# 目录

# SSO概览

金山云支持基于SAML 2.0的SSO（Single Sign On，单点登录），也称为身份联合登录。

## 使用场景

如果您的企业或组织已有自己的账号体系，同时希望管理组织内成员使用金山云资源，金山云提供SSO功能，您不必在金山云账户中为每一位组织成员创建子用户，您可以使用此功能管理外部用户身份，可以向这些外部用户身份授予权限使用您的金山云资源。为了更好的理解SSO，下面简要介绍与SAML/SSO相关的一些基本概念。

## 基本概念

### 身份提供商（IdP）

- 一个包含有关外部身份提供商元数据的实体，身份提供商可以提供身份管理服务。
- 企业本地IdP：Microsoft Active Directory Federation Service （AD FS）、Shibboleth等。
- Cloud IdP：Azure AD、Google G Suite、Okta、OneLogin等。

### 服务提供商（SP）

利用IdP的身份管理功能，为用户提供具体服务的应用，SP会使用IdP提供的用户信息。一些非SAML协议的身份系统（例如：OpenID Connect），也把服务提供商称作IdP的信赖方。

### 安全断言标记语言（SAML 2.0）

实现企业级用户身份认证的标准协议，它是SP和IdP之间实现沟通的技术实现方式之一。SAML 2.0已经是目前实现企业级SSO的一种事实标准。

### SAML断言（SAML assertion）

SAML协议中用来描述认证请求和认证响应的核心元素。例如：用户的具体属性就包含在认证响应的断言里。

### 信赖（Trust）

建立在SP和IdP之间的互信机制，通常由公钥和私钥来实现。SP通过可信的方式获取IdP的SAML元数据，元数据中包含IdP签发SAML断言的签名验证公钥，SP则使用公钥来验证断言的完整性。

## 功能特性

- 无需创建金山云账号 企业客户无需为组织内每个成员创建金山云账号，避免因用户所分配的长期访问证书（例如云 API 密钥）泄露而导致的安全问题。
- 提供联合单点登录（SSO） 企业客户已有身份验证体系的场景下，通过身份提供商可实现联合单点登录（SSO）。
- 简化身份验证登录流程 因身份提供商提供登录代码，企业客户能够低成本完成与金山云的联合身份验证，便捷上云。

# 基于 SAML 2.0 的SSO

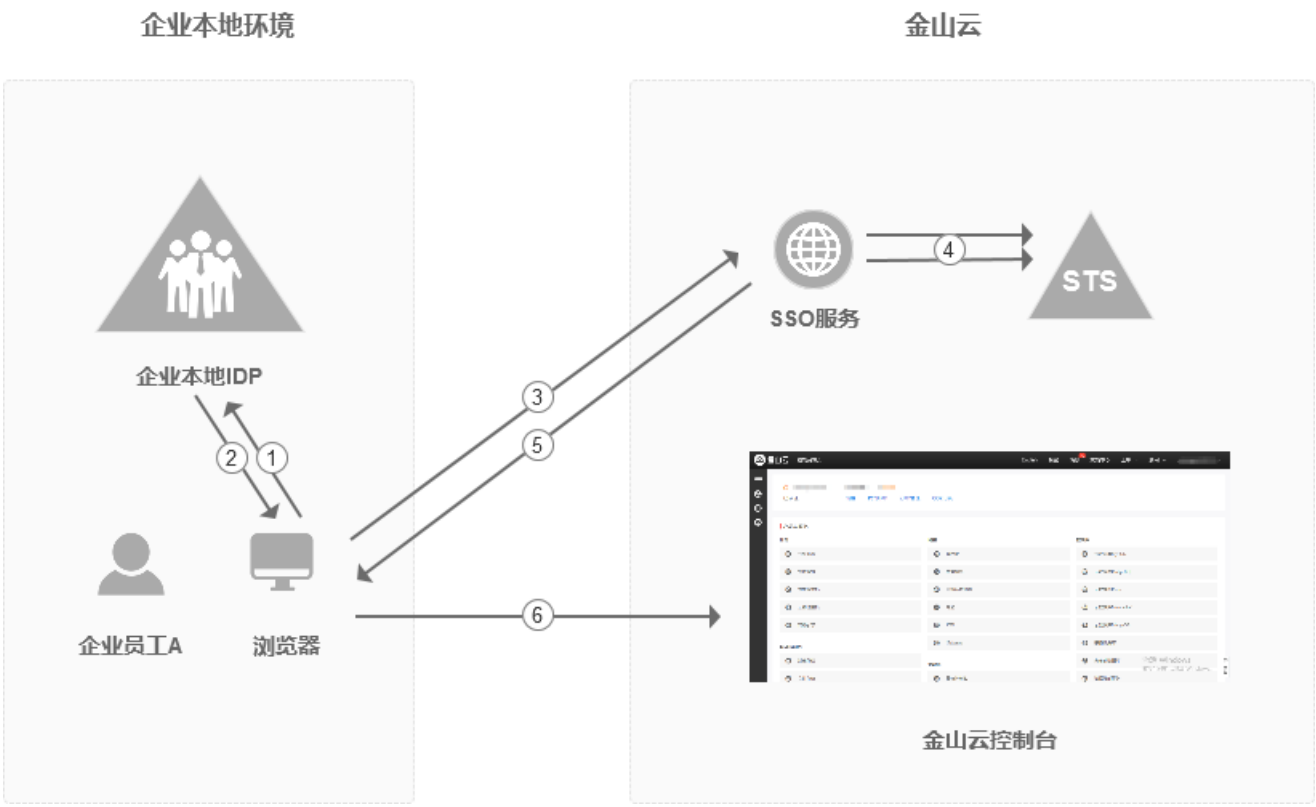
本文主要介绍使用基于 SAML 2.0 联合身份验证实现联合单点登录（SSO）的基本流程和步骤。

