云SSO

目录

产品动态

产品动态.....2

产品介绍

产品定义.....3
基本概念.....3
使用场景.....3

计费说明

快速入门

开通云SSO.....5

用户指南

管理用户.....6
管理用户组.....7
管理权限集配置.....7
管理访问配置实例.....8
云SSO用户登录访问.....8

最佳实践

统一登录访问管理.....10
客户系统单点登录访问.....10

常见问题

常见问题.....12

使用协议

产品动态

2025年12月

时间节点	功能名称	功能描述	相关文档
2025年12月	云SSO	内测转商用	云SSO

产品介绍

产品定义

云SSO（SingleSignOn）是基于“组织管理”实现的多帐号统一身份管理与访问登陆控制的功能。并支持客户通过配置企业的身份管理系统与天翼云的单点登录，完成对天翼云多账号的登录访问。

基本概念

概念	说明
企业组织	企业组织是多账号下的成员关系管理服务，可以通过创建或者邀请账号加入，构建多账号的企业中心环境。
主账号	是企业组织中的管理员账号，可以统筹管理企业组织关系内各成员账号的资源、操作权限、财务关系等。
子账号	是通过被主账号创建或者邀请加入的成员账号。
云SSO用户/用户组	是主账号创建的虚拟用户，该用户可以通过云SSO门户登录到企业组织内的成员账号中，对成员账号进行访问管理。
权限集	主账号可以为云SSO实例自定义分配指定的权限集合。
绑定权限集	为云SSO用户（组）在指定账号范围内，绑定权限集。
云SSO登录门户	云SSO用户登入URL地址：https://www.ctyun.cn/h5/auth/sso/login/d-3f2516cbfb0444e2b0f64134c62c9baa
身份同步	云SSO支持基于SCIM协议的用户和用户组同步，称为身份同步，也可以称其为身份部署或身份推送等。使用身份同步，您只需在您的企业身份管理系统中管理身份，而不必在云SSO中手工管理用户、用户组及其成员关系，提升管理效率和安全性。
单点登录（SSO）	云SSO支持基于SAML 2.0的单点登录SSO（Single Sign On）。天翼云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过单点登录，企业员工可以使用IdP中的用户身份以云SSO用户身份访问天翼云。

使用场景

通过云SSO（SingleSignOn）可以创建用户和用户组，创建的用户通过指定的云SSO门户地址登录后，可集中管理和访问天翼云下多个帐号的资源。云SSO可与满足条件的企业身份管理系统进行单点登录（SSO）配置，可以直接使用企业原有的身份管理系统，以云SSO用户身份访问天翼云账号，提升企业用户管理效率，降低安全风险。

计费说明

开通云SSO

请确保您已开通了企业中心，并搭建了企业的多账号组织结构，只有企业中心的主账号才能开通并管理云SSO。

开通云SSO

前提条件

您已完成企业实名认证，并作为企业主账号开通了企业中心功能。

操作步骤

登录天翼云官网首页

单击右上角“个人账号”，选择“账号中心”

单击左侧导航栏“企业中心”，选择“云SSO”

按操作提示完成“云SSO”功能开通。

管理用户

创建用户

1.登录云SSO控制台（ 中国电信天翼云-管理中心 ）。

2.左侧菜单栏点击“云SSO”用户

3.点击右上角“创建用户”

4.在创建用户面板，设置用户基本信息，然后单击确定

- 用户名：用于天翼云识别登录用户
- 姓名：用于客户侧内部识别云SSO使用者
- 登录邮箱：不同云SSO用户不能使用相同邮箱
- 补充信息：可按需填写，满足客户的管理要求

5.选择密码初始化方式

- 向用户发送一封包含密码设置说明的邮件:用户可登录邮箱后自行设置密码
- 生成随机的一次性密码:由系统自动生成，云SSO用户创建完成后会弹窗显示

6.为云SSO用户分配用户组；

7.主账号进入云SSO用户的详情页，点击发送验证邮件（注意：请进入管理页面手动点击发送验证邮件）；

8.登录云SSO用户的关联邮箱，完成云SSO用户的创建验证

9.登录“云SSO控制台”-“云SSO用户”选择该用户信息，点击“启用”按钮。

9.完成创建。

查看用户详情

在云SSO用户页面，单击目标用户名称，可查看用户的以下信息：

用户名、用户ID、姓名、状态、邮件地址、创建时间、创建方式、更新时间等信息。

启用云SSO用户

完成邮箱初始化验证的用户可以进行用户启用。

主账号可进入云SSO用户详情页，点击发送验证邮件。

在“云SSO控制台”-“云SSO用户”选择该用户信息，点击“启用”按钮

禁用云SSO用户

在“云SSO控制台”-“云SSO用户”选择该用户信息，点击“禁用”按钮

禁用后，云SSO用户将无法登录组织内的成员账号

删除云SSO用户

删除用户前，请确保用户未关联以下资源，否则会删除失败。

授权：您需要移除用户在权限集上的绑定关系。

用户组：您需要将用户从用户组中移除。

删除方式

在云SSO用户页面，单击目标用户名称，进入“云SSO详情”页面

点击右上角“删除”

