应用身份管理服务

最佳实践

文档版本 01

发布日期 2024-12-26

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 OneAccess 最佳实践汇总

本文汇总了基于应用身份管理服务 OneAccess中常见应用场景的操作实践，为每个实践提供详细的方案描述和操作指导，帮助用户轻松在不同应用场景中使用OneAccess。

表 1-1 集成身份源最佳实践一览表

最佳实践	说明
集成AD身份源	OneAccess支持通过AD身份源导入用户和组织信息，实现OneAccess实时同步AD身份源中用户和组织信息。OneAccess集成企业AD，支持LDAPv3协议。
集成LDAP身份源	OneAccess支持通过LDAP身份源导入用户和组织信息，实现OneAccess实时同步LDAP身份源中用户和组织信息。OneAccess集成企业LDAP，支持LDAPv3协议。

表 1-2 集成企业应用最佳实践一览表

最佳实践	说明
使用OneAcceess用户门户登录华为云	华为云支持基于SAML、OIDC协议的单点登录，企业管理员在华为云和OneAccess进行配置后，普通用户登录OneAccess用户门户，即可免密进入华为云Console系统或者是某个具体的华为云应用。

最佳实践	说明
通过SAML协议单点登录至应用	SAML即安全断言标记语言（Security Assertion Markup Language），是OASIS安全服务技术委员会的一个产品，是基于XML的开源标准数据格式。SAML可以解决Web端应用系统的单点登录（SSO）需求，在不同的安全域（security domain）之间交换认证和授权数据。
通过OAuth2.0协议单点登录至应用	OAuth2.0（开放授权）是一个开放标准，允许用户授权第三方应用访问其存储在资源服务器上的信息，而不需要将用户名和密码提供给第三方应用。
通过OIDC协议单点登录至应用	OIDC是OpenID Connect的简称，是一个基于OAuth 2.0协议的身份认证标准协议。关于OIDC的详细描述请参见欢迎使用OpenID Connect。 本文主要介绍OneAccess以OIDC协议集成应用的方法。
通过CAS协议单点登录至应用	CAS是一个基于HTTP2、HTTP3的协议，要求每个组件都可以通过特定的URL访问。通过CAS协议将OneAccess作为身份服务提供商，使第三方应用可以读取OneAccess的用户账号数据。支持CAS1.0、CAS2.0、CAS3.0三种协议。
以插件代填的方式集成应用	OneAccess可在PC端集成不支持标准协议（OAuth2、SAML、OIDC、CAS）且不可改造的应用。 本文主要介绍OneAccess以插件代填的方式集成应用。

表 1-3 同步企业数据最佳实践一览表

最佳实践	说明
通过SCIM协议同步数据至Atlassian	SCIM（System for Cross-domain Identity Management），主要用于多租户的云应用身份管理。SCIM 2.0建立在一个对象模型上，所有SCIM对象都继承Resource，它有id、externalId和meta属性，RFC7643定义了扩展公共属性的User、Group和EnterpriseUser。 本文主要介绍OneAccess以SCIM协议同步用户至Atlassian的方法。

最佳实践	说明
通过LDAP协议同步数据	LDAP（Lightweight Directory Access Protocol）即轻量目录访问协议。它是一种树状结构的组织数据，可以简单理解成一个存储用户和组织信息的树形结构数据库。单点登录是LDAP的主要使用场景之一，即用户只在公司计算机上登录一次后，便可以自动在公司内部网上登录。

表 1-4 集成认证源最佳实践

最佳实践	说明
内置认证源	本文为您介绍通过FIDO2认证源（人脸、指纹等生物认证）来登录OneAccess平台集成的应用系统。您可以在OneAccess平台中配置FIDO2认证源，在登录页面选择FIDO2登录方式登录各应用系统，从而实现单点登录的效果，在给用户带来更简易便捷的登录方式的同时提供更安全可靠的登录体验。
SAML认证登录	为方便企业用户的认证登录，OneAccess平台支持配置SAML协议作为认证源，用户可以通过SAML协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。
OIDC认证登录	为方便企业用户的认证登录，OneAccess平台支持配置OIDC协议作为认证源，用户可以通过OIDC协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。 OIDC是OpenID Connect的简称，是一个基于OAuth 2.0协议的身份认证标准协议。关于OIDC的详细描述请参见**欢迎使用OpenID Connect**。

最佳实践	说明
CAS认证登录	CAS是一个基于HTTP2、HTTP3的协议，要求每个组件都可以通过特定的URL访问。通过CAS协议将OneAccess作为服务提供商，使第三方应用的用户账号数据可以访问OneAccess。支持CAS1.0、CAS2.0、CAS3.0三种协议。 CAS 协议涉及两个主体。两个主体通过用户浏览器进行信息交换。如 CAS Client可以返回带参数的重定向，将信息转发给CAS Server。登录验证成功后CAS Server会返回CAS Client一个包含用户信息的XML， CAS Client验证用户信息后会返回给用户访问资源。 ● CAS Client：CAS客户端，资源提供方，如第三方应用。 ● CAS Server：CAS服务端，身份认证提供方，如OneAccess认证服务。 为方便企业用户的认证登录，OneAccess平台支持配置CAS协议作为认证源，用户可以通过CAS协议认证登录各应用系统以及实现应用系统间单点登录效果，为企业用户带来更简易便捷的登录方式和更好的用户体验。
OAuth认证登录	OAuth（开放授权）是一个开放标准，允许用户授权第三方应用访问其存储在资源服务器上的信息，而不需要将用户名和密码提供给第三方应用。 为方便企业用户的认证登录，OneAccess平台支持配置OAuth协议作为认证源，用户可以通过OAuth协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。

最佳实践	说明
Kerberos认证登录	Kerberos是一种计算机网络认证协议，它允许某实体在非安全网络环境下通信，向另一个实体以一种安全的方式证明自己的身份。具体请参考https://web.mit.edu/kerberos。 AD（Active Directory），即活动目录。您可以将AD简单理解成一个数据库，其存储有关网络对象的信息，方便管理员和用户查找所需信息。 SPN（Service Principal Name），即服务主体名称。是服务实例的唯一标识符。 在Kerberos认证过程中，使用SPN将服务实例与服务登录账号关联。所以，必须在内置计算机账户或用户账户下为服务器注册SPN。对于内置账户，SPN会自动注册。如果需要在域用户账户下运行服务，必须要为使用的账户手动注册SPN。 为方便企业用户的认证登录，OneAccess平台支持配置Kerberos协议作为认证源，用户可以通过Kerberos协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。
AD认证登录	AD全称Active Directory，即活动目录。您可以将AD简单理解成一个数据库，其存储有关网络对象的信息，方便管理员和用户查找所需信息。 为方便企业用户的认证登录，OneAccess通过LDAP协议把认证指向AD域，AD通过认证后，根据AD返回的用户属性与OneAccess用户关联属性做匹配校验，验证通过即可登录OneAccess。
LDAP认证登录	LDAP（Lightweight Directory Access Protocol），即轻量目录访问协议。 它是一种树状结构的组织数据，可以简单理解成一个存储用户和组织信息的树形结构数据库。单点登录是LDAP的主要使用场景之一，即用户只在公司计算机上登录一次后，便可以自动在公司内部网上登录。

表 1-5 其他最佳实践一览表

最佳实践	说明
授权IAM用户访问OneAccess实例管理门户	IAM用户是账号在IAM中创建的用户，是云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据账号授予的权限使用资源。 OneAccess支持IAM用户通过华为云访问服务实例，方便企业管理员安全的控制OneAccess服务和资源的访问权限。
企业API使用	OneAccess提供第三方API的授权管理功能，API提供者将API配置到OneAccess之后，API消费者在使用API之前需要先到OneAccess获取鉴权Token，在使用API时携带该鉴权Token，API提供者根据鉴权Token判断是否可以提供服务，用以实现API的授权管理功能。
用户登录二次认证配置	OneAccess支持用户登录时进行二次认证的功能，提供更为安全的保障，本文以用户门户为例，为您介绍如何实现二次认证的配置以及使用。

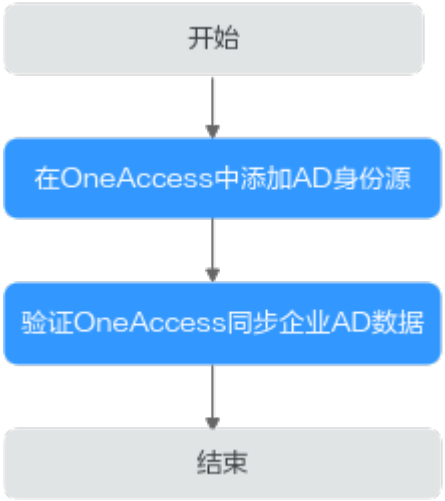
2 集成身份源

2.1 集成 AD 身份源

OneAccess支持通过AD身份源导入用户和组织信息，实现OneAccess实时同步AD身份源中用户和组织信息。OneAccess集成企业AD，支持LDAPv3协议。

本文主要介绍OneAccess集成企业AD身份源的方法。

配置流程



前提条件

- 请确保您已拥有企业AD平台账号管理员权限。
- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保当前OneAccess管理门户可以访问到企业AD平台。
- 请确保您已了解企业AD系统，了解企业AD系统参数获取方式、熟练使用企业AD系统。

在 OneAccess 中添加 AD 身份源

在OneAccess中配置身份源参数，确保OneAccess可同步企业AD中的数据。

步骤1 在OneAccess中创建身份源。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“用户 > 身份源管理”。
3. 在身份源管理页面，单击AD身份源操作列的“添加身份源”，输入“身份源名称”，单击“确定”。

步骤2 设置导入配置。

1. 在AD身份源列表页面，单击目标身份源的“详情”。

图 2-1 AD 身份源详情

2. 选择“导入配置”页签，填写导入配置参数并单击“确定”。
   - 基础配置：企业AD服务器的连接参数，实现OneAccess和企业AD的连接，请务必填写正确。

