用户目录（UD）概述 v1.2

UD(User Directory)用户目录，它主要是集中管理公司的组织机构，组及账户，管理员通过设置IDaaS中的组织单位、组及账户，实现用户的统一身份管理。一个用户，一套账户密码，对账户进行统一管理，可以在功能上替代传统的AD 。其中的账户同步是我们提供给开发者一项重要的功能，在保证安全的前提下，可以保证账户数据的一致性，实时性。

本文档默认你已经拥有了开发者权限，并已经阅读了 准备开发 文档。如果需要分配新的开发者权限的话，请联系 IT 管理员进行授权操作。

实现原理

账户同步：
IDaaS平台支持 SCIM 协议，账户同步机制支持两种方式：

1. 推的方式：IDaaS平台通过API将IDaaS中的账户信息同步到应用服务器（即SP Service Provider），需要业务系统提供API，如下图中第1步所示；
2. 送的方式：IDaaS系统提供API，应用服务器（即SP Service Provider）调用IDaaS平台API接口将业务账户信息同步到IDaaS中，如下图中第2步所示：

建议使用第一种方式；
优势：在保证安全的前提下，可以保证账户数据的一致性，实时性；
如果各业务系统（SP）采用第二种方式，IDaaS平台可提供相应技术文档及API接口；

集成流程

SP推至IDaaS

准备

本章节是应用服务器推向IDaaS（即方式2 送）的准备工作。本章节内容需要你已经创建至少一个单点登录SSO应用。如果需要创建无插件式CAS单点登录应用的话，请前往： 无插件式SSO 。如果要创建插件式JWT单点登录应用的话，请前往 插件式SSO。

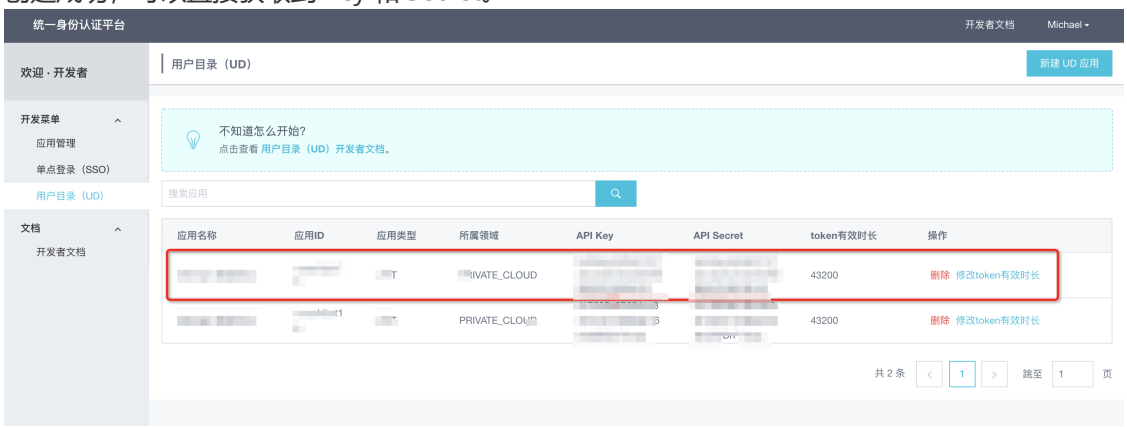
如果你只想使用IDaaS推往应用服务器（即方式1 推）的接口的话请跳过，直接浏览下一章节 IDaaS推至SP。

添加账户同步

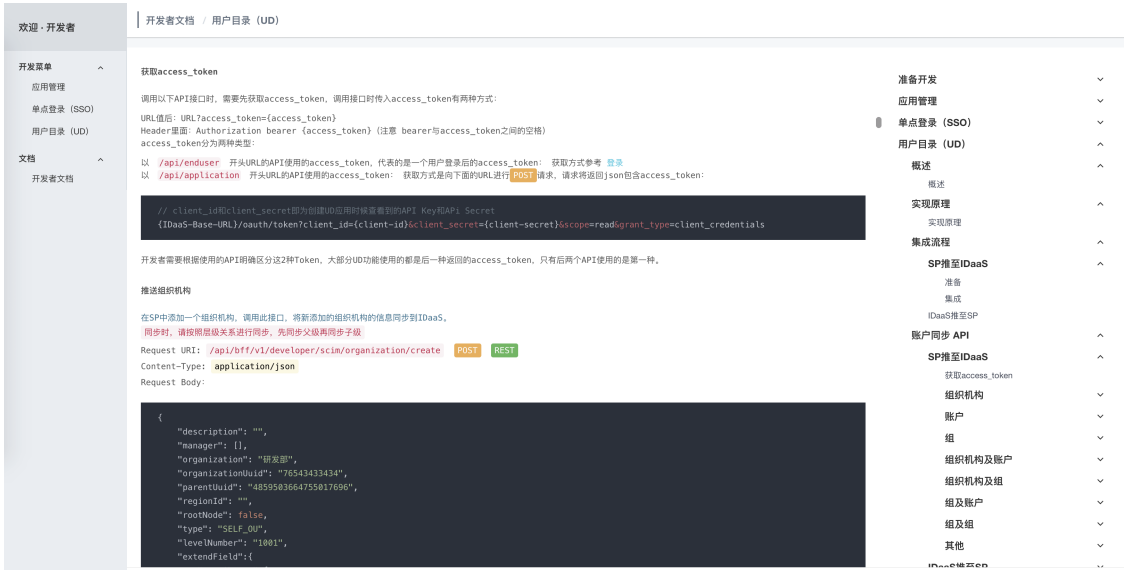
1. 申请完SSO应用后，点击左侧菜单中的用户目录（UD），来到用户同步页面，然后点击右上角-添加用户同步应用。

2. 点击-请选择单点登录(SSO)应用,选择一个我们之前创建的单点登录应用，然后保存。

3. 创建成功，可以直接获取到 Key 和 Secret。



4. 在开发者文档中可以查看到如何使用 Key 和 Secret 获取 access_token，并使用 access_token 调用接口。



集成

IDaaS提供了一系列接口，除了帮助你从你的应用服务器将用户同步到我们的IDaaS平台之外，还可以辅助你实现你自己的单点登录应用管理。

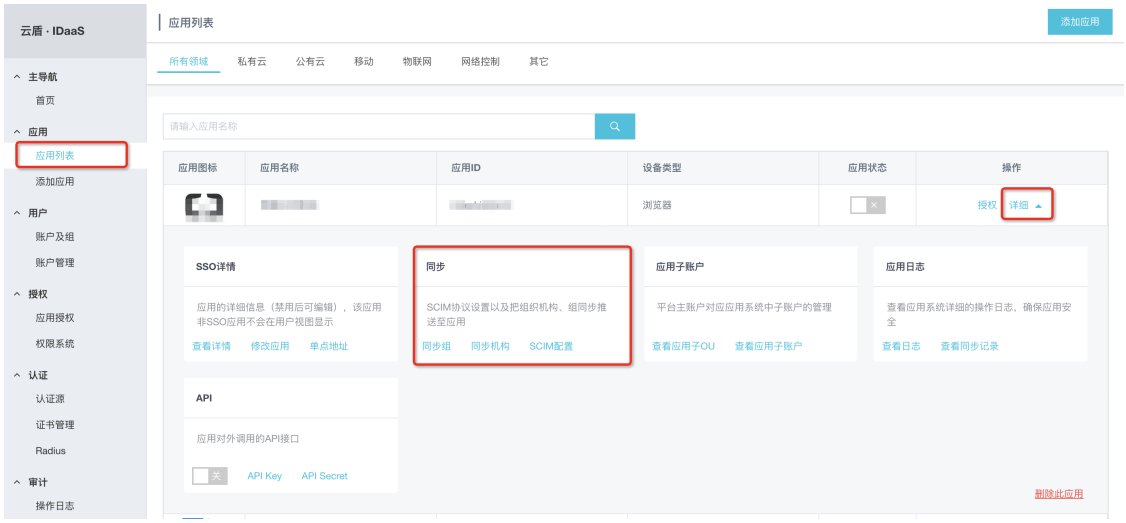
进行用户同步，首先要使用我们的 获取组织单位列表 接口，得到你可以添加到的组织单位列表。然后你需要从上至下，按组织单位到用户组到用户的顺序依次将所有的用户信息和组织结构推送至IDaaS。具体请查看我们的 SP推至IDaaS的API。

