Paraview IAM 快速入门指南

版本：6.1

简体中文版

翻译日期：2025 年 5 月 27 日

目录

1 统一认证

IAM 提供统一认证服务，用户只需认证一次即可访问所有业务系统。

1.1 配置认证方法

首先，通过选择支持的认证方法进行集成配置。这些方法可用于登录认证或多因素认证（MFA）。

让我们配置两种认证方法：[企业安全应用动态码] 和 [企业安全应用二维码]，以在不同场景中使用，如下所示：

功能菜单：安全认证 > 认证方法 > 认证设置

认证方法	**描述**
企业安全应用动态码 企业安全应用二维码	保持默认配置

表 1: 认证方法配置

1.2 登录认证

在配置 [企业安全应用动态码] 和 [企业安全应用二维码] 认证方法后，我们将使用 [企业安全应用动态码] 进行登录。

功能菜单：策略管理 > 登录页面策略 > 登录页面配置

在此功能中，您可以自由配置登录页面样式。选择 [默认登录页面]，在 [常规登录] 下勾选 [企业安全应用动态码] 认证方法，然后保存。现在，退出登录并返回登录页面查看效果！您应该可以使用 [企业安全应用动态码] 登录。

安装企业安全应用并尝试使用它登录。
企业安全应用 - iOS 安装方法：
企业安全应用 - Android 安装方法：
使用企业安全应用中提供的测试账户和密码登录以获取动态码。在 IAM 登录界面输入动态码即可登录！

1.3 单点登录（SSO）

为实现单点登录，成功配置后用户可以通过单点登录方式登录。

1.3.1 SSO 配置

功能菜单：应用管理 > 应用配置

使用提供的 DEMO 应用。编辑 DEMO 应用的基本信息并输入认证信息。开启 SSO 开关，选择 OIDC SSO 协议，并按以下参数配置：

认证参数	描述
clientID	
clientSecret	
回调 URL	
访问令牌最大有效期（秒）	
访问令牌有效期（秒）	
令牌刷新	
TGT 刷新	
单点登出	
自定义授权参数	
授权模式	
用户信息字段	

表 2: SSO 认证参数

1.3.2 单点登录方式

SSO 配置完成后，您可以在以下两种场景中使用单点登录：

SSO 场景

1. 用户访问 IAM 系统，登录后在门户页面点击应用图标进行 SSO
2. **配置要求**：
   - 应用管理 > 应用配置 > 编辑 > 认证信息已配置。
   - 应用管理 > 应用配置 > 编辑 > 基本信息中 [在自助服务中显示] 字段已启用。
   - 如果下游业务系统账户未在 IAM 系统中维护，禁用 [强制账户验证] 字段。
   - 如果下游业务系统账户在 IAM 系统中维护，用户必须拥有启用账户才能显示图标。
   - 要配置默认浏览器，在 [安全认证 > 认证方法 > 更多认证设置] 中勾选 [跨浏览器登录认证]。用户在第一次点击时需安装 ESSO 插件。

3. 用户直接访问业务系统，经过统一认证后自动登录

2 二次认证

对于高风险的外部用户登录或访问敏感应用，仅一次登录认证不足以确保安全。二次认证可实现更精确的访问控制。

使用之前配置的 [企业安全应用动态码] 和 [企业安全应用二维码] 方法，我们将使用 [企业安全应用二维码] 进行二次认证。

2.1 登录二次认证

登录认证后，用户需进行二次认证才能成功登录。为不同用户组配置不同的二次认证方法。

让我们配置以下场景：[陌生设备登录] 触发 [企业安全应用二维码] 进行二次认证。

功能菜单：认证策略 > 用户风险策略

- **步骤 1**：选择 [默认用户风险策略]，编辑为 [所有用户]，点击 [下一步] 进入 [IDA 风险策略]。
- **步骤 2**：选择 [或]，勾选 [陌生设备登录]，将处理方式设置为 [二次认证]，点击 [下一步] 进入 [二次认证]。
- **步骤 3**：选择 [单一认证]，选择 [企业安全应用二维码]，点击 [下一步] 进入 [认证成功/失败]。
- **步骤 4**：启用认证成功状态，配置为 1 天内账户和设备可信；取消所有认证失败选项。
- **步骤 5**：预览后保存。