表 2-1 基础配置

参数	说明
*主机	运行企业AD服务器的主机名称或 IP 地址。
*TCP端口	用于与企业AD服务器进行通信的服务器TCP/IP 端口号。默认为389。 **说明** OneAccess目前只支持公网访问，需要提供公网地址，并开启389端口。
SSL	系统默认true，即使用 SSL 连接到 企业AD服务器。
StartTLS	是否启用startTLS进行加密通信 ■ true：启用StartTLS，且SSL不能设置为true； ■ false：不启用StartTLS。
校验证书	是否校验证书。仅在SSL为true或者StartTLS为true时有效。true: 校验证书，false: 不校验证书。证书必须是公网认证的证书，自签名证书不可以。
协议版本	系统默认TLSv1.2，推荐使用TLSv1.3、TLSv1.2。
*主体	进行企业AD服务器验证时使用的标识名，即拥有AD域读取权限的账号名。传参带域名，如“admin@test.com ”或“TEST\admin”。

参数	说明
*密码	主体账号的密码。
*基本上下文	搜索企业AD树时将使用该树中的一个或多个节点作为起始点，需填写要同步AD用户所在AD中的树的根节点，如“OU=huaweitest,DC=test,DC=com”。
*UID 属性	映射到UID属性的AD属性的名称。
*账户对象类	在AD树中创建新用户对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。

- 可选配置：可默认配置，如需同步密码需配置密码的相关参数，包括启用密码同步和要同步的密码属性，如出现同步异常，可根据实际的使用情况进行参数调整，包括但不限于账户对象类、机构对象类等参数。

表 2-2 可选配置

参数	说明
域名	域名存在时，回收的用户名中将该域名排除掉（存在多个域名用","分隔，默认用户名会排除域名）
账户用户名属性	保存账户用户名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的用户名的AD 条目。
机构对象类	在AD 树中创建新机构对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。
机构名属性	保存机构名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的机构名的 AD 条目。
故障转移服务器	列出首选服务器发生故障时将用于故障转移的所有服务器。如果首选服务器发生故障，JNDI 将连接到列表中的下一个可用服务器。按照 "ldap://ldap.example.com:389/" 格式（符合RFC 2255中所述的标准AD v3 URL）列出所有服务器。只有 URL 的主机和端口部分在此设置中是相关的。

参数	说明
密码属性	用于保存密码的AD属性的名称。在更改用户的密码时，会为该属性设置新密码。
用于检索账户的AD过滤器	用于控制从AD资源返回的账户的可选AD过滤器。如果未指定任何过滤器，则只返回包含所有指定对象类的账户。
密码散列算法	指出Identity System对密码执行散列时应使用的算法。目前支持的值为SSHA、SHA、SMD5和MD5。空值表示系统不会对密码执行散列。除非LDAP服务器执行散列（Netscape Directory Server 和 iPlanet Directory Server执行散列），否则这将导致明文密码存储在AD中。
优先处理资源密码策略重置后更改	如果在登录模块中指定此资源（即，此资源是传递验证目标），并且将资源的密码策略配置为在重置后更改，则以管理方式重置了资源账户密码的用户需要在成功验证后更改该密码。
使用VLV控件	指定是否在标准AD控件上强制使用VLV控件。默认为“false”。
VLV 排序属性	指定用于资源上 VLV 索引的排序属性。
读取模式	如果为TRUE，连接器将从服务器中读取模式。如果为FALSE，连接器将根据配置中的对象类提供一个默认模式。要使用扩展对象类，该属性必须为TRUE。
要同步的基本上下文	AD树中用于确定是否应同步更改的一个或多个起始点。如果未设置此属性，则将使用基本上下文属性来同步更改。

参数	说明
要同步的对象类	要同步的对象类。更改日志针对所有对象；它会根据所列出的对象类来对更新进行过滤。除非您要将对象与任何超类值同步，否则不应列出对象类的超类。例如，如果仅应同步 "inetOrgPerson" 对象，但应过滤掉 "inetOrgPerson" 的超类（"person"、"organizationalperson" 和 "top"），则此处仅应列出 "inetOrgPerson"。AD中的所有对象都是 "top" 的派生子类。因此，绝不应列出 "top"，否则将无法过滤任何对象。
要同步的属性	要同步的属性的名称。设置此项后，如果更改日志中的更新没有对任何命名属性进行更新，则会忽略这些更新。例如，如果仅列出 "department"，则只处理影响 "department" 的更改。而忽略所有其他更新。如果将其留空（默认设置），则处理所有更改。
要同步的账户的 AD 过滤器	同步对象时使用的可选AD过滤器。由于更改日志适用于所有对象，因此此过滤器只更新符合指定过滤器条件的对象。如果指定了过滤器，则只有在对象符合过滤器条件并且包含已同步的对象类时，才会对其进行同步。
更改日志块大小	每个查询获取的更改日志条目数。
更改编号属性	更改编号属性
使用 OR 而不是 AND 进行过滤	通常，用于获取更改日志条目的过滤器是基于AND条件检索一段时间间隔内的更改条目。如果设置了此属性，则过滤器将改用OR条件配合所需的更改数量进行过滤。
从过滤器中删除日志条目对象类	如果设置了此属性（默认设置），用于获取更改日志条目的过滤器不会包含 "changeLogEntry" 对象类，因为更改日志中应该不包含其他对象类型的条目。
要同步的密码属性	在执行密码同步时要同步的密码属性的名称。

参数	说明
状态管理类	用于管理启用/禁用状态的类。 如果未指定类，则无法进行身份状态管理。
是否搜索密码	搜索时是否检索用户密码。 默认值为“否”。
DN属性	条目DN属性名称（默认：entryDN）
AD过滤器	一个可选的AD过滤器，用于控制从AD资源返回的组。 如果未指定过滤器，则仅返回包含所有指定对象类的组。
读超时	等待接收响应的时间。如果在指定的时间内没有响应，读取尝试将被中止。值为0或小于0表示没有限制。
连接超时	打开新服务器连接时的等待时间。值0表示将使用TCP网络超时，可能是几分钟。 值小于0表示没有限制。
账号DN前缀	默认值cn，也可以为uid等其它用于dn前缀的属性名。

- 高级配置：用于配置顶层组织、组织、用户映射策略。

表 2-3 高级配置

参数	说明
开启定时回收	可设置是否开启定时回收，若开启，每天定时执行回收任务。
定时频率	定时频率固定为1天。 **说明** 当开启了定时回收后，显示此参数。
选择回收开始时间	可在选择框中设置回收开始时间。 **说明** 当开启了定时回收后，才需设置此参数。
选择根组织	企业AD身份源组织同步至OneAccess后的父级组织。如果不填，将自动创建顶层组织。
组织匹配策略	企业AD组织与OneAccess组织的映射关系。当OneAccess同步企业AD中的组织时，根据该策略进行匹配。如属性名为**编码**、身份源属性名为**组织编码**，企业AD中的组织将以编码为匹配策略映射至OneAccess。

参数	说明
创建组织	开启后，如果同步组织时匹配失败，则OneAccess将自动创建对应组织。默认开启，为了您的数据完整，建议开启。
更新组织	开启后，如果同步组织时匹配成功，则OneAccess将自动更新该组织。默认开启，为保证您的数据正确，建议开启。
删除组织	当AD的组织数据成功同步至OneAccess后，如果删除AD中的组织，则OneAccess会和设置的删除阈值进行对比，删除组织数和上次同步数据总数的比值大于阈值则删除失败，删除组织数和上次同步数据总数的比值小于阈值则删除成功。
用户匹配策略	企业AD用户与OneAccess用户的映射关系。当OneAccess同步企业AD中的用户时，根据该策略进行匹配。如属性名为用户ID、身份源属性名为**员工唯一标识ID**，企业AD的用户将以编码为匹配策略映射至OneAccess。
创建用户	开启后，如果同步用户时匹配失败，则OneAccess将自动创建对应用户。默认开启，为了您的数据完整，建议开启。
更新用户	开启后，如果同步用户时匹配成功，则OneAccess将自动更新该用户。默认开启，为保证您的数据正确，建议开启。
删除用户	当AD的用户数据成功同步至OneAccess后，如果删除AD中的用户，则OneAccess会和设置的删除阈值进行对比，删除用户数和上次同步数据总数的比值大于阈值则删除失败，删除用户数和上次同步数据总数的比值小于阈值则删除成功。
禁用用户阈值调节	默认20%，该功能为平台提供的一种保护机制，支持自定义设置比例。当上游身份源应用禁用/删除超过设定的阈值数据，平台接到指令后，不会进行同步禁用/删除。

步骤3 （可选）设置对象模型。

在身份源详情页面，选择“对象模型”页签，修改、添加、删除用户和机构的属性、映射规则。

表 2-4 对象模型

参数		说明
用户对象	属性定义	AD身份源的用户属性。
	映射定义	AD与OneAccess用户数据同步时的映射规则，支持脚本转换。

参数		说明
机构对象	属性定义	AD身份源的组织属性。
	映射定义	AD与OneAccess组织数据同步时的映射规则，支持脚本转换。

- 添加属性。
  a. 在“属性定义”页签，单击“添加”，弹出“添加属性”弹框。

  b. 选择“身份源可选属性”，输入“显示标签”、描述。
  c. 选择“类型”。当“类型”选择为“文本”时，需要设置“格式”。
  d. 设置该属性是否为必填，单击“确定”，属性添加完成。
- 设置映射规则。
  在“映射定义”页签，单击“编辑”，通过设置转换方式、脚本表达方式、执行方式、系统用户设置映射规则。

----结束

验证 OneAccess 同步企业 AD 数据

- 导入同步：
  a. 在AD身份源列表页面，单击目标身份源的“详情”进入新增AD身份源详情页面，单击“导入同步”，单击“执行”。OneAccess将主动同步AD身份源的用户及组织数据，并生成操作记录。
  b. 执行完成后，单击目标记录的“详情”，查看详细信息。