IDaaS推至SP

IDaaS推至SP的方式无须创建一个UD实例，只需要在IT管理员界面下为希望推送到的应用配置一些参数，即可实现从IDaaS推送内容到SP，而后SP需要在系统中按照我们给出的接口格式添加3个能接收数据的接口，解析并自行存储。

为应用配置SCIM

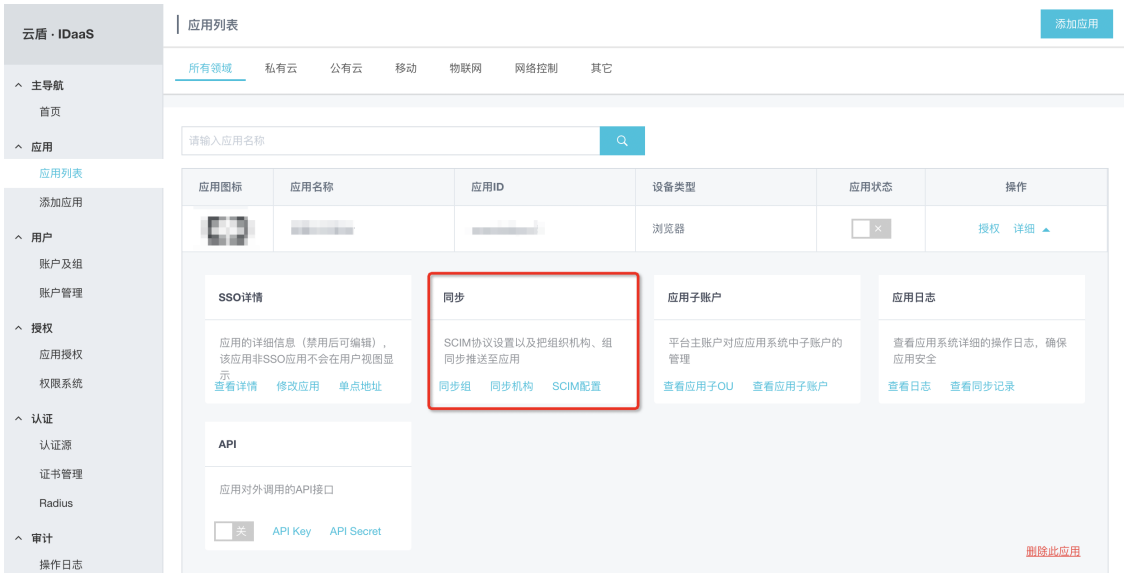
1. 我们需要切换到IT管理员的角色，在左侧菜单中点击应用列表，在希望实现用户同步的应用右侧点开更多，并选择SCIM配置。如图所示：



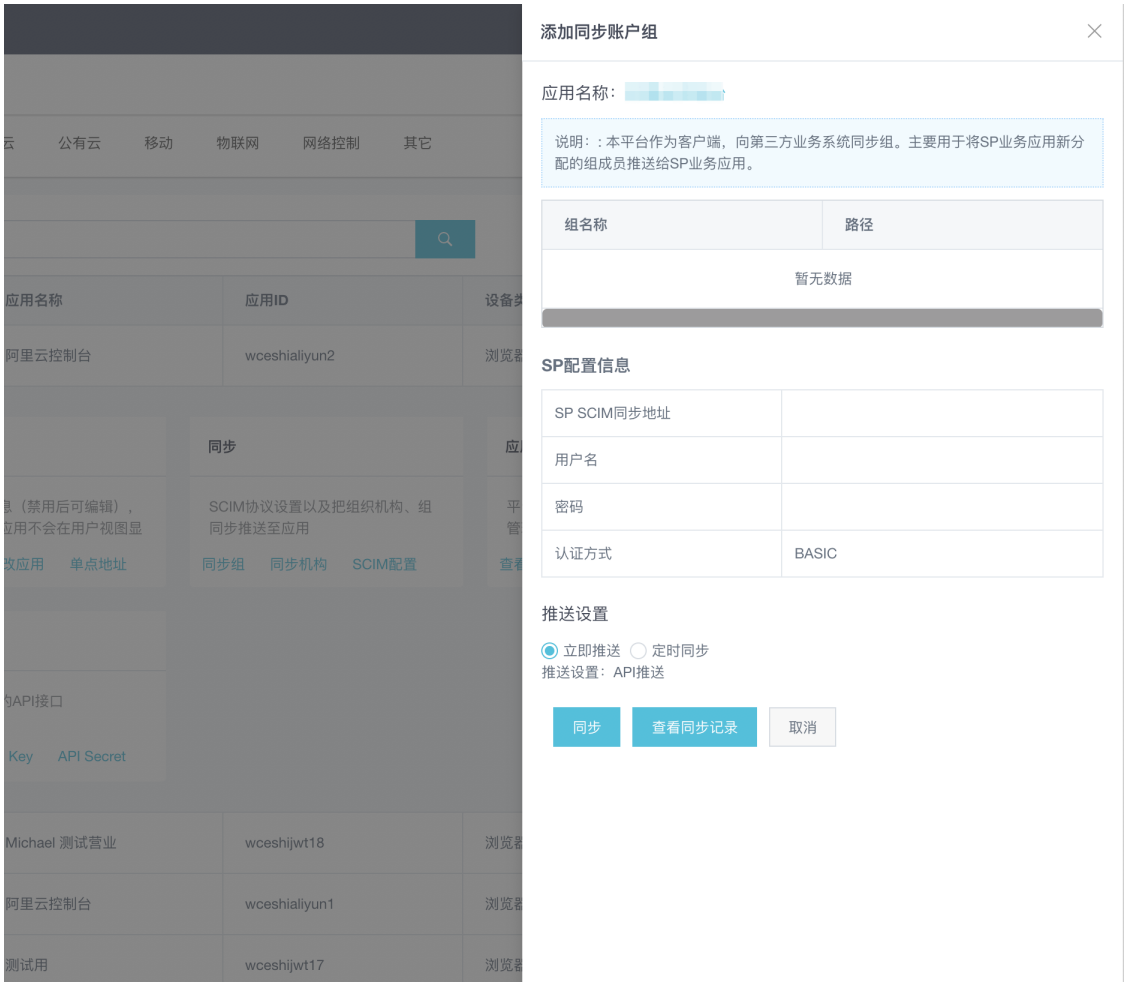
2. 在SCIM配置界面我们可以为账户、账户组和组织单位设置他们的同步地址（即IDaaS向应用服务器SP发送数据的目标位置），请确保账户同步是开启的，并且选择Basic认证方式。你需要在你的

