2.10 日志审计 13](#_Toc173244558)

[2.10.1 登录日志 13](#_Toc173244559)

[2.10.2 应用访问日志 14](#_Toc173244560)

[2.11 系统配置 14](#_Toc173244561)

[2.11.1 菜单管理 14](#_Toc173244562)

[2.11.2 策略管理 14](#_Toc173244563)

[2.11.3 LDAP数据源 15](#_Toc173244564)

[2.11.4 第三方认证 16](#_Toc173244565)

[2.11.5 短信配置 16](#_Toc173244566)

[2.11.6 系统信息 17](#_Toc173244567)

# 引言

## 编写目的

企业经过多年的建设发展，在信息基础设施、信息系统、信息安全保障以及信息化管理等方面经过长期发展，现已建成多套应用系统，在企业经营、日常管理等管理方面发挥了重要作用，信息化建设取得了阶段性的成果，但随着企业信息化水平的提高以及信息系统在单位内的全面推广，企业的业务朝着互联网化移动化、数字化的方向快速发展，对信息系统的依赖程度不断增强，对业务和信息系统的紧密关联性和信息的安全性也提出了更高的要求及挑战。

为全面保障企业信息化安全工作能力和水平，有效提升信息系统内控管理水平，实现信息化业务向全流程无纸化、高效统一、安全可靠、合法合规方向发展，企业将按照“统一身份、集中管理、简化应用、保障安全”的原则，打破各系统独自进行认证和账号管理的格局，逐步形成以“用户为中心”的“业务便捷、安全可信”认证服务系统，实现人员身份认证“可管、可控、可信”，促进企业各类信息系统互认互通，为企业数字化转型保驾护航。

## 功能简介

基于OpenLDAP企业级认证平台(EIAM)，用于管理企业组织架构、员工账号、身份认证、应用访问，帮助整合本地或云端的业务系统及第三方 SaaS 系统的所有身份，实现一个账号登录访问所有应用。支持OAuth2.x、OIDC、SAML2.0、JWT、CAS等SSO标准协议。

## 主要功能

### 统一认证中心

* 提供统一的单点登录认证系统所有应用系统共享一个身份认证系统
* 从单点登录系统所有应用系统能够识别和提取ticket信息

### 标准协议

|  |  |  |
| --- | --- | --- |
| 序号 | 协议 | 支持 |
| 1.1 | OAuth 2.0  OpenID Connect | 高 |
| 1.2 | SAML 2.0 | 高 |
| 1.3 | JWT | 高 |
| 1.4 | CAS | 高 |

### 登录支持

|  |  |  |
| --- | --- | --- |
| 序号 | 登录方式 | 支持 |
| 2.1 | 动态验证码 | 字母/数字 |
| 2.2 | 短信认证 | 阿里云短信 |
| 2.3 | 时间令牌 | Google/Microsoft Authenticator/FreeOTP/支持TOTP或者HOTP |
| 2.4 | LDAP | OpenLDAP |
| 2.5 | 社交账号 | 微信/支付宝/微博/钉钉/飞书/企业微信等 |

### 提供标准的接口

提供标准的认证接口以便于其他应用集成SSO，安全的移动接入，安全的API、第三方认证和互联网认证的整合。

简化标准LDAP服务器机构和账号管理，密码自助服务重置密码。

### 平台扩展行性

基于Java EE平台，微服务架构，采用Spring、MySQL、Redis、Vue3等开源技术，扩展性强。

## 单点登录的安全性

### 二次密码登录

单点登录使用户能在一个入口完成登录后，一般情况下用户在点击应用图标时，直接通过相应的协议，登录到应用系统；但是有时要针对特定的用户、特定的应用进行二次密码校验的功能，防止关键系统的登录，导致的信息敏感泄露，比如财务系统或者个人工资账单，在实际工作中经常出现工作代理的情况，即使出现单点登录的密码泄露，二次密码也很好地保护敏感应用系统；

### 单点退出

单点退出是指用户在一个系统退出后，其所能单点登录访问的所有系统都同时退出。单点退出主要是为提高安全性，避免用户忘记退出所有应用而造成信息的泄密。 其实现方式也非常简单，由于SSO和单点登录的应用都是分开的，使用不同的域名，只是通过认证协议帮助用户在多个应用系统中传递身份和登录系统。因此，首先注销单点登录应用，然后修改每个应用系统都使用MaxKey的单点退出页面，单点登录的退出页面会将用户登录的Session注销掉。

### 会话超时设计

为节约服务端资源，并基于安全性考虑，对于长时间没有活动的客户端其会话将被自动终结。同时，为保证用户的单点登录不受影响，其所有超时都在MaxKey端集中控制，即MaxKey的会话超时时间比集成的应用系统会话超时时间略长。例如希望实现用户不活动30分钟就终止会话，则将MaxKey的不活动超时时间设置成30分钟，集成应用的不活动超时时间设置成40分钟。 如果用户登录后打开多个应用，并一直只访问某个应用，而其他应用长时间没有被访问导致应用会话超时，用户再次点击该已超时的应用时，用户会被应用要求重新登录。为避免这种情况，应用检测到用户会话超时后需将用户重定向到登录页面，MaxKey此时再次实现单点登录，登录成功后应用可重新将用户定向到期之前访问的URL或者该应用的首页。

### 防暴力破解

由于认证系统需对互联网提供服务，为避免互联网中恶意的暴力破解，系统需提供防暴力破解能力。防暴力破解的关键是提供一种机制，能阻止计算机用穷举法试探用户口令。 目前一种广泛使用的防暴力破解技术是CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart），即在登录界面除用户名+口令之外再增加一个扭曲的数字或字母字段，让用户输入，这种字段人很容易看懂，但是计算机却很难识别，从而避免计算机用穷举法猜测用户密码，这种技术的应用在互联网应用上经常可以看到。

### 连续登陆次失败策略

使用连续多次登录失败即锁定帐号一定时间的设置，例如如果某个帐号连续6次登录失败就锁定该帐号两小时，这种方式也可以避免暴力破解。

### 静态密码策略

对密码进行限制无非是为了强制用户设置一个更加安全的密码，密码策略主要有以下几种：

（1）密码必须符合复杂性要求

（2）密码长度最小值

（3）密码最长使用期限

（4）密码最短使用期限

（5）强制密码历史

（6）使用可还原的加密存储密码

### 单点注销-Single Logout

单点注销是指用户在一个系统退出后，其所能单点登录访问的所有系统都同时退出。单点注销主要是为提高安全性，避免用户忘记退出所有应用而造成信息的泄密。

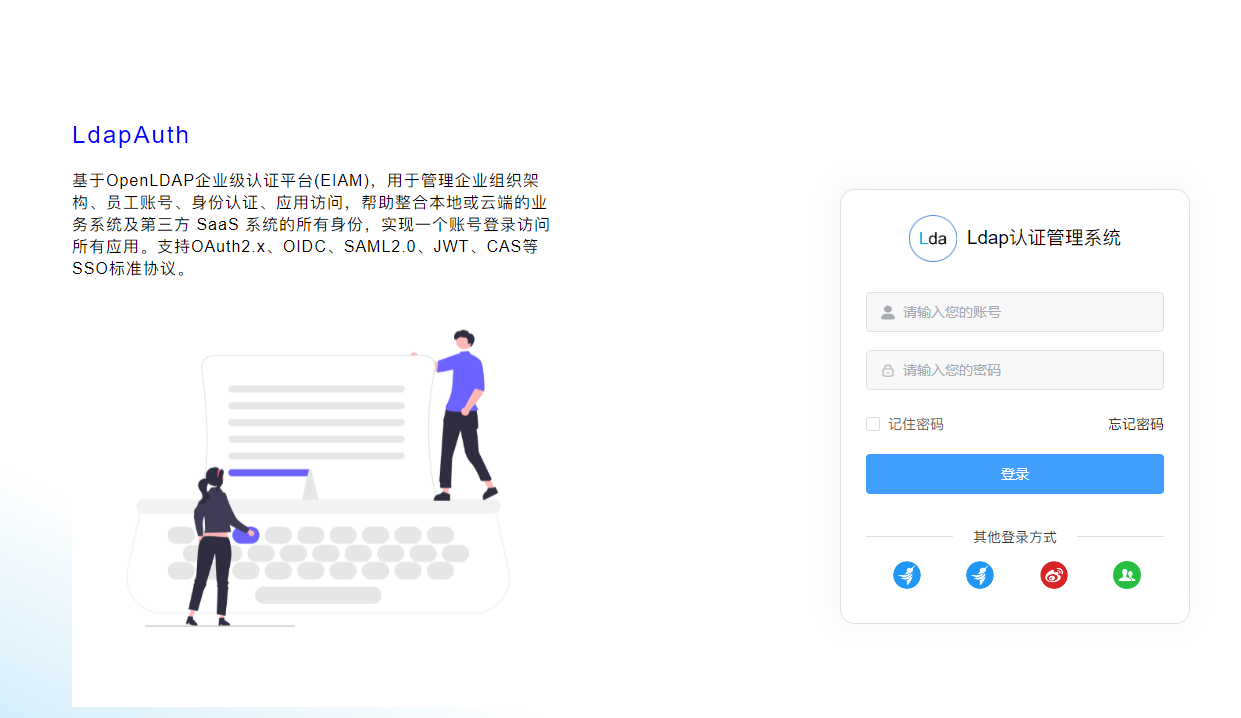
IDP支持单点注销(SLO),即用户不仅仅从认证中心注销，同时也注销从认证中心访问的应用系统。