图 2-2 查看详情

c. 同步成功后，在“组织与用户”可查看已同步至OneAccess的用户和组织。

图 2-3 查看已同步的数据

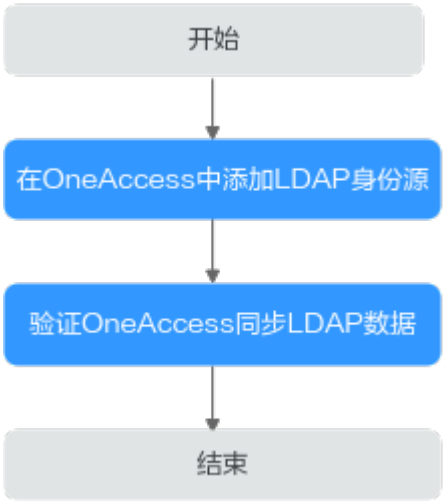
- 定时同步：如果“导入配置 > 高级配置”中设置了“定时同步”，即可在AD身份源列表页面，单击目标身份源的“详情”进入新增AD身份源详情页面，单击“定时同步”在“定时同步”页签查看定时同步的记录。

2.2 集成 LDAP 身份源

OneAccess支持通过LDAP身份源导入用户和组织信息，实现OneAccess实时同步LDAP身份源中用户和组织信息。OneAccess集成企业LDAP，支持LDAPv3协议。

本文主要介绍OneAccess集成LDAP身份源的方法。

配置流程



前提条件

- 请确保您已拥有LDAP平台账号管理员权限。
- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保当前OneAccess管理门户可以访问到LDAP平台。
- 请确保您已了解LDAP协议及LDAP服务器获取方式。

在 OneAccess 中添加 LDAP 身份源

在OneAccess中配置身份源参数，确保OneAccess可同步LDAP服务器中的数据。

步骤1 在OneAccess中创建身份源。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“用户 > 身份源管理”。
3. 在身份源管理页面，单击LDAP身份源操作列的“添加身份源”，输入“身份源名称”，单击“确定”。

步骤2 设置导入配置。

1. 在LDAP身份源列表页面，单击目标身份源的操作列的“详情”。

2. 单击“导入配置”，在该页签填写导入配置参数并单击“确定”。
   - 基础配置：LDAP服务器的连接参数，实现OneAccess和LDAP服务器的连接，请务必填写并保证正确。

表 2-5 基础配置

参数	说明
*主机	运行LDAP服务器的主机名称或 IP 地址。 **说明** OneAccess目前只支持公网访问，LDAP服务器需要提供公网地址。
*TCP端口	用于与LDAP服务器进行通信的服务器TCP/IP 端口号。默认为636。
SSL	系统默认true，即使用SSL连接到LDAP服务器。
StartTLS	是否启用startTLS进行加密通信。 ■ true：启用StartTLS，且SSL不能设置为true； ■ false：不启用StartTLS。

参数	说明
校验证书	是否校验证书。仅在SSL为true或者StartTLS为true时有效。true: 校验证书，false: 不校验证书。证书必须是公网认证的证书，自签名证书不可以。
协议版本	系统默认TLSv1.2，推荐使用TLSv1.3、TLSv1.2。
主体	进行LDAP服务器验证时使用的账号名。传参带域名，如“admin@test.com ”或“TEST \admin”。
密码	主体账号的密码。
*基本上下文	搜索 LDAP 树时将使用该树中的一个或多个节点作为起始点，需填写要同步LDAP中数据所在的根节点。在从 LDAP 服务器寻找用户或搜寻某个用户所属的组时，将从该节点开始执行搜索。 如“OU=huaweitest,DC=test,DC=com”。
UID 属性	映射到UID属性的LDAP属性的名称。
账户对象类	在LDAP树中创建新用户对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。

- 可选配置：可默认配置，如需同步密码需配置密码的相关参数，包括启用密码同步和要同步的密码属性，如出现同步异常，可根据实际的使用情况进行参数调整，包括但不限于账户对象类、机构对象类等参数。

表 2-6 可选配置

参数	说明
域名	域名存在时，回收的用户名中将该域名排除掉（存在多个域名用","分隔，默认用户名会排除域名）
账户用户名属性	保存账户用户名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的用户名的LDAP条目。

参数	说明
机构对象类	在LDAP树中创建新机构对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。
机构名属性	保存机构名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的机构名的LDAP条目。
故障转移服务器	列出首选服务器发生故障时将用于故障转移的所有服务器。如果首选服务器发生故障，JNDI将连接到列表中的下一个可用服务器。按照 "ldap://ldap.example.com:389/" 格式（符合 RFC 2255 中所述的标准 LDAP v3 URL）列出所有服务器。只有 URL 的主机和端口部分在此设置中是相关的。
密码属性	用于保存密码的LDAP属性的名称。在更改用户的密码时，会为该属性设置新密码。
用于检索账户的 LDAP过滤器	用于控制从LDAP资源返回的账户的可选LDAP过滤器。如果未指定任何过滤器，则只返回包含所有指定对象类的账户。
密码散列算法	指出Identity System对密码执行散列时应使用的算法。目前支持的值为SSHA、SHA、SMD5和MD5。空值表示系统不会对密码执行散列。除非LDAP服务器执行散列（Netscape Directory Server 和 iPlanet Directory Server 执行散列），否则这将导致明文密码存储在LDAP中。
优先处理资源密码策略重置后更改	如果在登录模块中指定此资源（即，此资源是传递验证目标），并且将资源的密码策略配置为在重置后更改，则以管理方式重置了资源账户密码的用户需要在成功验证后更改该密码。
使用VLV控件	指定是否在标准LDAP控件上强制使用VLV控件。默认为“false”。
VLV 排序属性	指定用于资源上VLV索引的排序属性。
读取模式	如果为TRUE，连接器将从服务器中读取模式。如果为FALSE，连接器将根据配置中的对象类提供一个默认模式。要使用扩展对象类，该属性必须为TRUE。
要同步的基本上下文	LDAP树中用于确定是否应同步更改的一个或多个起始点。如果未设置此属性，则将使用基本上下文属性来同步更改。

参数	说明
要同步的对象类	要同步的对象类。更改日志针对所有对象；它会根据所列出的对象类来对更新进行过滤。除非您要将对象与任何超类值同步，否则不应列出对象类的超类。例如，如果仅应同步 "inetOrgPerson" 对象，但应过滤掉 "inetOrgPerson" 的超类（"person"、"organizationalperson" 和 "top"），则此处仅应列出 "inetOrgPerson"。LDAP 中的所有对象都是 "top" 的派生子类。因此，绝不应列出 "top"，否则将无法过滤任何对象。
要同步的属性	要同步的属性的名称。设置此项后，如果更改日志中的更新没有对任何命名属性进行更新，则会忽略这些更新。例如，如果仅列出 "department"，则只处理影响 "department" 的更改。而忽略所有其他更新。如果将其留空（默认设置），则处理所有更改。
过滤更改的方式	用于从更改中过滤的目录管理员名称 (DN)。可过滤出所有“modifiersName”属性与该列表中的条目相匹配的更改。为避免循环，标准值设置为该适配器使用的管理员名称。条目应该采用“cn=Directory Manager”格式。
要同步的账户的AD 过滤器	同步对象时使用的可选LDAP过滤器。由于更改日志适用于所有对象，因此此过滤器只更新符合指定过滤器条件的对象。如果指定了过滤器，则只有在对象符合过滤器条件并且包含已同步的对象类时，才会对其进行同步。
更改日志块大小	每个查询获取的更改日志条目数。
更改编号属性	更改编号属性
使用 OR 而不是 AND 进行过滤	通常，用于获取更改日志条目的过滤器是基于AND条件检索一段时间间隔内的更改条目。如果设置了此属性，则过滤器将改用OR条件配合所需的更改数量进行过滤。
从过滤器中删除日志条目对象类	如果设置了此属性（默认设置），用于获取更改日志条目的过滤器不会包含“changeLogEntry”对象类，因为更改日志中应该不包含其他对象类型的条目。
要同步的密码属性	在执行密码同步时要同步的密码属性的名称。
状态管理类	用于管理启用/禁用状态的类。 如果未指定类，则无法进行身份状态管理。
是否搜索密码	搜索时是否检索用户密码。 默认值为“否”。
DN属性	条目DN属性名称（默认：entryDN）。
LDAP过滤器	一个可选的LDAP过滤器，用于控制从LDAP资源返回的组。 如果未指定过滤器，则仅返回包含所有指定对象类的组。

参数	说明
读超时	等待接收响应的时间。如果在指定的时间内没有响应，读取尝试将被中止。值为0或小于0表示没有限制。
连接超时	打开新服务器连接时的等待时间。 值0表示将使用TCP网络超时，可能是几分钟。 值小于0表示没有限制。
账号DN前缀	默认值cn，也可以为uid等其它用于dn前缀的属性名。

- 高级配置：用于配置顶层组织、组织、用户映射策略。

表 2-7 高级配置

参数	说明
定时同步	每天定时执行同步任务的时间。
选择组织	LDAP服务器的组织同步至OneAccess后的父级组织。如果不填，将自动创建顶层组织。
删除阈值	默认20%，该功能为平台提供的一种保护机制，支持自定义设置比例。当上游身份源应用禁用/删除超过设定的阈值数据，平台接到指令后，不会进行同步禁用/删除。
组织匹配策略	LDAP 服务器组织与OneAccess组织的映射关系。当OneAccess同步LDAP服务器中的组织时，根据该策略进行匹配。如属性名为**编码**、身份源属性名为**组织编码**，LDAP服务器中的组织将以编码为匹配策略映射至OneAccess。
创建组织	开启后，如果同步组织时匹配失败，则OneAccess将自动创建对应组织。默认开启，为了您的数据完整，建议开启。
更新组织	开启后，如果同步组织时匹配成功，则OneAccess将自动更新该组织。默认开启，为保证您的数据正确，建议开启。
删除组织	当LDAP的组织数据成功同步至OneAccess后，如果删除LDAP中的组织，则OneAccess会和设置的删除阈值进行对比，删除组织数和上次同步数据总数的比值大于阈值则删除失败，删除组织数和上次同步数据总数的比值小于阈值则删除成功。
用户匹配策略	LDAP 服务器用户与OneAccess用户的映射关系。当OneAccess同步 LDAP 服务器中的用户时，根据该策略进行匹配。如属性名为用户ID、身份源属性名为**员工唯一标识ID**，LDAP服务器的用户将以编码为匹配策略映射至OneAccess。
创建用户	开启后，如果同步用户时匹配失败，则OneAccess将自动创建对应用户。默认开启，为了您的数据完整，建议开启。

