ALIBABA CLOUD

阿里云

应用身份服务 IDaaS

用户指南

文档版本：20230215

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.IT管理员指南 06
1.1. 登录 06
1.2. 应用 06
1.2.1. 同步账户到应用配置 06
1.2.2. 添加应用 08
1.3. 用户 10
1.3.1. 组 10
1.3.2. 组织机构 17
1.3.3. 账户 24
1.3.4. 账户管理 32
1.3.5. 分类管理ABAC 34
1.4. 授权 40
1.4.1. 应用授权 40
1.4.2. 权限系统 43
1.4.3. 权限系统介绍 48
1.5. 认证 51
1.5.1. 认证源 51
1.5.2. 证书管理 51
1.6. 审计 57
1.6.1. 日志 57
1.7. 其他管理 58
1.7.1. 审批中心 58
1.7.2. 向员工发送公告及通知 60
1.7.3. 同步中心 63
1.7.4. 消息管理 69
1.7.5. 会话管理 70

1.7.6. 我的消息 70
1.8. 设置 71
1.8.1. 邮件网关 71
1.8.2. 安全设置 72
1.8.3. 用户自助注册及风险识别 72
1.8.4. 自动同步账户配置 77
1.8.5. 个性化设置 78
2.普通用户指南 79
2.1. 操作导航 79
2.2. 登录 81
2.3. 设置 87

1.IT管理员指南

1.1. 登录

介绍IT管理员如何在开通云盾IDaaS服务后，登录到IDaaS管理平台。

前提条件

已开通云盾IDaaS服务，且实例已完成初始化。

操作步骤

1. 登录云盾IDaaS管理控制台
2. 在**实例列表**中，选择要访问的IDaaS实例，单击其操作列下的**管理**。

执行结果

进入选择的云盾IDaaS实例的**主导航 > 首页**。

1.2. 应用

1.2.1. 同步账户到应用配置

介绍IT管理员如何在云盾IDaaS控制台为企业应用添加账户同步配置。

背景信息

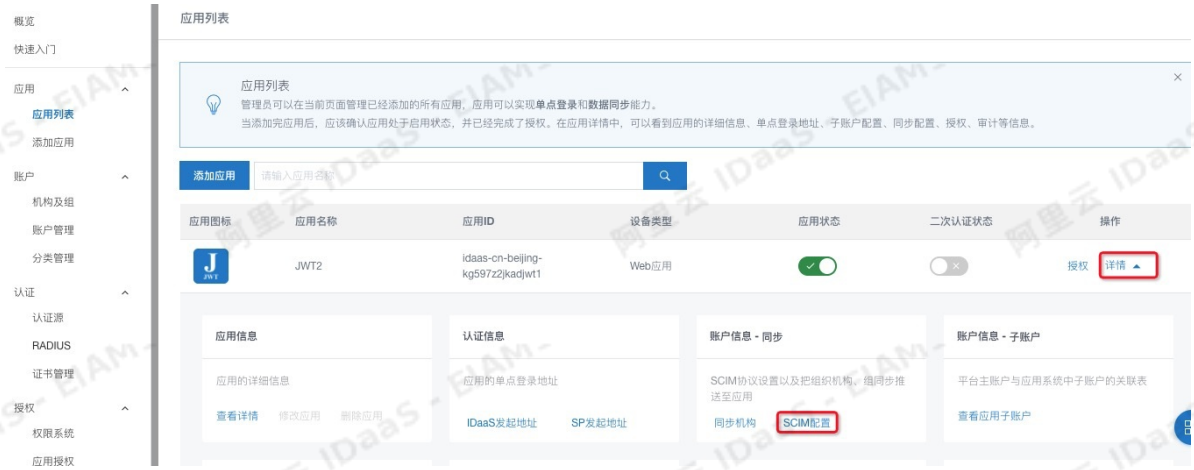
IT管理员在进行由云盾IDaaS平台推送账户至SP应用（业务系统）时，首先进行SCIM配置。

云盾IDaaS平台向SP应用（业务系统）推送账户需要配置并开启账户的SCIM同步，账户组和组织机构同理。若要求云盾IDaaS平台向SP应用（业务系统）既能同步账户也能同步账户组，则需两者都配置并开启SCIM同步。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**应用 > 应用列表**。

3. 定位到要配置同步的应用，单击其操作列下的**详细**。



4. 在**账户信息 - 同步**框中，单击**SCIM配置**。
5. 在**SCIM配置**侧边页，通过页签选择要配置同步对象，并完成以下同步配置。

   支持配置的同步对象包括：**账户**、**组织单位**（本平台作为客户端，向第三方业务系统同步账户）。

配置	描述
应用名称	确认要配置同步的应用。
SCIM同步地址	接收同步账户的接口。例如，http://jzyt.idp-local.com/api/application/cs_multibrowser/scim/account_password。
是否开启	是否开启SCIM同步。开启后，在手动推送组织单位时，会向已授权应用推送组织单位。
协议类型	勾选应用提供的保护接口的协议类型，可选值： ○ **Basic** ○ **OAuth2**
用户名	若使用BASIC协议，输入管理员用户名。
密码	若使用BASIC协议，输入管理员用户名。
oauth url	若使用OAuth2协议，输入OAuth URL。
client_id	若使用OAuth2协议，输入客户端ID。
client_secret	若使用OAuth2协议，输入客户端密钥。

6. 单击**保存**。

1.2.2. 添加应用

介绍IT管理员如何在云盾IDaaS控制台添加第三方应用，集成单点登录。

背景信息

IT管理员可以在云盾IDaaS控制台添加公司使用中的应用系统，为其集成单点登录。添加应用并同步账户信息后，IDaaS账户可以通过IDaaS控制台单点登录到应用系统中。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**应用 > 添加应用**。

> **说明** 您可以通过**全部**、**标准协议**、**定制模板**页签选择要添加的应用类型。

3. 在应用模板列表中选择要添加的应用，单击其操作列下的**添加应用**。

> **说明** 支持使用应用名称搜索应用。

4. 根据要添加应用的具体要求，在添加应用配置对话框完成添加配置。

> **重要** 每个应用需要配置的参数不完全相同，具体以添加应用页面的配置选项为准。

> **说明** 若配置名称旁有红星标识，表示该配置为必填项。

5. 完成配置后，单击**保存提交**。

执行结果

应用添加成功，您可以在**应用>应用列表**中查看新添加的应用。新添加的应用，默认是已启用状态。

下一步

应用授权

1.3. 用户

1.3.1. 组

介绍IT管理员如何在云盾IDaaS控制台管理组，包括新建、编辑、移除/删除等操作。

新建组

您可以在组织机构下添加岗位组，用来同时管理（同步）多个账户或组。一个组下面可以添加其他组或者账户作为成员；组可以将所有成员作为整体进行同步。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**用户 > 机构及组**。
3. 在左侧组织机构树上，右键点击想要创建的组隶属的组织机构，单击**新增 > 组**。

4. 在**新建组**侧边页**组属性**页签下，完成以下配置。

配置	描述
父级	确认组的父级节点。
名称	为组命名。
外部ID	为组设置外部ID。外部ID是组在云盾IDaaS中的唯一身份标识，如不填将由系统自动生成。
描述	为组添加描述信息。

5. 若在数据字典中定义了扩展属性，则在**扩展属性**页签下添加动态扩展属性。

6. 若新建组与已有组存在互斥关系，则在**互斥组**页签下勾选互斥组。

7. 完成配置后，单击**添加**。
8. 在**增量同步**对话框中，依次完成**LDAP同步**、**应用授权**和**SCIM同步**。

添加完成后，新建组显示在其父级组织机构的**组**页签列表中，且默认启用。

编辑组属性

对于已添加的组，您可以随时修改其属性信息，如组名称、组中的账户成员和组成员、互斥组等。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**用户 > 机构及组**。
3. 在左侧组织机构树上，定位到要操作的组隶属的组织机构，单击其名称。
4. 在右侧组织机构信息页，选择**组**页签。
5. 在组列表中，定位到要操作的组，单击其操作列下的**修改**。

6. 在组属性侧边页，参照**新建组步骤4、5、6**编辑组的常规属性，完成后单击**确定**。
7. 分别在**成员（账户）**、**互斥组**页签下查看和维护当前组的子账户、互斥组。
   - 添加成员账户

a. 在**成员（子）**页签下，单击添加成员。

b. 在添加子级成员侧边页，勾选要添加到组的账户。

> **说明** 添加的成员不能是当前组的互斥组的成员。

c. 单击确定。

> **说明** 已添加的成员账户可在**成员（子）**列表中移除。

- 添加互斥组

a. 在**互斥组**页签下，单击**添加互斥组**。

b. 在**添加互斥组**对话框，勾选要添加的互斥组。

c. 单击**确定**。

> **说明** 已添加的互斥组可在**互斥组**列表中移除。

删除组和从组织机构中移除组

对于不再需要的组，您可以将其从组织机构根节点的组列表中删除。删除组之前，必须先移除组中成员；只有组中无成员时，才可以被删除。

对于非根节点下的组，您可以将其从父级组织机构的组列表中移除，解除其与组织机构的隶属关系。从非根节点移除的组可以进一步在根节点下删除。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，选择**用户 > 机构及组**。
3. 根据需要选择删除组或移除组：
   - 删除组
     a. 在左侧组织机构树上，单击组织结构根节点。
     b. 在**组**页签下，通过搜索定位到要删除的组，单击其操作列下的**删除**。

     c. 在**系统提示**对话框中，单击**确定**。

> **说明** 只有当组下无成员时，才可以被直接删除。

     d. 删除组后，在**增量同步**对话框中完成同步。
   - 移除组
     a. 在左侧组织机构树上，定位到要操作的组隶属的组织机构，单击其名称。

b. 在**组**页签下，定位到要移除的组，单击其操作列下的**移除**。

c. 在**系统提示**对话框中，单击**确定**。

1.3.2. 组织机构

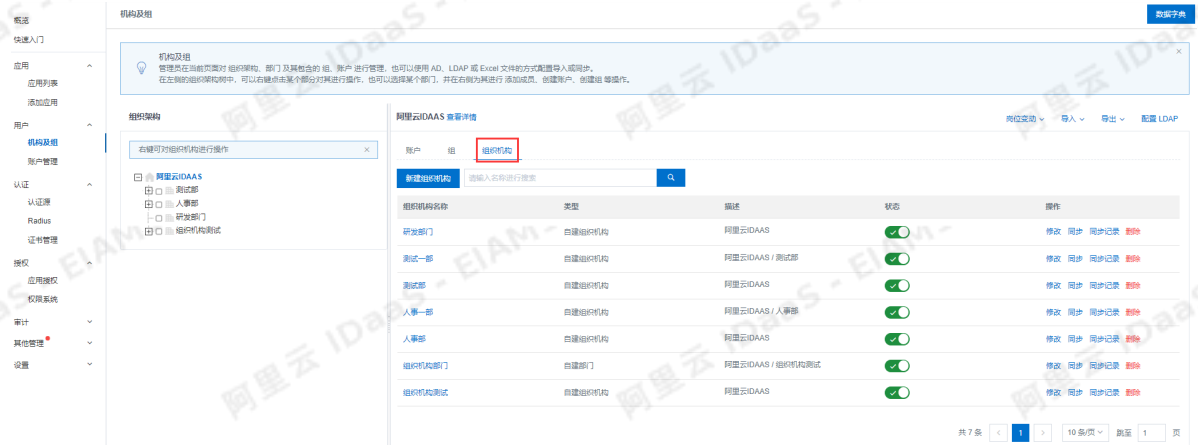
介绍IT管理员如何在云盾IDaaS控制台管理组织机构，包括新建、编辑、禁用/启用、删除等操作。

新建组织机构

您可以在组织机构树根节点（公司）或子节点（现有组织机构）下新建组织机构。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**用户 > 机构及组**。
3. 在左侧组织机构树上，定位到新建组织机构的父节点，单击其名称。
4. 在右侧父节点组织机构信息页面，打开**组织机构**页签，单击**新建组织机构**。



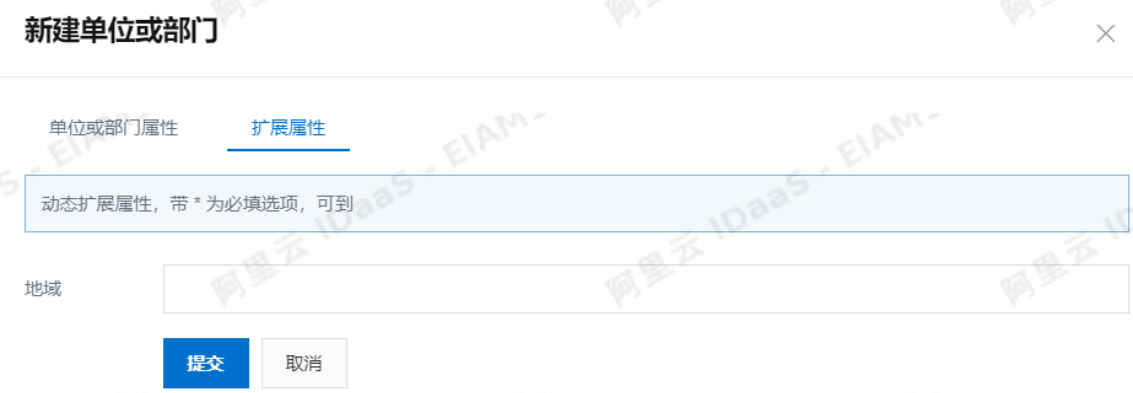
> **说明**
>
> 您也直接在组织机构树上，打开父节点的右键菜单，单击**新增 > 单位或部门**。

5. 在**新建单位或部门**侧边页，单击**单位或部门属性**页签，完成以下配置。

配置	描述
父级	确认该组织机构的父级节点。
类型	选择该组织机构的类型，取值： ○ **组织** ○ **部门** **说明** 组织一般与行政区域相关； 部门一般指职能机构；通常一个组织会分成多个部门。
行政区域	选择行政区域，具体到：省份+市+县区。
名称	为该组织机构命名。
外部ID	设置该组织机构的外部ID。外部ID是组织机构在IDaaS中的唯一标识，传入后不可修改。若不传入该参数，则由IDaaS自动生成。
描述	填写该组织机构的描述信息。

排序号	设置该组织机构在组织机构树同级别对象中的顺序号。
部门主管	部门或组织的管理者，可以通过精确搜索进行添加。 说明 线上版本不支持此功能，如有需要请联系我们。

6. 若在数据词典中定义了扩展属性，单击**扩展属性**页签，添加动态扩展属性。



7. 完成配置后，在新建单位或部门页面，单击**添加**。
8. 在**增量同步**对话框中，依次完成**LDAP同步**、**应用授权**和**SCIM同步**。

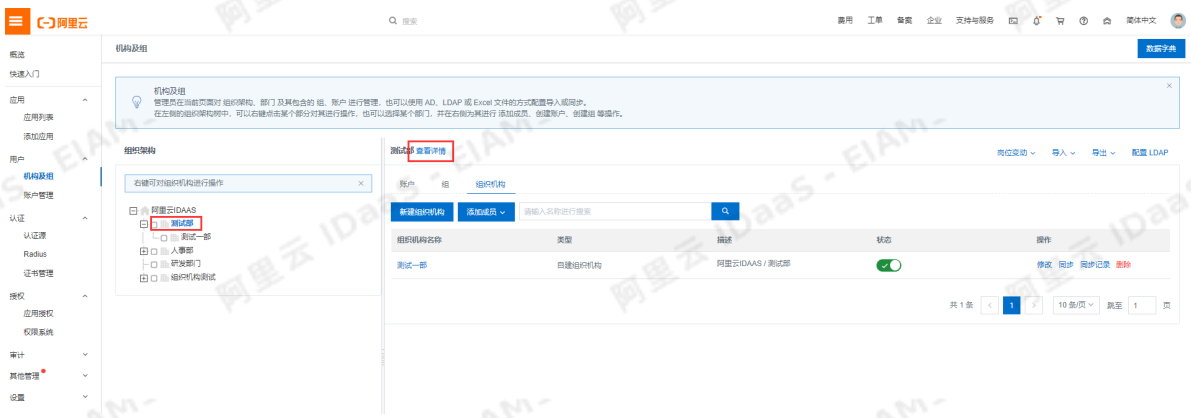
新建组织机构成功，且默认启用。您可以在左侧组织机构树上看到新建的组织机构，也可以在新建组织机构的父节点的**组织机构**页签下查看该组织机构。

编辑组织机构信息

对于已添加的组织机构，您可以随时修改其属性信息。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，选择**用户 > 机构及组**。
3. 在左侧组织机构树上，定位到要修改属性的组织机构节点，单击其名称。
4. 在右侧组织机构信息页面，单击组织机构名称右侧的**查看详情**。



> **说明**
>
> 您也可以直接在组织机构树上，打开要操作的组织机构节点的右键菜单，选择**属性**。
>
> 
>

5. 在**组织机构属性**页签下，参照新建组织机构步骤5和步骤6完成属性配置。
6. 单击**确定**。
7. 在**增量同步**对话框中，依次完成**LDAP同步**、**应用授权**和**SCIM同步**。

禁用/启用组织机构

如果您暂时不想使用某个组织机构，您可以将其禁用。禁用的组织机构不会直接显示在组织机构树中，但可以在其父节点的**组织机构**页签中被重新启用。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，选择**用户 > 机构及组**。
3. 在左侧组织机构树上，定位到要禁用的组织机构的父节点，单击其名称。

> **说明**
>
> 您也可以直接在组织机构树上，打开要操作的组织机构节点的右键菜单，单击**禁用**。这样操作后，直接跳转到步骤6。

4. 在右侧父节点组织机构信息页面，打开**组织机构**页签。
5. 定位到要禁用的组织机构，操作其状态列下的状态开关。

6. 在**系统提示**对话框中，单击**确定**。

已禁用的组织机构，可在父节点**组织机构**页签下查看；操作其状态列下的状态开关，可将其重新启用。

删除组织机构

对于不再需要的组织机构，您可以将其删除。删除一个组织机构时，同时会将其对应的默认组删除掉。只有当一个组织机构下不存在除默认组以外的成员时，您才能将其删除。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，选择**用户 > 机构及组**。
3. 在左侧组织机构树上，定位到要删除的组织机构的父节点，单击其名称。