系统中实现这几个接口的Basic认证方式，如下所示：

3. 配置完成后，我们就可以尝试传输用户信息了，回来应用列表页，点开该应用详情，可以看到有同步相关的操作。如下所示：



4. 点击同步。这里会出现一个确认界面，确认无误后即可开始尝试推送，推送的结果会显示在页面的最下方：



IDaaS 推至 SP 的下一步，就是在你的系统中集成接口用来接收用户、用户组和组织机构的信息了，请跳转到 IDaaS 推至 SP 的 API 前往查看接口格式。

账户同步API

文档中的“IDaaS-Base-URL”需要替换为当前访问地址的主域，文中接口地址前也都需要替换主域地址；接口地址中的版本号以当前使用系统版本为准，也可以查看开发者文档中右侧菜单顶部的接口版本。

SP推至IDaaS

IDaaS提供一些UD同步的接口API（所有的API都是遵循SCIM协议的），SP通过调用这些API，可以将数据同步到IDaaS。SP在调用IDaaS接口时，必须传递access_token(具体使用方式请查看获取access_token)。以下，我们将常用的API按照 组织机构，账户，组进行分类。另外，为了满足开发者的需要，我们还提供了更加灵活的API，组织机构及账户，组织机构及组，组及账户，组及组之间的API。

以下是我们的接口列表：

获取access_token

调用以下API接口时，需要先获取access_token，调用接口时传入access_token有两种方式：

- URL值后：URL?access_token={access_token}
- Header里面：Authorization bearer {access_token}（注意 bearer与access_token之间的空格）

access_token分为两种类型：

- 以 `/api/enduser` 开头URL的API使用的access_token，代表的是一个用户登录后的access_token： 获取方式参考 登录

- 以 `/api/application` 开头URL的API使用的access_token： 获取方式是向下面的URL进行POST请求，请求将返回json包含access_token：

```
// client_id和client_secret即为创建UD应用时候查看到的API Key和APi Secret
{IDaaS-Base-URL}/oauth/token?client_id={client-id}&client_secret={client-
secret}&scope=read&grant_type=client_credentials
```

开发者需要根据使用的API明确区分这2种Token，大部分UD功能使用的都是后一种返回的access_token，只有后两个API使用的是第一种。

推送组织机构

在SP中添加一个组织机构，调用此接口，将新添加的组织机构的信息同步到IDaaS。

同步时，请按照层级关系进行同步，先同步父级再同步子级

Request URI: /api/bff/v1.2/developer/scim/organization/create POST REST

Content-Type: application/json

Request Body：

```
{
    "organizationName": "成都研发部",
    "externalId": "123456",
    "parentExternalId": "test3",
    "type": "DEPARTMENT",
    "sortNumber": "3",
    "enabled":true,
    "description": "负责产品研发",
    "extendFields":{
         "test1":"123"
    }
}
```

参数说明：

参数名	参数值	类型	长度	备注
organizationName	{organizationName}	String	>=1	组织机构名称。必填
externalId	{externalId}	String	ou外部id(唯一)	组织机构的唯一id,该id是SP同步过来的，所以在IDaaS中称为外部id,如果不填IDP将随机生成一个外部id。选填
parentExternalId	{parentExternalId}	String	>=1	所属的父级组织机构的唯一id, 该id是SP同步过来的, 所以在IDaaS中称为父级外部id，通过在系统"机构及组"中在组织机构属性中查看参数“外部ID”即可。必填
type	{type}	String	组织机构或部门	自建组织单位：SELF_OU,自建部门：DEPARTMENT，默认为DEPARTMENT.选填
rootNode	{rootNode}	boolean	是否rootNode	如果填true,将更新IDP中原本的根节点。选填
enabled	{enabled}	boolean	账户状态	true:启用，false:禁用，默认为true。选填
sortNumber	{sortNumber}	int	机构排序号	用于展示排序。选填
description	{description}	String	描述信息	用于说明当前OU，不超过500个字符。选填
extendFields	{extendFields}	Map<String,String>	自定义扩展的字段	在IDP数据字典中定义，如果自定义扩展的字段是必填选项，则该属性必填

Response Body：


```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "D326A9EA-119D-4E51-B374-EF2E07B092C6",
    "data": {
        "externalId": "123456",
        "id": "123456"
    }
}
```


succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：externalId:123456重复	请求参数错误
400	InvalidParameter.ExternalId.Exist	例如：外部ID重复，externalId：123456	外部id重复
400	InvalidParameter.Name.Exist	例如：OU名称重复，OrganizationName：研发部	组织机构的名称已存在
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

修改或移动组织机构

在SP中修改一个组织机构，调用此接口，将修改的组织机构的信息同步到IDaaS。

Request URI: /api/bff/v1.2/developer/scim/organization/update PUT REST

Content-Type: application/json

Request Body：

```
{
    "description": "",
    "organizationName": "成都研发部",
    "externalId": "123456",
    "parentExternalId": "test3",
    "enabled":false,
    "type": null,
    "sortNumber": "5",
    "extendFields":{
       "test1":"1235123"
    }
}
```

参数说明：

参数名	参数值	类型	长度	备注
externalId	{externalId}	String	ou外部id(唯一)	组织机构的唯一id,该id是SP同步过来的,在IDaaS中称为外部id。必填
organizationName	{organizationName}	String	>=1	组织机构名称。必填
parentExternalId	{parentExternalId}	String	>=1	所属的父级组织机构的唯一id, 该id是SP同步过来的, 所以在IDaaS中称为父级外部id，通过在系统"机构及组"中在组织机构属性中查看参数“外部ID”即可。必填
type	{type}	String	组织机构或部门	自建组织单位:SELF_OU,自建部门:DEPARTMENT。选填，填写则代表更新该项信息。
enabled	{enabled}	boolan	账户状态	true:启用，false:禁用。选填，填写则代表更新该项信息。
sortNumber	{sortNumber}	int	机构排序号	用于展示排序。选填，填写则代表更新该项信息。
description	{description}	String	描述信息	用于说明当前OU，不超过500个字符。选填，填写则代表更新该项信息。
extendFields	{extendFields}	Map<String,String>	自定义扩展的字段	在IDP数据字典中定义，如果自定义扩展的字段是必填选项，则该属性必填

Response Body:


```
    {
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "D326A9EA-119D-4E51-B374-EF2E07B092C6",
    "data": {
        "externalId": "123456",
        "id": "123456"
    }
}
```


succes代表请求是否成功，code为错误码，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明:

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：描述信息不能超过500个字符	请求参数错误
400	EntityNotFound	例如：组织机构不存在	未查找到要更新的OU
400	InvalidParameter.Name.Exist	例如：OU名称重复，OrganizationName：研发部	组织机构的名称已存在
400	OperationDenied	例如：OU不能移动到自己子级下	不被允许的操作
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

删除组织机构

在SP中删除一个组织机构，调用此接口，在IDaaS中也删除这个组织机构

Request URI: IDaaS提供API地址:/api/bff/v1.2/developer/scim/organization/delete DELETE REST

Content-Type: application/json

参数说明：

参数名	参数值	备注
externalId	{externalId}	应用系统中组织机构的唯一标识，对应IDaaS中的外部id

请求示例：

```
/api/bff/v1.2/developer/scim/organization/delete?externalId=1694618271068407094
```