其实现方式也非常简单，由于SSO和单点登录的应用都是分开的，使用不同的域名，只是通过认证中心在多个应用系统中传递身份和登录系统。因此，首先注销单点登录应用，然后修改每个应用系统都使用SSO的单点注销页面，SSO的退出页面会将用户登录的Session注销掉。

# 使用说明

## 登录

1、用户通过输入用户名+密码+验证码（可配置）进行登录。



2、记住密码，系统记住当前用户登录的密码，在下次登录后自动获取存储在Cookie中的密码，完成记住密码功能。



3、其他登录方式,社交账号登录，用户点击飞书、企业微信、微博等社交账号图标，在社交网站上完成认证后，跳转回LdapAuth，LdapAuth信任社交账号的认证结果。注：这种认证方式要预先在LdapAuth进行配置，参见“第三方认证”。



## 忘记密码

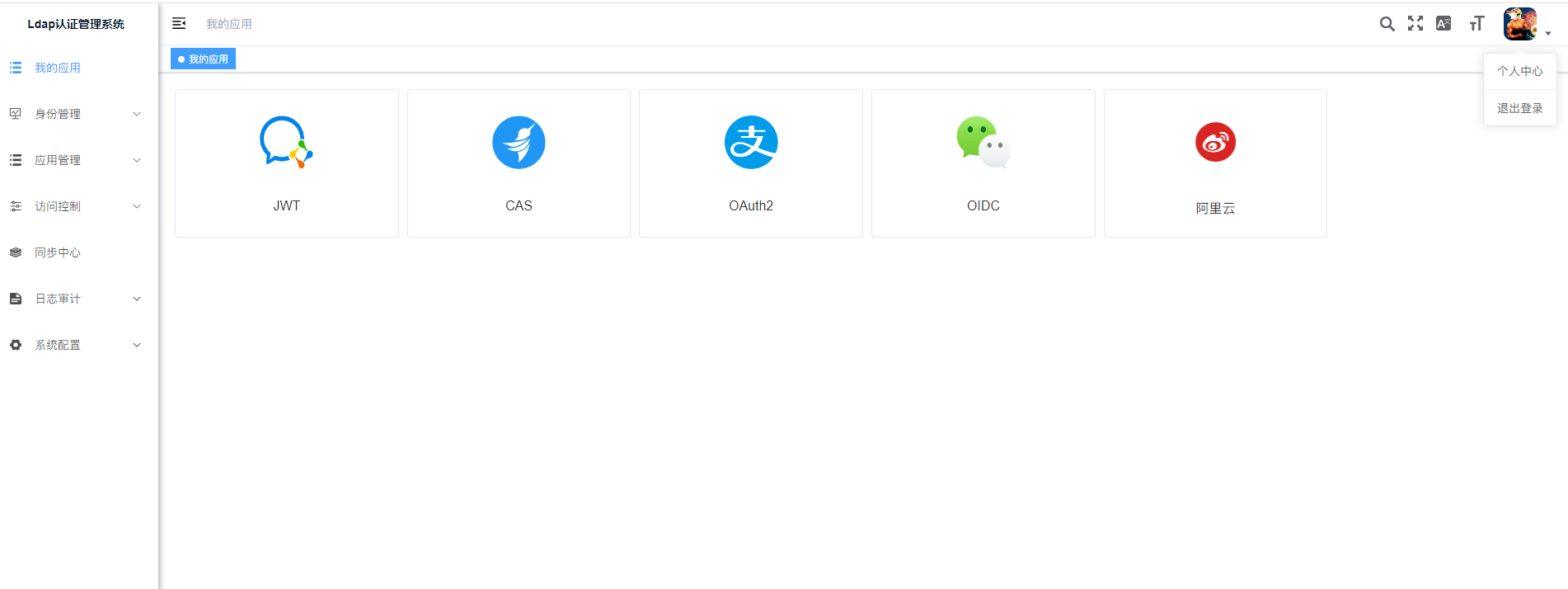
在用户登录界面上有“忘记密码”链接，用户忘记密码可以通过忘记的功能重置新密码。



通过手机号码找回：输入手机号码，点击发送验证码，输入手机接受到的验证码后点击下一步，进入设置密码页面。