参数	说明
更新用户	开启后，如果同步用户时匹配成功，则OneAccess将自动更新该用户。默认开启，为保证您的数据正确，建议开启。
删除用户	当LDAP的用户数据成功同步至OneAccess后，如果删除LDAP中的用户，则OneAccess会和设置的删除阈值进行对比，删除用户数和上次同步数据总数的比值大于阈值则删除失败，删除用户数和上次同步数据总数的比值小于阈值则删除成功。

步骤3 （可选）设置对象模型。

在身份源详情页面，选择“对象模型”页签，修改、添加、删除用户和组织的属性、映射规则。

表 2-8 对象模型

参数		说明
用户对象	属性定义	LDAP身份源的用户属性。
	映射定义	LDAP与OneAccess用户数据同步时的映射规则，支持脚本转换。
机构对象	属性定义	LDAP身份源的组织属性。
	映射定义	LDAP与OneAccess组织数据同步时的映射规则，支持脚本转换。

- 添加属性。
  a. 在“属性定义”页签，单击“添加”，弹出“添加属性”弹框。

b. 选择“身份源可选属性”，输入“显示标签”、描述。
c. 选择“类型”。当“类型”选择为“文本”时，需要设置“格式”。
d. 设置该属性是否为必填，单击“确定”，属性添加完成。

- 设置映射规则。

  在“映射定义”页签，单击“编辑”，通过设置转换方式、脚本表达方式、执行方式、系统用户设置映射规则。

----结束

验证 OneAccess 同步 LDAP 数据

- 导入同步：
  a. 在LDAP身份源列表页面，单击目标身份源的“详情”进入新增LDAP身份源详情页面，单击“导入同步”，在“导入同步”页签单击“执行”。OneAccess将主动同步LDAP身份源的用户及组织数据，并生成操作记录。
  b. 执行完成后，单击目标记录的“详情”，查看详细信息。
  c. 同步成功后，在“组织与用户”可查看已同步至OneAccess的用户和组织。
- 定时同步：如果“导入配置 > 高级配置”中设置了“定时同步”，即可在LDAP身份源列表页面，单击目标身份源的“详情”进入新增LDAP身份源详情页面，单击“定时同步”在“定时同步”页签查看定时同步的记录。

3 集成企业应用

3.1 使用 OneAcceess 用户门户登录华为云

3.1.1 概述

华为云支持基于SAML、OIDC协议的单点登录，企业管理员在华为云和OneAccess进行配置后，普通用户登录OneAccess用户门户，即可免密进入华为云Console系统或者是某个具体的华为云应用。

前提条件

- 请确保您的浏览器可以访问华为云控制台。
- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已拥有华为账号。如需注册，请参见**注册账号并实名认证**。

3.1.2 通过 OneAccess 免密登录单个华为云账号（SAML-虚拟用户SSO）

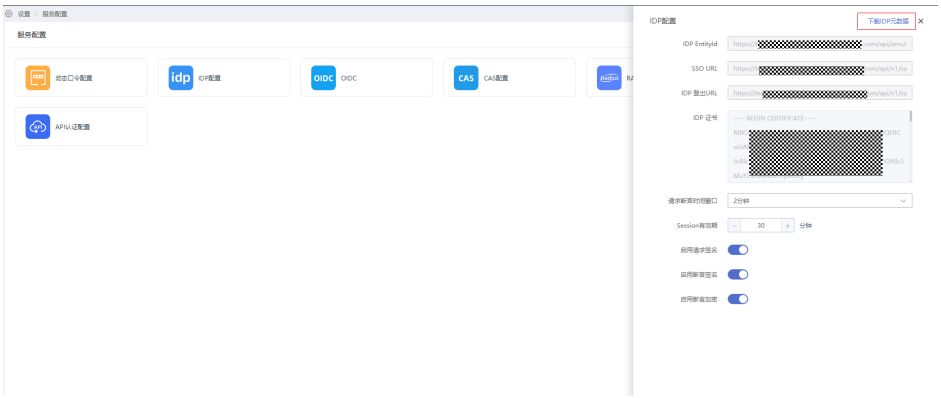
本文以SAML协议为例介绍如何实现使用OneAccess免密登录单个华为云账号。如需了解华为云身份提供商详情，请参考**身份提供商概述**。

在华为云上创建身份提供商

在华为云控制台创建身份提供商，配置身份提供商的元数据文件后，可以在华为云中建立对OneAccess的信任关系。

步骤1 登录OneAccess管理门户，下载OneAccess系统的元数据文件（metadata文件）。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”。
3. 在“服务配置”页面，单击“IDP配置”。
4. 在弹出的IDP配置页面，单击右上角的“下载IDP元数据”，数据会自动保存。



步骤2 参考**在华为云上创建身份提供商**创建身份提供商，其中“类型”选择“虚拟用户SSO”。

说明

- 身份提供商名称不能重复，建议以域名唯一标识命名。
- 虚拟用户SSO定义可参见**虚拟用户SSO与IAM用户SSO的适用场景**。
- 一个华为云账号只能存在“IAM用户SSO”和“虚拟用户SSO”中的一种类型的身份提供商。

步骤3 获取华为云登录链接。

步骤4 参考**在华为云上配置元数据文件**把OneAccess IdP的Metadata文件配置到华为云。

步骤5 参考**配置身份转换规则**在华为云上配置身份转换规则，使得OneAccess用户拥有华为云访问云服务和资源的权限。

以每个OneAccess用户都对应同一个IAM用户组，登录华为云之后，子用户名称展示为OneAccess用户名为例，转换规则配置如下：

```
[
  {
    "remote": [
      {
        "type": "name"
      }
    ],
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      }
    ]
  }
]
```

其中，remote为OneAccess映射到IAM的信息，取其中的name字段，可取的映射字段可以参考**步骤2**。

local为IAM本地的信息，其中user为IAM的用户信息，其中的name为展示的子用户名称，{0}为取remote中的第一个字段。group为IAM的用户组信息，表示所有用户都映射到admin的用户组，拥有其所有权限。

同理，也可以在remote中添加多个字段，将其中某个字段设置为用户组名称，来实现不同的用户对应不同的用户组。

```
[
  {
    "remote": [
      {
        "type": "name"
      },
      {
        "type": "Roles"
      }
    ],
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "groups": "{1}"
      }
    ]
  }
]
```

其中，remote为多映射一个Roles字段（可使用用户属性定义中的自定义字段，多值类型），可以为单值，也可以为多值。

local为使用groups，可以映射到多个IAM用户组，取remote中的第二个Roles字段。

----结束

建立 OneAccess 对华为云的信任关系

在OneAccess中配置华为云的元数据文件，以建立OneAccess对华为云的信任。

步骤1 在OneAccess上添加华为云应用。

1. 登录OneAccess管理门户，选择“资源 > 应用”。
2. 在应用页面，单击“新增预集成应用”。
3. 在新增预集成应用页面，单击“华为云”应用。
4. 在弹出的添加应用页面，确认通用信息，单击“下一步”。
5. 在认证参数配置页面，选择“导入SP应用元数据 > 选择文件”，选择获取的华为云元数据文件。系统会自动上传文件并提取元数据。

   说明

   - 预集成应用为OneAccess专业版用户功能，如果是OneAccess基础版用户，请参考**在OneAccess中添加企业应用**创建自定义应用后进行**步骤1.5**操作。
   - 在**https://auth.huaweicloud.com/authui/saml/metadata.xml**下载华为云元数据文件，并设置文件名称，例如“SP-metadata.xml”。
   - OneAccess同时支持“选取文件”和“手动输入配置数据”方式配置元数据，了解详情请参考**在OneAccess中配置元数据文件**。
6. 待“选取文件”变为“√”时，代表系统已提取元数据，单击“下一步”，成功添加华为云应用。
7. 在认证集成页面，在“参数配置”页签，单击“编辑”，将“Single Logout URL”对应值中的“/saml/LogoutServiceHTTPRedirect”替换为“/logout”。

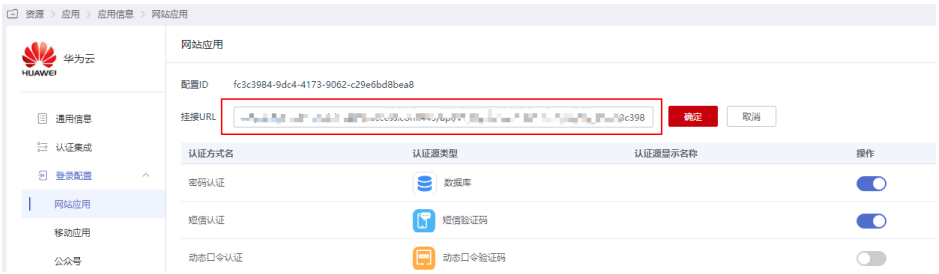
步骤2 配置OneAccess与华为云之间的映射关系。

1. 单击已添加的华为云应用，在应用信息页面，单击应用图标，进入应用详情页面。
2. 选择“认证集成 > 映射配置”，单击“添加映射”，建立OneAccess与华为云之间的属性映射。参数详细说明可参考**映射配置**。

步骤3 在OneAccess配置华为云登录入口。

在华为云应用详情页面，选择“登录配置 > 网站应用”，单击“编辑”，将挂接URL替换为**步骤3**中获取的“登录链接”，单击“确定”保存此次编辑。

图 3-1 编辑挂接 URL



说明

如果需要跳转华为云Console中的特定业务页面，需要对华为云创建的身份提供商的“登录链接”进行拼接后填入挂接URL中，此处以跳转CodeArts服务页面为例进行说明：

华为云创建的身份提供商的“登录链接”为：https://auth.huawei.com/authui/federation/websso?domain_id=e35f94**********14839c&idp=SAML-OneAccess&protocol=saml

CodeArts服务地址为：https://console-intl.huaweicloud.com/devcloud/?region=cn-east-3&locale=zh-cn#

如果服务地址中带有“agencyId=***&”字段，需要将该字段删除后，使用“&service=”将两个地址进行拼接后填入挂接URL中：

https://auth.huawei.com/authui/federation/websso?domain_id=e35f94**********14839c&idp=SAML-OneAccess&protocol=saml&service=https://console.huaweicloud.com/devcloud/?region=cn-south-1&locale=zh-cn#