> **说明**
>
> 您也可以直接在组织机构树上，打开要操作的组织机构节点的右键菜单，单击**删除**。这样操作后，直接跳转到步骤6。

4. 在右侧父节点组织机构信息页面，打开**组织机构**页签。
5. 定位到要删除的组织机构，单击其操作列下的**删除**。

6. 在**系统提示**对话框中，单击**确定**。
7. 在**增量同步**对话框中，依次完成**LDAP同步**、**应用授权**和**SCIM同步**。

1.3.3. 账户

介绍IT管理员如何在云盾IDaaS控制台管理账户，包括新建、编辑、转岗、删除等操作。

新建账户（入职）

新员工入职时，IT管理员需要在IDaaS平台为新员工创建账户。

操作步骤

1. **以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。**
2. 在左侧导航栏，单击**用户 > 机构及组**。

3. 在左侧组织机构树上，定位到新建账户隶属的组织机构，单击其名称。

> **说明** 您也可以直接在组织机构树上，打开新建账户隶属的组织机构的右键菜单，单击**新增** > **账户**。这样操作后，直接跳转到 **步骤5**。

4. 在账户页面，单击**新建账户**。

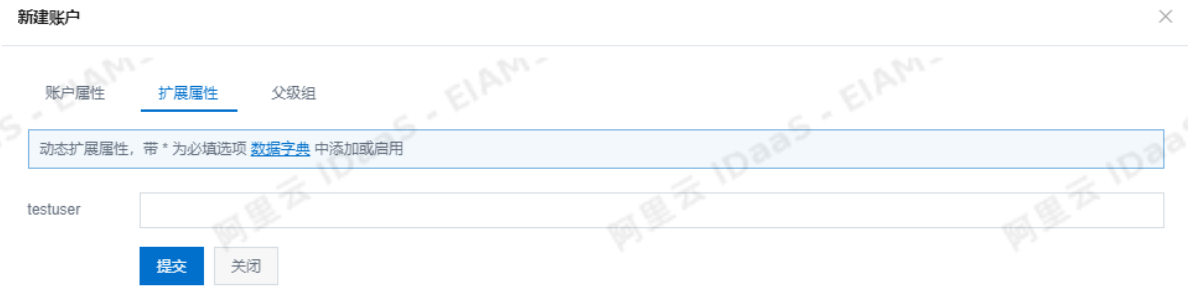
> **说明** 您也可以单击**岗位变动** > **入职**。

5. 在**新建账户**侧边页**主账户属性**页签下，完成以下配置。

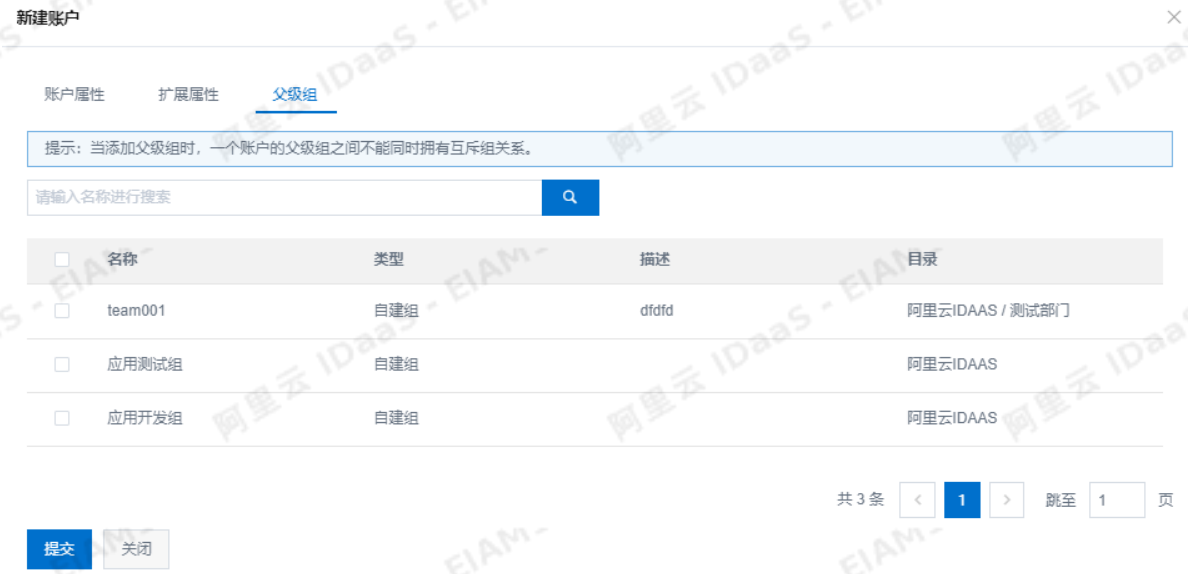
配置	描述
父级	确认账户隶属的父级节点。
显示名称	设置账户的显示名称或昵称。长度限制为2~18位字符。

配置	描述
账户名称	设置账户的登录名称。账户名称允许包含大写字母、小写字母、数字，以及字符“-”、“_”、“.”；长度限制为4~18位。
密码	为账户设置密码。密码必须是大小写字母、数字和特殊符号的组合；长度至少为6位。
邮箱	为账户添加关联邮箱地址。 **说明** 邮箱和手机号至少提供一个。
手机号	为账户添加关联手机号。 **说明** 邮箱和手机号至少提供一个。
外部ID	为账户设置外部ID。外部ID是云盾IDaaS中的唯一身份标识，如不填将由系统自动生成。
过期时间	为账户设置过期时间。不填将使用系统默认过期时间。
备注	填写账户备注信息。

6. 若在数据字典中定义了扩展属性，则在**扩展属性**页签下添加动态扩展属性。



7. 在**父级组**页签下，为账户勾选隶属组。



8. 完成配置后，单击**添加**。
9. 在**增量同步**对话框中，依次完成**LDAP同步**、**应用授权**和**SCIM同步**。

已添加的账户显示在其父节点的**账户**列表中。

编辑账户属性

添加账户后，IT管理员可以随时修改账户属性信息，如显示名称、关联邮箱或手机、过期时间、外部ID、隶属组等。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**用户 > 机构及组**。
3. 在左侧组织机构树上，定位到要操作的账户隶属的组织机构，单击其名称。
4. 在右侧组织机构信息页，单击**账户**页签。
5. 在账户列表中定位到要操作的账户，单击其操作列下的**修改**。

> **说明** 支持使用账户名称或显示名称搜索账户。

6. 在账户属性页，参照 新建账户步骤5、步骤6和步骤7编辑其属性。
7. 完成配置后，单击**确定**。
8. 修改账户属性后，执行账户同步，将最新账户信息同步到已授权当前组织机构的应用中。
   i. 前往账户隶属的组织机构信息页。
   ii. 在**账户**页签下，定位到要操作的账户，单击其操作列下的**账户同步**。

iii. 在**账户同步**侧边页，从已获得授权的第三方系统中，选择用来接收账户同步信息的应用系统。

iv. 单击**同步**。

v. 确认同步记录。

账户转岗

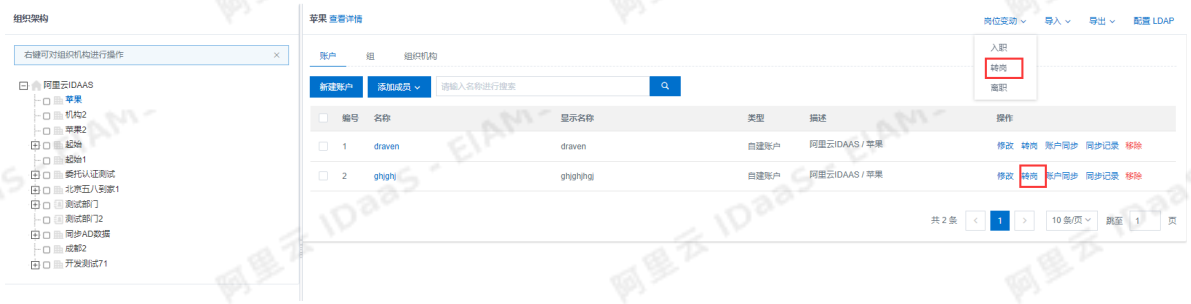
在员工转岗时，IT管理员需要为其账户设置转岗。

操作步骤

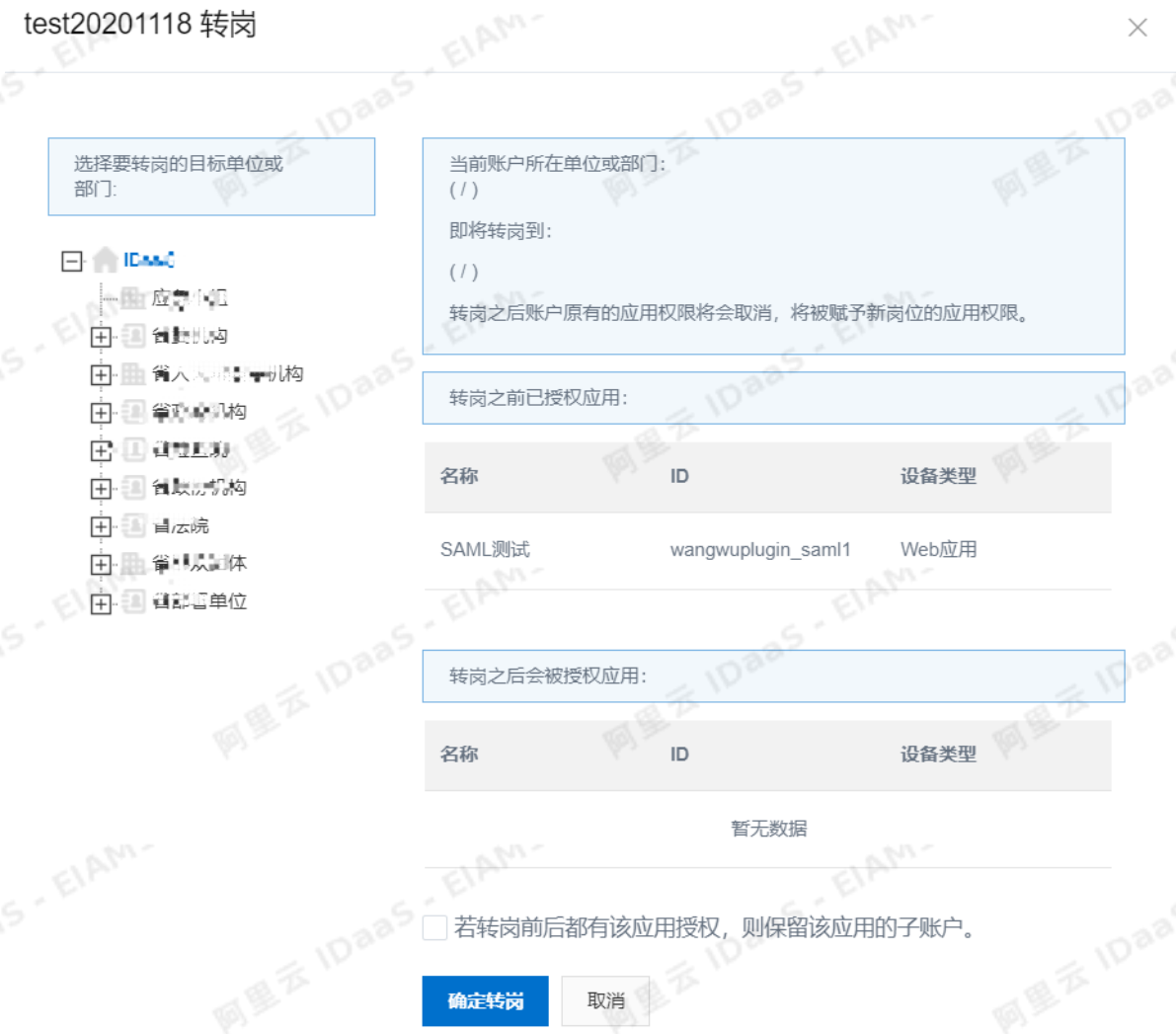
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**用户 > 机构及组**。
3. 在左侧组织机构树上，定位到要操作的账户隶属的组织机构，单击其名称。

> **说明** 您也可以直接在右侧组织机构信息页，单击**岗位变动 > 转岗**，通过搜索找到要转岗的账户，单击**转岗**。这样操作后，直接跳转到**步骤5**。

4. 在右侧组织机构信息页**账户**页签下，定位到要操作的账户，单击其操作列下的**转岗**。



5. 在转岗页面，从左侧组织机构树中选择要转到的目标单位或部门。



6. 确认转岗操作后的授权应用信息，单击**确定转岗**。

删除账户（离职）

在员工离职时，对于不再需要的账户，IT管理员可以将其账户删除。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**用户 > 机构及组**。

3. 在左侧组织机构树上，定位到组织机构树根节点，单击其名称。

> **说明** 您也可以直接在右侧组织机构信息页，单击**岗位变动 > 离职**，通过搜索找到要删除的账户，单击**离职**。这样操作后，直接跳转到**步骤6**。

4. 打开**账户**页签，使用账户名搜索定位到要删除的账户。
5. 单击操作列下的**删除**。

6. 在**系统提示**对话框中，单击**确定**。
7. 在**增量同步**对话框中，依次完成**LDAP同步**、**应用授权**和**SCIM同步**。

1.3.4. 账户管理

介绍IT管理员如何在云盾IDaaS控制台账户管理页面对已添加账户进行统一管理，具体包括查看账户详情、开启/关闭二次认证、重置密码、启用/禁用账户、删除账户。

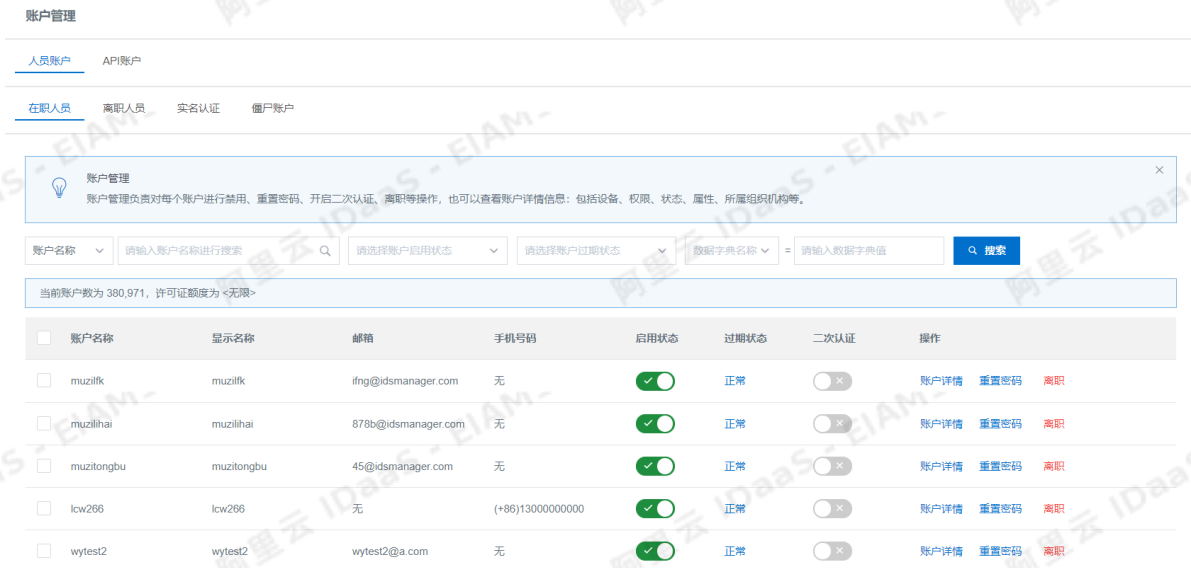
操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**用户 > 账户管理**。
3. 通过页签选择要操作的账户类型：**人员账户**、**API账户**。

> **说明** API账户功能线下版本支持，若有需要请联系我们。

4. 在账户列表中定位到要操作的账户。

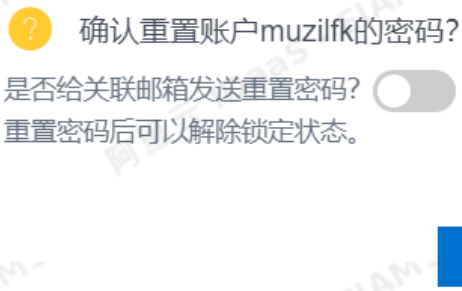
> **说明** 支持使用关联邮箱、关联手机号、账户名称搜索账户。



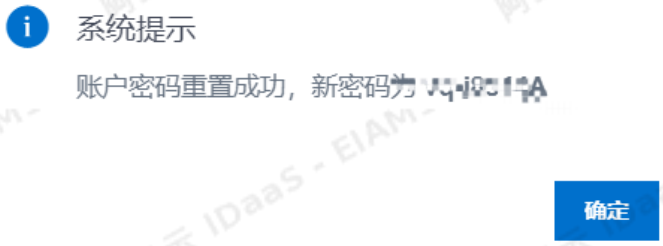
5. 根据需要执行以下操作：
   - 查看账户详情
     a. 单击账户操作列下的**账户详情**。
     b. 在账户管理页面查看当前账户的相关信息，具体包括：
        - **账户信息**：当前账户的基础信息、扩展信息、证书信息和绑定的第三方账户。
        - **已授权应用**：已授权当前账户访问的应用。
        - **应用子账户**：当前账户下创建的应用子账户。
        - **隶属于组织机构**：当前账户所属的组织机构和组列表。
        - **设备**：当前账户已关联的认证设备。
        - **报表**：生成当前账户的操作报表。

     c. 单击账户页面右上角的**修改**，可以设置账户的**过期时间**。
   - 开启/关闭二次认证。
     单击账户**二次认证**列下的状态开关，为其开启/关闭二次认证。
   - 重置密码
     a. 单击账户操作列下的**重置密码**。

b. 在确认重置密码对话框中，勾选**是否给关联邮箱发送重置密码**（账户无邮箱请忽略此选项），单击**确定**。



账户密码重置成功。您可以在系统提示对话框中查看重置后的新密码。



- 启用/禁用账户
  - 处于**已禁用**状态的账户，单击其操作列下的**启用**，可以将其启用。
  - 处于**正常**状态的账户，单击其操作列下的**禁用**，可以将其禁用。
- 离职账户

a. 单击账户操作列下的**离职**。

b. 在**系统提示**对话框中，确认变更用户状态为离职，单击**确定**。

> **说明** 关于离职账户，您也可以在 **机构及组**页面进行操作。具体请参考删除账户（离职）。

1.3.5. 分类管理ABAC

本文为您介绍通过账户属性对账户进行分类管理，对满足条件的账户实现自动授权管理，提升管理人员和员工的办公体验。

背景信息：

某些企业员工流动大，导致员工对应的权限也需要频繁变动，加上满足特定条件的员工分布在不同的组织架构中，没有任何规律，如果管理员手动找出这些员工并授权，需要增加管理人员不少工作量，严重降低工作效率。