## 我的应用

用户登录后，显示的界面如下



“我的应用”界面显示用户有权限访问的应用，当用户点击应用图标，浏览器跳转至对应的应用并实现用户单点登录认证。

## 个人中心

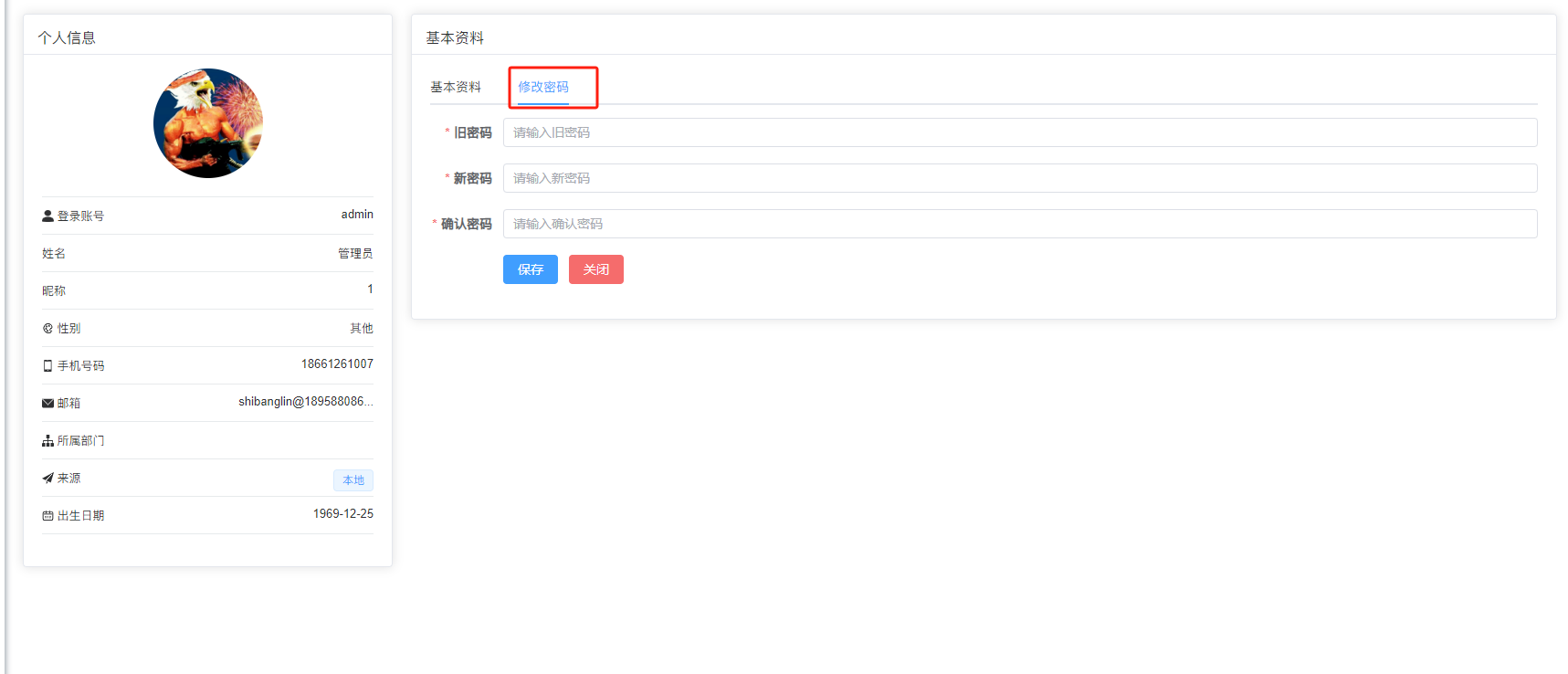
自助个人信息修和密码修改

### 个人信息



点击右上角头像下拉进入“个人信息”，用户可以在此界面对个人基本信息进行修改。

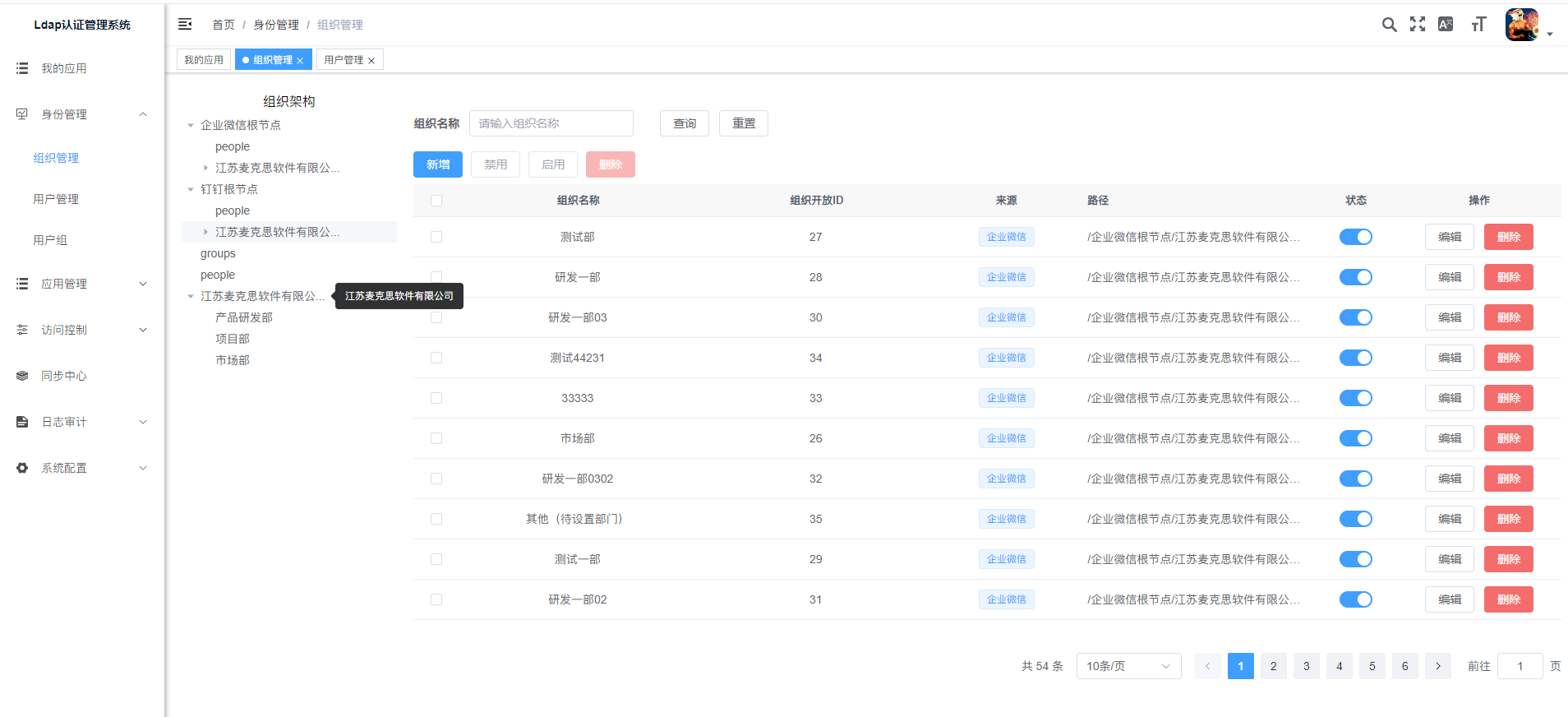
### 密码修改



点击右上角头像下拉进入“个人信息”，切换tab“密码修改”，用户可以在此界面对登录密码进行修改。

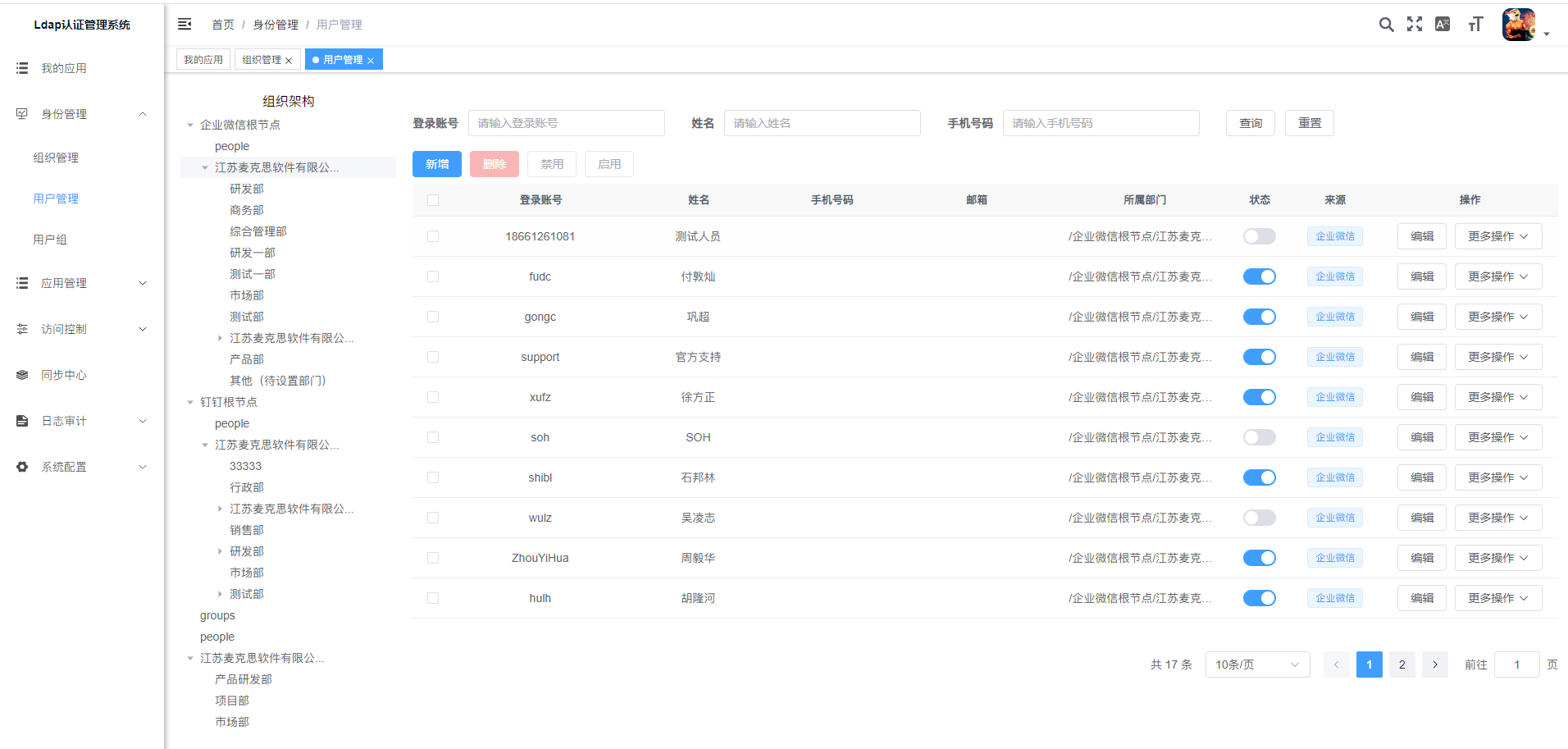
## 身份管理

### 组织管理



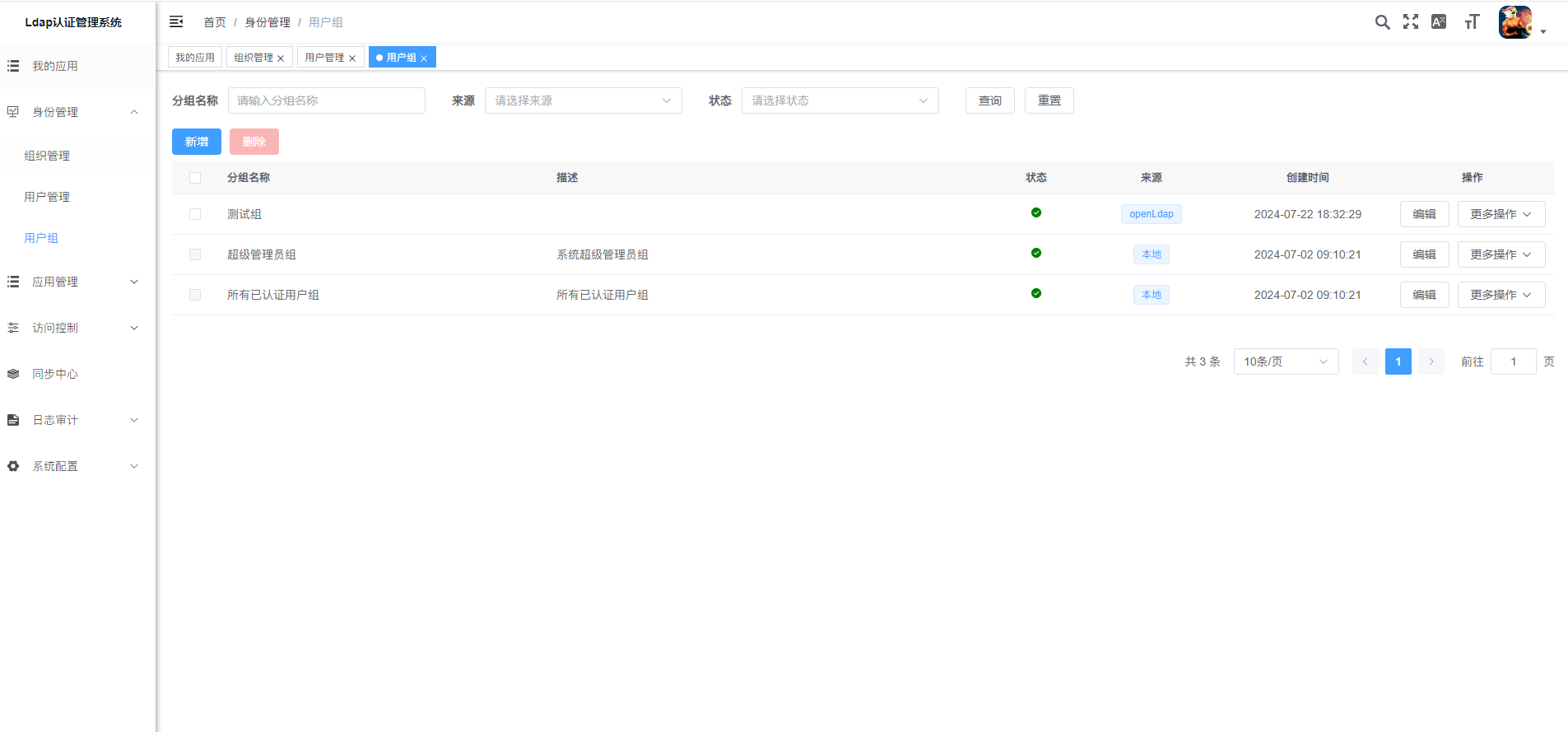
点击“身份管理”下的“组织管理”，用户可以在此界面对组织架构中所有组织或部门进行新增、修改、删除、启用、禁用操作，同时也支持用户通过组织名称查询组织信息。