Response Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "30A38CA4-D640-4CBA-B85F-A0234D0181F1"
}
```

succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	例如：组织机构不存在	未查找到要更新的OU
400	OperationDenied.OUContainsChildren	例如：该OU存在关联关系，不能删除	未查找到要更新的OU
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

查询组织机构

查询单个组织机构

Request URI: IDaaS提供API地址:/api/bff/v1.2/developer/scim/organization/detail GET REST

参数说明：

参数名	参数值	备注
externalId	{externalId}	应用系统中组织机构的唯一标识，对应IDaaS中的外部id

请求示例：

```
/api/bff/v1.2/developer/scim/organization/detail?externalId=1694618271068407094
```

Response Body：


```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "B5D4A6D1-9C51-4AC3-A413-4A27EE1C1474",
    "data": {
        "organizationName": "ceshi导入0009",
        "externalId": "9999",
        "parentExternalId": "764712910283009725",
        "type": "SELF_OU",
        "rootNode": false,
        "sortNumber": 0,
        "enabled": true,
        "description": null,
        "extendFields": {
            "4": "asd"
        }
```

```
    }
}
```

succes代表请求是否成功，code为错误码 ，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	例如：组织机构不存在	未查找到要更新的OU
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

返回参数说明：

参数名	说明
externalId	组织机构的外部id
organizationName	组织机构名称
externalId	组织机构的外部id，和id一样
parentExternalId	父组织机构外部id
type	类型
enabled	账户是否可用
description	描述
extendFields	扩展字段

获取组织机构列表

SP通过调用此接口，可以查看所有的OU或者某OU及其所有子OU的组织机构列表。

Request URL: /api/bff/v1.2/developer/scim/organization/list GET

参数说明：

参数名	参数值	类型	备注
externalId	{externalId}	String	组织单位的外部id(externalId)。选填

- 如果不传值则返回该公司的所有组织机构
- 如果id不为空：则返回该OU下的组织机构的信息

请求示例：

获取该公司的所有组织机构：/api/bff/v1.2/developer/scim/organization/list

获取某个OU下所有组织机构的信息：/api/bff/v1.2/developer/scim/organization/list?id=5986176890912195413

Response Body：


```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "3CCA4939-170C-46AA-BE11-F3DE924FC0E9",
    "data": {"organizations": [
            {
                "organizationName": "成都研发部",
                "externalId": "2858068028015036528",
                "parentExternalId": "129733886490329012",
                "type": "DEPARTMENT",
                "rootNode": false,
                "sortNumber": 0,
                "enabled": true,
                "description": "",
                "extendFields": {}
            },
            {
                "organizationName": "成都分公司",
                "externalId": "129733886490329012",
                "parentExternalId": "6721629573848908864",
                "type": "SELF_OU",
                "rootNode": false,
                "sortNumber": 0,
                "enabled": true,
                "description": "",
                "extendFields": {}
            },
            {
                "organizationName": "测试研发部3-3",
                "externalId": "test3-3",
                "parentExternalId": "test3",
                "type": "DEPARTMENT",
                "rootNode": false,
                "sortNumber": 3,
                "enabled": true,
                "description": "通过SCIM同步组织机构",
                "extendFields": {
                    "test1": "1235123"
                }
            },
            {
                "organizationName": "研发部3-4",
                "externalId": "test3-4",
                "parentExternalId": "test3",
                "type": "DEPARTMENT",
                "rootNode": false,
```

```
                "sortNumber": 3,
                "enabled": true,
                "description": "研发分部",
                "extendFields": {
                    "test1": "123"
                }
            }
            ]
    }
}
```

succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	EntityNotFound	例如：组织机构123456不存在	未查找到externalId对应的OU
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

返回参数说明：

参数名	说明
organizations	返回的组织机构信息
├ externalId	组织机构的外部id
├ organizationName	组织机构名称
├ externalId	组织机构的外部id，和id一样
├ parentExternalId	父组织机构外部id
├ type	类型
├ enabled	账户是否可用
└ description	描述
└ extendFields	扩展字段

获取根节点组织机构信息

获取当前租户的根节点组织机构信息

Request URI: IDaaS提供API地址:/api/bff/v1.2/developer/scim/organization/root GET REST

请求示例：

```
/api/bff/v1.2/developer/scim/organization/root
```

Response Body:


```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "C757F8D6-E96A-4399-823C-E55AED4D59C3",
    "data": {
        "organizationName": "泰斯特技术有限公司",
        "externalId": "6721629573848908864",
        "parentExternalId": null,
        "type": "SELF_OU",
        "rootNode": true,
        "sortNumber": 0,
        "enabled": true,
        "description": "",
        "extendFields": {}
    }
}
```


succes代表请求是否成功，code为错误码，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：cannot get current enterpriseUuid（获取不到当前租户信息）	请求参数错误
400	EntityNotFound	例如：cannot get rootOU	未查找根OU
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

返回参数说明：

参数名	说明
externalId	组织机构的外部id
organizationName	组织机构名称
externalId	组织机构的外部id，和id一样
parentExternalId	父组织机构外部id
type	类型
rootNode	是否为根节点
enabled	账户是否可用
description	描述
extendFields	扩展字段

获取组织机构的直属子级

SP通过调用此接口，可以查看指定OU的所有直属子OU。

Request URL: /api/bff/v1.2/developer/scim/organization/children GET

参数说明：

参数名	参数值	类型	备注
externalId	{externalId}	String	组织单位的外部id。必填

- 如果不传值则返回该公司的所有组织机构
- 如果id不为空：则返回该OU下的组织机构的信息

请求示例：

/api/bff/v1.2/developer/scim/organization/children?externalId=1

Response Body：


```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "26AD790D-FB7D-4ED9-B07E-82448C929F88",
    "data": {
        "organizations": [
            {
                "organizationName": "销售部",
                "externalId": "130015784",
                "parentExternalId": "1",
                "type": "DEPARTMENT",
                "rootNode": false,
                "sortNumber": 130015784,
                "enabled": true,
                "description": null,
```

```
                "extendFields": {
                }
            },
            {
                "organizationName": "研发部",
                "externalId": "129387071",
                "parentExternalId": "1",
                "type": "DEPARTMENT",
                "rootNode": false,
                "sortNumber": 129387071,
                "enabled": true,
                "description": null,
                "extendFields": {
                }
            },
            {
                "organizationName": "测试部",
                "externalId": "129083981",
                "parentExternalId": "1",
                "type": "DEPARTMENT",
                "rootNode": false,
                "sortNumber": 129083981,
                "enabled": true,
                "description": null,
                "extendFields": {
                }
            }
        ]
    }
}
```


succes代表请求是否成功，code为错误码，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	例如：组织机构1不存在	未查找到externalId对应的OU
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

返回参数说明：

参数名	说明
organizations	返回的组织机构信息
├ externalId	组织机构的外部id
├ organizationName	组织机构名称
├ externalId	组织机构的外部id，和id一样
├ parentExternalId	父组织机构外部id
├ type	类型
├ enabled	是否可用
└ description	描述
└ extendFields	扩展字段

推送账户

SP中添加一个账户，调用此接口，将新添加的账户的信息同步到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/account/create POST REST

Content-Type: application/json

Request Body:

```
{
    "externalId": "123456",
    "userName": "developer2",
    "displayName": "开发人员3",
    "password": "Jdev@12345",
    "email": "test2@test.com",
    "phoneNumber": "",
    "description": "",
    "belongs": [
        "test1","test2"
        ],
    "extendFields": {
        "test":"123456",
        "test1":"woman"
    }