解决方案：

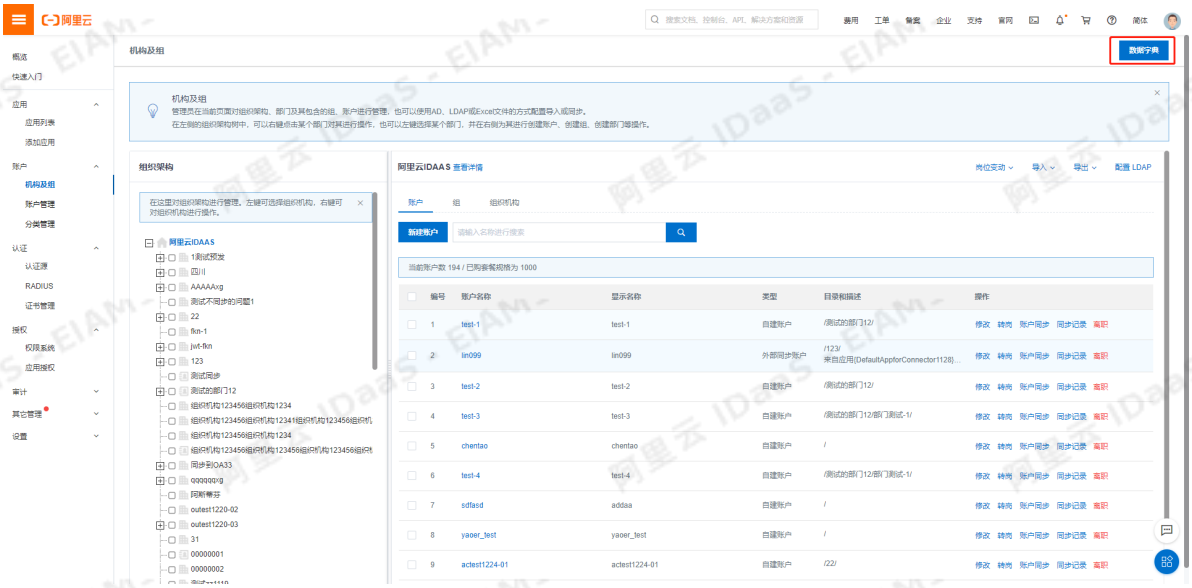
IDaaS应用身份服务通过分类管理功能将满足特定条件的员工账户一次性找出，直接对这个分类进行授权，属于这个分类的账户会自动继承权限，同样，一旦员工属性值有变化导致不满足分类设置的条件，就会自动从该分类移除，继承的权限也会被收回，完全不用管理人员手动维护，大大提升了管理人员的工作效率，减少失误率。

操作步骤：

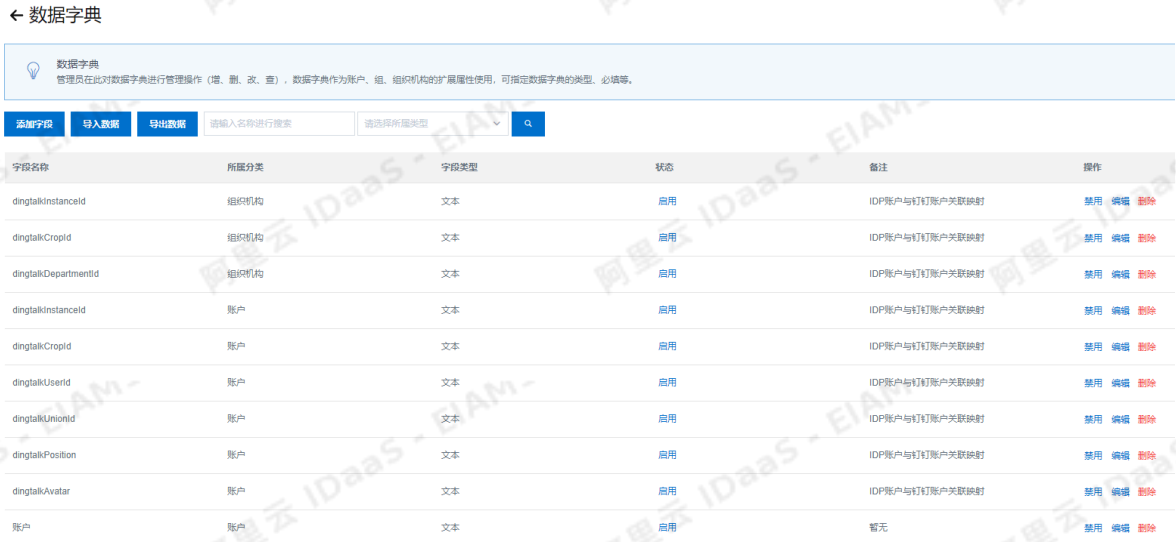
一、准备数据字典字段

分类是基于特定的账户属性值将账户进行分类，所以需要先准备数据字典字段，为账户增加该属性，通过属性与属性值匹配该分类的条件。

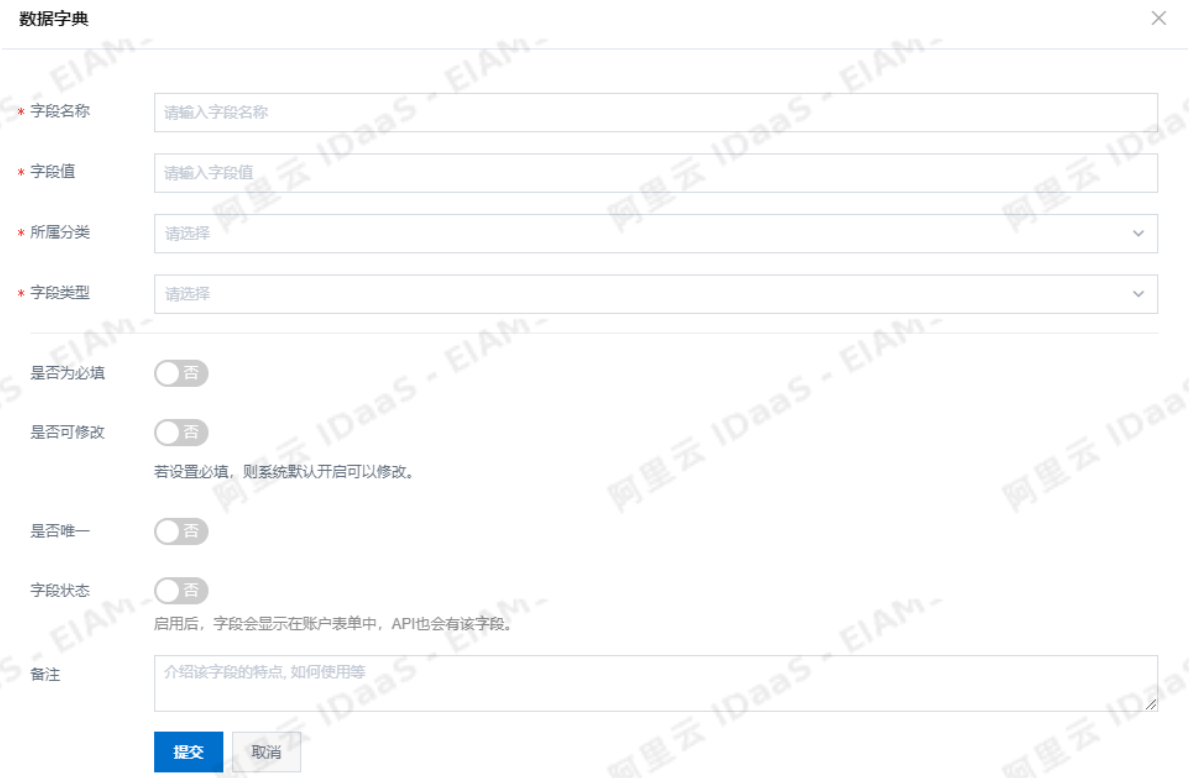
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**账户 > 机构及组**，查看账户列表及管理菜单



3. 点击【数据字典】按钮，进入扩展字段列表页。此页面展示了为账户、组、组织机构创建的扩展字段。



4. 点击【添加字段】按钮，进入新建页面：

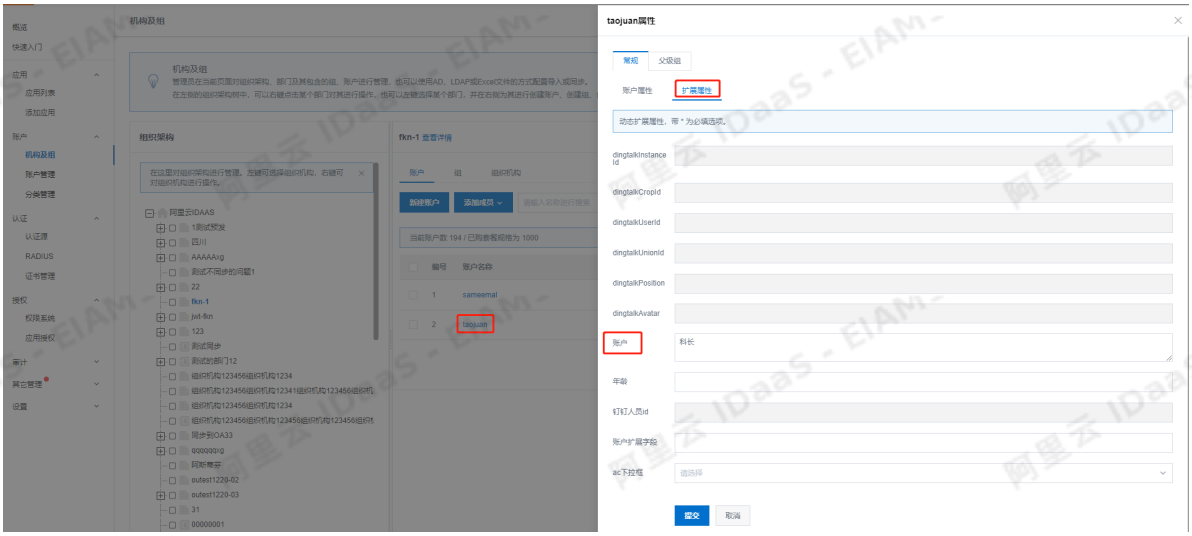


依次输入数据字典的各个属性并点击提交

- **字段名称**
- **字段值**：字段在数据库中的唯一标识
- **所属分类**：选择账户
- **字段类型**：根据实际需要选择字段的类型
- **是否为必填**：该字段是否为必填字段
- **是否可修改**：管理员是否可以修改
- **是否唯一**：该字段的值是否唯一

- **字段状态**：是否启用该字段，启用后可以在账户属性中进行管理

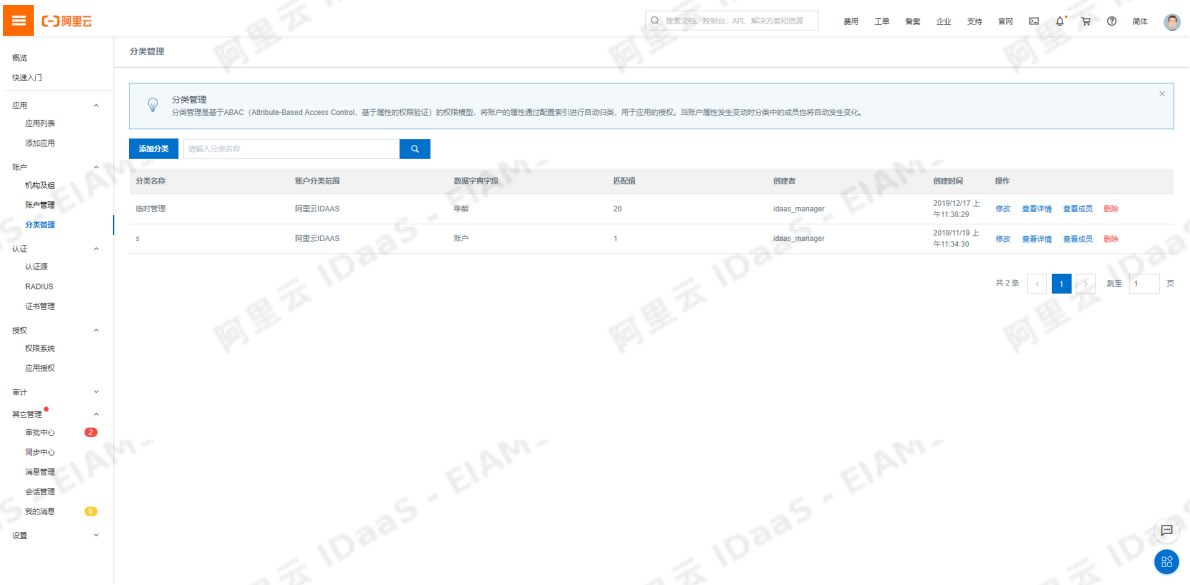
5. 进入**账户 > 机构及组**，找到需要通过分类管理的账户，点击账户名称，切换到**扩展属性**标签：



找到新建的数据字典并输入属性值。

二、创建分类

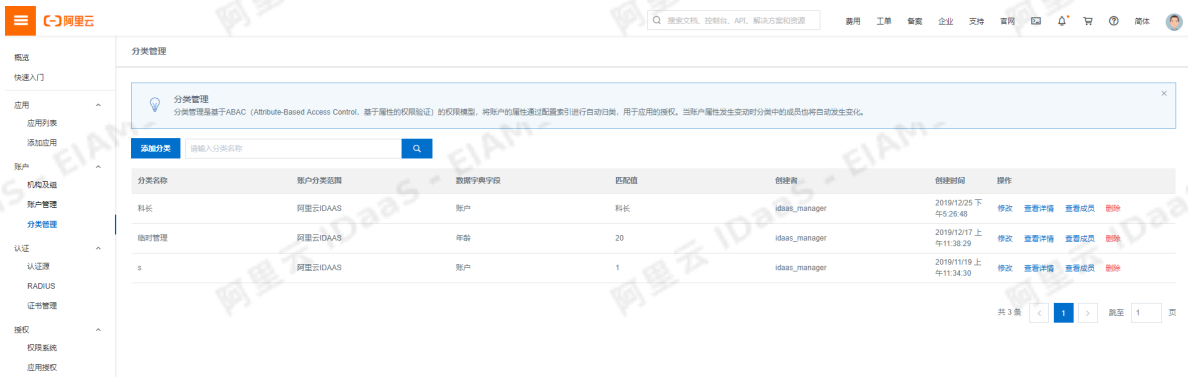
1. 在左侧导航栏，单击**账户 > 分类管理**



2. 点击【添加分类】按钮，进入新建分类页面：

3. 输入分类名称、选择需要匹配的数据字典字段、输入对应的匹配值：

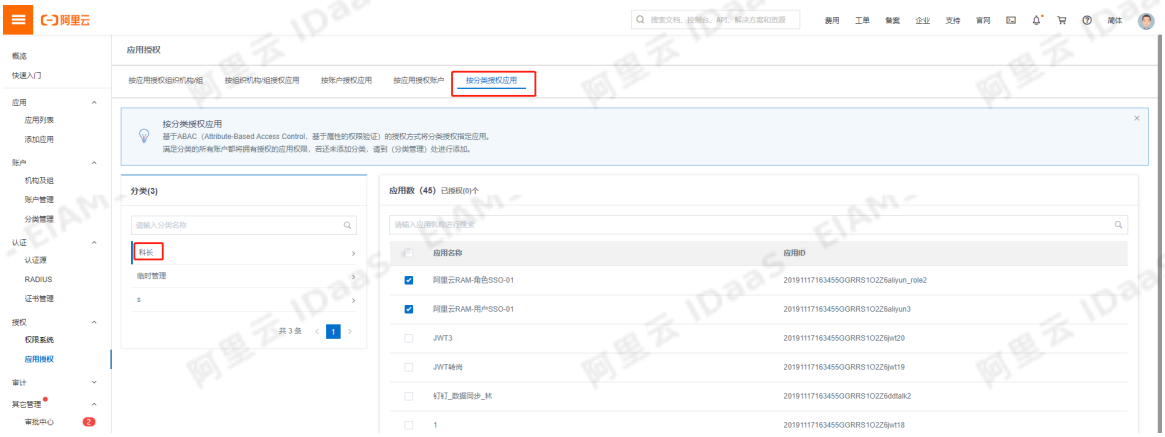
4. 保存后，进入分类列表页面。



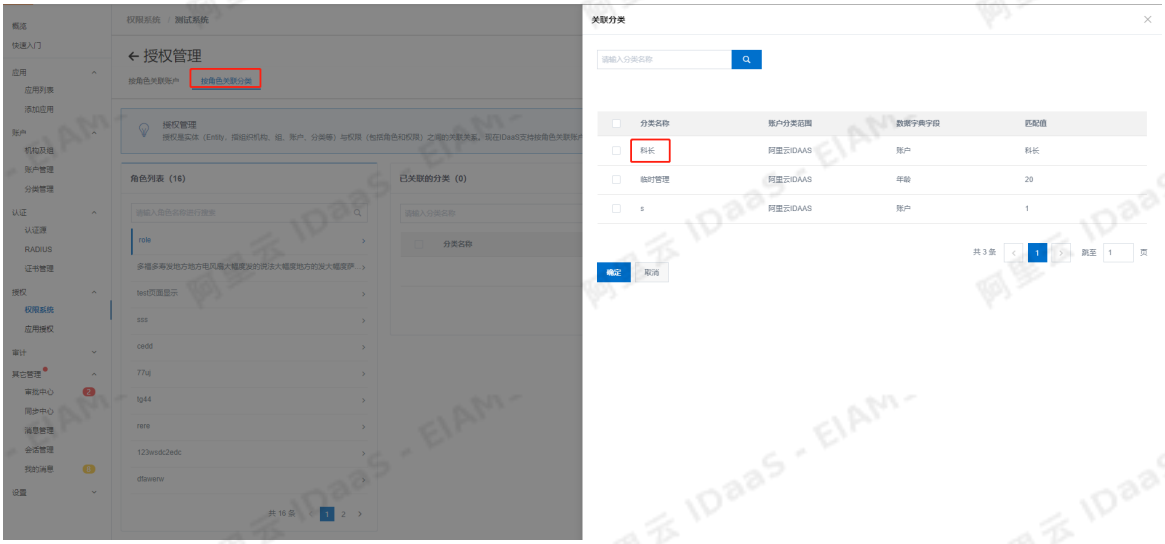
分类创建完成后，满足条件的账户会自动进入该分类，点击【查看成员】可查看该分类对应的账户