现在，退出登录并返回登录页面。使用正确账户和密码登录后，系统将提示使用 [企业安全应用二维码] 进行二次认证。

认证成功后，退出并再次登录，无需二次认证，因为您的账户和设备已被信任！但更换设备将需要再次进行二次认证。

2.2 应用单点登录二次认证

对于某些应用或用户，即使完成 SSO 后仍需二次认证才能访问。让我们为登录 DEMO 应用配置 [企业安全应用二维码] 进行二次认证。

- **步骤 1**：选择 [默认应用强认证策略]，编辑为 [所有用户]，点击 [下一步] 进入 [二次认证]。
- **步骤 2**：选择 [单一认证]，选择 [企业安全应用二维码]，点击 [下一步] 进入 [认证失败]。
- **步骤 3**：配置认证失败为 1 天内失败 999 次，取消报警框。
- **步骤 4**：预览后保存。

现在，尝试单点登录。您将被提示使用 [企业安全应用二维码] 进行二次认证。

3 身份管理

在后台管理界面中，管理系统的基本数据，如组织、职位和用户数据。

3.1 上游数据源同步

除手动创建/导入用户信息外，主要数据通常从上游系统同步到 IAM。让我们配置 AD 身份源同步的场景。

功能菜单：身份管理 > 身份源管理

- **步骤 1**：创建新的身份源并配置基本信息。

字段	**描述**
身份源名称	根据需要命名，例如“AD 数据源同步”
状态	启用
CRON	默认每天凌晨 2:00 同步，测试时调整为 10 分钟后
仅当范围内字段发生变化时同步	保持默认
启用同步异常通知	保持默认

表 3: 身份源基本信息

- **步骤 2**：数据源同步配置

选择 [AD] 同步类型插件并按以下参数配置：

点击 [测试连接] 检查效果。

- **步骤 3**：映射配置

同步参数	**描述**
IP 或主机名	
端口号	
BaseDN	
启用 SSL	
密钥库路径	
密钥库密钥	
域名	
用户名	
密码	
组织过滤 BaseDn	
用户过滤 BaseDn	
组织过滤包含子级别	
用户过滤包含子级别	
组织过滤条件	
用户过滤条件	
应用代码	

表 4: AD 同步参数

中间表同步配置

中间表上游属性

主表同步配置：AD 数据源同步需要映射关系。首先在 [平台管理 > 映射字典] 中维护映射关系。

用户表同步动作模式	中间表/表达式	映射字典

表 5: 映射配置

配置完成后，等待几分钟同步时间。在 [身份管理 > 组织管理 & 职位管理 & 用户管理] 中查看 IAM 系统中同步的组织、职位和用户信息。

3.2 账户管理

在管理账户之前，确保系统中已维护需要账户管理的应用，例如提供的 DEMO 应用（应用管理 > 应用配置）。

IAM 系统允许集中查看和控制 DEMO 系统中的账户。让我们创建一个账户。

功能菜单：应用管理 > 账户管理

- **步骤 1**：选择 DEMO 应用，进入账户管理，创建新账户。
- **步骤 2**：选择 [用户名]，输入账户详情和名称，选择账户类型为 [个人账户]，然后保存。

账户创建成功。但账户尚未同步到 DEMO 业务系统。需要配置账户同步。

3.3 同步配置

功能菜单：应用管理 > 应用配置

请使用提供的 DEMO 应用。编辑 DEMO 应用的基本信息后，进入同步信息，开启数据同步开关，选择 API 同步方法，选择 DIM-API 推送插件，并按照以下说明配置参数。尝试一下（详情待补充）：

同步参数	描述
URL 加密方法 认证方法 AppID AppSecret 推送明文密码	

表 6: 同步参数配置

仅配置同步参数不足以完成同步，还需配置同步映射管理。

返回应用列表，点击 DEMO 应用的 [字段同步配置] 功能。在此配置用户属性与业务系统账户属性之间的映射关系。勾选 [账户]、[账户名称]、[密码] 和 [状态]。

现在，返回功能菜单：应用管理 > 账户管理，尝试创建新账户。账户是否已同步到下游系统?

4 用户生命周期管理（配置策略）

通过 [身份管理] 功能配置，我们可以在 IAM 系统中分别管理用户和账户。然而，在实际管理中，我们希望根据人员入职、调动、调整和离职自动处理账户。此时，需要使用 [配置策略] 功能。