}
```

参数说明:

参数名	参数值	类型	长度	备注	是否必填
userName	{userName}	String	>=4	云IDaaS平台主账户	必填
password	{password}	String	>=6	云IDaaS平台主账户密码	非必填，若为空，则将使用系统随机密码。
displayName	{displayName}	String	>2且<18	用户的显示名称	必填
externalId	{externalId}	String		用户的唯一id	选填。如果不填，将随机生成一个，并在结果中返回
email	{email}	String		邮箱	和手机号必有一个
phoneNumber	{phoneNumber}	String		手机号，只能一个且唯一	和邮箱必有一个
belongs	{belongs}	String		所属ou的外部id	为OU外部id的集合，必填，具体看请求参数示例
locked	{locked}	boolean		账户是否锁定，ture:锁定账户,false:不锁定账户。锁定账户后将不能登录IDaaS	选填。填写则代表需要更新。

参数名	参数值	类型	长度	备注	是否必填
enabled	{enabled}	boolean		用户启用状态，ture启用,false禁用。禁用账户将不能登录IDaaS	非必填，不填默认启用账户
description	{description}	String		描述信息	选填
expireTime	{expireTime}	String		过期时间。格式:yyyy-MM-dd,例如:2020-01-12	选填
extendFields	{extendFields}	Map<String,String>		自定义扩展的字段,在IDP数据字典中定义。	选填，填写则代表更新该项信息。更新时，如果自定义扩展的字段是必填选项，则该属性必填

Response Body:

失败示例:

```
{
    "success": false,
    "code": "InvalidParameter",
    "message": "密码不符合密码策略 / 邮箱（email）： test@test.com 已经存在 / 所属组织机构(belongs):123456不存在",
    "requestId": "7BA02087-4789-4FA6-A414-45BAC671945E",
    "data": null
}
```

成功示例:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": {
        "externalId": "123456"
    }
}
```

succes代表请求是否成功，code为错误码，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：账户名称不能为空	请求参数错误
400	InvalidParameter.ExternalId.Exist	例如：externalId外部ID重复	外部id重复
400	InvalidParameter.Name.Exist	例如：账户名（username）已经存在	账户名称已经存在
400	InvalidParameter.Name.Exist	例如：账户名（username）已经存在	账户名称已经存在
400	InvalidParameter.DisplayName.Exist	例如：显示名已经存在	显示名已经存在
400	InvalidParameter.Email.Exist	例如：邮箱(email)已被其他账户绑定	邮箱(email)已被其他账户绑定
400	InvalidParameter.PhoneNumber.Exist	例如：手机号(phoneNumber)已被其他账户绑定	手机号(phoneNumber)已被其他账户绑定
400	InvalidParameter.PhoneEmail.AllEmpty	例如：手机号（phoneNumber）和邮箱（email）必须选填一个	手机号（phoneNumber）和邮箱（email）不能全为空
400	EntityNotFound	例如：所属组织机构(belongs):123456不存在	未查找到externalId对应的OU

修改或移动账户

SP中修改一个账户，调用此接口，将修改的账户的信息同步到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/account/update PUT REST

Content-Type: application/json

参数说明：

参数名	参数值	类型	长度	备注	是否必填
userName	{userName}	String	>=4 且 <18	云IDaaS平台主账户	选填，userName和externalId选填一个。
password	{password}	String	>=6	云IDaaS平台主账户密码	选填。填写则代表需要更新。
displayName	{displayName}	String	>2 且 <18	用户的显示名称	选填。填写则代表需要更新。
externalId	{externalId}	String		用户的唯一id	选填，userName和externalId选填一个。
email	{email}	String		邮箱	和手机号必有一个。选填。填写则代表需要更新。
phoneNumber	{phoneNumber}	String		手机号, 只能一个且唯一	和邮箱必有一个。选填。填写则代表需要更新。
belongs	{belongs}	String		所属ou，必须存在	为OU外部id的集合，选填。填写则代表需要更新。具体看请求参数示例
locked	{locked}	boolean		账户是否锁定，ture:锁定账户,false:不锁定账户。锁定账户后将不能登录IDaaS	选填。填写则代表需要更新。
enabled	{enabled}	boolean		用户启用状态，ture启用,false禁用。禁用账户将不能登录 IDaaS	非必填，不填默认启用账户
description	{description}	String		描述信息	选填。填写则代表需要更新。

参数名	参数值	类型	长度	备注	是否必填
expireTime	{expireTime}	String		过期时间。格式: yyyy-MM-dd,例如：2020-01-12	选填。填写则代表需要更新。
extendFields	{extendFields}	Map<String,String>		自定义扩展的字段,在IDP数据字典中定义。	选填，填写则代表更新该项信息。更新时，如果自定义扩展的字段是必填选项，则该属性必填

IDaaS需要的Request Body示例：

```
{
    "externalId": "test-2",
    "userName": "test-2",
    "displayName": "test-3",
     "password": "Jzyt@123456",
     "email": "test2@test2.com",
    "phoneNumber": "18890900900",
     "expireTime": "2117-01-01",
     "description": "123ttt",
     "locked":false,
    "belongs": [
        "test2"
        ],
    "extendFields": {
        "test":"t",
        "test1":"woman123"
    }
}
```

Response Body：

失败示例：

```
{
    "success": false,
    "code": "InvalidParameter",
    "message": "密码不符合密码策略 / 邮箱（email）： test@test.com 已经存在 / 所属组织机构(belongs):123456不存在",
    "requestId": "7BA02087-4789-4FA6-A414-45BAC671945E",
    "data": null
}
```

成功示例：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": null
 }
```

succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：账户名称不能为空	请求参数错误
400	InvalidParameter.ExternalId.Exist	例如：externalId外部ID重复	外部id重复
400	InvalidParameter.Name.Exist	例如：账户名（username）已经存在	账户名称已经存在
400	InvalidParameter.DisplayName.Exist	例如：显示名已经存在	显示名已经存在
400	InvalidParameter.Email.Exist	例如：邮箱(email)已被其他账户绑定	邮箱(email)已被其他账户绑定
400	InvalidParameter.PhoneNumber.Exist	例如：手机号(phoneNumber)已被其他账户绑定	手机号(phoneNumber)已被其他账户绑定
400	InvalidParameter.PhoneEmail.AllEmpty	例如：手机号（phoneNumber）和邮箱（email）必须选填一个	手机号（phoneNumber）和邮箱（email）不能全为空
400	InvalidParameter.ExternalId.NotExist	例如：通过externalId查询不到账户	未查找到externalId对应的账户
400	EntityNotFound	例如：所属组织机构(belongs):123456不存在	未查找到externalId对应的OU

删除账户

在SP中删除一个账户，通过调用此接口，删除IDaaS中该账户信息。

Request URI: /api/bff/v1.2/developer/scim/account/delete DELETE REST

参数说明：

参数名	参数值	备注
externalId	{externalId}	应用系统中的唯一标识，对应IDaaS中的外部id

请求示例：

```
/api/bff/v1.2/developer/scim/account/delete?externalId=4544581305390943066
```

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": null
}
```

succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	EntityNotFound	例如：账户不存在	未查找到要删除的账户
403	OperationDenied	例如：管理员 admin 不能删除	删除操作不被允许

