统一身份管理平台

账号服务接口规范

目录

[1 引言 2](#_Toc426115507)

[1.1 目的 2](#_Toc426115508)

[1.2 对象 3](#_Toc426115509)

[1.3 术语 3](#_Toc426115510)

[2 应用帐号集成 3](#_Toc426115511)

[2.1 创建帐号接口 4](#_Toc426115512)

[2.2 修改帐号 6](#_Toc426115513)

[2.3 禁用帐号 7](#_Toc426115514)

[2.4 启用帐号 8](#_Toc426115515)

[2.5 删除帐号 8](#_Toc426115516)

[3 SSO接入说明 9](#_Toc426115517)

[3.1 总体设计 9](#_Toc426115518)

[3.2 应用集成 11](#_Toc426115519)

[3.2.1 WebGate部署 12](#_Toc426115520)

[3.2.2 接入应用改造 12](#_Toc426115521)

# 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 |
| WebGate | WebGate | WebGate插件，安装在业务系统应用服务器前端，用于拦截用户访问请求 |

# 应用帐号集成

业务系统参与集成后，用户账户的创建、修改、删除、禁用和启用均由统一身份认证管理系统通过各自业务系统对应的connector进行管理。对于AD、Exchange以及关系型数据库基础的应用系统都有标准的帐号管理接口，可实现这些系统用户账户的全生命周期管理，而对其他没有提供标准接口的业务系统，则需要分别提供以下Web服务接口（最好为WSDL），供身份管理系统集成，实现账户供给：

1. addAccount：创建一个新账号；
2. deleteAccount：删除一个账号；
3. suspendAccount：禁用一个有效账号；
4. restoreAccount：启用一个已禁用的账号；
5. modifyAccount：修改一个账号的可修改属性。
6. modifyPassword：修改一个帐号的密码

注：若业务系统中用户账户没有某个/些操作，则不需要提供对应的Web服务接口，如：业务系统中没有删除账号操作，则不需要提供deleteAccount接口，只需要提供addAccount、suspendAccount、restoreAccount、modifyAccount接口。

原则上各应用系统提供Web Service接口，这些接口表明了该业务系统在维护用户帐号系统时需要哪些用户属性， 在双方进行Web Service的开发与联调过程中可以根据需要调整属性数量；在完成Web Service的联调后，务必遵循以下原则与约束：

1. 业务系统不再提供账号的密码维护功能，如密码修改，密码重置等；
2. 业务系统不再提供账号的管理功能，如账号创建、禁用等。

应用可以根据自己的需要提供出自己的维护帐号接口的WSDL描述文档，但是至少需要有示例中的描述项：**服务接口名称，功能描述，参数说明。**

## 创建帐号

* **服务接口名称**：addAccount
* **功能描述**：提供创建一个新账号的服务，应用接收并解析参数对象，校验请求来源合法性，创建账号并返回处理结果；
* **参数说明**：

|  |  |  |
| --- | --- | --- |
| 请求参数 | | |
| 参数名 | 类型 | 描述 |
| ValidCode | String | 请求校验码 |
| ContentXml | String | Xml格式的字符串信息，格式为：  <account>  <!—可以写多个属性 🡪  <帐号属性>属性值</帐号属性>  </account>  例如：  <account>  <loginName>登录名</loginName>  <email>邮件</email>  </account> |
| 响应返回 | | |
| ResultMsg | String | Xml格式的字符串信息。格式为：  <result>  <code>响应结果码</code>  <msg>响应描述</msg>  </result> |

## 修改帐号

* **服务接口名称**：modifyAccount
* **功能描述**：提供创建一个新账号的服务，应用接收并解析参数对象，校验请求来源合法性，创建账号并返回处理结果；
* **参数说明**：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 请求参数 | | | | |
| 参数名 | 类型 | | 描述 | |
| ValidCode | String | | 请求校验码 | |
| ContentXml | String | | Xml格式的字符串信息，格式为：  <account>  <!—可以写多个属性 🡪  <帐号属性>属性值</帐号属性>  </account>  例如：  <account>  <loginName>登录名</loginName>  <email>邮件 </email>  </account> | |
| 响应返回 | | | | |
| ResultMsg | | String | | Xml格式的字符串信息。格式为：  <result>  <code>响应结果码</code>  <msg>响应描述</msg>  </result> |

## 禁用帐号

* **服务接口名称**：suspendAccount
* **功能描述**：提供创建一个新账号的服务，应用接收并解析参数对象，校验请求来源合法性，创建账号并返回处理结果；
* **参数说明**：

|  |  |  |
| --- | --- | --- |
| 请求参数 | | |
| 参数名 | 类型 | 描述 |
| ValidCode | String | 请求校验码 |
| userId | String | 帐号登录名 |
| 响应返回 | | |
| ResultMsg | String | Xml格式的字符串信息。格式为：  <result>  <code>响应结果码</code>  <msg>响应描述</msg>  </result> |

## 启用帐号

* **服务接口名称**：restoreAccount
* **功能描述**：提供创建一个新账号的服务，应用接收并解析参数对象，校验请求来源合法性，创建账号并返回处理结果；
* **参数说明**：

|  |  |  |
| --- | --- | --- |
| 请求参数 | | |
| 参数名 | 类型 | 描述 |
| ValidCode | String | 请求校验码 |
| userId | String | 帐号登录名 |
| 响应返回 | | |
| ResultMsg | String | Xml格式的字符串信息。格式为：  <result>  <code>响应结果码</code>  <msg>响应描述</msg>  </result> |

## 删除帐号

* **服务接口名称**：deleteAccount
* **功能描述**：提供创建一个新账号的服务，应用接收并解析参数对象，校验请求来源合法性，创建账号并返回处理结果；
* **参数说明**：

|  |  |  |
| --- | --- | --- |
| 请求参数 | | |
| 参数名 | 类型 | 描述 |
| ValidCode | String | 请求校验码 |
| userId | String | 帐号登录名 |
| 响应返回 | | |
| ResultMsg | String | Xml格式的字符串信息。格式为：  <result>  <code>响应结果码</code>  <msg>响应描述</msg>  </result> |

## 修改密码

* **服务接口名称**：modifyPassword
* **功能描述**：提供创建一个新账号的服务，应用接收并解析参数对象，校验请求来源合法性，创建账号并返回处理结果；
* **参数说明**：

|  |  |  |
| --- | --- | --- |
| 请求参数 | | |
| 参数名 | 类型 | 描述 |
| ValidCode | String | 请求校验码 |
| userId | String | 帐号登录名 |
| password | String | 新的密码 |
| 响应返回 | | |
| ResultMsg | String | Xml格式的字符串信息。格式为：  <result>  <code>响应结果码</code>  <msg>响应描述</msg>  </result> |