三、授权

- 按分类授权应用
  i. 在左侧导航栏，点击**授权 > 应用授权**
  ii. 点击**按分类授权应用**，可以将应用授权给新建分类，分类下的账户会自动继承该应用权限。



- 按分类授权权限角色
  i. 在左侧导航栏，点击进入**授权 > 权限系统**，
  ii. 点击权限系统的【授权管理】按钮，进入授权管理页面
  iii. 点击【按角色关联分类】，可将角色授权给分类，该分类下的账户会继承该角色权限。



四、收回权限

当账户的属性值发生变化，不匹配该分类设置的属性值后，会自动移除该分类，继承获得的应用权限和角色权限都会被收回。

1.4. 授权

1.4.1. 应用授权

介绍IT管理员如何在云盾IDaaS控制台进行统一授权，支持根据应用向组授权，或者根据组向应用授权。

前提条件

进行本文操作前，请确保已完成以下任务：

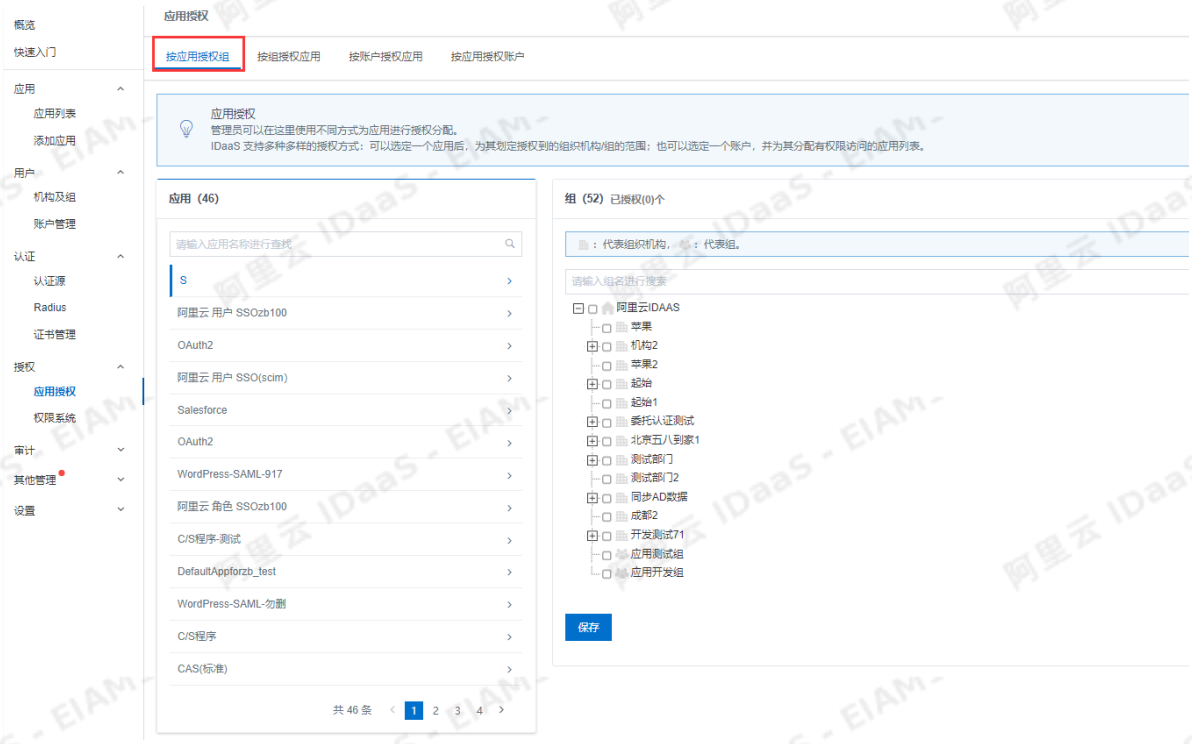
- 添加应用
- 新建组

按应用授权组

管理某个应用可以被哪些组织机构和组成员访问。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 应用授权**。
3. 打开**按应用授权组**页签。



4. 在左侧**应用**列表中，单击要授权的应用。

> 说明　支持使用应用名称搜索应用。

5. 在右侧组织机构树上，勾选为哪些组织机构和组授予当前应用的访问权限。

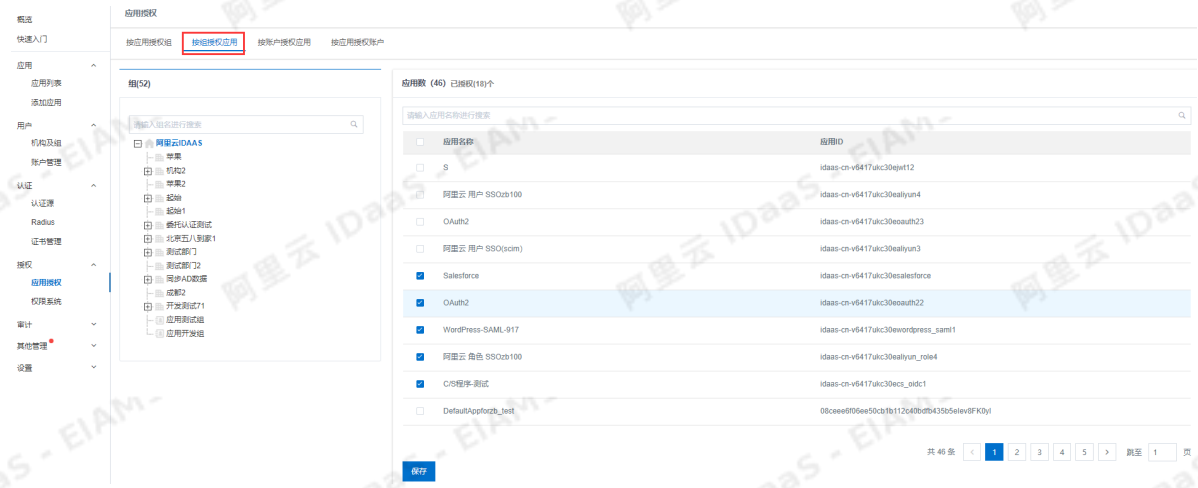
> 说明　支持使用组名搜索目标组。

按组授权应用

管理某个组下的成员可以访问哪些应用。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 应用授权**。
3. 打开**按组授权应用**页签。



4. 在左侧组织机构树上，单击要操作的组。

> 说明 支持使用组名搜索组。

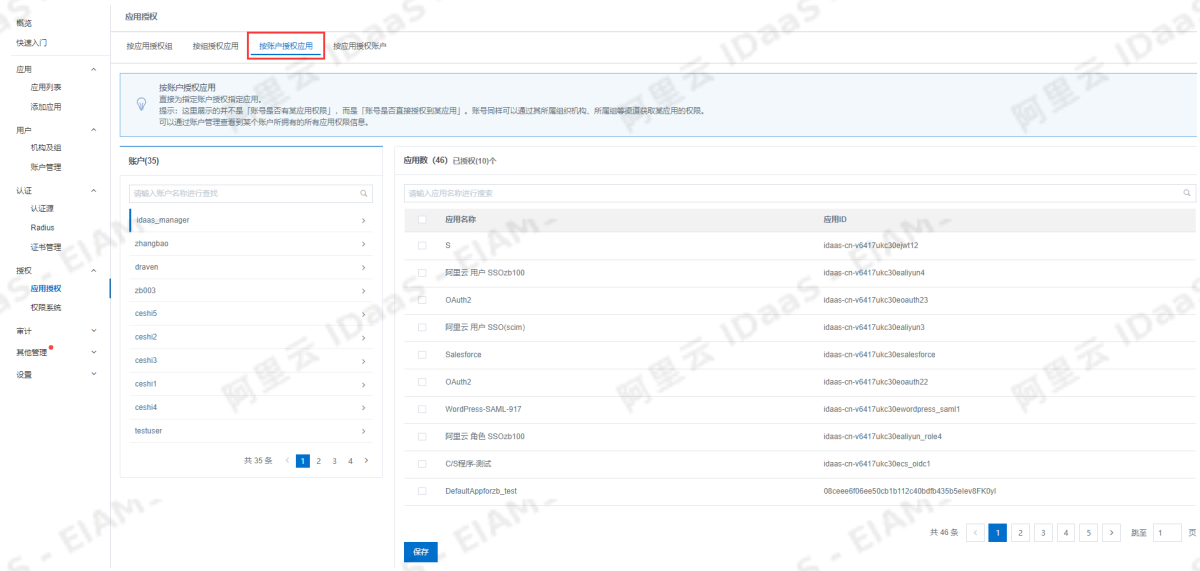
5. 在右侧的应用列表，勾选应用授予当前组应用的访问权限。

按账户授权应用

管理某个账户可以访问哪些应用。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 应用授权**。
3. 打开**按账户授权应用**页签。



4. 点击左侧账户可以进行模糊和精确搜索。

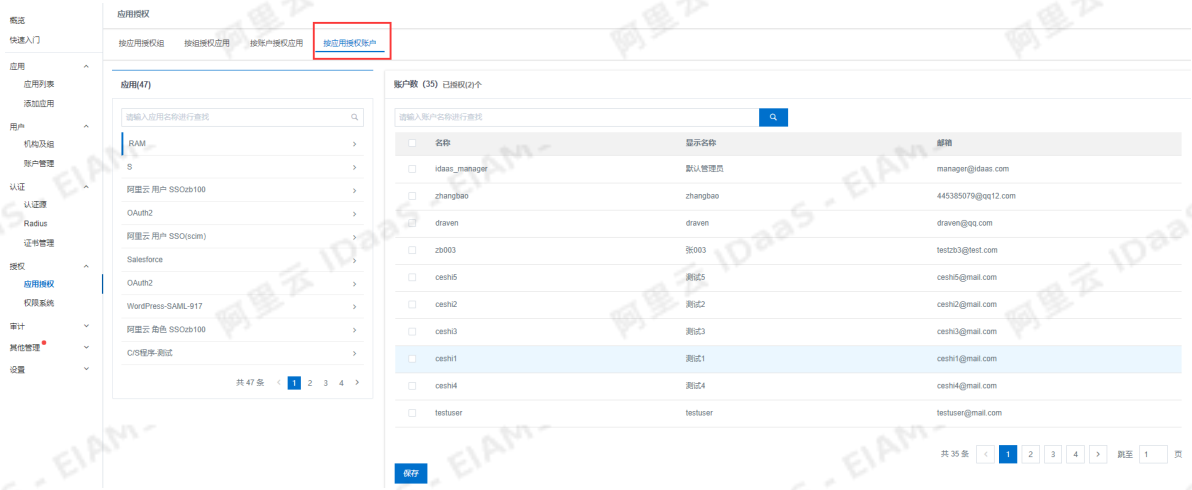
> 说明 支持应用的搜索。

按应用授权账户

管理某个应用可以被哪写账户访问。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 应用授权**。
3. 打开**按应用授权账户**页签。



4. 点击左侧应用可以进行模糊和精确搜索。

> 说明 支持账户的搜索。

1.4.2. 权限系统

介绍IT管理员如何在云盾IDaaS控制台维护IDaaS权限系统，具体包括查看系统详情、使用管理员查询、角色管理。

查看系统详情

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 权限系统**。
3. 在IDaaS权限系统下，单击操作列中的**系统详情**。

4. 在**系统详情**侧边页，查看IDaaS权限系统的基础信息和API信息。

使用新增系统

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 权限系统**。
3. 单击页面右上角的**新增系统**。

4. 在**新增系统**侧边页，填写系统名称点击**确定**。

5. 在新增系统操作下面可以看到**系统详情**、**角色管理**、**资源管理**、**授权管理**、**修改**、**启用**、**删除**。

角色管理

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**授权 > 权限系统**。
3. 在新增的权限系统下，单击操作列中的**角色管理**。

4. 根据需要，执行以下任务。
   - 新增角色

a. 在角色管理页面，单击**新增角色**

b. 在**新增角色**侧边页，完成以下配置。

a. **名称**：为角色命名。角色名称应唯一。

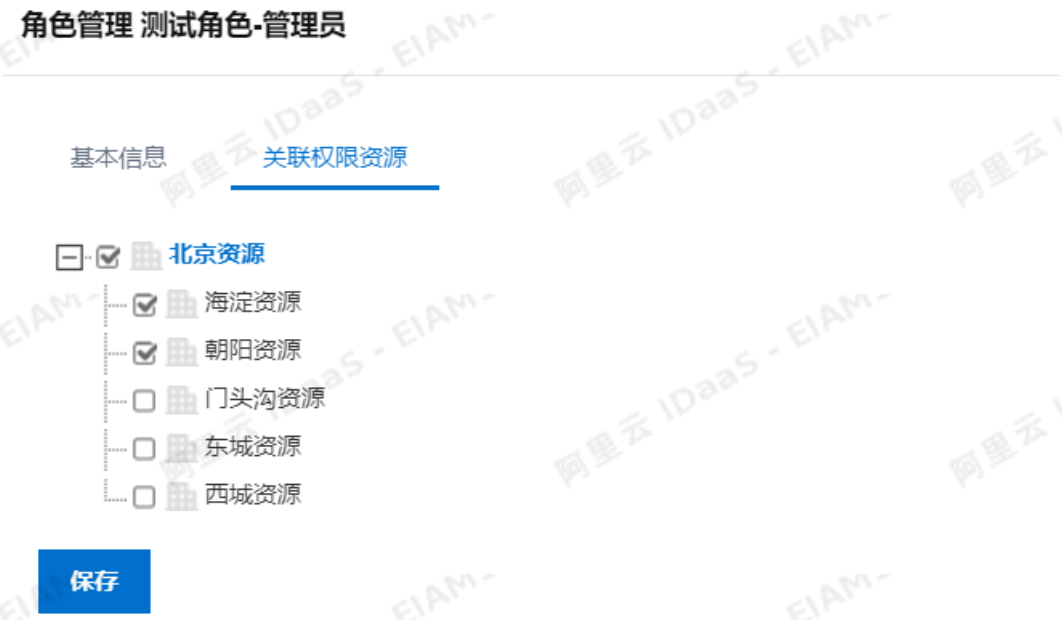
b. **权限值**：设置角色的权限值。

c. **状态**：是否启用角色。

d. **描述**：添加角色备注信息。

c. 完成配置后，单击**提交**。

- 为角色关联权限
  a. 在角色管理页面，定位到要操作的角色，单击其操作列下的**关联权限**。
  b. 在**角色管理**侧边页**关联权限资源**页签下，勾选关联给角色的权限。



成功关联权限后，角色的**权限数**列下显示已关联给角色的权限数量。

- 编辑角色
  a. 在角色管理页面，定位到要操作的角色，单击其操作列下的**编辑**。
  b. 在**角色管理**侧边页**基本信息**页签下，根据需要修改角色的配置属性。
  c. 修改完配置后，单击**保存**。
- 删除角色

a. 在角色管理页面，定位到要操作的角色，单击其操作列下的**删除**。

> **说明** 系统默认角色不支持删除操作。

b. 在**提示**对话框中，单击**确定**。

- 批量删除角色

a. 在角色管理页面，勾选要操作的角色，单击页面下面的**批量删除**。

> **说明** 系统默认角色不支持删除操作。

b. 在**提示**对话框中，单击**确定**。

1.4.3. 权限系统介绍

本文主要介绍了RBAC授权模式，和IDaaS的权限系统的设计架构以及权限系统的主要功能。

一、RBAC模型

RBAC，基于角色的权限访问控制（Role-Based Access Control）：

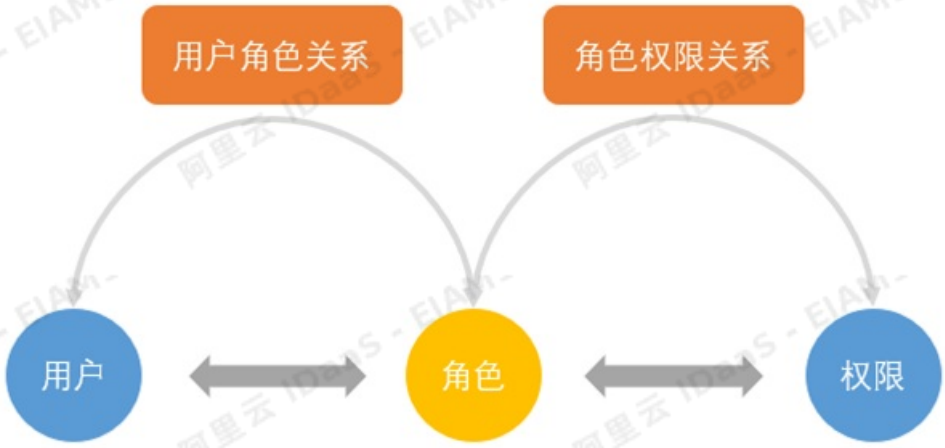
RBAC的核心在于用户只和角色关联，而角色代表对了权限，是一系列权限的集合。

RBAC三要素：

- 用户：系统中所有的账户
- 角色：一系列权限的集合（如：管理员，开发者，审计管理员等）
- 权限：菜单，按钮，数据的增删改查等详细权限。

在RBAC中，权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限。角色是为了完成各种工作而创造，用户则依据它的责任和资格来被指派相应的角色，用户可以很容易地从一个角色被指派到另一个角色。角色可依新的需求和系统的合并而赋予新的权限，而权限也可根据需要而从某角色中回收。角色与角色的关系同样也存在继承关系防止越权。