### 用户管理



点击“身份管理”下的“用户管理”，用户可以在此界面对组织架构中所有用户进行新增、修改、启用、禁用操作，在“更多操作”下拉项中有重置密码和删除按钮，同时也支持用户通过登录账号、姓名和手机号码查询用户信息。

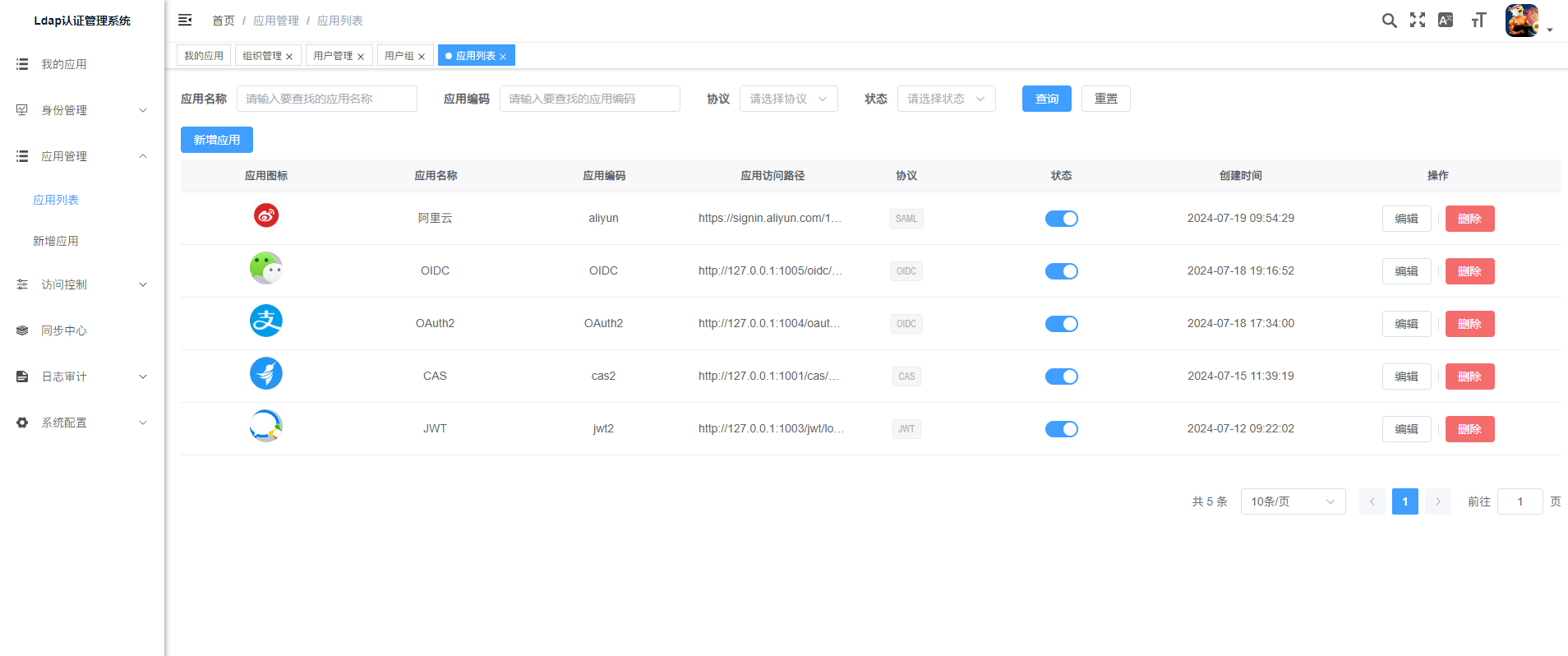
### 用户组



点击“身份管理”下的“用户组”，用户可以在此界面新增、修改、删除用户组，其中“超级管理员组”和“所有已认证用户组”为系统用户组，无法进行删除操作。在“更多操作”下，用户可以通过“成员管理”和“菜单权限”分别管理用户组的成员和菜单的访问权限。

## 应用管理

### 应用列表



点击“应用管理”下的“应用列表”，用户可以在此界面修改、删除、启用、禁用应用，同时支持用户通过应用名称、应用编码、协议和状态查询应用。点击“新增应用”时会跳转到“新增应用”界面。

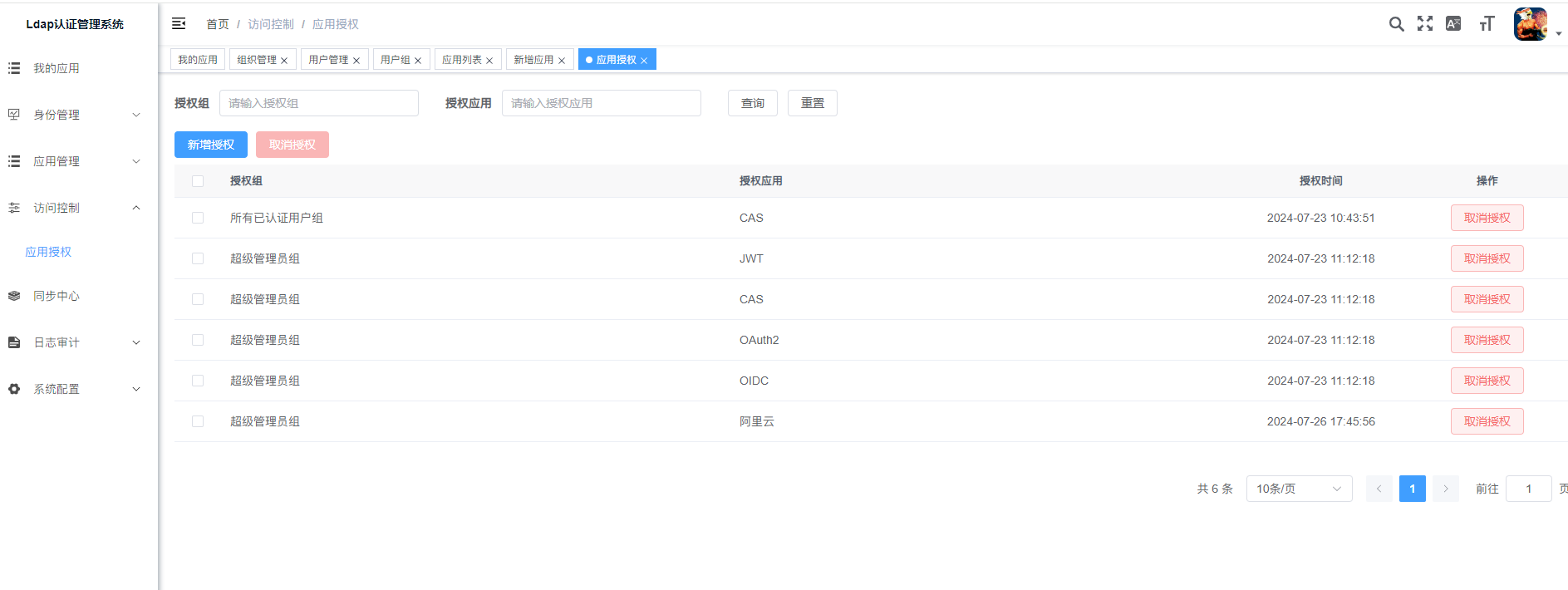
### 新增应用



点击“应用管理”下的“新增应用”，用户可以在此界面新增各种协议的应用。点击“操作”列下的“新增应用”按钮即可打开对应协议的新增模板，用户需要按照模板内容提示完成新增操作。