获取账户信息

在SP中通过调用此接口，获取IDaaS中账户列表信息。

Request URI: /api/bff/v1.2/developer/scim/account/detail GET REST

参数说明：

参数名	参数值	备注
externalId	{externalId}	指定账户的外部id,必填

请求示例：

```
/api/bff/v1.2/developer/scim/account/detail?
externalId=123456&access_token=4616b26c-5a90-4b96-a789-73082615978e
```

Response Body:

```
{
    "success": true,
    "code": "200",
```

```
    "message": null,
    "requestId": "278D7B88-6C26-4C7F-90A7-F126CF52F3E1",
    "data": {
        "externalId": "123456",
        "username": "test-2",
        "displayName": "test-3",
        "phoneNumber": "18890900900",
        "email": "test2@test2.com",
        "enabled": true,
        "locked": false,
        "description": "123ttt",
        "extendFields": {
            "test": "t",
            "test1": "woman123"
        },
        "belongs": [
            "test2"
        ]
    }
}
```


succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：外部id(externalId)不能为空	请求参数错误
400	InvalidParameter.ExternalId.NotExist	例如：externalId不存在	未查找到该账户

响应参数说明：

参数名	参数值	备注
externalId	{externalId}	用户的外部id
username	{username}	用户名
displayName	{displayName}	显示名
phoneNumber	{phoneNumber}	手机号
email	{email}	邮箱
locked	{locked}	账号是否锁定,true为锁定,false为未锁定
enabled	{enabled}	账号是否可用,true为启用,false禁用
belongs	{belongs}	账户所属组织机构列表
extendFields	{extendFields}	扩展字段，用于账户保存的自定义字段

获取账户列表

在SP中通过调用此接口，获取IDaaS中账户信息。

Request URI: /api/bff/v1.2/developer/scim/account/enterprise/list_all GET REST

参数说明：

参数名	参数值	备注
ouUuid	{ouUuid}	指定具体组织机构的UUID, 可选
username	{username}	通过账户名称进行过滤, 可选
createStartDate	{createStartDate}	指定账户创建开始日期, 格式: yyyy-MM-dd, 如: 2018-01-01, 可选
createEndDate	{createEndDate}	指定账户创建结束日期, 格式: yyyy-MM-dd, 如: 2018-01-30, 可选
start	{start}	可选，分页开始位置, 默认0
limit	{limit}	可选，分页数据条件限制, 默认20, 最大50

请求示例：

```
/api/bff/v1.2/developer/scim/account/enterprise/list?
ouExternalId=test2&access_token=4616b26c-5a90-4b96-a789-73082615978e
```

Response Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "5709C39A-D53A-4D74-8765-7D763907877B",
    "data": {
        "total": 3,
```

```
        "accounts": [
            {
                "externalId": "3543180585310896590",
                "username": "developer2",
                "displayName": "开发人员3",
                "phoneNumber": "",
                "email": "test2@test.com",
                "enabled": true,
                "locked": false,
                "description": "来自应用{test-developer}的同步",
                "extendFields": {
                    "test": "123456",
                    "test1": "woman"
                },
                "belongs": [
                    "test2",
                    "test1"
                ]
            },
            {
                "externalId": "test-2",
                "username": "test-2",
                "displayName": "test-3",
                "phoneNumber": "18890900900",
                "email": "test2@test2.com",
                "enabled": false,
                "locked": false,
                "description": "123ttt",
                "extendFields": {
                    "test": "t",
                    "test1": "woman123"
                },
                "belongs": [
                    "test2"
                ]
            },
            {
                "externalId": "test-1",
                "username": "test-1",
                "displayName": "test-1",
                "phoneNumber": "",
                "email": "tangyuehan@idsmanager.com",
                "enabled": false,
                "locked": false,
                "description": "来自应用{test-developer}的同步",
                "extendFields": {},
                "belongs": [
                    "test2",
                    "test1"
                ]
            }
        ]
    }
}
```


succes代表请求是否成功，code为错误码， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：Invalid createStartDate	请求参数错误

响应参数说明：

参数名	参数值	备注
externalId	{externalId}	用户的外部id
username	{username}	用户名
phoneNumber	{phoneNumber}	手机号
email	{email}	邮箱
locked	{locked}	账号是否锁定,true为锁定,false为未锁定
enabled	{enabled}	账号是否可用,true为启用,false禁用
belongs	{belongs}	账户所属组织机构列表
extendFields	{extendFields}	扩展字段，用于账户保存的自定义字段

推送账户组

在SP中添加一个组，通过调用此接口，将组的信息推送到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/group/create POST REST

Content-Type: application/json

Request Body：

```
{
    "externalId": "121-11",
    "displayName": "测试同步组11",
    "ouExternalId": "605016592710192945",
    "members": [
        {
            "accountExternalId":"",
            "username":"test1"
        }
    ],
    "extendFields": {
        "test":"123456"
    }
}
```

参数说明：

参数名	参数值	类型	长度	备注
externalId	{externalId}	String	>=1	账户组id,唯一。选填，不填时，系统会随机生成一个，并在结果中返回
displayName	{displayName}	String	>=1	组显示名称。必填
ouExternalId	{ouExternalId}	String	>=43	所属组织单位(OU)的外部ID，必填
description	{description}	String		描述信息，选填
members	{members}	String	>=43	组成员,已经存在的账户外部ID和账户名，accountExternalId是账户外部ID,username是账户名
extendFields	{extendFields}	Map	无	自定义扩展字段，选填

Response Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": {
    "externalId":"123456"
    }
}
```

succes代表请求是否成功，code为错误码，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：组名称不能为空	请求参数错误
400	InvalidParameter.DisplayName.Exist	例如：当前OU下，组名已经存在	显示名已经存在
400	InvalidParameter.ExternalId.Exist	例如：externalId已存在	externalId已存在
400	EntityNotFound	例如：OU不存在	组隶属的OU不存在
403	Forbidden	例如：没有权限操作该组	没有权限操作该组

更新账户组

在SP中更新一个组，通过调用此接口，将组的信息推送到IDaaS中。

Request URI: /api/bff/v1.2/developer/scim/group/update PUT REST

Content-Type: application/json

Request Body:

```
{
    "externalId": "121",
    "description": "tttt测试",
    "displayName": "测试t121",
    "extendFields": {
        "test":"ttt测试"
    }
}
```

参数说明:

参数名	参数值	类型	长度	备注
externalId	{externalId}	String	>=1	账户组id,唯一。必填
displayName	{displayName}	String	>=1	组显示名称。选填，填写时代表更新。
description	{description}	String		描述信息，选填。填写则代表需要更新。
extendFields	{extendFields}	Map	无	自定义扩展字段，选填，填写时代表更新。

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": null
}
```

succes代表请求是否成功，code为错误码，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明:

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：组的externalId参数不能为空	请求参数错误
400	InvalidParameter.DisplayName.Exist	例如：当前OU下，组名已经存在	显示名已经存在
400	InvalidParameter.ExternalId.NotExist	例如：externalId不存在	externalId不存在
403	Forbidden	例如：没有权限操作该组	没有权限操作该组

删除账户组

在SP中删除一个组，通过调用此接口，将IDaaS中的组删除。

Request URI: /api/bff/v1.2/developer/scim/group/delete DELETE REST

Content-Type: application/json

参数说明：

参数名	参数值	备注
externalId	{externalId}	账户组的唯一id, 在IDaaS中称为外部id

IDaaS需要的Request Body示例：