- 优点：便于角色划分，更灵活的授权管理；最小颗粒度授权

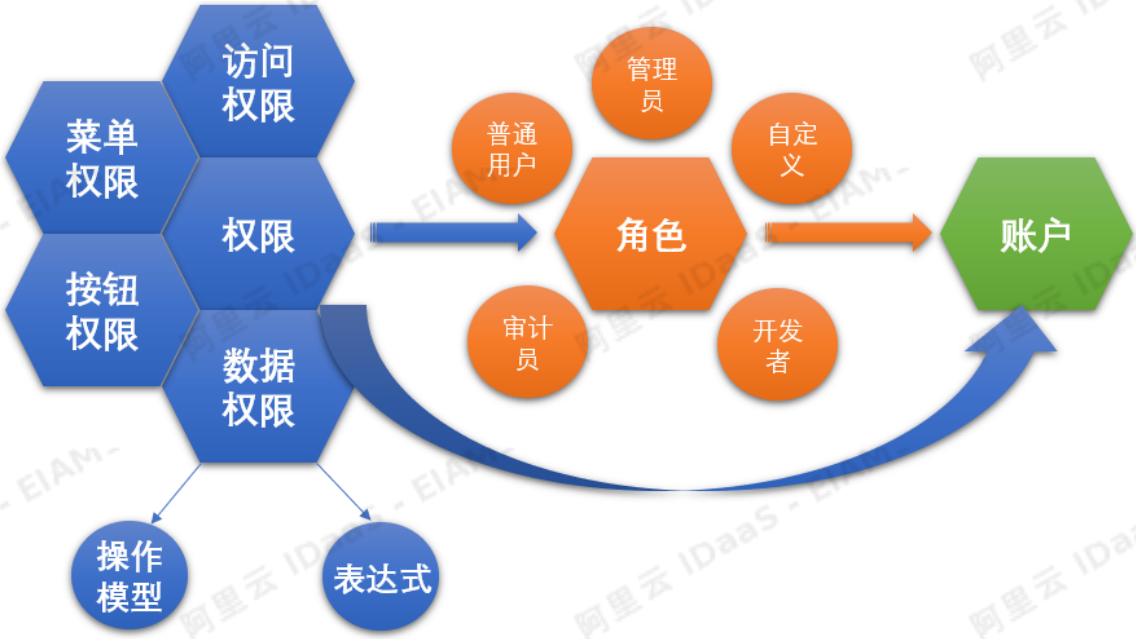


二、设计架构

1. 授权架构

IDaaS权限系统的架构依赖于RBAC模型，无论是在功能设计思路还是在用户体验上，权限，角色，用户三者关联关系可灵活组合，从而实现精细化授权。

此外，我们不仅支持按角色授权，同时也支持按账户直接授权。让用户的授权变的更加便捷，尤其是人员较少的企业极为使用。我们满足各类授权方式，按需求可灵活自由操作，极大地简化了权限分配的管理。



2. 三级权限

我们将整体授权类型划分为三级

（1）一级权限：访问权限

（2）二级权限：菜单、按钮权限

（3）三级权限：数据权限

依据不同等级的授权，来控制授权的最小的颗粒度。

访问控制

IDaaS登录访问控制，应用SSO单点登录访问控制

菜单、按钮控制

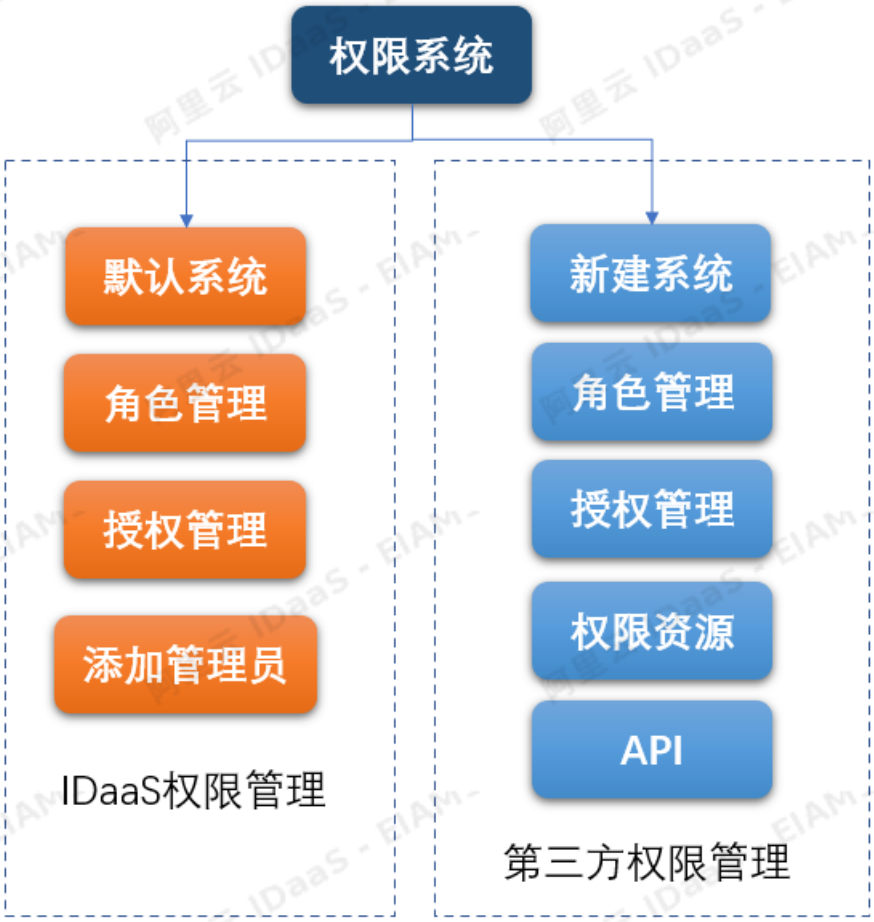
应用-账户-认证-授权-审计-其他管理-设置
新增，修改，同步，删除，离职等

数据控制

组织机构数据　　人员基本信息
人员扩展字段信息　API接口数据字段

3. 权限系统

IDaaS权限系统，不仅支持IDaaS本身的一系列授权活动，还支持第三方接入，做到真正意义上的集中授权。我们提供丰富的API接口，方便业务系统能够更好对接。



三、主要功能

权限系统主要包括以下功能：

（1）默认权限系统（IDaaS平台）

1、角色管理

1）可以授予用户开发者角色

2、授权管理

1）授权->角色：支持授权到角色

2）授权->个人：支持授权到个人

3、查看系统详情

1）默认权限系统的权限详情查看

（2）第三方接入（外部系统接入）

1、新增系统

1）系统新建，管理

2、角色管理

1）用户可以按需定义角色

2）支持批量导入

3、授权管理

1）授权->角色：支持授权到角色

2）授权->个人：支持授权到个人

3）表格导入

4、资源管理

1）资源新增

2）资源导入、导出

5、查看系统详情

1）第三方接入系统的权限信息详情查看

5、权限系统API接口清单

1）权限系统全局接口

2）角色管理接口

3）授权管理接口

4）鉴权接口

最佳第三方接入实践，详见第三方业务系统接入权限系统

1.5. 认证

1.5.1. 认证源

1.5.2. 证书管理

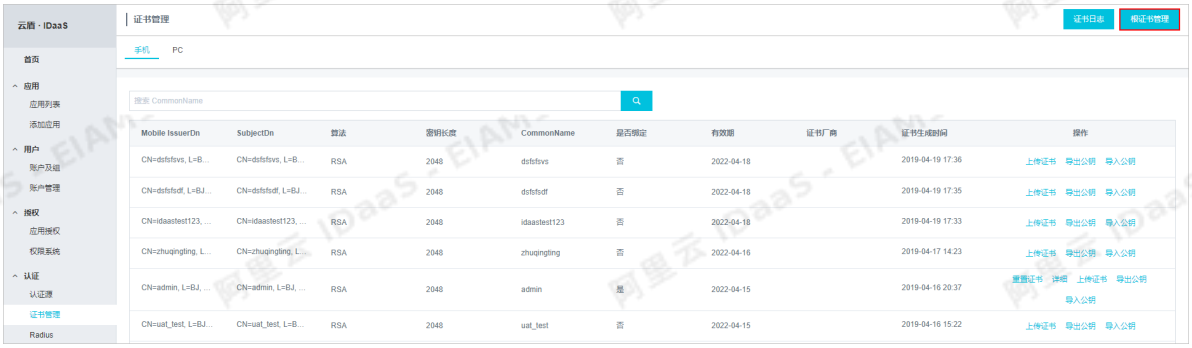
介绍IT管理员如何在云盾IDaaS控制台管理用户证书，包括根证书和对应每个账户的PC端和手机端证书。

根证书管理

根证书管理用于用户自定义生成根证书。生成根证书后，当您新建账户或将证书重置时，都将使用新生成的根证书进行个人证书的签发。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考IT管理员登录。
2. 在左侧导航栏，单击**认证 > 证书管理**。
3. 单击根证书管理。



4. 在根证书管理侧边页，完成以下配置。

配置	描述
名称	证书名称。
组织单位	组织单位名称。
组织	组织名称。
地址	地址。
省	省份。
国家	国家。
根证书有效期	根证书的有效年限。
子证书有效期	子证书的有效年限。必须小于根证书有效期。
是否启用	是否启用根证书。若启用，则公司所有证书将用根证书签发。

5. 单击保存，生成根证书。

手机/PC端证书管理

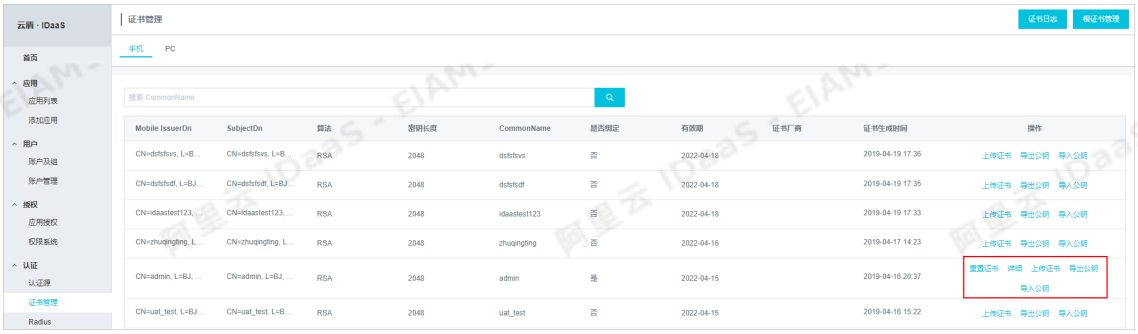
手机端证书用于管理移动端免密码登录的P12证书。IT管理员可以查看所有账户的手机端证书。用户第一次登录移动端时，会自动下载对应的P12证书。

PC端证书用于管理用户PC端证书文件，IT管理员可以查看所有账户的PC证书。当您成功新建账户后，系统自动为账户签发个人PC端证书。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考IT管理员登录。
2. 在左侧导航栏，单击**认证 > 证书管理**。
3. 分别在手机和PC页签下管理移动端免密码登录的P12证书和用户PC端证书文件。
   - 管理手机证书

a. 单击手机页签。



b. 使用用户名搜索并定位到要操作的证书文件。

c. 根据需要单击执行以下操作：

- 重置证书：只有在移动端成功下载证书后，才会出现该操作，用来重置已下载的证书。重置证书后，当前证书失效不可用。

- 详细：当证书在移动端被下载后或上传证书成功后，您可以查看证书和设备的相关信息。

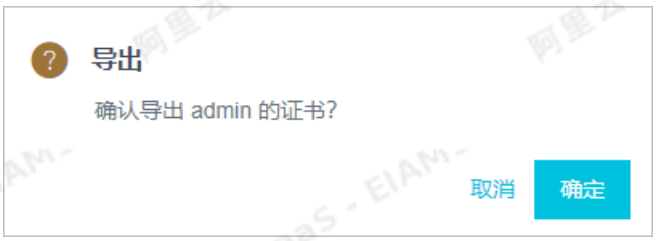
- 上传证书：为用户上传一个IDaaS支持的厂商的.p12或.pfx证书。上传证书后，原先证书文件将失效。
  在 上传证书页面，确认当前证书信息，完成上传证书配置，包括 证书厂商、 证书文件、 证书密码，然后单击 上传证书。

- 导入公钥：上传公钥文件。

  说明 上传公钥后将删除用户已经存在的证书。若该证书未绑定，则不能再进行绑定。

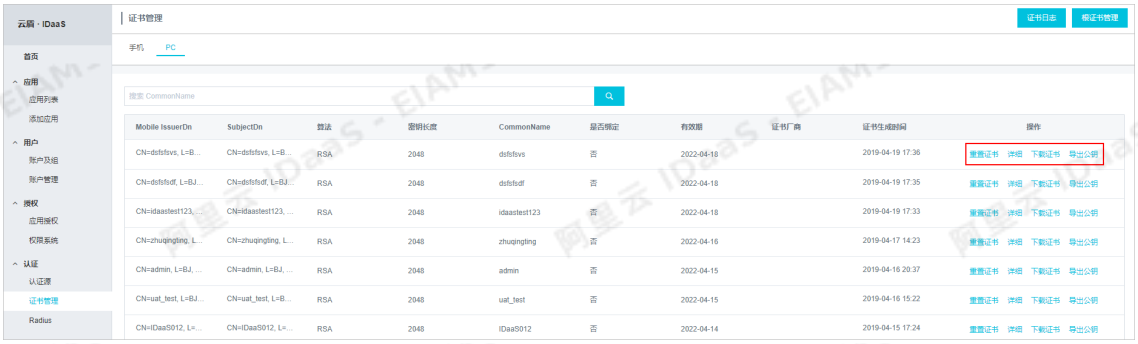
  在 导入公钥页面，确认当前证书信息，完成导入公钥配置，包括 证书厂商、 公钥文件，然后单击 上传公钥。

- 导出公钥：将证书中的公钥信息导出至本地文件。



  - 管理PC端证书

a. 单击PC页签。



b. 使用用户名搜索并定位到要操作的证书文件。

c. 根据需要单击执行以下操作：

- 重置证书：只有在PC端成功下载证书后，才会出现该操作，用来重置已下载的证书。重置证书后，当前证书失效不可用。
- 详细：当证书在PC端被下载后或上传证书成功后，可查看证书和设备的相关信息。
- 下载证书：将证书下载至本地，文件格式为.p12。
- 导出公钥：将证书中的公钥信息导出至本地，文件格式为.p12。

1.6. 审计

1.6.1. 日志

介绍IT管理员如何在云盾IDaaS控制台查看操作日志和用户进/出日志。

背景信息

统一审计将所有账户的操作日志集中记录管理和分析，帮助您对账户行为进行监控，并且通过集中的审计数据进行数据挖掘，以便于事后的安全事故责任认定。

所有通过云盾IDaaS操作的行为都有归档。IT管理员可以通过该信息查看具体账户的操作记录。

查看操作日志

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**审计 > 操作日志**。
3. 在**操作日志**页面，查看所有日志记录。您也可以使用搜索和筛选功能，查看指定的记录。

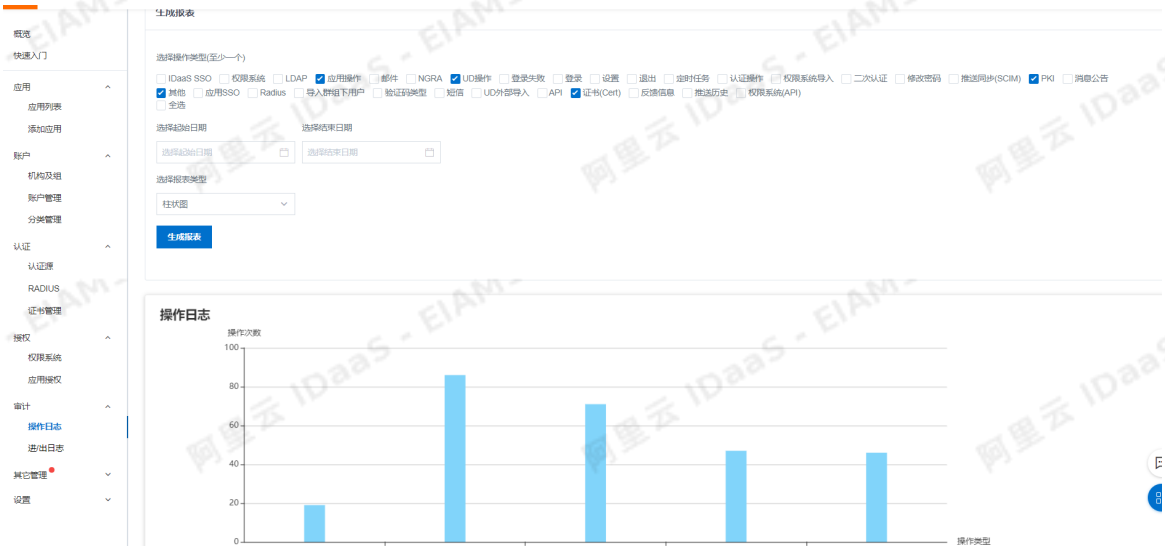
> **说明** 支持以、操作人、起止时间进行搜索；同时也支持以**操作类型**进行筛选。

