## 统一身份认证

### 系统概述

基于学校在信息化身份管理和应用中出现的问题，需要建立统一的认证授权平台来进行应用系统的统一安全管理。

统一身份认证平台为应用系统提供统一的身份管理、认证服务和权限管理，目的是为了减少系统开发的不一致性，减少开发成本和风险，可实现对人员、权限、认证的统一管理，减少人员变化、系统扩展带来的管理复杂度。学校用户角色分类分四大类：学生、教职工、校友、访客。需在用户体验、账户安全性、应用系统开发和维护方面达到如下功能目标：

建设以认证服务为基础的统一用户管理、授权管理和身份认证体系，将组织信息、用户信息统一存储，进行分级授权和集中身份认证，规范应用系统的用户认证方式。提高应用系统的安全性和用户使用的方便性，实现全部应用的单点登录。

### 功能介绍

### 用户端功能清单

|  |  |  |
| --- | --- | --- |
| **功能分类** | **模块名称** | **概述** |
| 登录与激活 | 用户激活 | **说明：传统系统初始化密码通常为比较简单的特定密码或身份证后6位，用户激活机制是解决账号系统初始化密码带来的安全隐患，用户首次使用验证信息后进行手机号绑定和初始化密码设定，以避免弱密码问题和后续用户忘记密码找回对管理员带来的压力。** |
| 1、支持验证用户基本信息； |
| 2、可支持手机号绑定或密保问题设置绑定； |
| 3，支持高强度密码校验； |
| 4，支持5分钟内连续验证错误5次以上，暂停用户验证15分钟，防止撞库；10次错误后，暂停验证1个小时，20次错误后暂停验证24小时； |
| 用户登录 | **说明：支持多终端自适应，支持账号密码、手机动态码、APP扫码登录等多种类型的登录方式。** |
| 1、可支持账号密码登录； |
| 1. 可支持学习通App扫码登录；
 |
| 1. **支持微信和QQ授权登录；**
 |
| 1. 支持三次账号密码登录错误后，加入验证码；
 |
| 1. 支持当天登录失败连续超过15次后对账号采取自动冻结24小时，防止撞库；
 |
| 忘记密码 | **说明：用于用户的账号密码找回。** |
| 1、支持验证用户基本信息； |
| 2、支持绑定手机号二次验证； |
| 3、支持密保问题二次验证； |
| 4、支持高强度密码重设； |
| 5，支持连续验证错误20次后冻结该账号24小时，防止恶意撞库篡改密码； |
| 个人中心 | 基本信息 | 1，支持显示微服务平台用户基本信息：姓名、学工号、角色和所在组织架构； |
| 修改密码 | 1，支持登录后，经过验证修改原密码为高强度密码； |
| 修改绑定手机号/密保问题 | 1，支持登录后，经过验证修改原绑定手机号码； |
| 2，支持登录后，经过验证修改激活时所设置的密码问题提示和答案； |
| 登录地址和IP | 1，支持查看用户最近5次的登录时间； |
| 2，支持查看用户最近5次的登录IP； |
| 3，支持查看用户最近5次的登录IP地址（视运营商和用户网络代理而定）； |

#### 管理端功能清单

|  |  |  |
| --- | --- | --- |
| **功能分类** | **模块名称** | **概述** |
| 统一身份认证管理后台 | 首页与统计 | 1、支持查看全校用户总人数和已激活账号人数； |
| 2、支持查看全校学生角色总人数和已激活账号人数； |
| 3、支持查看全校老师角色总人数和已激活账号人数 |
| 4、支持查看全校校友角色总人数； |
| 5、支持查看最近7天激活人数； |
| 6，支持查看最近1年（每月）激活人数； |
| 7，支持查看最近7天登录人数； |
| 8，支持查看最近1年（每月）登录人数； |
| 9，支持查看已接入统一认证系统的第三方系统的访问次数； |
| 10，支持查看近30天用户异常访问次数（包括登录失败、频繁登录等） |
| 11，支持查看近30天用户访问次数排行； |
| 12，支持查看近30天最后一级部门（例如班级）访问次数排行； |
| 组织架构和用户管理 | 1、支持查看和管理用户组（在校用户、校友和回收站） |
| 2、支持分栏式查看用户和所属组织架构； |
| 3，支持按照字段筛选用户信息； |
| 4，支持单个用户的添加和移除； |
| 5，支持用户的批量添加和批量修改； |
| 6，支持单个用户或用户的批量导出； |
| 7，支持对用户账号临时冻结和恢复； |
| 8，支持用户的移除； |
| 9，支持用户被移除后在回收站保留； |
| 10，支持查看和编辑用户信息； |
| 11，支持查看和编辑部门信息； |
| 12，支持添加下级部门； |
| 13，支持对单个用户查看账号激活时间； |
| 14，支持生成和查看用户导入时文档错误信息； |
| 15，支持重置单个用户的密保问题； |
| 16，支持一键查询单个用户的操作日志记录； |
| 17，支持设置用户的有效时间； |
| 角色管理 | 1、支持自带超级管理员、老师、学生和校友四种默认角色； |
| 2、支持新建、编辑和删除自定义角色； |
| 3、支持自定义角色组； |
| 4、支持对对接系统进行角色授权； |
| 5、支持查看角色对应授权的访问对接系统和授权时间； |
| 授权管理 | 1，支持查看和添加对接的第三方系统； |
| 2，支持编辑已对接的第三方系统； |
| 3，支持对已对接的第三方系统进行临时冻结和恢复； |
| 4，支持对已对接的第三方系统取消访问授权； |
| 5，支持记录第三方对接统一认证系统的时间； |
| 6，支持一键查看对接的第三方系统的访问详情； |
| 7，支持查看对接的第三方系统的总访问次数； |
| **日志管理** | 1，支持查看用户的常见操作日志； |
| 2，支持查看第三方对接系统的访问日志； |
| 3，支持查看管理员在后台操作的日志； |
| 4，支持对操作类型和操作时、对象等进行筛选； |
| 5，支持查看操作人姓名、操作时间、操作IP和操作详情、操作对象等； |
| 6，支持使用操作人姓名和学工号进行日志查询； |
| **高级设置** | 1、支持查看管理员的基本信息； |
| 2、支持管理员自定义登陆方式为学习通账号体系或统一认证账号登陆系统体系； |
| 3、支持管理员自定义切换激活过程使用绑定手机号或设置密保问题； |
| 4、支持管理员查看版本更新时间和更新日志；（需云部署） |
| 5，支持管理员查看当前版本统一身份认证使用手册； |
| 6，支持查看当前版本统一身份认证用户协议和隐私政策； |

### 集成能力

#### 对外服务

认证接口服务为外部应用访问统一身份认证平台提供了高可用性和跨平台的接口通道。通过认证接口可以获得用户身份认证、用户身份数据提取、单点登录等服务，同时可以获得认证服务负责均衡的能力。

身份认证对外提供如下类型接口，分别为：

* 遵循CAS协议，基于HTTP的身份认证接口。
* 遵循SAML1.1协议的可以无缝接入。
* OAuth2.0协议
* LDAP访问接口
* 身份认证支持如下接口语言：
* JAVA，JDK1.4及以上
* .NET2.0及以上
* PHP
* 支持Android、ios手机的登录接入

#### 数据同步

可支持与学校权威数据源进行同步。

支持API、数据视图、中间库等多种方式。