```
/api/application/group?externalId=1694618271068407094
```

Response Body：

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "BF66FA08-E57B-4387-90C0-A72E41307239",
    "data": null
}
```

succes代表请求是否成功，code为错误码，message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：组的externalId参数不能为空	请求参数错误
400	EntityNotFound	例如：查询不到组信息	未查询到组信息
400	OperationDenied.GroupContainsChildren	例如：组有关联成员(如有子成员),不能删除	组有关联成员(如有子成员),不能删除
403	Forbidden	例如：没有权限操作该组	没有权限操作该组

获取应用已经授权的组织机构及账户列表

根据应用的uuid获取直接授权的组织机构及账户的外部id。

Request URI: IDaaS提供API地址:/api/bff/v1.2/developer/scim/application/authorized/list GET REST

Request Body:

```
/api/bff/v1.2/developer/scim/application/authorized/list?
applicationUuid=1694618271068407094
```

参数说明:

参数名	参数值	备注
applicationUuid	{applicationUuid}	IDaas中应用的唯一标识

Response Body:

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "2230CE9E-4674-407C-A006-D29ACD9DADDB",
    "data": {
        "ouExternalIds": [
            "1",
            "129387071",
            "4122068885249961546"
        ],
        "accountExternalIds": [
```

```
            "4484474128951618300",
            "5812895747601718104"
        ]
    }
}}
```

succes代表请求是否成功，code为错误码 ， message为错误信息为接口。

success为true时，代表请求成功，此时code为200，data返回数据。请求失败时，success为false，code为一串语义化的错误码，如：InvalidParameter.ParentOUUuid.NotExist

错误码说明：

HttpCode(请求状态码)	code(错误码)	message(错误信息)	备注
200	200	null	请求成功
400	InvalidParameter	例如：applicationUuid不能为空	请求参数错误
400	EntityNotFound	例如：无效的applicationUuid	通过applicationUuid未找到对应的应用
403	Forbidden	例如：没有权限操作该父OU	没有权限操作

返回参数说明：

参数名	说明
ouExternalIds	已授权的组织机构外部id列表
accountExternalIds	已授权的账户外部id列表

IDaaS推至SP

此同步方式，需要SP提供接口API。IDaaS通过调用这些API将数据同步到SP。其中需要注意的就是这个接口需要业务系统根据我们提供的字段名称和错误返回码来进行开发，此接口的开发需要提供Basic协议或者Oauth协议来保护接口。现在，我们将常用的按照组织机构，账户，组来进行分类.

IDaaS请求SP所有的地址都基于在IT管理员应用处的SCIM配置的地址基础上,以不同的请求方式(POST,PUT,DELETE)请求该地址。

前言

下面的是账户同步的第二种方式，即IDaaS推送到业务系统(SP)中，目前IDaaS仅提供一个给SP添加账户功能，其中需要注意的就是这个接口需要业务系统根据我们提供的字段名称和错误返回码来进行开发。

IDaaS请求SP所有的地址都基于在IT管理员应用处的SCIM配置的地址基础上,以不同的请求方式请求该地址。

IDaaS给SP添加组织机构

IDaaS通过API给业务系统添加一个组织机构。此接口可以与“SP推至IDaaS的推送组织机构接口”共用一个实体类。

Request URI: /api/bff/v1.2/developer/scim/organization POST REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明:

参数名	参数值	备注
organization	{organization}	组织机构的名称
parentUuid	{parentUuid}	所属父级组织机构的uuid或外部ID
rootNode	{rootNode}	是否是根节点
organizationUuid	{organizationUuid}	本组织机构的uuid或外部ID
manager	{manager}	组织机构的管理者,value是管理者账户的外部ID,displayName是用户名,管理者可为空
regionId	{regionId}	组织机构所属的区域id,type为SELF_OU(自建组织机构)时有可能会有值,可为空,type为DEPARTMENT("自建部门")不会出现值
type	{manager}	SELF_OU(自建组织机构)或DEPARTMENT("自建部门")
levelNumber	{levelNumber}	部门排序号
extendField	{extendField}	扩展字典,attributes为系统定义扩展字段

IDaaS需要的Request Body示例:

```
{
    "childrenOuUuid": [],
    "description": "",
    "extendField": {
        "attributes": {
            "ParentID": "ee",
            "dutyuserid": "",
            "OrganizationLevel": "eeee",
            "ouDisplayName": "",
            "ouCode": "123",
            "cRY": "hIght",
            "organizationLine": "eee"
        },
        "description": "",
        "expireTime": ""
    },
    "manager": [],
    "organization": "op",
    "organizationUuid": "1090561725224650754",
    "parentUuid": "4859503664755017696",
    "regionId": "",
    "rootNode": false,
```

```
    "type": "SELF_OU",
    "levelNumber":"1001"
}
```

SP需要返回 Response Body示例：

```
{ "errorNumber": 0, "errors": [] }
```

参数说明：

字段名	错误码	备注
errorNumber,int类型	0	SP返回错误码0,即视为成功
errors,错误信息,String集合类型	400	参数异常

IDaaS给SP修改或移动组织机构

IDaaS通过API给业务系统修改一个组织机构。此接口可以与“SP推至IDaaS的修改或移动组织机构接口”共用一个实体类。

Request URI: /api/bff/v1.2/developer/scim/organization PUT REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明：

参数名	参数值	备注
organization	{organization}	组织机构的名称
parentUuid	{parentUuid}	所属父级组织机构的uuid或外部ID
organizationUuid	{organizationUuid}	本组织机构的uuid或外部ID
manager	{manager}	组织机构的管理者,value是管理者账户的外部ID,displayName是用户名,管理者可为空
regionId	{regionId}	组织机构所属的区域id,type为SELF_OU(自建组织机构)时有可能会有值,可为空,type为DEPARTMENT("自建部门")不会出现值
type	{manager}	SELF_OU(自建组织机构)或DEPARTMENT("自建部门")
levelNumber	{levelNumber}	部门排序号
extendField	{extendField}	扩展字段,attributes为系统定义扩展字段

IDaaS需要的Request Body示例：

```
{
    "childrenOuUuid": [],
    "description": "",
    "extendField": {
```

```
        "attributes": {
            "ParentID": "ee",
            "dutyuserid": "",
            "OrganizationLevel": "eeee",
            "ouDisplayName": "",
            "ouCode": "123",
            "cRY": "hIght",
            "organizationLine": "eee"
        },
        "description": "",
        "expireTime": ""
    },
    "manager": [],
    "organization": "op",
    "organizationUuid": "1090561725224650754",
    "parentUuid": "4859503664755017696",
    "regionId": "",
    "rootNode": false,
    "type": "SELF_OU",
    "levelNumber": "1001"
}
```


SP需要返回 Response Body示例：


```
{ "errorNumber": 0, "errors": [] }
```


参数说明：

字段名	错误码	备注
errorNumber	0	SP返回错误码0,即视为成功
errors,错误信息,String集合类型	400	参数异常

IDaaS给SP删除组织机构

IDaaS通过API给业务系统删除一个组织机构。

Request URI: /api/bff/v1.2/developer/scim/organization DELETE REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明：

参数名	参数值	备注
id	{id}	IDaaS中本组织机构的外部ID，对应应用系统的唯一标识

IDaaS需要的Request Body示例：


```
/api/application/scim/organization?organizationUuid=4544581305390943066
```


SP需要返回 Response Body示例：