4. 查看审计报表。
   i. 在**操作日志**页面，单击**审计报表**。

ii. 在**报表**页面，完成以下报表配置。

- **选择操作类型**： IDP SSO、权限系统、LDAP、应用操作、NGRA、邮件、UD操作、登录失败、设置、登录、退出、定时任务、认证操作、权限系统导入、二次认证、修改密码、推送同步（SCIM）、PKI、消息公告、应用SSO、Radius、导入群组下用户、验证码类型、UD外部导入、短信、API 证书（Cert）、反馈信息、推送历史、权限系统（API）。至少勾选一个。
- **选择起始日期**
- **选择结束日期**
- **选择报表类型**：饼状图、柱状图。

iii. 单击**生成报表**。



查看进/出日志

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，单击**审计 > 进/出日志**。
3. 在左侧**账户**列表中，单击选择要查看的账户。支持使用账户名搜索账户。
4. 在右侧**登录登出日志**页面，查看当前账户的所有登录/退出日志。您也可以设置日志筛选条件后，单击搜索图标，查看特定记录。

> **说明** 支持以操作类型（登录/退出）、IP、起止时间筛选日志。

1.7. 其他管理

1.7.1. 审批中心

介绍IT管理员如何在云盾IDaaS控制台集中处理所有需要审批内容的页面。

子账户审批

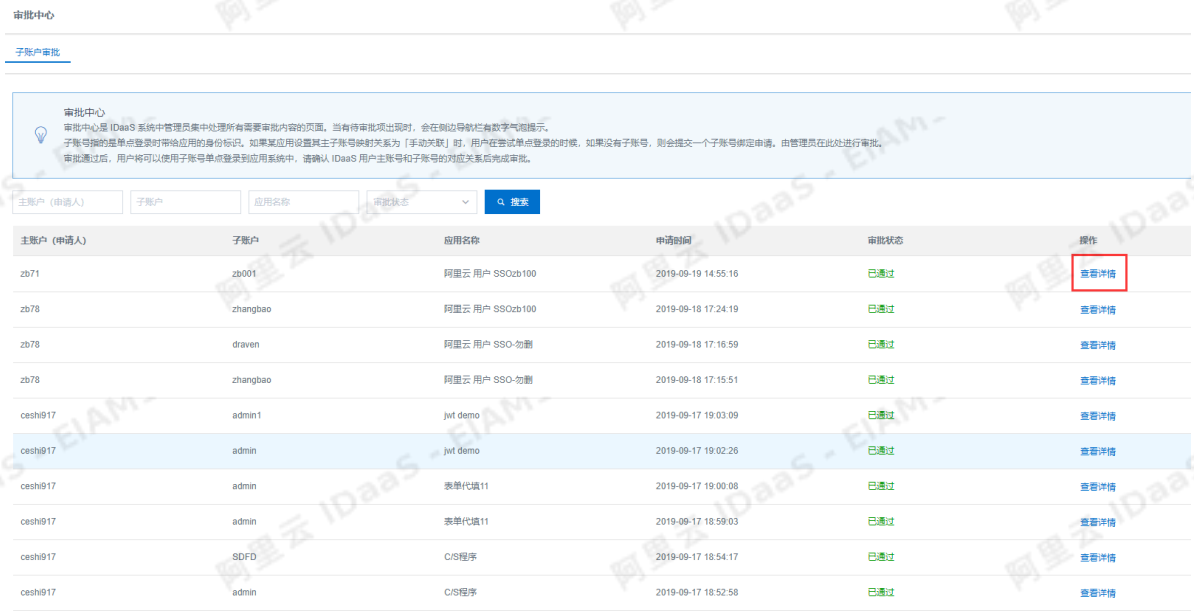
当有待审批项出现时，会在左侧导航栏有数字气泡提示有几条未审批状态。子账号指的是单点登录时带给应用的身份标识。如果某应用设置其主子账号映射关系为「手动关联」时，用户在尝试单点登录的时候，如果没有子账号，则会提交一个子账号绑定申请。由管理员在此处进行审批。管理员确认 IDaaS 用户主账号和子账号的对应关系后完成审批，审批通过后，用户将可以使用子账号单点登录到应用系统中。

操作步骤

1. 以IT管理员账号登录云盾IDaaS控制台。
2. 在左侧导航栏，单击**其它管理 > 审批中心**。
3. 在审批中心页面，默认为子账户审批页面。
4. 单击操作下面的审批。

5. 点击未审批信息操作下面的审批进入审批页面，点击同意，该条信息变为已通过。

6. 可以查看审批以后的详情，点击查看详情。



7. 在子账户审批页面，默认查看未审批信息。您也可以设置申请人筛选条件后，单击搜索图标，查看特定记录。

   支持子账户、应用名称、审批状态进行筛选。

1.7.2. 向员工发送公告及通知

本文为您介绍如何通过IDaaS消息管理功能，将企业公告及通知，准时无误的发布给企业内部员工或特定人群。

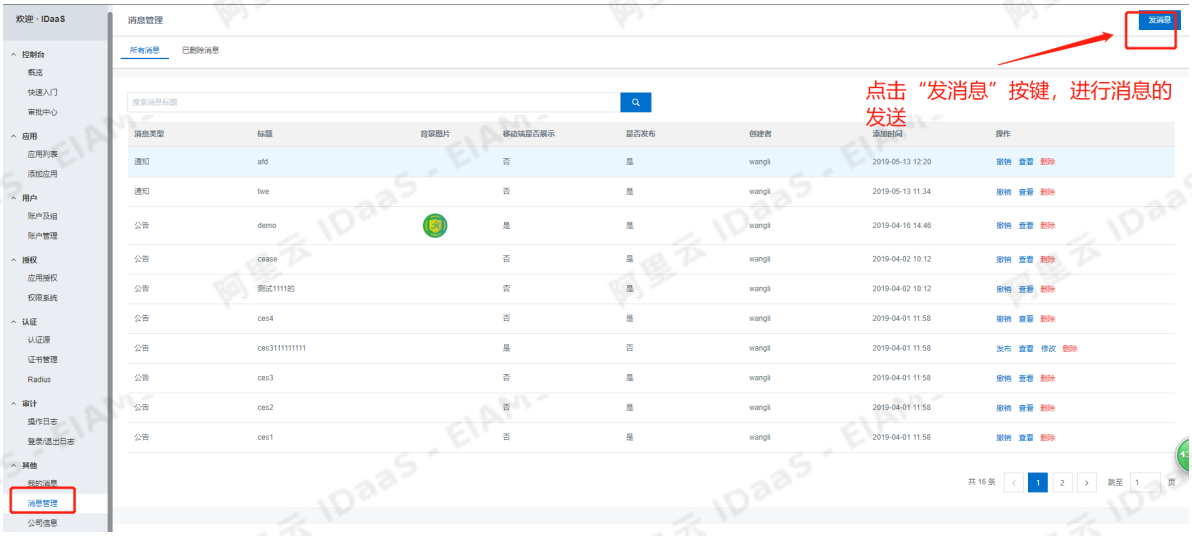
背景信息

企业日常办公中会向内部员工发送假期公告、节日祝福、会议通知及业务相关信息等，如何将信息统一、准时且无遗漏的发送到相关人员手中，并确保被通知人是否收到变得异常复杂。

- 管理员向企业所有员工发送公告，并确保无遗漏；
- 管理员将某项业务相关通知发送给特定人群。

操作步骤：

1. 在管理员页面，点击左侧导航栏中的消息管理进入消息管理页面；在消息管理页面点击右上角的“发消息”，进行消息的发送。



2. 在发消息页面，可以选择类型，支持“公告”和“通知”。

3. 选择“公告”的话，公司全员都可以收到；用户可以通过PC登录IDaaS进行消息的查看

4. 选择“通知”，需要指定消息的接收人。“通知”的接收对象可以是个人或者某个组下的所有用户，可通过在输入框输入关键词搜索个人账户或者组的名称进行查找。通知只有在PC端登录IDaaS才能查看。

通过以上步骤，即可实现公告和通知的发送。

1.7.3. 同步中心

同步中心包括 IDaaS 系统中从第三方应用/AD 中获取组织架构和账户信息，以及从 IDaaS 同步组织架构和账户信息到第三方应用/AD 的配置、管理、审计中心。

背景信息

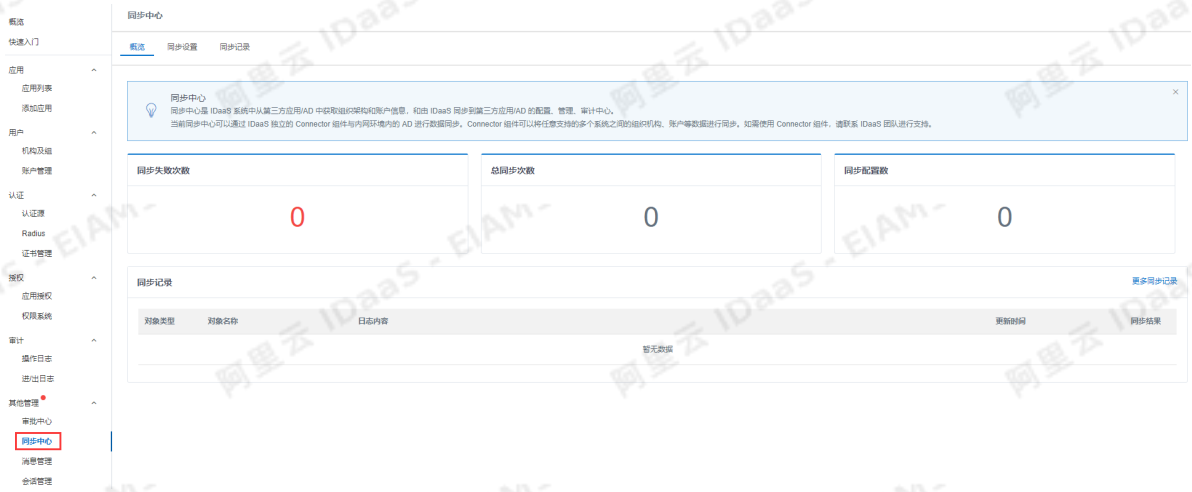
当前同步中心可以通过 IDaaS 独立的 Connector 组件与内网环境内的 AD 进行数据同步。Connector 组件可以将任意支持的多个系统之间的组织机构、账户等数据进行同步。如需使用 Connector 组件，请联系 IDaaS 团队进行支持。

概览

概览页主要展示同步失败次数、总同步次数、同步配置数，默认为概览页。

操作步骤

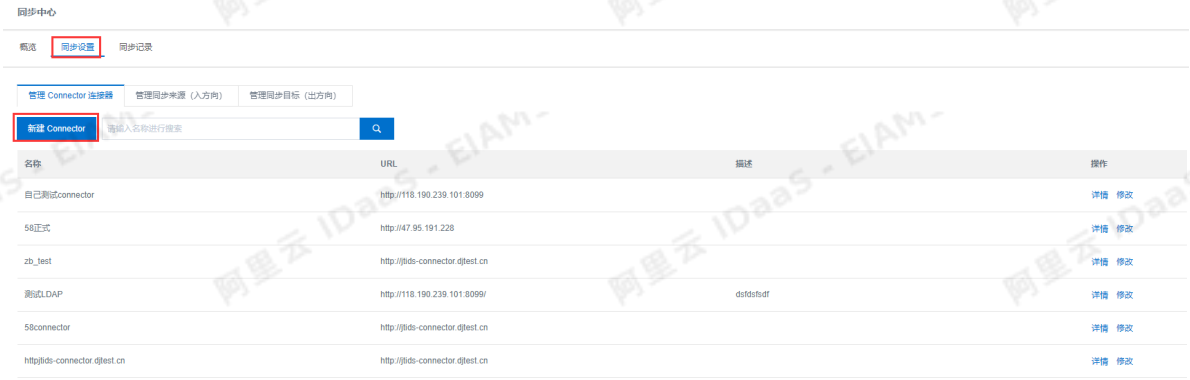
1. 以IT管理员账号登录云盾IDaaS控制台。
2. 在左侧导航栏，单击**其它管理 > 同步中心**。
3. 打开同步中心页面。



同步设置

管理connector的入方向和出方向。

1. 在左侧导航栏，单击**其它 > 同步中心 > 同步设置**。
2. 打开管理connector连接器，进行新建connector。



说明 在使用connector之前需要这里新建个可以使用的connector。

3. 在同步中心侧边页，完成新建connector以下配置。
   - 名称：connector名称。名称应唯一。
   - 接口调用地址：为接口调用地址，由connector提供。为必填项。
   - 接口 ClientId：为接口调用时，用于获取access_token，由connector提供。为必填项。
   - 接口 ClientSecret：为接口调用时，用于获取access_token，由connector提供。为必填项。
   - 描述信息：为接口调用时，用于描述connector相关信息。为选填。
   - 在左侧导航栏，单击**其它管理 > 同步中心 > 同步设置 > 新建Connector**。
   - 进入新建connector页面。

4. 在同步设置第二个tab页，完成新建connector同步来源。首先需要选择一个connector链接器，然后进行新建。

5. 打开管理同步来源（入方向），点击新建来源。

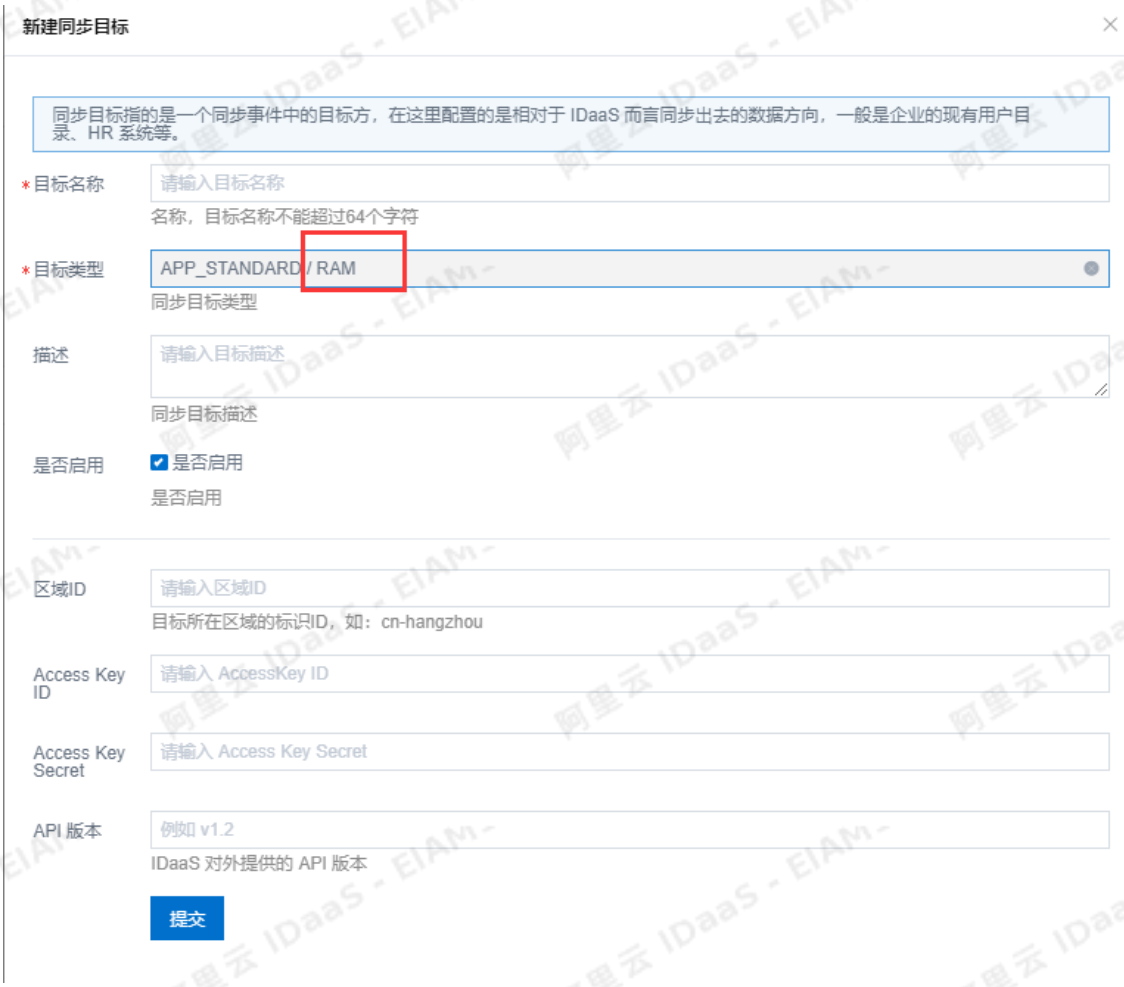
- 名称：为必填项。
- 来源类型：为必选项。
  - WINDOWS_AD：填写windows_ad的相关配置，如：服务器地址、端口号、Base DN、管理员DN、管理员密码。
  - OPEN_LDAP：填写linux_ladp的相关配置，如：服务器地址、端口号、Base DN、管理员DN、管理员密码。