重置用户密码

在云SSO用户页面，单击目标用户名称，进入云SSO详情页面

点击右上角“重置密码”，您可选择随机生成密码，或通过邮件方式重新配置。

管理用户组

创建用户组

进入“云SSO”-“云SSO用户组”界面，点击“创建用户组”

输入用户组信息后，按需指定云SSO用户，点击“保存”。

查看用户组信息

在“云SSO用户组”界面，点击用户组名称，即可查看用户组信息。

删除用户组

在“云SSO用户组”界面，点击用户组名称进入用户组详情页后，点击“删除”，删除前请确认组内成员已移除。

为用户组添加/移除用户

在“云SSO用户组”界面，点击用户组名称，进入用户组详情页，点击“添加用户”或“移除用户”。

管理权限集配置

权限集概述

权限集是由客户自行在系统配置的访问权限集合。可以勾选需要的系统策略组合，也可以创建自定义权限策略。

权限集与云SSO用户（组）、待访问账号（组织成员），三者共同组成一个访问配置实例。

创建权限集

进入“权限集”界面，点击“创建权限集”

1. 填入基本信息，点击“下一步”，请注意权限集命名不能重复。
2. 为权限集分配系统权限，您也可以自定义配置权限集的授权。
3. 确认后点击“保存”

4. 查看与修改已创建的权限集

进入“权限集”界面，根据名称与描述选择对应的权限集，点击“编辑”进入编辑界面。

在编辑界面可查看与修改之前配置的权限集合。

复制已创建的权限集

进入“权限集”界面，根据名称与描述选择对应的权限集，点击“复制”，可快速创建相同配置的权限集，请注意修改权限集命名。

删除已创建的权限集

进入“权限集”界面，根据名称与描述选择对应的权限集，点击“删除”，可对权限集进行删除。

删除前，请确保该权限集已经从云SSO用户及成员账号中进行解绑，否则无法删除。

管理访问配置实例

通过权限集绑定，实现云SSO用户（组）、成员账号、权限集的关系建立，三者相互绑定形成一个访问配置实例。

创建权限集绑定

进入“权限集绑定”界面，点击“创建权限集绑定”，分别完成“选择账号与组织”“选择SSO用户/组”“选择权限集”“确认配置”后，即可创建一个访问配置实例。一个访问配置实例包含云SSO用户/组、所配置的权限集、需访问的账号或组织。

查询云SSO用户所绑定的访问配置实例

进入“权限集绑定”界面，上方找到“用户名称”搜索框，输入对应的云SSO用户名称后，点击“查询”。

修改云SSO用户所绑定的访问配置实例

进入“权限集绑定”界面，找到该云SSO用户所对应的访问配置实例，点击“编辑”后，对访问配置实例进行按需修改后保存。

删除访问配置实例

进入“权限集绑定”界面，列表中找到对应的实例，点击“删除”后确认。

云SSO用户登录访问

成员账号访问方式

云SSO用户有两种登入成员账号方式：

- 方式一：通过账号密码登录，登录地址可从“云SSO中心”-“概览”页查询并复制

默认地址：https://www.ctyun.cn/h5/auth/sso/login/d-3f2516cbfb0444e2b0f64134c62c9baa

门户地址支持自定义修改：可在“云SSO中心”-“管理设置”-“身份源” - “门户URL”中配置子网地址。

- 方式二：通过身份提供商以单点登录形式登录，需要预先完成相关配置。配置方式详见“外部身份同步及单点登录配置-云SSO-用户指南 - 天翼云”

系统默认使用账号密码方式登录，若您已完成单点登录配置，可在“云SSO”-“管理设置”-“身份源” 中，点击“身份提供商”，进行登入访问方式切换。完成切换后，系统将关闭云SSO用户通过账号密码的登录访问方式。