步骤4 在OneAccess给用户授予华为云访问权限。

在华为云应用详情页面，选择“授权管理 > 应用账号”，单击“添加账号”，按需勾选账号，单击“保存”，所选用户即可在OneAccess中免密访问华为云。

----结束

OneAccess 用户登录验证

在OneAccess中授予华为云访问权限的用户，登录OneAccess用户门户，单击华为云应用即可进入华为云控制台首页访问云服务。

3.1.3 通过 OneAccess 免密登录多个华为云账号（SAML-虚拟用户SSO）

本文以SAML协议为例介绍如何实现使用OneAccess免密登录多个华为云账号。如需了解华为云身份提供商详情，请参见**身份提供商概述**。

在华为云上创建身份提供商

在华为云控制台创建身份提供商，配置身份提供商的元数据文件后，可以在华为云中建立对OneAccess的信任关系。

步骤1 登录OneAccess管理门户，下载OneAccess系统的元数据文件（metadata文件）。

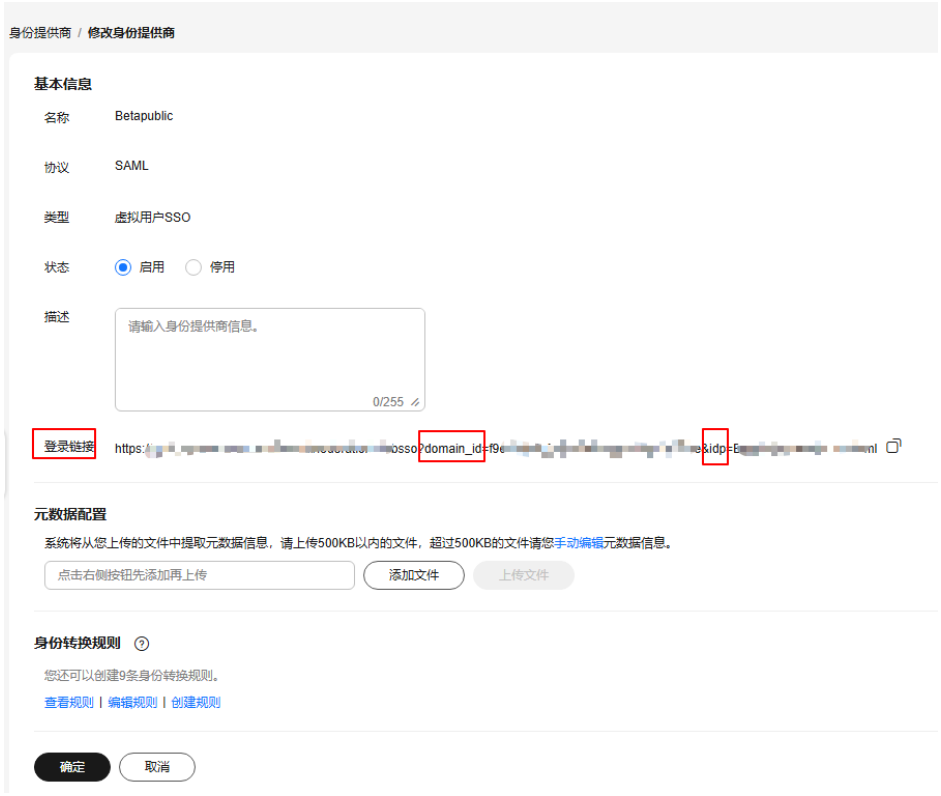
1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”。
3. 在“服务配置”页面，单击“IDP配置”。
4. 在弹出的IDP配置页面，单击右上角的“下载IDP元数据”，数据会自动保存。

步骤2 参考**在华为云上创建身份提供商**创建身份提供商，其中“类型”选择“虚拟用户SSO”。

说明

- 身份提供商名称不能重复，建议以域名唯一标识命名。
- 虚拟用户SSO定义可参考**虚拟用户SSO与IAM用户SSO的适用场景**。
- 一个华为云账号只能存在“IAM用户SSO”和“虚拟用户SSO”中的一种类型的身份提供商。

步骤3 获取华为云登录链接中的domain_id和idp的值。



步骤4 参考**在华为云上配置元数据文件**把OneAccess IdP的Metadata文件配置到华为云。

步骤5 参考**配置身份转换规则**在华为云上配置身份转换规则，使得OneAccess用户拥有华为云访问云服务和资源的权限。

以每个OneAccess用户都对应同一个IAM用户组，登录华为云之后，子用户名称显示为OneAccess用户名为例，转换规则配置如下：

```
[
  {
    "remote": [
      {
        "type": "name"
      }
    ],
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      },
      {
        "group": {
          "name": "admin"
        }
      }
    ]
  }
]
```

其中，remote为OneAccess映射到IAM的信息，取其中的name字段，可取的映射字段可以参考**步骤2**。

local为IAM本地的信息，其中user为IAM的用户信息，其中的name为展示的子用户名称，{0}取remote中的第一个字段。group为IAM的用户组信息，表示所有用户都映射到admin的用户组，拥有其所有权限。

同理，也可以在remote中添加多个字段，将其中某个字段设置为用户组名称，来实现不同的用户对应不同的用户组。

```
[
 {
  "remote": [
   {
    "type": "name"
   },
   {
    "type": "Roles"
   }
  ],
  "local": [
   {
    "user": {
     "name": "{0}"
    }
   },
   {
    "groups": "{1}"
   }
  ]
 }
]
```

其中，remote为多映射一个Roles字段（可使用用户属性定义中的自定义字段，多值类型），可以为单值，也可以为多值。

local为使用groups，可以映射到多个IAM用户组，取remote中的第二个Roles字段。

步骤6 在其他华为云账号上面重复**步骤2**~**步骤5**进行配置。

----结束

建立 OneAccess 对华为云的信任关系

在OneAccess中配置华为云的元数据文件，以建立OneAccess对华为云的信任。

步骤1 在OneAccess上添加华为云应用。

1. 登录OneAccess管理门户，选择“资源 > 应用”。
2. 在应用页面，单击“新增预集成应用”。
3. 在新增预集成应用页面，单击“华为云”应用。
4. 在弹出的添加应用页面，确认通用信息，单击“下一步”。
5. 在认证参数配置页面，选择“导入SP应用元数据 > 选择文件”，选择获取的华为云元数据文件。系统会自动上传文件并提取元数据。

   说明

   - 预集成应用为OneAccess专业版用户功能，如果是OneAccess基础版用户，请参考**在OneAccess中添加企业应用**创建自定义应用后进行**步骤1.5**操作。
   - 在**https://auth.huaweicloud.com/authui/saml/metadata.xml**下载华为云元数据文件，并设置文件名称，例如“SP-metadata.xml”。
   - OneAccess同时支持“选取文件”和“手动输入配置数据”方式配置元数据，了解详情请参考**在OneAccess中配置元数据文件**。

6. 待“选取文件”变为“√”时，代表系统已提取元数据，单击“下一步”，成功添加华为云应用。
7. 在认证集成页面，在“参数配置”页签，单击“编辑”，将“Single Logout URL”对应值中的“/saml/LogoutServiceHTTPRedirect”替换为“/logout”。

步骤2 配置OneAccess与华为云之间的映射关系。

1. 单击已添加的华为云应用，在应用信息页面，单击应用图标，进入应用详情页面。
2. 选择“认证集成 > 映射配置”，单击“添加映射”，建立OneAccess与华为云之间的属性映射。参数详细说明可参考**映射配置**。
3. 选择“认证集成 > 映射配置”，单击“添加映射”，添加应用属性名为“IAM_SAML_Attributes_identityProviders”的映射，映射类型为“固定属性值”，值为“iam::{domain_id}:identityProvider:{idp_id}”，其中“{domain_id}”为步骤**步骤3**中获取的domain_id，“{idp_id}”为步骤**步骤3**中获取的idp_id，支持多个华为云账号的拼接，使用“;”进行分隔，实现跳转过程中选择某个华为云账号跳转，两个华为云账号时值举例如下：

   iam::657ba0e**********19fd684d8758c:identityProvider:SAML-IAM;iam::e35f949b3*********2b79ba14839c:identityProvider:SAML-OneAccess
4. （可选）单击“添加映射”，添加应用属性名为“IAM_SAML_Attributes_redirect_url”的映射，映射类型为“固定属性值”，值为华为云Console中的特定业务页面（如果业务地址中带有“agencyId=***&”字段，需要将该字段删除），可以实现单点登录直接跳转至特定业务页面，如果不添加，默认跳转华为云主页面。

步骤3 在OneAccess给用户授予华为云访问权限。

在华为云应用详情页面，选择“授权管理 > 应用账号”，单击“添加账号”，按需勾选账号，单击“保存”，所选用户即可在OneAccess中免密访问华为云。

----结束

OneAccess 用户登录验证

在OneAccess中授予华为云应用访问权限的用户，登录OneAccess用户门户，单击华为云应用，选择需要访问的身份提供商，即可进入华为云控制台首页访问云服务。

3.1.4 通过 OneAccess 免密登录单个华为云账号（SAML-IAM 用户 SSO）

本文以SAML协议为例介绍如何实现使用OneAccess免密登录单个华为云账号。如需了解华为云身份提供商详情，请参考**身份提供商概述**。

在华为云上创建身份提供商

在华为云控制台创建身份提供商，配置身份提供商的元数据文件后，可以在华为云中建立对OneAccess的信任关系。

步骤1 登录OneAccess管理门户，下载OneAccess系统的元数据文件（metadata文件）。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”。

3. 在“服务配置”页面，单击“IDP配置”。
4. 在弹出的IDP配置页面，单击右上角的“下载IDP元数据”，数据会自动保存。

步骤2 参考**在华为云上创建身份提供商**创建身份提供商，其中“类型”选择“IAM用户SSO”。

说明

- 身份提供商名称不能重复，建议以域名唯一标识命名。
- IAM用户SSO定义可参考**虚拟用户SSO与IAM用户SSO的适用场景**。
- 一个华为云账号只能存在“IAM用户SSO”和“虚拟用户SSO”中的一种类型的身份提供商。