4.1 权限模型配置

首先，我们需要配置权限模型，将特定用户组与特定应用组关联。

功能菜单：授权中心 > 权限模型

为所有用户创建一个权限模型。

字段	**描述**
名称	根据需要命名，可设为“公共权限模型”
模型类型	公共权限
描述	-
状态	启用
配置权限信息	选择提供的 DEMO 应用

表 7: 权限模型配置

流程权限信息

4.2 配置策略配置

功能菜单：授权中心 > 配置策略 > 账户配置

创建一个配置策略。

字段	**描述**
策略名称	根据需要命名，可设为“DEMO 配置策略”
配置状态	启用
模型类型	公共权限
模型名称	选择刚刚配置的权限模型
备注	-

表 8: 配置策略配置

接下来，在第二步生命周期中，配置添加、修改、删除、启用、禁用或更改用户密码时如何处理业务系统账户。

首先，配置添加效果。勾选生命周期中的 [添加] 并保存。现在可以查看效果。

- **步骤 1**：返回功能菜单 [身份管理 > 用户管理] 创建用户。
- **步骤 2**：用户创建成功后，返回功能菜单 [应用管理 > 账户管理]，打开 DEMO 应用。您能看到为新创建的用户自动创建了账户吗?
- **步骤 3**：打开 DEMO 应用。您能看到自动创建的账户吗?

此时，您已了解配置策略的基本功能，还有更多功能等待您探索!

5 身份治理

通过 [身份管理] 功能配置，我们学习了一系列身份管理操作。

除日常管理外，我们还需要持续监控身份异常并及时处理。此时，我们进入身份合规治理，可以配置适当的策略进行自动化处理。

5.1 平台用户身份治理

功能菜单：授权中心 > 账户策略 > 平台账户策略

异常类型	描述
平台僵尸账户	未在一定时间内登录 IAM 系统的用户为 [平台僵尸账户]
平台空账户	未关联任何业务系统账户的用户为 [平台空账户]

表 9: 平台账户异常类型

让我们创建一个 [平台僵尸账户] 策略查看效果。

字段	描述
策略名称	根据需要命名，可设为“平台僵尸账户策略”
配置状态	-
策略类型	平台僵尸账户
模型名称	1 天
策略操作	将账户操作勾选为 [禁用]
策略执行方法	设置为自动执行，保持默认检查频率（默认每天 00:00 检查）
策略状态	启用

表 10: 平台僵尸账户策略

前往功能菜单：身份管理 > 用户管理，创建测试用户。退出登录，等待 2 天（检查时间为每天 00:00，需等待检查执行以查看效果），然后重新登录 IAM 平台，查看账户是否已被禁用。

5.2 应用账户治理

功能菜单：授权中心 > 账户策略 > 应用账户策略

让我们创建一个 [应用孤儿账户] 策略查看效果。

异常类型	描述
应用僵尸账户	未在一定时间内登录业务系统的账户为 [应用僵尸账户]
应用孤儿账户	未关联任何 IAM 用户的账户为 [应用孤儿账户]
应用重复账户	关联多个 IAM 用户的账户为 [应用重复账户]

表 11: 应用账户异常类型

字段	描述
策略名称	根据需要命名, 可设为“应用孤儿账户策略”
策略备注	-
策略类型	应用孤儿账户
策略范围	选择提供的 DEMO 应用
策略操作	将账户操作勾选为 [禁用]
策略执行方法	设置为手动执行
策略状态	启用

表 12: 应用孤儿账户策略

前往功能菜单：应用管理 > 账户管理，创建测试用户，然后返回账户列表，点击 [主账户绑定] 功能解除 IAM 用户绑定。

然后，返回功能菜单：授权中心 > 账户策略 > 应用账户策略，找到刚创建的策略，点击 [立即执行]。

查看新创建的应用账户是否已成功禁用！

6 隐私保护

通过 [身份管理] 功能配置，创建 IAM 用户后，我们需要全面保护用户信息，支持前端脱敏显示和数据库加密存储。

功能菜单：策略管理 > 脱敏策略

6.1 前端脱敏显示

我们可以尝试配置手机号码的脱敏显示，效果如下：

返回自助服务门户，进入个人中心。您可以看到手机号码已以脱敏方式显示！

字段	描述
脱敏字段	手机号码
用户角色	普通用户
脱敏方法	无效
脱敏范围	从开头第 2 个字符到结尾倒数第 2 个字符
允许用户查看明文	否

表 13: 前端脱敏显示配置

6.2 后端存储加密

我们可以按照以下说明配置手机号码加密。

字段	描述
脱敏字段	手机号码
加密算法	DES（默认为 DES，可在功能菜单：平台管理 > 系统设置 > 安全配置 > 业务字段加密中修改）

表 14: 后端存储加密配置

配置完成后，检查数据库中 IAM 用户表的手机号码字段。手机号码已加密。

7 安全审计

功能菜单：审计管理

IAM 系统提供安全审计服务。进入相应功能查看审计相关信息。