会话保持设置

会话保持设置指会话最长持续时间，及在用户必须重新进行身份验证之前可以登录的最长时间

可在“云SSO”-“管理设置”-“会话设置”中按需配置，系统默认为8小时。

统一登录访问管理

应用实践：主账号创建云SSO用户后，以云SSO用户身份访问子账号1与子账号2，且按需配置不同的权限

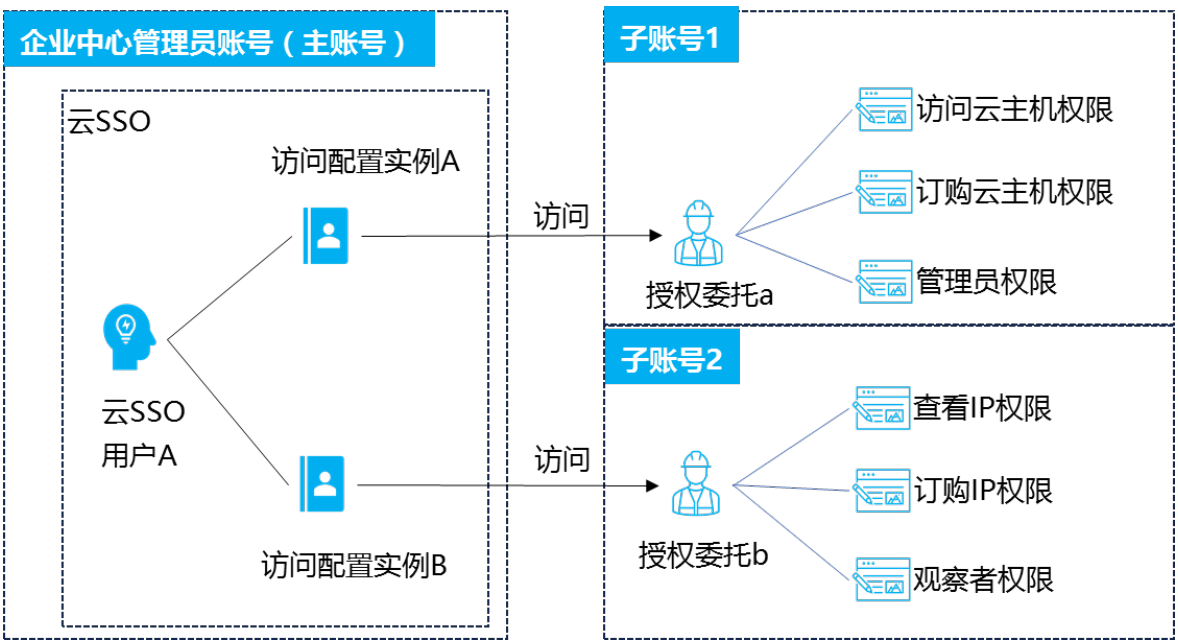
云SSO用户只能由企业中心主账号在云SSO中心创建，创建成功后，通过云SSO登录门户地址跳转访问组织内成员账号

步骤1：登录中国电信天翼云-管理中心，创建云SSO用户

步骤2：在“权限管理”菜单栏，按需创建权限集

步骤3：在“绑定权限集”菜单栏，创建访问配置实例，访问配置由云SSO用户/权限集/成员账号组成

步骤4：通过“云SSO门户地址”跳转访问组织内账号。



场景示意：

主账号分别配置了两个“访问配置”实例A与实例B：

1.实例A允许主账号所创建的云SSO用户访问子账号 1，登录后具备云主机与管理员相关的权限；

2.实例B允许主账号所创建的云SSO用户访问子账号 2，登录后具备弹性IP与观察者相关的权限。

客户系统单点登录访问

应用实践：客户已有账号体系单点登录后以云SSO用户身份访问成员账号

客户已有账号体系可以通过SAML2.0直接单点访问天翼云账号，并可以通过SCIM同步客户侧的用户/组信息；

最佳实践

步骤1：进入“云SSO中心”“管理设置”中，“身份源”选择“身份提供商”

步骤2：配置IDP的身份提供商标识，单点登录登出地址，身份提供商签名公钥等信息

步骤3：客户端配置SP元数据。天翼云SP META可从“管理身份提供商”页面获取

步骤4：配置SCIM同步（可选），配置方式参考“用户指南”。

常见问题

问题1：企业中心云SSO单点登录与IAM统一身份认证SSO单点登录的区别

回答：企业中心云SSO单点登录与IAM统一身份认证SSO单点登录均是基于标准的单点登录协议如SAML2.0，完成的单点登录跳转配置。统一身份认证中的身份提供商（SSO）是以IAM用户身份登录，只能访问IAM用户所属账号。云SSO身份提供商（SSO）以云SSO用户身份登录，可以切换访问多个账号。

问题2：云SSO用户与IAM用户的区别

回答：云SSO用户与IAM用户都是虚拟用户，其用户与用户组相对独立，无关联关系。云SSO用户主要使用场景是跨账号访问，IAM用户主要使用场景是同租户内的访问。

问题3：云SSO用户信息与官网账号信息是否可以重复，如邮箱/电话

回答：可以重复，云SSO与官网账号体系相互独立。

问题4：云SSO用户登入成员账号后是否支持分配CTIAM或企业项目权限

回答：不支持。云SSO用户访问不同账号的权限当前支持在”云SSO-权限集绑定”中完成。

使用协议