## 背景说明

金山与企业进行角色SSO时，金山云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过角色SSO，企业可以在本地IdP中管理员工信息，无需进行金山云和企业IdP间的用户同步，企业员工将使用指定的角色来登录金山云。

## 基本流程

通过SSO，企业员工可以通过控制台访问金山云。




1. 企业员工A使用浏览器在IdP的登录页面中选择金山云作为目标服务。 例如：如果企业IdP使用AD FS（Microsoft Active Directory Federation Service），则登录URL为：https://ADFSServiceName/adfs/ls/IdpInitiatedSignOn.aspx。

   有些IdP会要求用户先登录，再选择代表金山云的SSO应用。

2. IdP生成一个SAML响应并返回给浏览器。
3. 浏览器重定向到SSO服务页面，并转发SAML响应给SSO服务。
4. SSO服务使用SAML响应向金山云STS服务请求临时安全凭证，并生成一个可以使用临时安全凭证登录金山云控制台的URL.

   如果SAML响应中包含映射到多个角色的属性，系统将会首先提示用户选择一个用于访问金山云的角色。

5. SSO服务将URL返回给浏览器。
6. 浏览器重定向到该URL，以指定角色身份登录到金山云控制台。

# SSO配置步骤

为了建立金山云与企业IdP之间的互信关系，需要进行金山云云作为SP的SAML配置和企业IdP的SAML配置，配置完成后才能进行SSO。

## 第一步：在企业组织中配置基于 SAML 2.0 的身份提供商

1. 企业IdP的SAML SP配置需要使用金山云云的SAML服务提供商元数据URL：[http://fe.ksyun.com/fs/ksyun-sp-metadata.xml]。

2. 在企业IdP中创建一个SAML SP，并根据实际情况选择下面任意一种方式配置金山云为信赖方：

   （1）直接使用上述金山云的元数据URL进行配置。

   （2）如果您的IdP不支持URL配置，您可以根据上述URL下载元数据文件并上传至您的IdP。

   （3）如果您的IdP不支持元数据文件上传，则需要手动配置以下参数：

   - Entity ID：urn:ksyun:cloudcomputing
     - ACS URL：https://signin.ksyun.com/saml-role/sso
     - RelayState：只支持配置跳转到金山云云控制台首页。

## 第二步：在企业IdP中配置SAML断言属性

金山云要求企业IdP生成的SAML断言里包含一些必要的信息以确定企业用户的登录身份，因此企业IdP必须进行属性配置来IAM角色，从而实现企业用户与金山云的SSO。

## 第三步：在金山云创建SAML身份提供商

1. 登录访问控制控制台。
2. 选择左侧菜单**SSO管理** 。
3. 在**SSO管理**页面中单击**创建身份提供商**按钮。
4. 在弹窗中输入**身份提供商名称**和**备注**，**上传元数据文档**。

- 元数据文档由企业IdP提供
- 一般为XML格式，包含IdP的登录服务地址、用于验证签名的公钥及断言格式等信息

5. 单击提交，完成创建。

## 第四步：在金山云为SAML身份提供商配置权限

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**界面，单击**新建角色**。
4. 在**新建角色**页面中，**设置授权实体类型**为**身份提供商**。
5. 输入角色名称和备注。
6. 在设置载体信息， 选择身份提供商。
7. 单击**下一步**，完成角色创建。

角色创建成功后，进入设置角色权限页面，您可以为该角色添加权限策略。

由于不同IdP的系统差异，关于SAML SP配置和断言属性配置的操作流程都有些差异。我们会提供一个以Azure AD与金山云进行角色SSO的示例，用于帮助理解企业IdP与金山云的端到端配置流程。