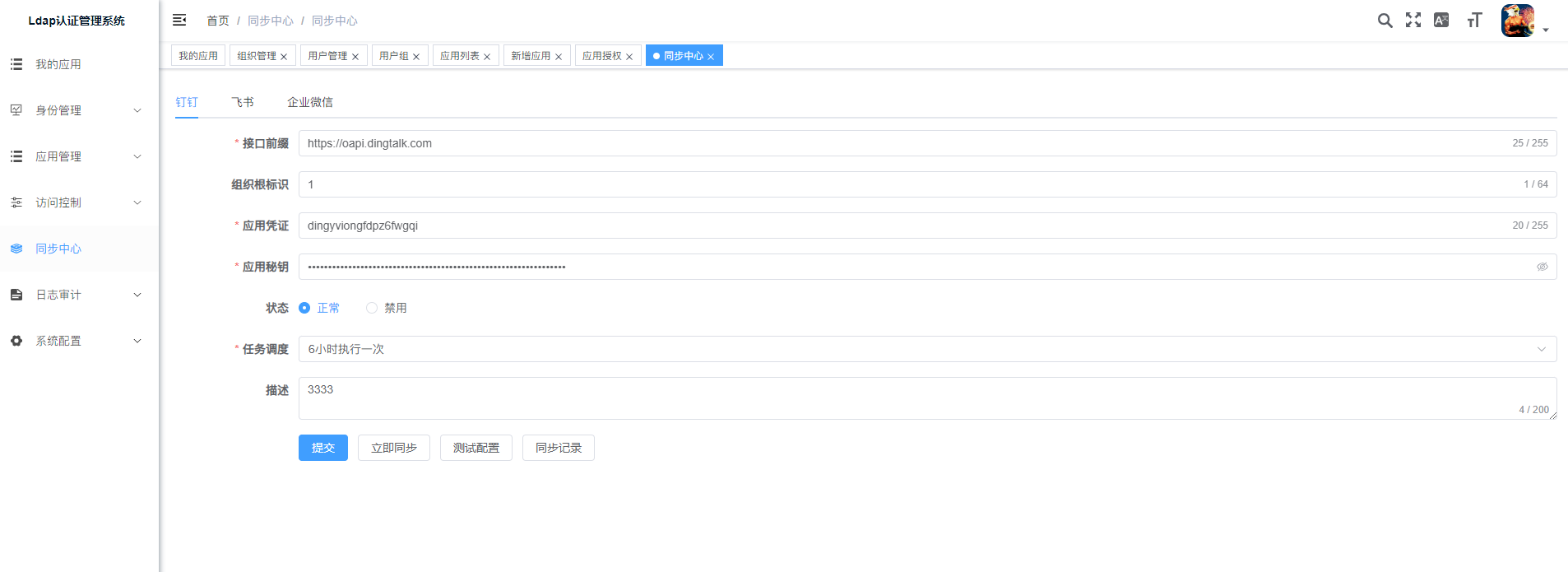
## 访问控制

### 应用授权



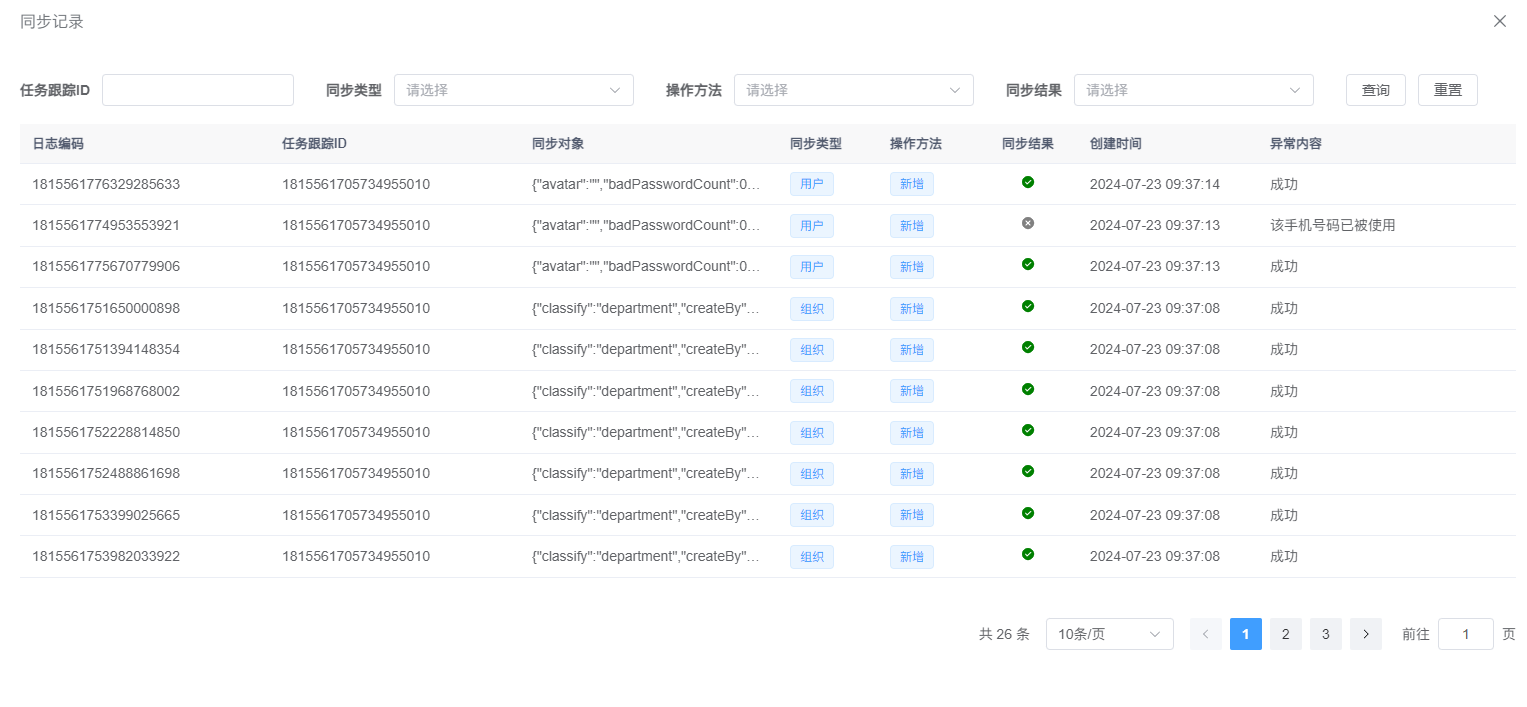
点击“访问控制”下的“应用授权”，用户可以在此界面新增或取消用户组的应用授权，同时也支持用户通过组名称和应用名称查询应用授权信息。为用户组授权应用后，所有处于该用户组的用户都能够在“我的应用”中看到并使用已授权的应用。