步骤3 获取华为云登录链接。

步骤4 参考**在华为云上配置元数据文件**把OneAccess IdP的Metadata文件配置到华为云。

步骤5 参考**配置外部身份ID**在华为云上配置IAM用户的外部身份ID，建立OneAccess用户和IAM用户的对应关系。

----结束

建立 OneAccess 对华为云的信任关系

在OneAccess中配置华为云的元数据文件，以建立OneAccess对华为云的信任。

步骤1 在OneAccess上添加华为云应用。

1. 登录OneAccess管理门户，选择“资源 > 应用”。
2. 在应用页面，单击“新增预集成应用”。
3. 在新增预集成应用页面，单击“华为云”应用。
4. 在弹出的添加应用页面，确认通用信息，单击“下一步”。
5. 在认证参数配置页面，选择“导入SP应用元数据 > 选择文件”，选择获取的华为云元数据文件。系统会自动上传文件并提取元数据。

说明

- 预集成应用为OneAccess专业版用户功能，如果是OneAccess基础版用户，请参考**在OneAccess中添加企业应用**创建自定义应用后进行**步骤1.5**操作。
- 在**https://auth.huaweicloud.com/authui/saml/metadata.xml**下载华为云元数据文件，并设置文件名称，例如“SP-metadata.xml”。
- OneAccess同时支持“选取文件”和“手动输入配置数据”方式配置元数据，了解详情请参考**在OneAccess中配置元数据文件**。

6. 待“选取文件”变为“√”时，代表系统已提取元数据，单击“下一步”，成功添加华为云应用。
7. 在认证集成页面，在“参数配置”页签，单击“编辑”，将“Single Logout URL”对应值中的“/saml/LogoutServiceHTTPRedirect”替换为“/logout”。

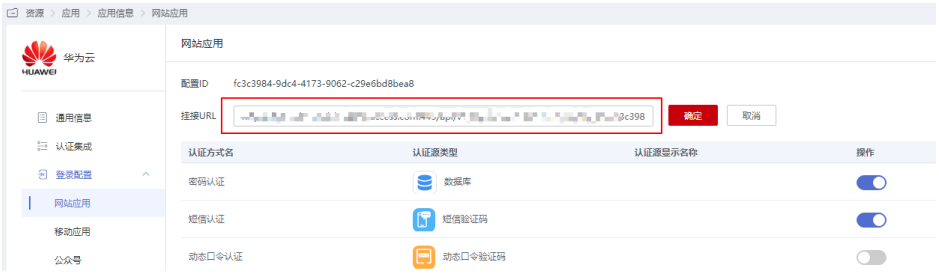
步骤2 配置OneAccess与华为云之间的映射关系。

1. 单击已添加的华为云应用，在应用信息页面，单击应用图标，进入应用详情页面。
2. 选择“认证集成 > 映射配置”，进入映射配置页面。
3. 单击“添加映射”，添加应用属性名为“IAM_SAML_Attributes_xUserId”的映射，建立OneAccess与华为云之间的属性映射。映射对象可以是OneAccess中用户已有的属性，也可以是新增的自定义属性，必须和**步骤5**中添加的IAM用户的外部身份ID一致。

步骤3 在OneAccess配置华为云登录入口。

在华为云应用详情页面，选择“登录配置 > 网站应用”，单击“编辑”，将挂接URL替换为**步骤3**中获取的“登录链接”，单击“确定”保存此次编辑。

图 3-2 编辑挂接 URL



说明

如果需要跳转华为云Console中的特定业务页面，需要对华为云创建的身份提供商的“登录链接”进行拼接后填入挂接URL中，此处以跳转CodeArts服务页面为例进行说明：

华为云创建的身份提供商的“登录链接”为：https://auth.huawei.com/authui/federation/websso?domain_id=e35f94**********14839c&idp=SAML-OneAccess&protocol=saml

CodeArts服务地址为：https://console.huaweicloud.com/devcloud/?region=cn-south-1&locale=zh-cn#

如果服务地址中带有“agencyId=***&”字段，需要将该字段删除后，使用“&service=”将两个地址进行拼接后填入挂接URL中：

https://auth.huawei.com/authui/federation/websso?domain_id=e35f94**********14839c&idp=SAML-OneAccess&protocol=saml&service=https://console.huaweicloud.com/devcloud/?region=cn-south-1&locale=zh-cn#

步骤4 在OneAccess给用户授予华为云访问权限。

在华为云应用详情页面，选择“授权管理 > 应用账号”，单击“添加账号”，按需勾选账号，单击“保存”，所选用户即可在OneAccess中免密访问华为云。

----结束

OneAccess 用户登录验证

在OneAccess中授予华为云应用访问权限的用户，登录OneAccess用户门户，单击华为云应用即可进入华为云控制台首页访问云服务。

3.1.5 通过 OneAccess 免密登录多个华为云账号（SAML-IAM 用户 SSO）

本文以SAML协议为例介绍如何实现使用OneAccess免密登录华多个华为云账号。如需了解华为云身份提供商详情，请参考**身份提供商概述**。

在华为云上创建身份提供商

在华为云控制台创建身份提供商，配置身份提供商的元数据文件后，可以在华为云中建立对OneAccess的信任关系。

步骤1 登录OneAccess管理门户，下载OneAccess系统的元数据文件（metadata文件）。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”。
3. 在“服务配置”页面，单击“IDP配置”。
4. 在弹出的IDP配置页面，单击右上角的“下载IDP元数据”，数据会自动保存。

步骤2 参考**在华为云上创建身份提供商**创建身份提供商，其中“类型”选择“IAM用户SSO”。

说明

- 身份提供商名称不能重复，建议以域名唯一标识命名。
- IAM用户SSO定义可参考**虚拟用户SSO与IAM用户SSO的适用场景**。
- 一个华为云账号只能存在“IAM用户SSO”和“虚拟用户SSO”中的一种类型的身份提供商。

步骤3 获取华为云登录链接、domain_id和idp的值。

步骤4 参考**在华为云上配置元数据文件**把OneAccess IdP的Metadata文件配置到华为云。

步骤5 参考**配置外部身份ID**在华为云上配置IAM用户的外部身份ID，建立OneAccess用户和IAM用户的对应关系。

步骤6 在其他华为云账号上面重复**步骤2**~**步骤5**进行配置。

----结束

建立 OneAccess 对华为云的信任关系

在OneAccess中配置华为云的元数据文件，以建立OneAccess对华为云的信任。

步骤1 在OneAccess上添加华为云应用。

1. 登录OneAccess管理门户，选择“资源 > 应用”。
2. 在应用页面，单击“新增预集成应用”。
3. 在新增预集成应用页面，单击“华为云”应用。
4. 在弹出的添加应用页面，确认通用信息，单击“下一步”。
5. 在认证参数配置页面，选择“导入SP应用元数据 > 选择文件”，选择获取的华为云元数据文件。系统会自动上传文件并提取元数据。

   说明

   - 预集成应用为OneAccess专业版用户功能，如果是OneAccess基础版用户，请参考**在OneAccess中添加企业应用**创建自定义应用后进行**步骤1.5**操作。
   - 在**https://auth.huaweicloud.com/authui/saml/metadata.xml**下载华为云元数据文件，并设置文件名称，例如“SP-metadata.xml”。
   - OneAccess同时支持“选取文件”和“手动输入配置数据”方式配置元数据，了解详情请参考**在OneAccess中配置元数据文件**。

6. 待“选取文件”变为“√”时，代表系统已提取元数据，单击“下一步”，成功添加华为云应用。

7. 在认证集成页面，在“参数配置”页签，单击“编辑”，将“Single Logout URL”对应值中的“/saml/LogoutServiceHTTPRedirect”替换为“/logout”。

步骤2 配置OneAccess与华为云之间的映射关系。

1. 单击已添加的华为云应用，在应用信息页面，单击应用图标，进入应用详情页面。
2. 选择“认证集成 > 映射配置”，进入映射配置页面。
3. 单击“添加映射”，添加应用属性名为“IAM_SAML_Attributes_xUserId”的映射，建立OneAccess与华为云之间的属性映射。映射对象可以是OneAccess中用户已有的属性，也可以是新增的自定义属性，必须和步骤**步骤5**中添加的IAM用户的外部身份ID一致。
4. 单击“添加映射”，添加应用属性名为“IAM_SAML_Attributes_identityProviders”的映射，映射类型为“固定属性值”，值为“iam::{domain_id}:identityProvider:{idp_id}”，其中“{domain_id}”为步骤**步骤3**中获取的domain_id，“{idp_id}”为步骤**步骤3**中获取的idp_id，支持多个华为云账号的拼接，使用“;”进行分隔，实现跳转过程中选择某个华为云账号跳转，两个华为云账号时值举例如下：

   iam::657ba0e**********19fd684d8758c:identityProvider:SAML-IAM;iam::e35f949b3*********2b79ba14839c:identityProvider:SAML-OneAccess
5. （可选）单击“添加映射”，添加应用属性名为“IAM_SAML_Attributes_redirect_url”的映射，映射类型为“固定属性值”，值为华为云Console中的特定业务页面（如果业务地址中带有“agencyId=***&”字段，需要将该字段删除），可以实现单点登录直接跳转至特定业务页面，如果不添加，默认跳转华为云主页面。

步骤3 在OneAccess给用户授予华为云访问权限。

在华为云应用详情页面，选择“授权管理 > 应用账号”，单击“添加账号”，按需勾选账号，单击“保存”，所选用户即可在OneAccess中免密访问华为云。

----结束

OneAccess 用户登录验证

在OneAccess中授予华为云应用访问权限的用户，登录OneAccess用户门户，单击华为云应用，选择需要访问的身份提供商，即可进入华为云控制台首页访问云服务。