```
{ "errorNumber": 0, "errors": [] }
```

参数说明：

字段名	错误码	备注
errorNumber	0	SP返回错误码0,即视为成功
400	参数异常	
errors,错误信息,String集合类型	557	同步删除组织或组时，存在关联的不能删除

IDaaS给SP添加账户

IDaaS通过API给业务系统添加一个新的账户。此接口可以与“SP推至IDaaS的推送账户接口”共用一个实体类。

Request URI: /api/bff/v1.2/developer/scim/account POST REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明：

参数名	参数值	备注
userName	{userName}	云IDaaS平台主账户唯一
id	{id}	用户ID,与外部ID值一样
displayName	{displayName}	用户的显示名称,唯一
emails	{emails}	邮箱
phoneNumbers	{phoneNumbers}	手机号, 只能一个且唯一
externalId	{externalId}	外部ID,唯一,不为空
belongs	{belongs}	为账户指定组织单位
locked	boolean	是否禁用账户，ture禁用账户,false启用账户。禁用账户后将不能登录应用系统
extendField	{extendField}	扩展字段,attributes为系统定义扩展字段

IDaaS需要的Request Body示例：

```
{
    "belongs": [
```

```
        {
            "belongOuUuid": "5088568925399532181",
            "ouDirectory": " /瀚华金融",
            "rootNode": true
        }
    ],
    "displayName": "dedee",
    "emails": [
        {
            "primary": "true",
            "type": "work",
            "value": "de@idsmanager.com"
        }
    ],
    "extendField": {
        "attributes": {
            "workCode": "123456",
            "sex": "woman"},
        "description": "",
        "expireTime": ""
    },
    "externalId": "1684952915216035459",
    "id": "1684952915216035459",
    "password": "",
    "phoneNumbers": [
        {
            "type": "work",
            "value": ""
        }
    ],
    "userName": "dedee"
}
```


SP需要返回 Response Body示例:


```
{ "errorNumber": 0, "errors": [] }
```


参数说明:

字段名	错误码	备注
errorNumber	430	用户已经存在
errors,错误信息,String集合类型	400	参数异常

IDaaS给SP修改或移动账户

IDaaS通过API给业务系统修改一个账户。此接口可以与“SP推至IDaaS的修改或移动账户接口”共用一个实体类。

Request URI: /api/bff/v1.2/developer/scim/account PUT REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明:

参数名	参数值	备注
userName	{userName}	云IDaaS平台主账户唯一
password	{password}	账户密码
id	{id}	修改后的外部id
displayName	{displayName}	修改后的用户显示名称,唯一
emails	{emails}	邮箱
phoneNumbers	{phoneNumbers}	修改后的手机号, 只能一个且唯一
externalId	{externalId}	修改后的外部ID,唯一
belongs	{belongs}	为账户指定组织单位
extendField	{extendField}	扩展字段,attributes为系统定义扩展字段

IDaaS需要的Request Body示例：

```
{
    "belongs": [
        {
            "belongOuUuid": "5088568925399532181",
            "ouDirectory": " /瀚华金融",
            "rootNode": true
        }
    ],
    "displayName": "dedee",
    "emails": [
        {
            "primary": "true",
            "type": "work",
            "value": "de@idsmanager.com"
        }
    ],
    "extendField": {
        "attributes": {
            "workCode": "123456",
            "sex": "woman"
        },
        "description": "",
        "expireTime": ""
    },
    "externalId": "16849529152160354 59",
    "id": "16849529152160354 59",
    "password": "",
    "phoneNumbers": [
        {
            "type": "work",
            "value": ""
        }
    ],
    "userName": "dedee"
}
```

SP需要返回 Response Body示例：

```
{ "errorNumber": 0, "errors": [] }
```

参数说明：

字段名	错误码	备注
errorNumber	0	代表成功
errors,错误信息,String集合类型	400	参数异常

IDaaS给SP删除账户

IDaaS通过API给业务系统删除一个账户。

Request URI: /api/bff/v1.2/developer/scim/account DELETE REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明：

参数名	参数值	备注
id	{id}	IDaaS中本账户的外部ID,对应应用系统的唯一标识

IDaaS需要的Request Body示例：

```
/api/application/scim/account?id=4544581305390943066
```

SP需要返回 Response Body示例：

```
{ "errorNumber": 0, "errors": [] }
```

参数说明：

字段名	错误码	备注
errorNumber	0	SP返回错误码0,即视为成功
errors,错误信息,String集合类型	400	参数异常

IDaaS给SP添加账户组

IDaaS通过API给业务系统添加一个账户组。此接口可以与“SP推至IDaaS的推送账户组接口”共用一个实体类。

Request URI: /api/bff/v1.2/developer/scim/group POST REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明：

参数名	参数值	备注
id	{id}	组的id
displayName	{displayName}	组的名称
ouUuid	{ouUuid}	所属父级组织机构的uuid或外部ID
display	{displayName}	用户的显示名称,唯一
members	{members}	组里的成员,value是成员的外部ID,唯一,display是用户名,成员可为空
belongs	{belongs}	为账户组指定组织单位
extendField	{extendField}	扩展字段,attributes为系统定义扩展字段

IDaaS需要的Request Body示例:

```
{
    "id":"",
    "displayName":"我的新建组",
    "ouUuid":"856585455256525655",
    "belongs":[
        {
            "ouDirectory":"九州/北京",
            "belongOuUuid":"db7ded581e854a8d9782795963122eb1jBu4QSp6hXn",
            "rootNode":false
        }
    ],
    "members":[
        {
            "value":"163ac7bbd3bc4714affa5c518d53a348Q3BtQC0FAFn",
            "display":"abc@idsmanager.com"
        }
    ] ,
    "extendField": {
        "description": "",
        "expireTime": "2117-01-01",
        "attributes":{
            "ReportManagerID":"123456",
            "mana":"woman"
        }
    }
}
```

SP需要返回 Response Body示例:

```
{ "errorNumber": 0, "errors": [] }
```

参数说明:

字段名	错误码	备注
errorNumber	0	SP返回错误码0,即视为成功
errors,错误信息,String集合类型	400	参数异常

IDaaS给SP删除账户组

IDaaS通过API给业务系统删除一个账户组。

Request URI: /api/bff/v1.2/developer/scim/group DELETE REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明:

参数名	参数值	备注
id	{id}	IDaaS中本账户组的外部ID,对应应用系统的唯一标识。唯一

IDaaS需要的Request Body示例:

```
/api/application/scim/group?id=665a46c056bc4445b381d869797cd6dbpHqdqNLe787
```

SP需要返回 Response Body示例:

```
{ "errorNumber": 0, "errors": [] }
```

参数说明:

字段名	错误码	备注
errorNumber	0	SP返回错误码0,即视为成功
errors	400	参数异常

常见问题

Q： 如果两个子系统中存在相同的账户名，同步到IDaaS平台如果处理，如果我本人在两个系统中的账户名不相同，同步到IDaaS又怎么处理?

A： 子业务系统同步到IDaaS中，会带一个唯一标识的参数，我们会根据唯一标识来判断是不是同一个账户，如果是则相互关联起来，如果不是则创建一个新的账户。唯一标识一般用邮箱或手机号。

Q： 账户同步的两种方式是什么？有什么区别?

A： 两种方式:
1）业务系统通过IDaaS提供的基于SCIM协议的接口将账户同步到IDaaS平台;
2）IDaaS平台通过SP提供的接口将在IDaaS中创建的接口同步到SP中;
区别：区别就是谁接收传过来的账户谁提供接口,接口需基于SCIM协议开发，在这里IDaaS已经给了SP需要开锁所用到的接口字段，详情请看上面提供的API接口。