## 同步中心



点击“同步中心”，在此界面用户可以管理钉钉、飞书和企业微信的同步配置信息，用户可以通过“测试配置”按钮测试链接是否正常，也可以通过“同步记录”查看数据同步情况。

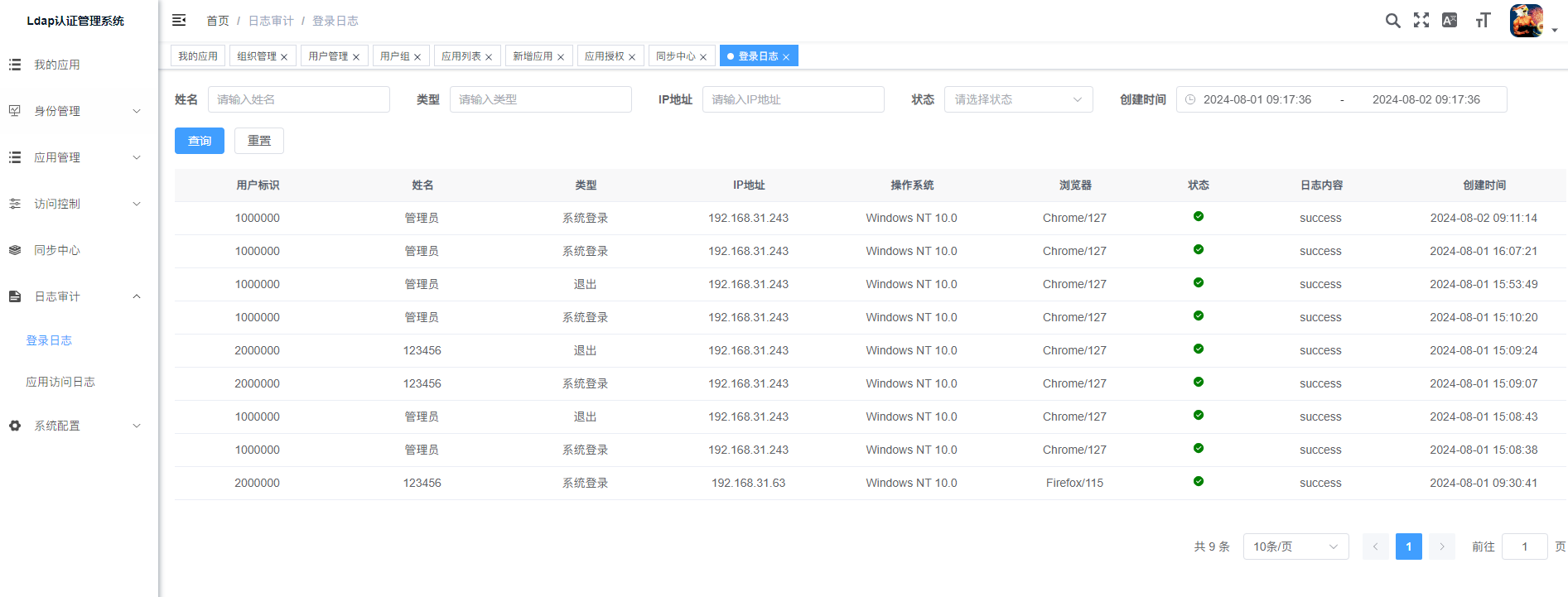
### 同步记录



点击“同步记录”进入当前同步的的日志列表，包含组织机构、用户等，详情字段包含，日志编码、任务跟踪ID，同步对象、同步类型、操作方法、同步结果、同步时间、和异常内容等字段的日志审计。