3.1.6 通过 OneAccess 免密登录华为云（OIDC）

本文以OIDC协议为例介绍如何实现使用OneAccess免密登录华为云Console中的CodeArts服务页面。

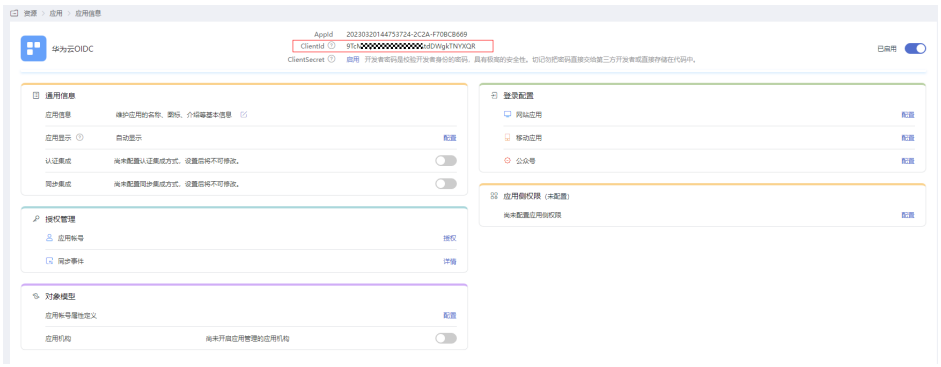
在 OneAccess 中创建华为云 OIDC 应用

在OneAccess管理门户中创建华为云OIDC应用，并获取OIDC相关设置，以建立OneAccess云华为云的信任关系。

步骤1 在OneAccess上添加华为云应用。

1. 登录OneAccess管理门户，选择“资源 > 应用”。
2. 在企业应用页面，单击“添加自建应用”。

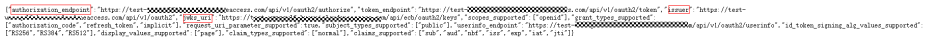
3. 输入应用名称，单击“保存”。
4. 单击新建的应用，进入应用信息页面，获取应用ClientId。



步骤2 获取OIDC相关配置。

1. 登录OneAccess管理门户，选择“设置 > 服务配置”。
2. 在服务配置页面，单击“OIDC”。
3. 在OIDC页面，单击“OIDC设置”。

4. 获取issuer、authorization_endpoint、jwks_uri地址。



5. 将jwks_uri地址复制到浏览器地址栏，获取签名公钥。

----结束

在华为云上创建身份提供商

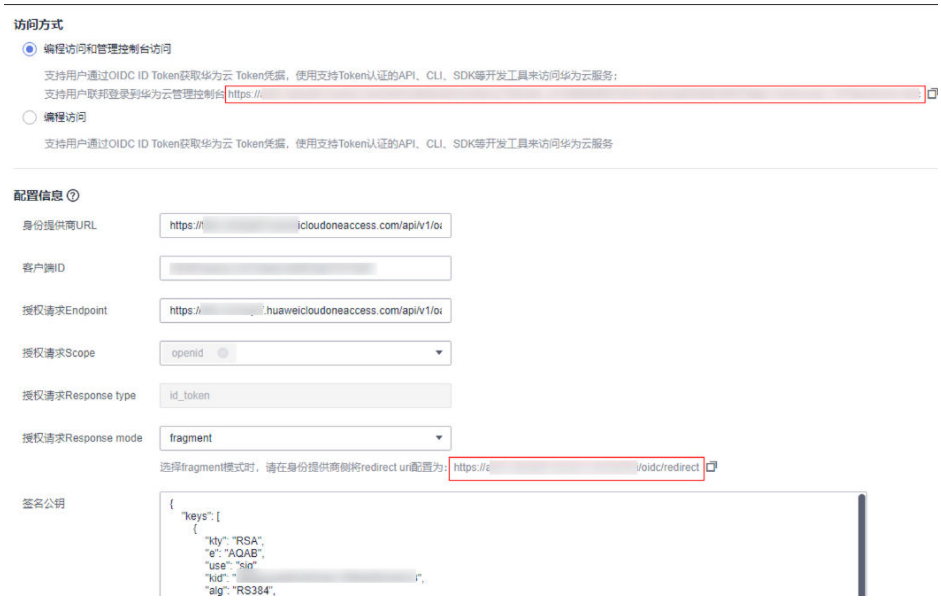
在华为云控制台创建身份提供商，配置OneAccess的应用以及OIDC信息后，可以在华为云中建立对OneAccess的信任关系。

步骤1 参考**在华为云上创建身份提供商**创建身份提供商 。

说明

- 身份提供商名称不能重复，建议以域名唯一标识命名。
- 在修改身份提供商页面，填写“配置信息”页面：
  1. “身份提供商URL”填写在OneAccess侧获取的issuer地址，见**步骤2.4**；
  2. “授权请求Endpoint”填写在OneAccess侧获取的authorization_endpoint地址，见**步骤2.4**；
  3. “客户端ID”填写在OneAccess侧获取的创建的OIDC应用的ClientId，见**步骤1.4**；
  4. “签名公钥”填写在OneAccess侧获取的前面公钥（需要将其格式化为json格式），见**步骤2.5**。

步骤2 配置过程中获取登录地址以及redirect uri地址。



步骤3 参考**配置身份转换规则**在华为云上配置身份转换规则，使得OneAccess用户拥有华为云访问CodeArts云服务的权限。

----结束

建立 OneAccess 对华为云的信任关系

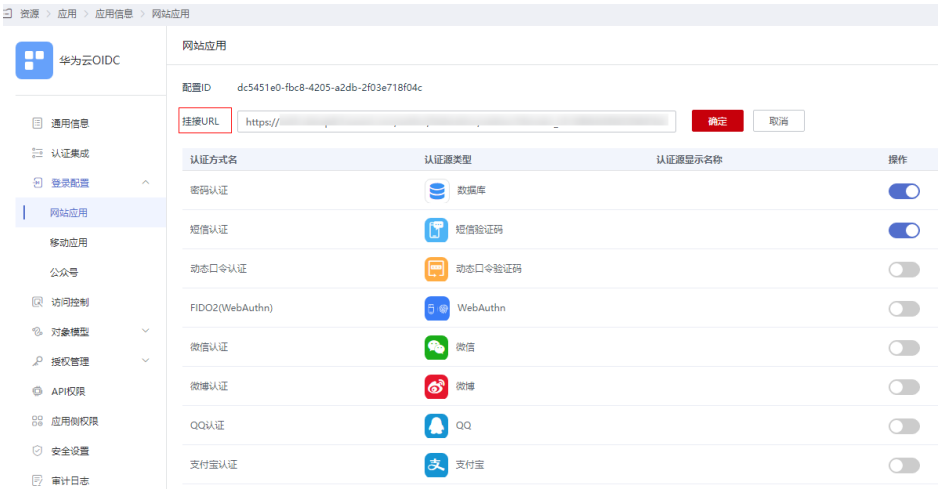
在OneAccess中配置华为云的跳转地址以及redirect uri。

1. 登录OneAccess管理门户，选择“资源 > 应用”。
2. 在企业应用页面，单击新增的华为云自定义应用。
3. 打开“认证集成”开关，并配置协议为“OIDC”，单击“保存”。

4. 单击“认证集成”后的“配置”，进入OIDC配置页面，“回调地址”配置为**步骤2**中获取的redirect uri值，并打开“隐式授权模式”开关。

5. 在OneAccess配置华为云登录入口。

   在华为云应用详情页面，选择“登录配置 > 网站应用”，单击“编辑”，将挂接URL替换为在华为云创建的身份提供商的“登录链接”，单击“确定”保存此次编辑。



说明

如果需要跳转华为云Console中的特定业务页面，需要对华为云创建的身份提供商的“登录链接”进行拼接后填入挂接URL中，此处以跳转CodeArts服务页面为例进行说明：

华为云创建的身份提供商的“登录链接”为：https://auth.huawei.com/authui/federation/websso?domain_id=e35f**********79ba14839c&idp=one001&protocol=oidc

CodeArts服务地址为：https://console.huaweicloud.com/devcloud/?region=cn-south-1&locale=zh-cn#

如果服务地址中带有“agencyId=***&”字段，需要将该字段删除后，使用“&service=”将两个地址进行拼接后填入挂接URL中：

https://auth.huawei.com/authui/federation/websso?domain_id=e35f**********79ba14839c&idp=one001&protocol=oidc&service=https://console.huaweicloud.com/devcloud/?region=cn-south-1&locale=zh-cn#

6. 在OneAccess给用户授予华为云访问权限。

   在华为云应用详情页面，选择“授权管理 > 应用账号”，单击“添加账号”，按需勾选账号，单击“保存”，所选用户即可在OneAccess中免密访问华为云。

   说明

   华为云“统一身份认证服务”中的用户，邮箱是必填字段，OneAccess系统中授权的用户必须有邮箱字段。

OneAccess 用户登录验证

在OneAccess中授予华为云访问权限的用户，登录OneAccess用户门户，单击自定义的华为云应用即可进入华为云中的CodeArts云服务。

3.2 通过 SAML 协议单点登录至应用

概述

SAML即安全断言标记语言（Security Assertion Markup Language），是OASIS安全服务技术委员会的一个产品，是基于XML的开源标准数据格式。SAML可以解决Web端应用系统的单点登录（SSO）需求，在不同的安全域（security domain）之间交换认证和授权数据。

从抽象的角度来看，SAML主要包括：主要术语和授权流程。

- 主要术语

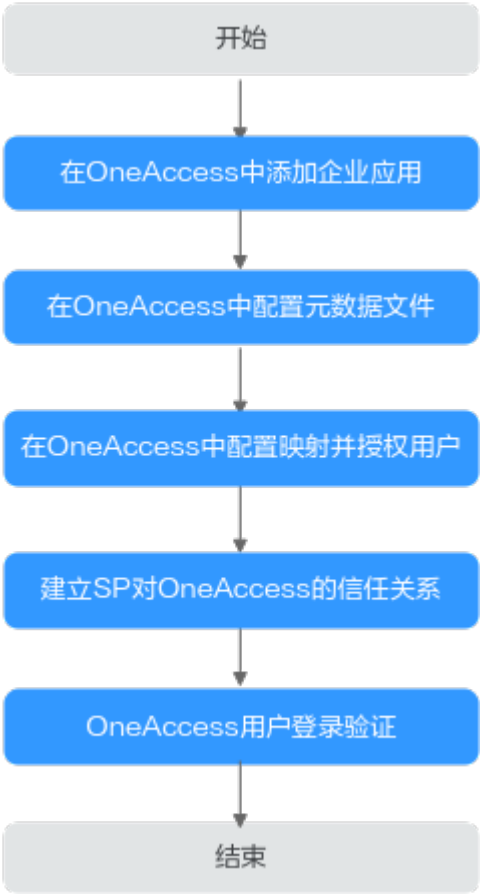
  表 3-1 主要术语

术语	说明
IdP	身份提供商（Identity Provider，简称IdP）。负责收集、存储用户身份信息，如用户名、密码等，在用户登录时负责认证用户的服务。
SP	服务提供商（Service Provider，简称SP）。与IdP建立信任关系，使用IdP提供的用户信息，为用户提供具体的服务。
SSO	单点登录（Single Sign-On，简称SSO）。用户在OneAccess系统登录后，就可以通过跳转链接访问已建立互信关系的SP系统。

