统一身份管理平台

企业目录服务接入规范

目录

[1 引言 2](#_Toc427589737)

[1.1 目的 2](#_Toc427589738)

[1.2 对象 3](#_Toc427589739)

[1.3 术语 3](#_Toc427589740)

[2 OUD数据共享 3](#_Toc427589741)

[2.1 组织架构数据 3](#_Toc427589742)

[2.2 人员数据 4](#_Toc427589743)

[2.3 帐号数据 5](#_Toc427589744)

[3 共享日志 5](#_Toc427589745)

[3.1 读取数据日志接口 6](#_Toc427589746)

[4 SSO接入说明 7](#_Toc427589747)

[4.1 总体设计 7](#_Toc427589748)

[4.2 应用集成 8](#_Toc427589749)

[4.2.1 WebGate部署 8](#_Toc427589750)

[4.2.2 接入应用改造 9](#_Toc427589751)

# 引言

## 目的

本文档旨在提供客户方统一身份认证管理项目系统接入规范的说明。

## 对象

该文档主要读者包括：客户方安全统一身份认证管理平台的系统管理员、系统的设计人员、开发人员、测试人员、各业务系统的管理员及其他项目组成员。

## 术语

|  |  |  |
| --- | --- | --- |
| **缩写** | **术语** | **解释** |
| SSO | Single Sign On | 单点登录 |
| OIM | Oracle Identity Manager | Oracle统一身份管理平台 |
| OAM | Oracle Access Manager | Oracle B/S应用统一访问控制平台 |
| OUD | Oracle Unified Directory | Oracle基于文件的中央目录服务器 |

# OUD数据共享

业务系统与统一身份认证系统进行SSO集成时，组织架构、帐号等信息通过OUD提供统一的LDAPv3接口协议进行数据共享。

## 组织架构数据

* **存储路径**：cn=orgs, dc=smg,dc=com
* **字段描述** :

|  |  |  |
| --- | --- | --- |
| 字段名 | 字段类型 | 描述 |
| OU | String | 组织编码 |
| CN | String | 组织名称 |
| PARENTOU | String | 上级组织编码，PARENTOU=-1标识为最上级 |
| SMGSORT | String | 排序编码 |
| OrgTypeCode | String | 组织类型编码  orgTypeCode=0代表公司  orgTypeCode=1代表部门 |
| |  |  | | --- | --- | | status |  | | String | 数据状态, status=-1时组织为已删除 |
| updateTime | String | 数据最后一次更新时间,以天为单位，存储格式为：  yyyy-MM-dd |

## 人员数据

* **存储路径**：cn=users, dc=smg,dc=com
* **字段描述** :

|  |  |  |
| --- | --- | --- |
| 字段名 | 字段类型 | 描述 |
| uid | String |  |
| cn | String |  |
| positionstatus | String | 状态：status=1代表在职  status=2 代表离职  status=3 代表退休  status=4 代表返聘 |
| locationAddress | String | 工作地点 |
| mobilefromhr | String | 手机号码 |
| position | String | 岗位 |
| gender | String | 性别，gender=0代表男  Gender=1代表女 |
| departmentNumber | String | 归属部门的部门编码 |
| updateTime | String | 数据最后一次更新时间,以天为单位，存储格式为：  yyyy-MM-dd |
| sharelevel | String | 共享级别 |
| superiorid | String | 上级领导 |
| shorttel | String | 座机短号 |
| idno | String | 身份证号 |
| emailfromhr | string | 邮箱 |
| telephonenumber | string | 座机 |

## 帐号数据

* **存储路径**：cn=APP003, cn=apps, dc=smg,dc=com，APP003为应用在统一身份认证系统中分配的应用编号。
* **字段描述** :

|  |  |  |
| --- | --- | --- |
| 字段名 | 字段类型 | 描述 |
| |  |  | | --- | --- | | orclSAMAccountName |  | | String | 业务系统的用户名 |
| OrclAMPWD | String | 业务系统中对应的明文密码，暂时使用 |
| UID | String | 人员工号 |
| STATUS | String | 帐号当前状态，status=1代表正常，status=2代表禁用，status=-1，代表帐号已删除 |
| updateTime | String | 数据最后一次更新时间,以天为单位，存储格式为：  yyyy-MM-dd |

# 共享日志

当业务系统从OUD中读取数据进行数据同步后，需将同步的日志信息记录到统一身份认证平台，供管理员进行审计使用，实现日志记录的方式为统一身份认证平台提供Webservice接口供接入应用调用。

## 读取数据日志接口

* **服务接口名称**：saveReadLog
* **功能描述**：提供给应用记录OUD读取记录的接口，记录应用在OUD中的数据读取时间和最终执行结果；
* **参数说明**：

|  |  |  |
| --- | --- | --- |
| 请求参数 | | |
| 参数名 | 类型 | 描述 |
| APP\_ID | String | 应用的编码，由统一身份认证平台进行定义。 |
| DATA\_TYPE | int | 数据类型，DATA\_TYPE=1，为组织数据  DATA\_TYPE=2, 为帐号数据 |
| READ\_TIME | String | 数据读取时间，时间格式为：  yyyy-MM-dd HH:mm:ss, |
| OPT\_RESULT | int | 数据操作结果，OPT\_RESULT=1执行成功  OPT\_RESULT=2部分执行成功  OPT\_RESULT=3 执行失败  OPT\_RESULT=4 读取失败 |
| 响应返回 | | |
| ResultMsg | String | Xml格式的字符串信息。格式为：  <result>  <code>响应码</code>  <msg>响应码描述</msg>  </result>  备注：具体响应码参考响应码表 |

* **响应码**

|  |  |
| --- | --- |
| 响应码 | 描述 |
| 1 | 成功 |
| 2 | 失败 |

* **参考WSDL**