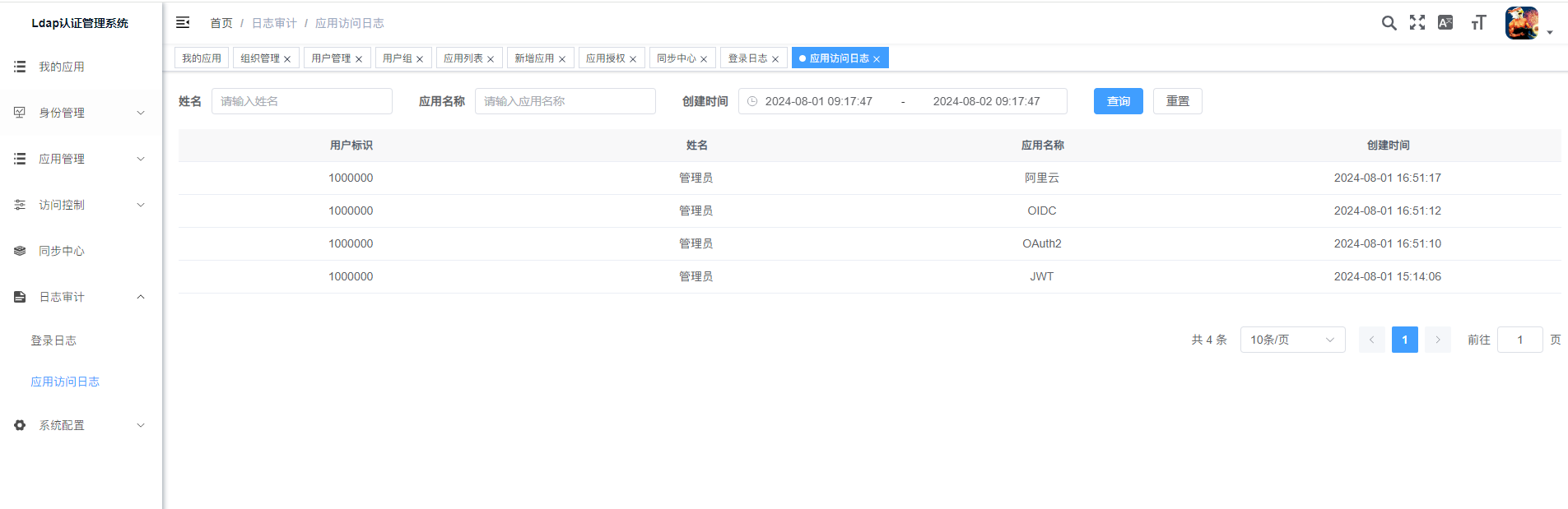
## 日志审计

### 登录日志



点击“日志审计”下的“登录日志”，用户在此界面能够查看到所有用户的登录日志，支持用户通过姓名、类型、IP地址、状态和时间范围查询日志信息。

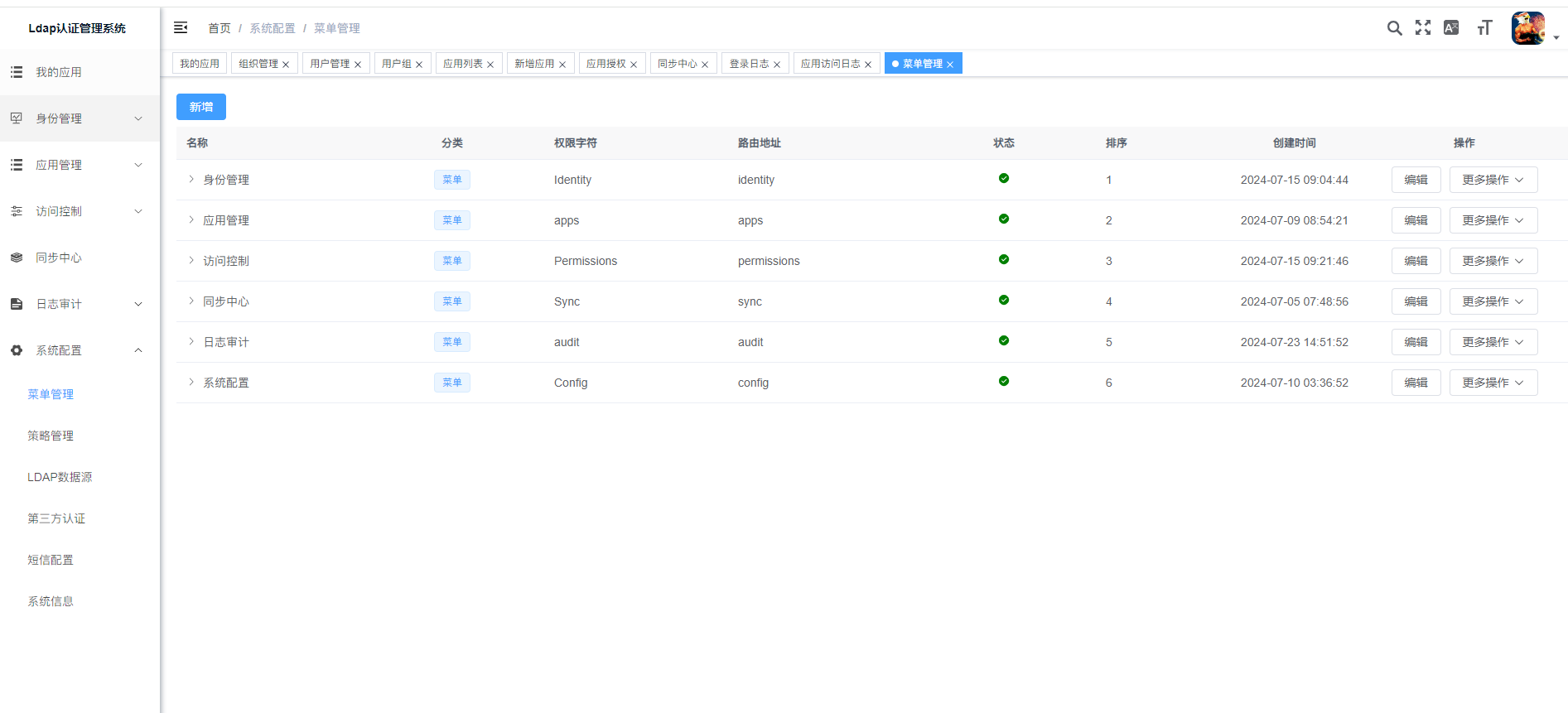
### 应用访问日志



点击“日志审计”下的“应用访问日志”，用户在此界面能够查看到用户访问应用的记录，支持用户通过姓名、应用名称和时间范围查询应用访问日志。

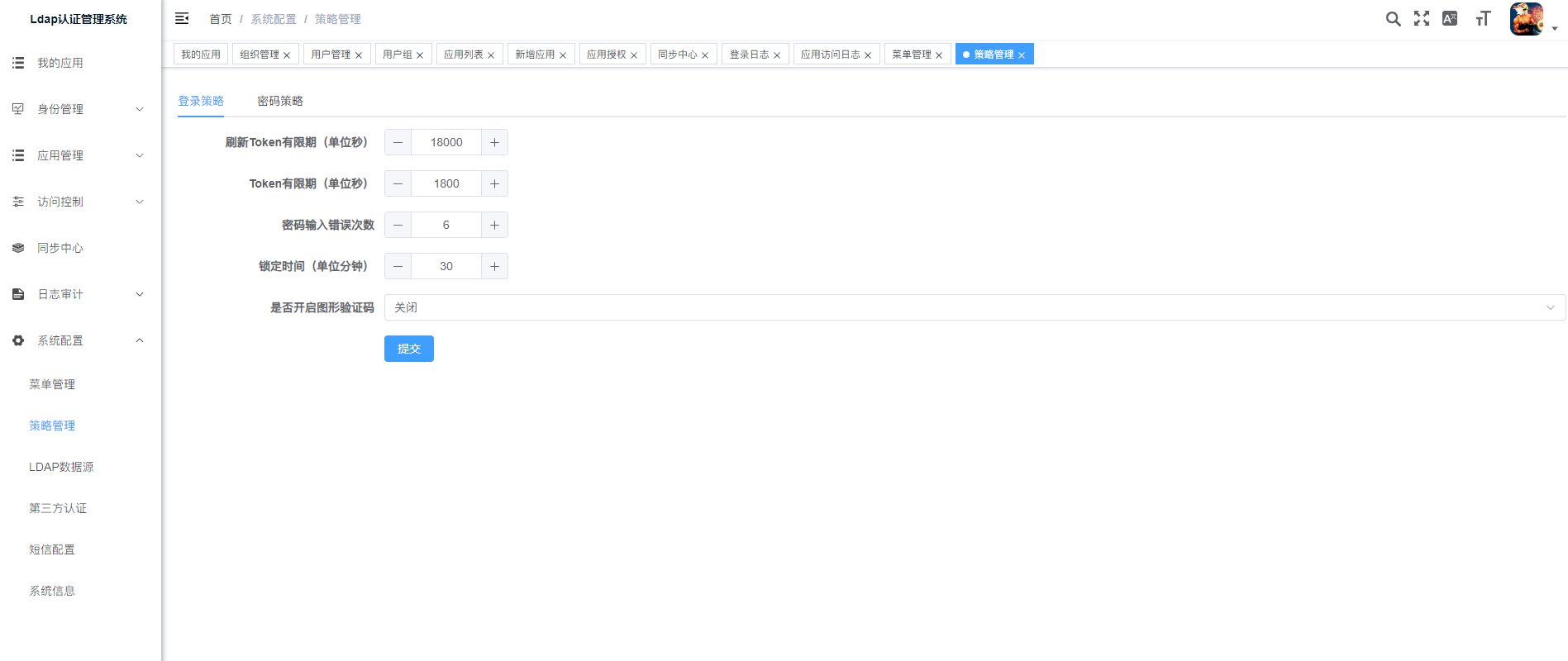
## 系统配置

### 菜单管理



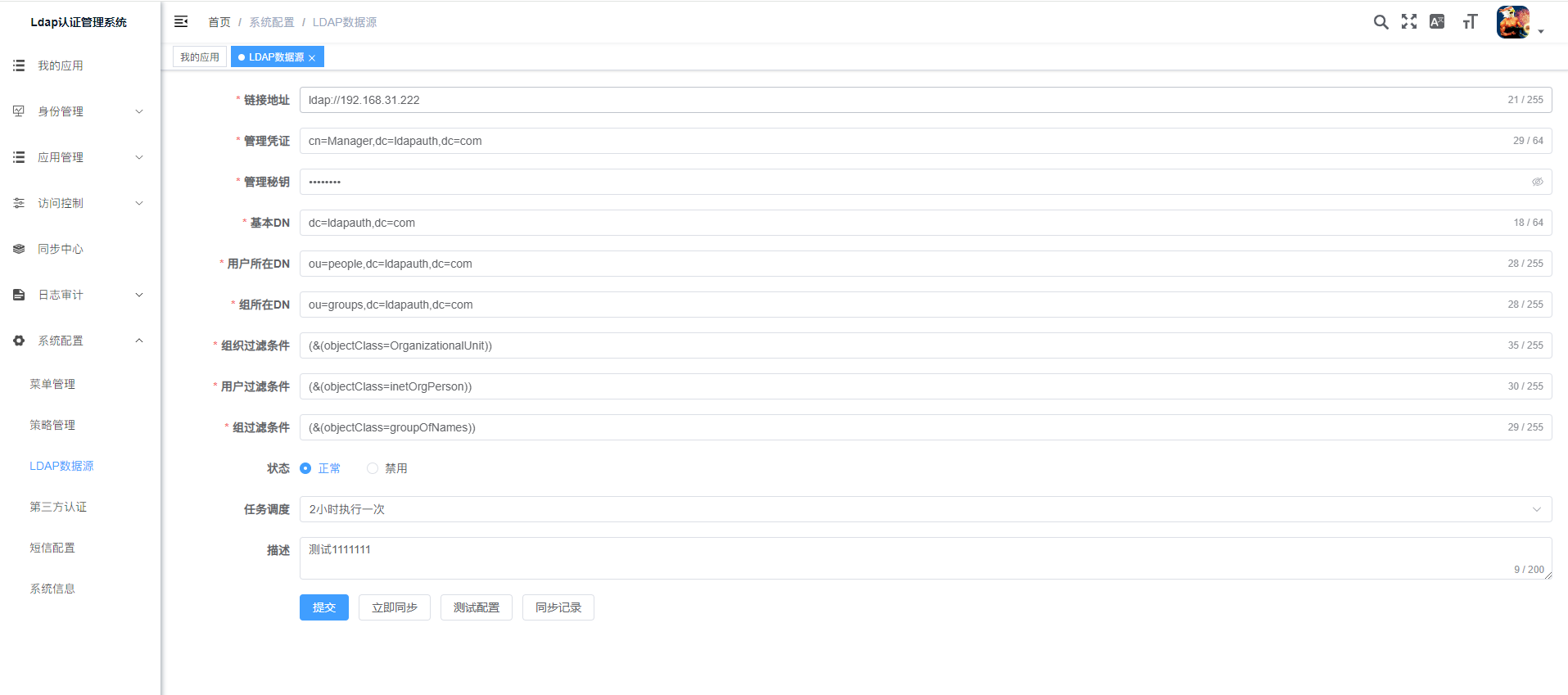
点击“系统配置”下的“菜单管理”，在此界面中用户能够对左侧菜单项的路由进行具体配置，包括新增、修改、删除操作。

### 策略管理



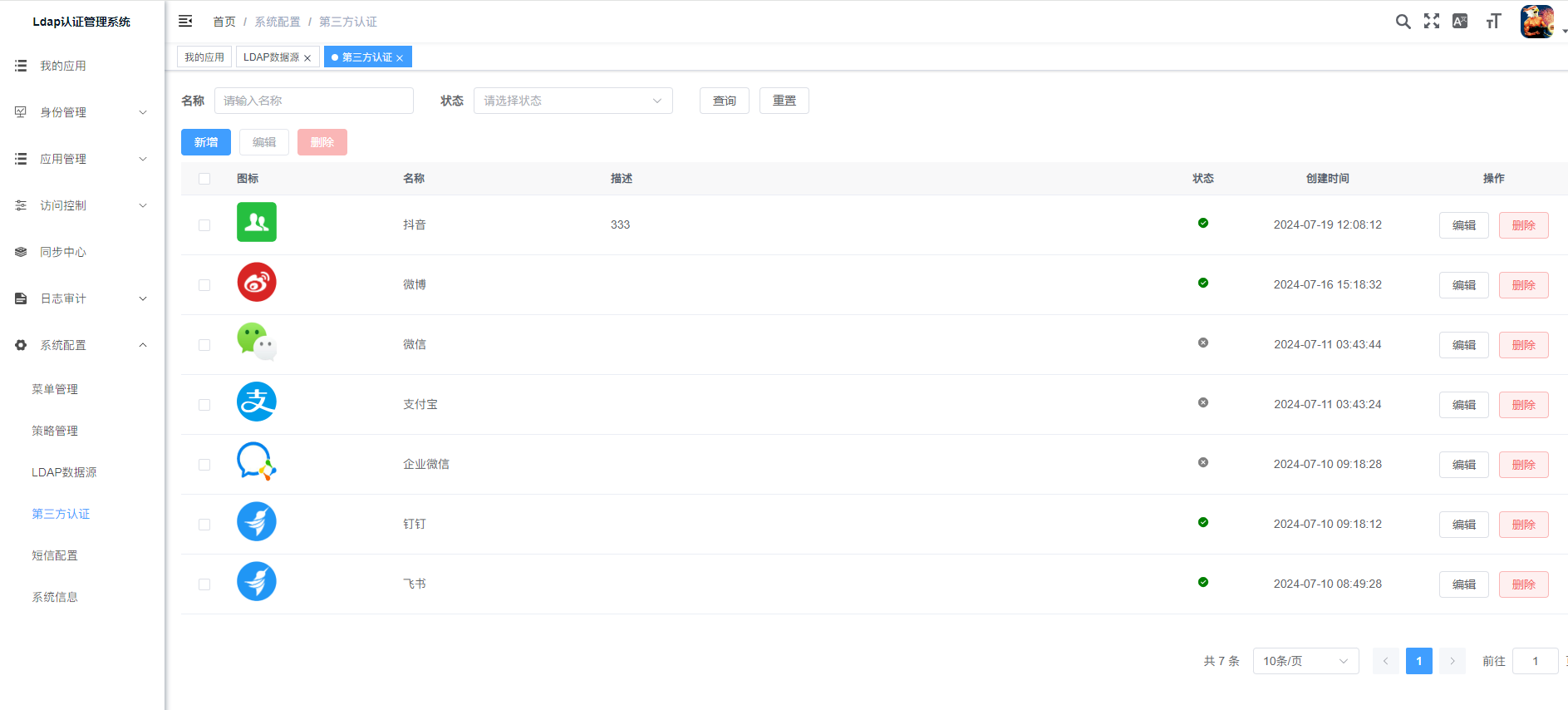
点击“系统配置”下的“策略管理”，在此界面用户能够配置登录策略和密码策略，登录策略和密码策略默认处于开启状态。配置好登录策略或密码策略后，点击“提交”按钮即可使策略生效。