新建同步来源
同步来源指的是一个同步事件中的源头方，在这里配置的是相对于 IDaaS 而言同步进来的数据来源，一般是企业的现有用户目录、HR 系统等。
*名称
sd
名称，来源名称不能超过64个字符
*来源类型
LDAP
WINDOWS_AD
同步来源类型
描述
请输入来源描述
同步来源描述
是否启用
是否启用
是否启用同步来源
服务器地址
请输入服务器地址
LDAP服务器地址, 如: 127.0.0.1
端口号
请输入端口号
LDAP服务器端口，如: 389
Base DN
请输入Base DN
搜索起始点专有名称， 如：DC=contoso,DC=com
连接方式
SSL 连接
LDAP服务器是否使用SSL连接方式
管理员DN
请输入管理员DN
LDAP管理员账号
管理员密码
请输入管理员密码
LDAP管理员密码
是否开启回收站查询功能
如果要开启该功能，请先确保AD域控上也已经启用了回收站功能，该功能开启后，Connector可以从AD同步删除的数据
提交

说明 添加同步源以后，可以在操作下面配置同步、查看详情、修改、删除，配置同步以后，单击立刻执行同步。

6. 打开管理同步目标（出方向),点击新建目标。

- 目标名称：为必填项。
- 目标类型：为必选项。
  - LDAP：WINDOWS_AD、OPEN_LDAP。
  - APP_STANDARD：RAM，需要获取Access Key ID、Access Key Secret。



同步记录

- 在同步记录页面可以看到同步推送的结果，可以通过账户和组织机构名称、对象类型、同步结果进行筛选查询。

1.7.4. 消息管理

介绍IT管理员如何在云盾IDaaS控制台发送消息和查看消息记录。

发消息

IT管理员可以通过发消息，对公司内部的账户发布公告/通知。

操作步骤

1. 以IT管理员账号登录云盾IDaaS控制台。
2. 在左侧导航栏，单击**其它 > 消息管理**。
3. 在消息管理页面，单击发消息。
4. 在发消息页面，编辑消息正文。具体包括以下内容：
   - 类型：公告、通知。
   - 标题：填写消息标题。
   - 内容：编辑消息正文。
   - PC端上传PDF：单击上传文件从PC端上传PDF文件，用作展示链接。支持上传的PDF文件最大5MB。
   - 移动端是否显示：是否在移动端显示消息。
   - 是否自动发布：是否自动发布该消息。若自动发布，则配置完消息后，单击发消息直接发布；否则，在保存消息后，要到消息记录中执行发布操作，才能发布消息。
   - 移动端上传图片：若允许在移动端显示消息，则应通过该接口上传在移动端显示的图片，图片大小不超过1MB。
5. 完成配置后，单击发消息。

消息记录

IT管理员可以在消息记录中管理消息发布、撤销、查看、删除等。

操作步骤

1. 以IT管理员账号登录云盾IDaaS控制台。
2. 在左侧导航栏，单击**设置 > 消息管理**。
3. 在消息管理页面所有消息页签下，查看所有消息记录。
4. 根据需要执行以下操作：
   - 查看：单击查看查看消息内容。

- 发布/撤销：未发布的消息，单击发布进行发布；已发布的消息，单击撤销可以撤销发布。
- 删除：单击删除可以删除消息记录。

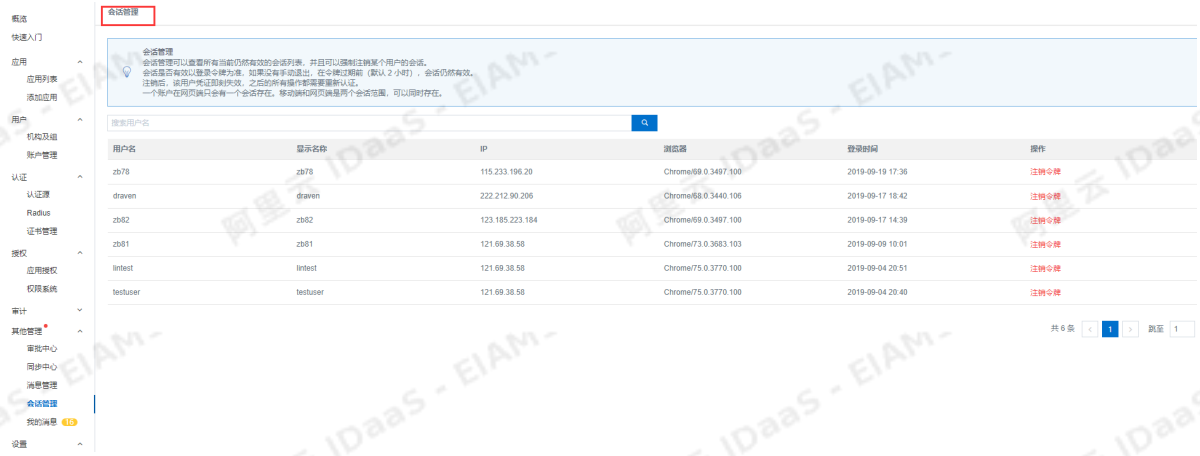
> **说明** 已删除的消息，您可以打开 已删除消息页签查看其记录。

1.7.5. 会话管理

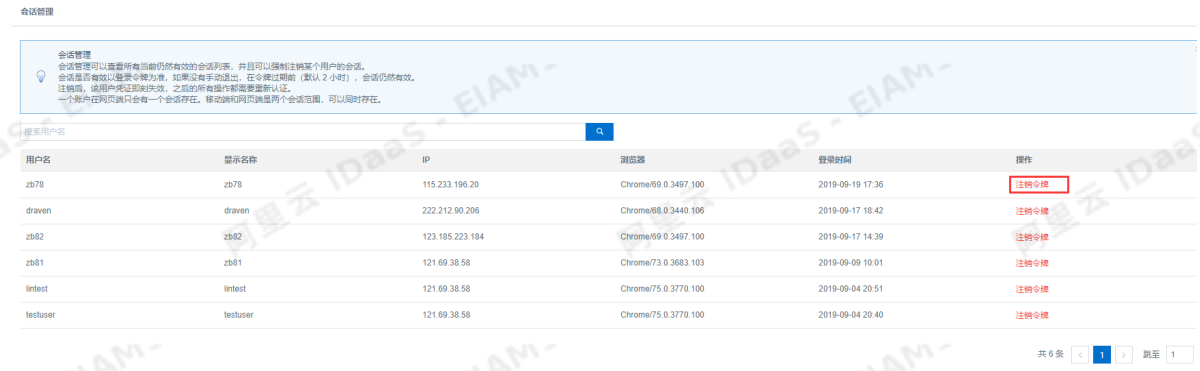
会话管理可以查看所有当前仍然有效的会话列表，并且可以强制注销某个用户的会话。会话是否有效以登录令牌为准，如果没有手动退出，在令牌过期前（默认 2 小时），会话仍然有效。注销后，该用户凭证即刻失效，之后的所有操作都需要重新认证。一个账户在网页端只会有一个会话存在。移动端和网页端是两个会话范围，可以同时存在。

操作步骤

1. 以IT管理员账号登录云盾IDaaS控制台。
2. 在左侧导航栏，单击**其它管理 > 会话管理**。



> **说明** 新建账户以后，会话管理生成一条会话，如果不想让该用户处于登录状态就点击“注销令牌”操作，用户会被强制下线。

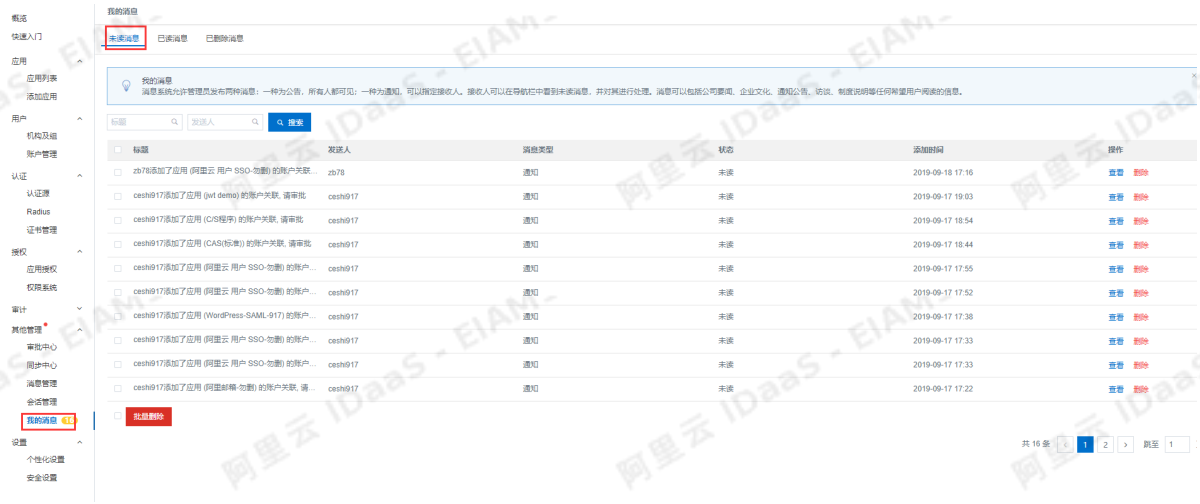


1.7.6. 我的消息

消息系统允许管理员发布两种消息：一种为公告，所有人都可见；一种为通知，可以指定接收人。接收人可以在导航栏中看到未读消息，并对其进行处理。消息可以包括公司要闻、企业文化、通知公告、访谈、制度说明等任何希望用户阅读的信息。

我的消息

1. 以IT管理员账号登录云盾IDaaS控制台。
2. 在左侧导航栏，单击**其它管理 > 我的消息，默认为未读消息页面。**

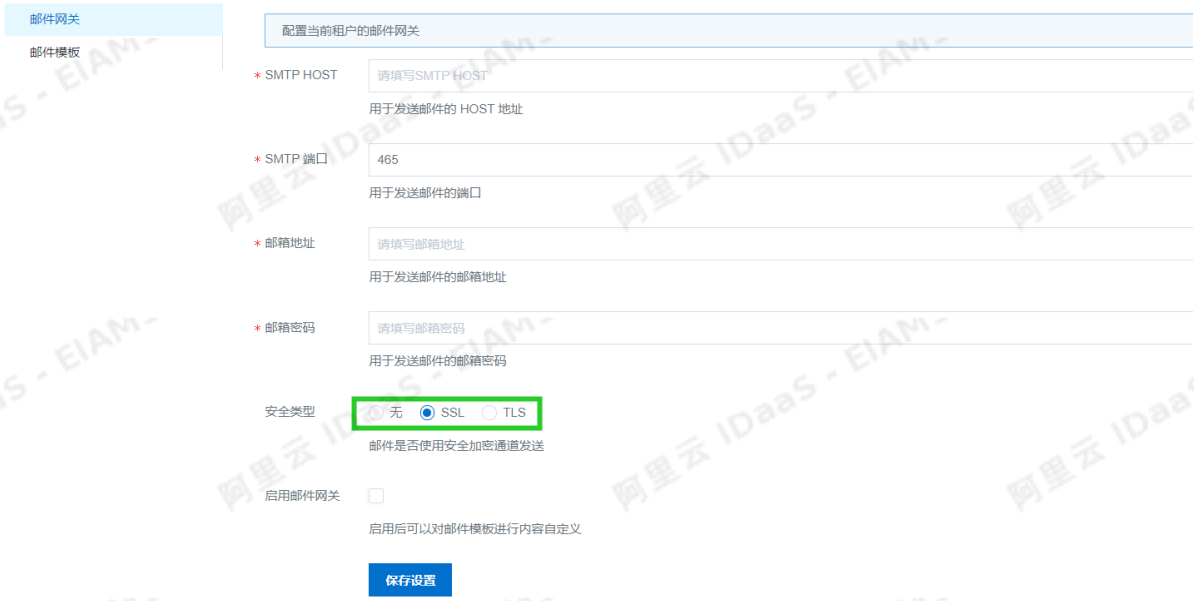


说明 未读的消息查看以后，会在已读消息栏展示，如果删除消息可以在已删除消息栏查看,也可以进行批量删除，

1.8. 设置

1.8.1. 邮件网关

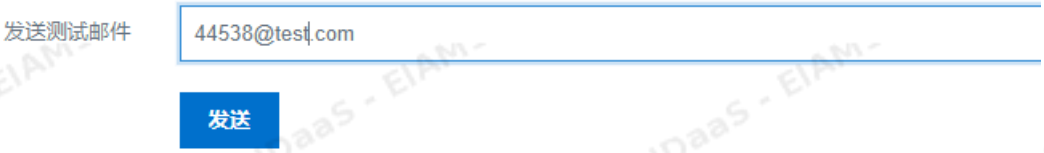
1. 请添加邮件网关正确的配置参数，并选择正确的安全类型



发送邮件进行测试，如果提示“发送失败，请检查配置”

a）请检查上文配置参数是否正确

b）请确认邮件网关白名单中添加了IDaaS出口的IP



1.8.2. 安全设置

1.8.3. 用户自助注册及风险识别

IDaaS支持管理员开启用户自助注册功能。IT管理员开启注册功能以后，用户登录页面会展示注册按钮，用户可以自助完成注册并登录到IDaaS系统。注册功能还接入了阿里云的风险识别系统，智能判断当前注册行为是否存在风险，加强保护客户的身份安全。

管理员开启自助注册功能

操作步骤：

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，点击设置 > 安全设置。
3. 点击 **登录/注册** 页签，然后勾选允许注册功能。

完成上述步骤后，用户登录页会展示注册按钮。用户点击后，会进入到注册页面。完成注册后即可登录到IDaaS系统。

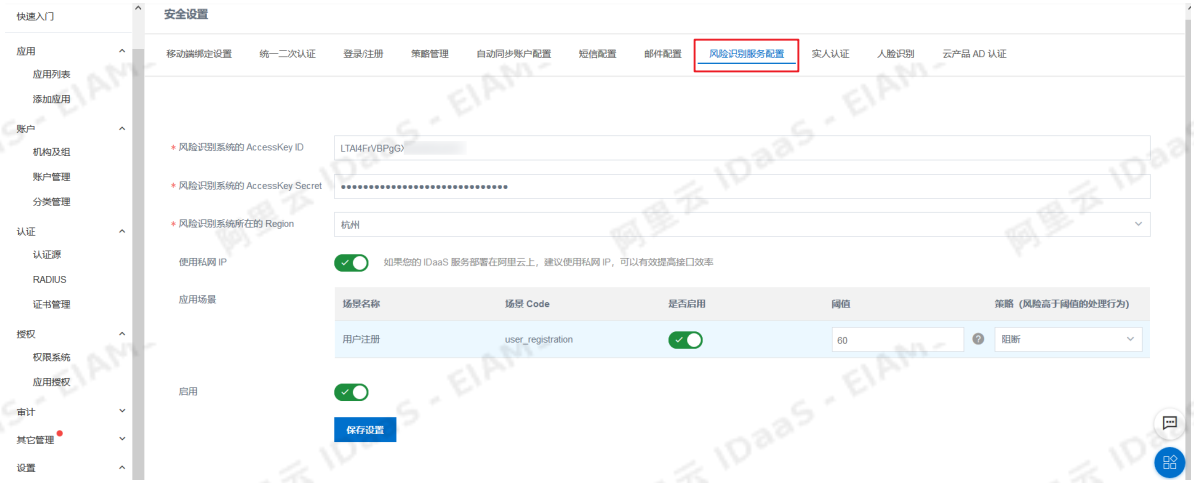

简体中文
扫码登录更便捷
阿里云 IDAAS
请输入账户 / 邮箱 / 手机号
请输入密码
请输入验证码
忘记密码
提交
注册
第三方认证登录
LDAP
LDAP
LDAP

注册功能接入风险识别

操作步骤

1. 开通阿里云风险识别服务。
2. 在阿里云AK管理平台获取用户的Access Key ID与Access KeySecret。
3. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
4. 在左侧导航栏，点击设置-安全设置。

5. 点击风险识别服务配置页签，在页面进行风险识别服务的配置



i. 将获取到的用户Access Key ID与Access KeySecre填写到对应的位置

ii. 选择服务器所在的region信息

iii. 启用用户注册场景并设定阈值

> **说明**
>
> 阈值只能填写 0-100 的数字。

iv. 启用风险识别功能并点击保存设置

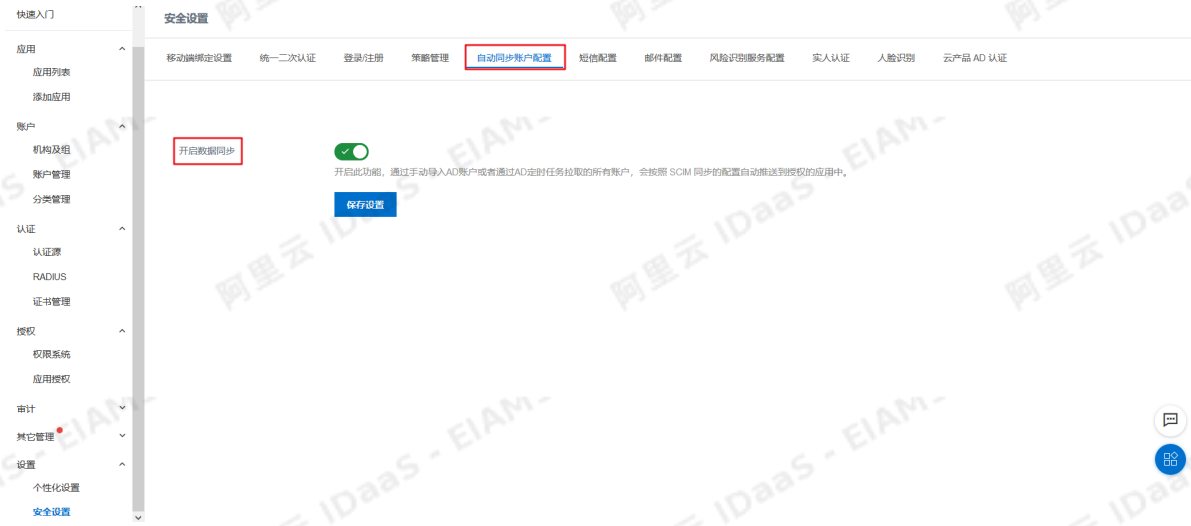
完成上述步骤后，注册功能就接入了风险识别服务。用户在提交注册请求时，系统会调用风险识别服务，然后根据风险识别服务的返回值和管理员设定的阈值进行对比，判断是否存在风险，有则阻止用户操作。