### LDAP数据源



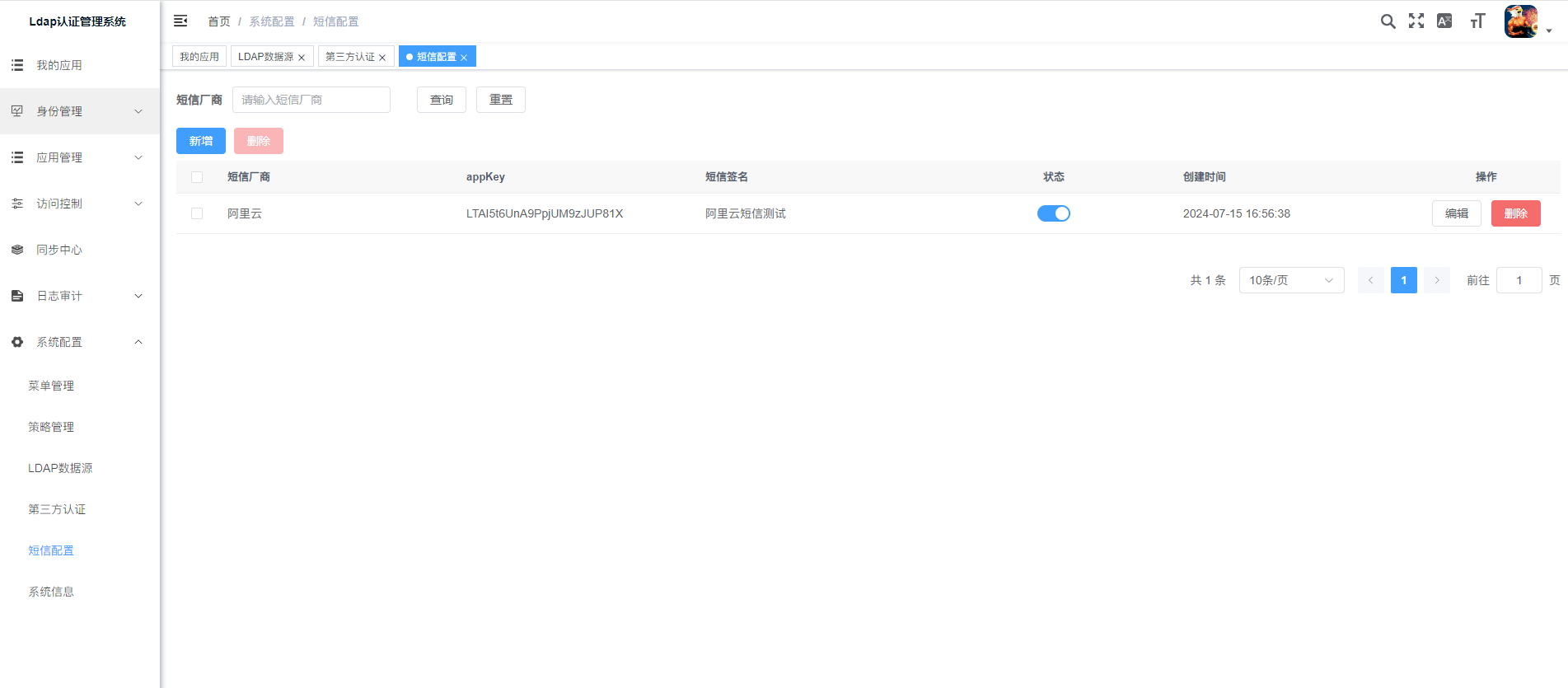
点击“系统配置”下的“LADP数据源”，用户可以在此界面配置本系统的数据源。

### 第三方认证



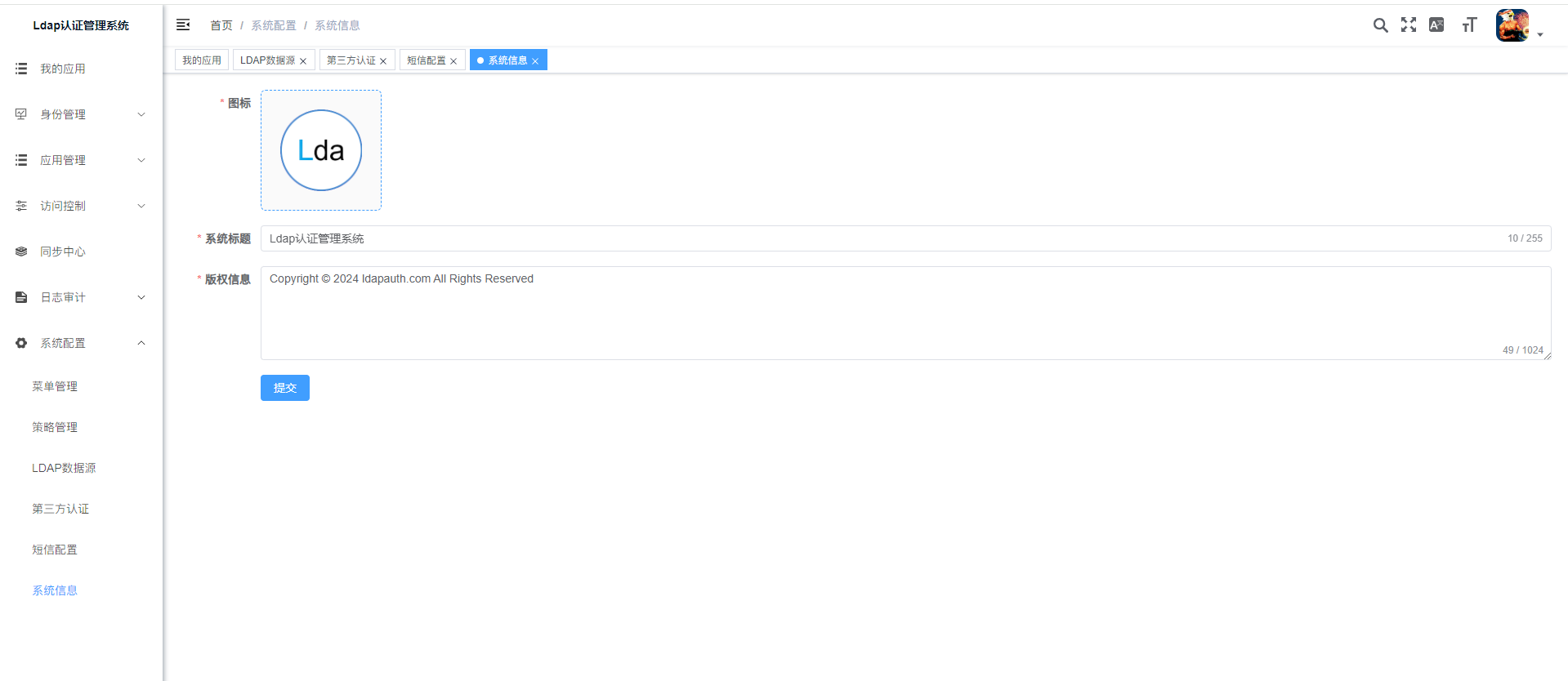
文本点击“系统配置”下的“第三方认证”，用户可以在此界面对第三方认证系统进行管理，支持用户通过名称和状态查询第三方认证系统信息。启用状态的第三方认证系统图标会展示在登录页的“其他方式”标签右侧。用户可以通过第三方认证系统登录本系统。

### 短信配置



点击“系统配置”下的“短信配置”，用户可以在此界面管理本系统的短信配置，同时支持用户通过短信厂商的名称查询配置信息。

### 系统信息



点击“系统配置”下的“系统信息”，管理员可以在本界面配置系统的信息。配置完成后点击“提交”按钮即可进行保存。