1.8.4. 自动同步账户配置

IDaaS支持定时或手动拉取 AD/LDAP 数据时，自动将账户数据推送到配置了SICM同步的应用系统中。

操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏，点击设置 > 安全设置。
3. 点击 **自动同步账户配置** 页签，然后点击启用数据同步。



4. 配置应用的SCIM同步，可参考同步账户到应用配置。

完成上述步骤，从AD导入账户及组织机构时，会自动将账户数据推送到配置了SICM同步的应用系统。

1.8.5. 个性化设置

2.普通用户指南

2.1. 操作导航

介绍普通用户在云盾IDaaS平台上的常用操作，具体包括免登应用、应用管理、关联应用子账户。

免登应用

普通用户登录后，首页即为免登应用页面。免登应用一般是与企业相关的业务应用，是可以通过IT管理员的配置实现单点登录的应用集合。要在免登应用页面直接登录应用，首先必须由IT管理员为您的账号添加应用访问权限，然后您必须完成以下任务：

- 配置关联应用子账户
- 启用应用

操作步骤

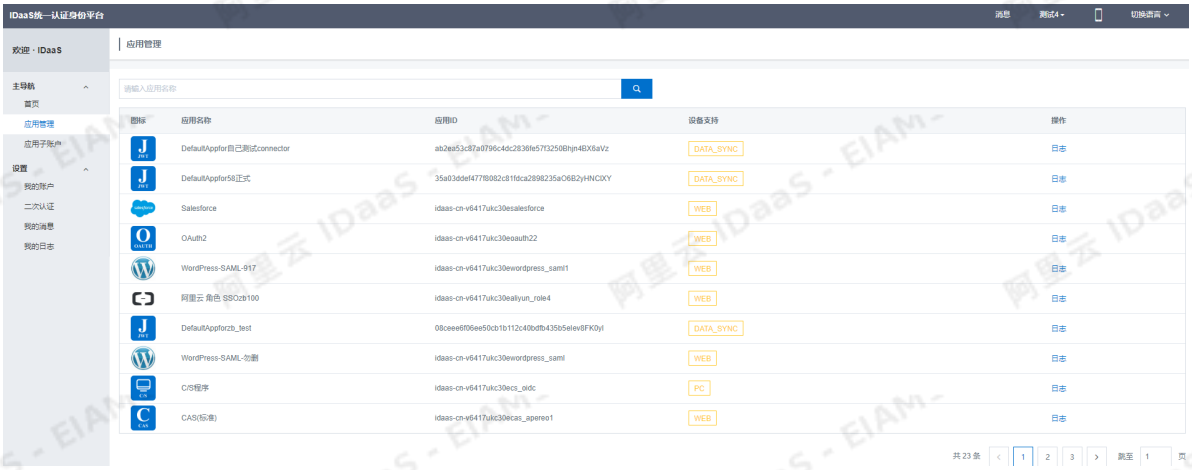
1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
2. 在**我的应用**页面，单击一个免登应用，直接访问。

应用管理

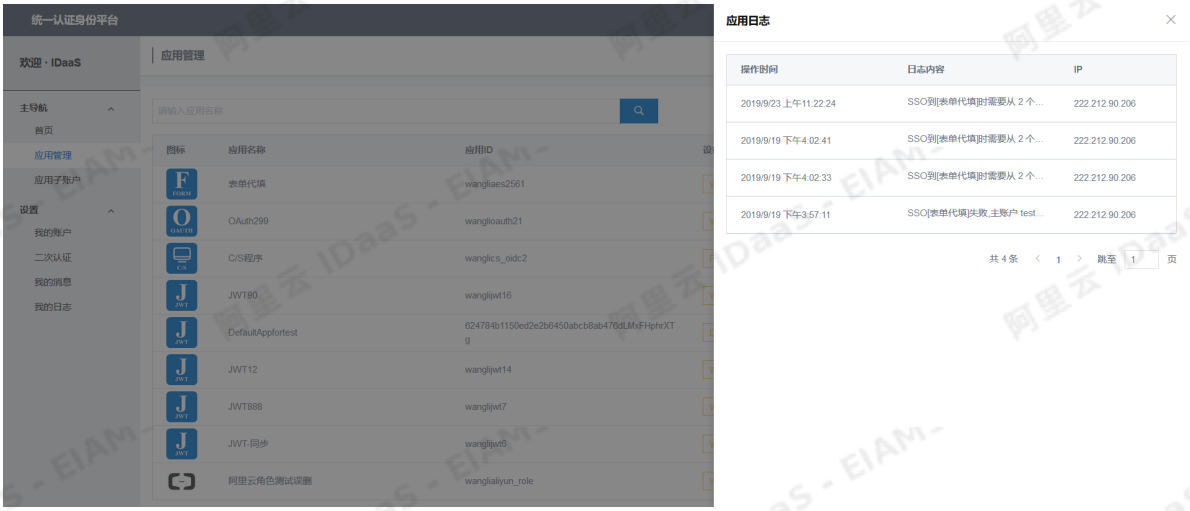
普通用户可以通过应用管理，自行维护免登应用页面所展示的应用信息。

操作步骤

1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
2. 在左侧导航栏，单击**主导航 > 应用管理**。



3. 查看应用操作日志。单击应用操作列下的**日志**，查看应用的操作记录。



关联应用子账户

当IT管理员为您的账号新添加一个应用的访问权限时，如果您想在免登应用页面中单点登录该应用，必须为应用配置子账户关联。

操作步骤

1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
2. 在左侧导航栏，单击**主导航 > 应用子账户**。
3. 在**应用子账户**页面，单击**添加应用子账户**。

4. 在**应用子账户**侧边页，完成以下配置。
   - **选择应用**：选择要关联的应用。

> **说明** 根据管理员在添加应用时为应用配置的账户关联方式，您可能需要不同的操作来完成账户关联。
>
> - 当应用采用手动关联（账户关联/账户映射）时，您需要提供正确的用户名， 后台管理员审批后才能关联成功； 或是管理员直接为您设置关联。
> - 当应用采用自动关联（账户+密码）时，您需要提供正确的用户名/密码， 后台校验通过后才能关联成功。

- **子账号**：输入子账户名称。
- （仅在应用采用自动关联时需要提供）**子账号密码**和**子账号密码确认**：输入子账户对应的密码。

> **说明** 同一个应用可添加多个子账户关联，免密登录时选择子账户进行登录即可。

5. 单击保存。

子账户关联成功后，且应用已启用，您就可以在免登页面单击已配置的应用，通过子账户直接登录。

2.2. 登录

介绍普通用户如何登录云盾IDaaS管理平台。

普通用户指由IT管理员创建或导入的员工账号，是云盾IDaaS身份管理系统的最终使用者。IT管理员创建普通用户账号后，为其分配应用权限并配置登录认证方式。

普通用户通过云盾IDaaS用户Portal地址登录，在免登应用页面查看被授权访问的应用，并执行关联应用子账户操作；完成子账户关联后，普通用户就可以通过单点登录方式免登录访问应用。

PC端登录

1. 通过PC端浏览器访问云盾IDaaS用户Portal地址。

> **说明** 该地址由IT管理员提供。IT管理员可以在云盾IDaaS实例列表中查看用户访问的Portal地址。

2. 在登录页面，输入手机号码/账户名称/邮箱和密码，并完成验证，进行登录。

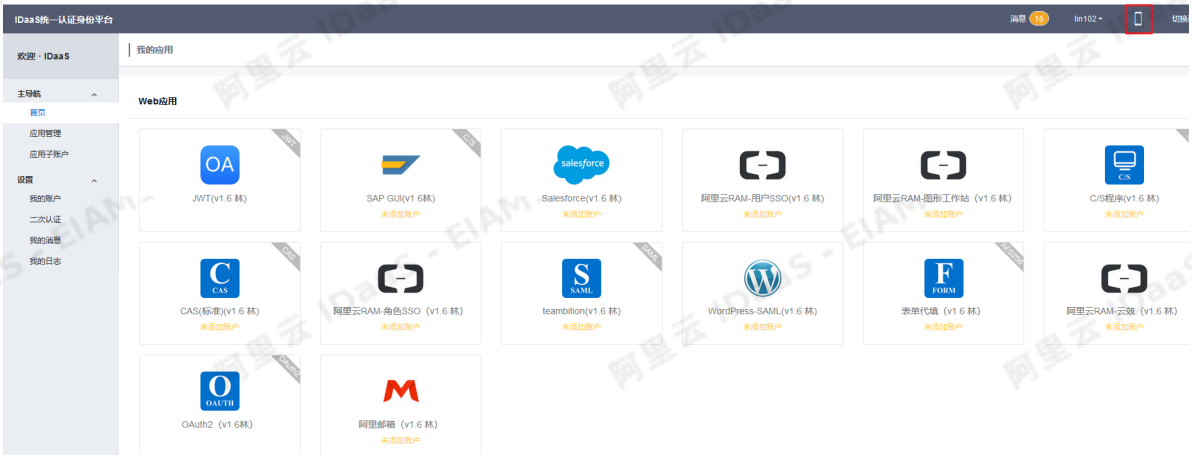
如果您已安装云盾IDaaS移动端App，推荐您使用扫码登录。扫码登录方式更便捷。

> **说明** 关于安装和配置云盾IDaaS App，请参考移动端登录。

移动端登录

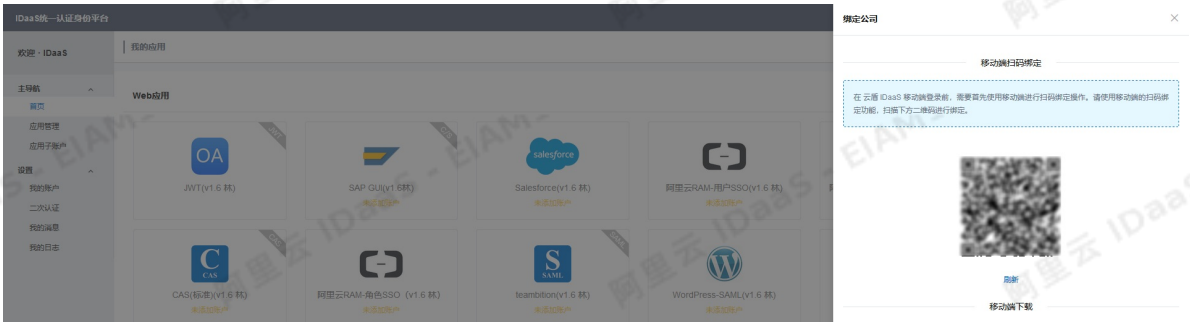
云盾IDaaS提供移动端App。您可以在用户首页扫码下载并安装云盾IDaaS App；安装云盾IDaaS App后，完成绑定公司操作，就可以使用云盾IDaaS App访问云盾IDaaS服务。

1. 用户登录PC端云盾IDaaS平台。
2. 在**主导航 > 首页**，单击页面右上角的移动端图标，展开侧边页。



3. 下载并安装移动端云盾IDaaS App

4. 打开云盾IDaaS App，扫描侧边页中的二维码，绑定公司。



5. 在登录页输入IDaaS的账户名和密码进行登录

说明 用户第一次登录需要输入账户名和密码，登录成功后会自动下载移动端证书，并开启免密登录功能。之后用户可以直接点击免密码登录，登录移动端云盾IDaaS APP。用户可以在安全中心关闭证书免密登录。

用户登录成功后，可以通过云盾IDaaS App直接使用云盾IDaaS服务。

2.3. 设置

介绍普通用户在云盾IDaaS平台上的常用设置，包括账户设置、二次认证设置、查看消息和日志。

账户设置

您可以在**我的账户**页面查看当前账户的完整信息。

操作步骤

1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
2. 在左侧导航栏，单击**设置 > 我的账户**。
3. 根据需要完成以下设置：
   - 在**账户安全**页签下，修改账户**登录密码**，绑定**邮箱账号**或**手机号码**。

     > **说明** 绑定后的手机号可用于手机号+密码登录，以及短信验证码登录；绑定后的邮箱可用于邮箱+密码登录，以及找回密码。

   - 在**个人信息**页签下，查看账户的应用和子账户信息，修改账户的**显示名称**。

   - 在**我的证书**页签下，查看用户个人证书及证书密码。并可以将用户证书下载至本地。

- 若IT管理员已开启外部认证且外部认证源支持绑定，您可以在**三方账户**页签下绑定第三方账户。

二次认证

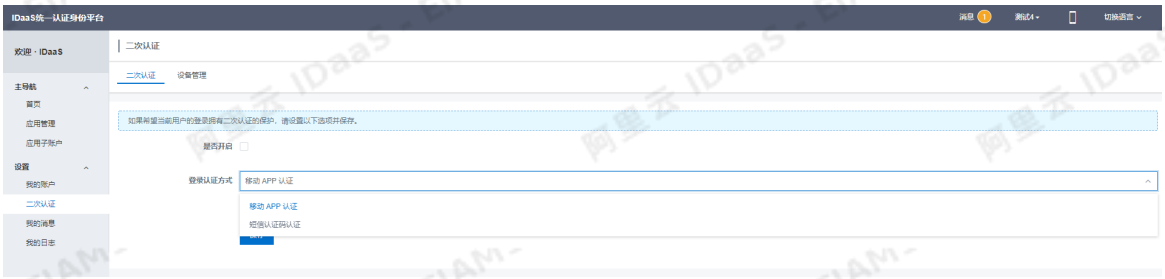
普通用户可以自行设置是否开通二次认证。开启二次认证后，普通用户在登录网页端时，手机端会收到推送或者动态口令，完成二次认证后，方可登录。

支持的二次认证方式包括：

- 移动App认证：通过云盾IDaaS App进行二次认证，具体支持以下实现方式。
  - 通过移动设备接收二次认证的推送或者二次认证的扫码认证。
  - 通过移动端显示的OTP Code 6位数进行二次认证，用于离线状态下的二次认证，特指手机接收不到推送的情况。
- 短信认证码认证：通过短信接收认证码进行二次认证。

操作步骤

1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
2. 在左侧导航栏，单击**设置 > 二次认证**。
3. 根据需要完成以下设置：
   - 在**二次认证**页签下，选择**是否开启**二次认证和**登录认证方式**：**移动APP认证**、**短信认证码认证**。



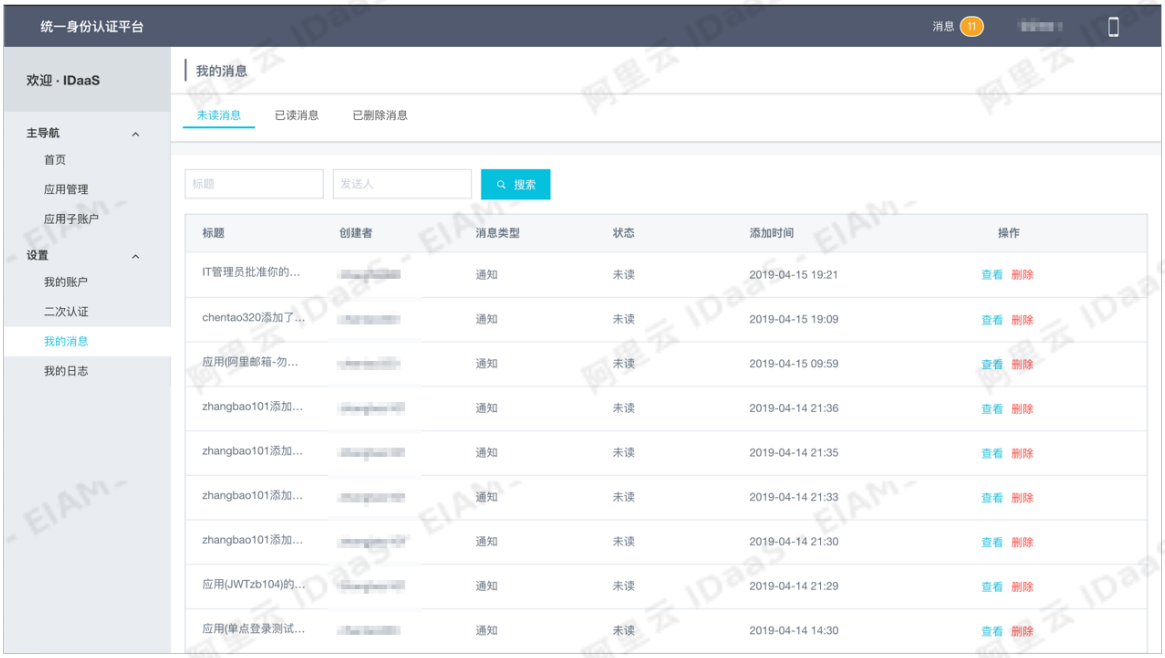
   - 在**设备管理**页签下，查看所有已绑定的设备，发现可疑设备及时删除,**可以展示二维码设备进行绑定**。

查看消息和日志

普通用户可以查看平台发出的消息信息，比如：通知、公告等。消息被查看后会归档在已读消息中，消息被删除后会归档在已删除消息中。

操作步骤

1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
2. 在左侧导航栏，单击**设置 > 我的消息**，查看所有收到的消息记录。
   - **未读消息**页签下罗列所有未读消息，您可以**查看**或**删除**某条消息。
   - **已读消息**页签下罗列所有已读消息，您可以**查看**或**删除**某条消息。
   - **已删除消息**页签下罗列所有已删除的消息，您可以**查看**某条消息。



3. 在左侧导航栏，单击**设置 > 我的日志**，查看所有日志记录。支持使用操作类型筛选日志记录。