- 授权流程
  a. 用户通过浏览器访问Web应用系统。
  b. Web应用系统生成一个SAML身份验证请求。
  c. Web应用系统将重定向网址发送到用户的浏览器，重定向网址包含应向SSO服务提交的编码SAML身份验证请求。
  d. IdP对SAML请求进行解码。
  e. IdP对用户进行身份验证。认证成功后，IdP生成一个SAML响应并编码返回到用户的浏览器，其中包括经过验证的用户的用户名。
  f. 浏览器将SAML响应转发到Web应用系统ACS URL。
  g. Web应用系统使用IdP的公钥验证SAML响应，验证成功，ACS则会将用户重定向到目标网址。
  h. 用户将重定向到目标网址并登录到 Web 应用系统。

本文主要介绍OneAccess以SAML协议集成应用的方法。

配置流程



前提条件

请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中添加企业应用

在OneAccess管理门户中添加企业应用，配置企业应用的元数据文件后，可以建立OneAccess对企业应用SP的信任关系。使用企业已有账号登录华为云，具体操作请参考**通过OneAccess免密登录华为云**。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

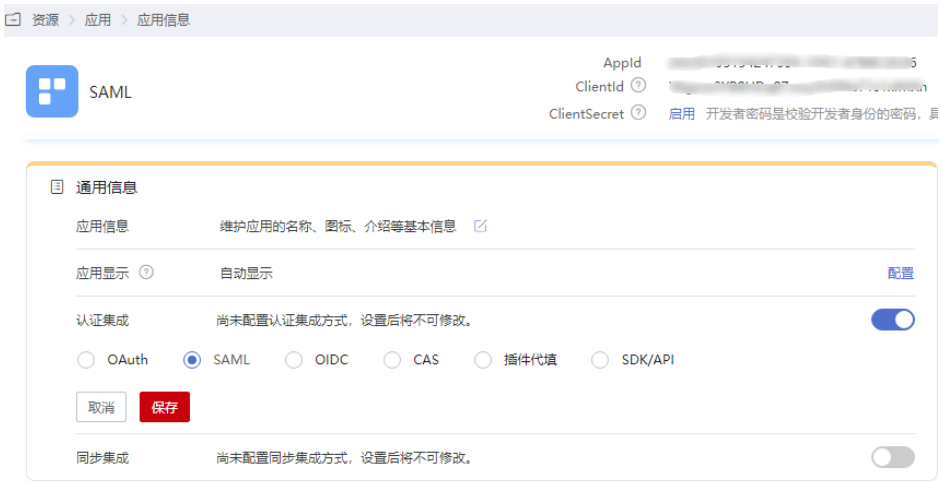
----结束

在 OneAccess 中配置元数据文件

配置元数据文件，即在OneAccess中配置企业SP的Metadata文件。OneAccess支持“上传文件”和“手动编辑”两种配置，选择其中一种即可。如果后续元数据有更新，需要重新上传或者编辑元数据，否则会影响企业用户通过OneAccess登录企业应用。

步骤1 单击**在OneAccess中添加企业应用**中添加的企业应用，在应用信息页面单击应用图标。

步骤2 在通用信息模块，单击“认证集成”后的  打开认证集成设置，此处选择SAML协议，单击“保存”。



说明

应用认证集成协议一旦设置不可修改。

步骤3 在通用信息模块，单击“认证集成”后的“配置”，进入“参数配置”页签配置元数据文件，可以选择上传文件和手动配置两种方式。

须知

配置参数会明文展示所输入的信息，请防止信息泄露。

- 上传文件
  a. 单击“上传文件”，选择获取的企业SP的元数据文件。

  b. 当显示“上传成功”时，即系统已提取元数据。

  说明

  - 如果提示“文件格式错误，仅支持上传xml格式文件”，需要您确认元数据文件的正确性后，重新上传或者通过手动编辑提取元数据。
  - 企业应用的元数据获取方法请参考SP提供商的帮助文档。

- 手动配置
  a. 在“参数配置”页签，单击“手动配置”。
  b. 在手动编辑元数据页面，输入从企业SP元数据文件中获取的“**SP Entity ID**”、“**ACS URL**”和“**签名证书**”等参数，单击“保存”。

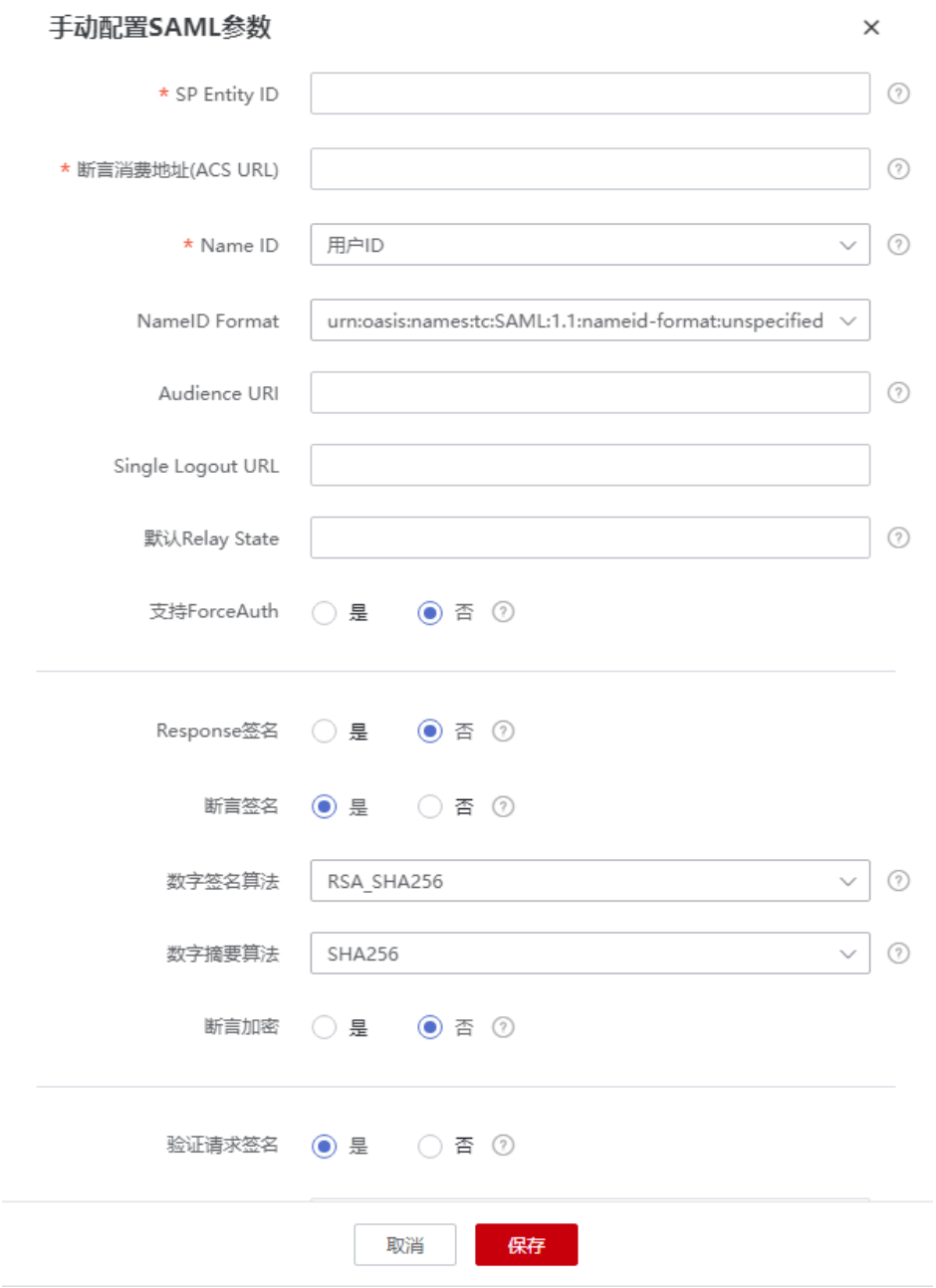


表 3-2 认证参数

参数	是否必选	说明
SP Entity ID	是	SP唯一标识，对应SP元数据文件中的“Entity ID”的值。
断言消费地址（ACS URL）	是	SP回调地址（断言消费服务地址），对应SP元数据文件中“AssertionConsumerService”的值，即当OneAccess认证成功后响应返回的地址。

参数	是否必选	说明
Name ID	是	用户在应用系统中的账号名对应字段，可以选择用户的属性或者对应的账号属性,此字段的值将作为断言中的subject。
NameID Format	是	SP支持的用户名称标识格式。对应SP元数据文件中“NameIDFormat”的值。
Audience URI	否	允许使用SAML断言的资源，默认和SP Entity ID相同。
Single Logout URL	否	服务提供商提供会话注销功能，用户在OneAccess注销会话后返回该地址。
默认Relay State	否	使用在idp发起的认证中，作为默认的一个值。
支持ForceAuth	是	默认为否。如果SP要求重新认证，则强制用户再次认证。
Response签名	是	默认为否。是否对SAML Response使用IdP的证书签名。
断言签名	是	默认为是。断言需使用IdP的证书签名，对应SP元数据文件中“WantAssertionsSigned”值。
数字签名算法	是	默认为RSA_SHA256，是SAML Response或者断言签名的算法，可在下拉框选择。
数字摘要算法	是	默认为SHA256，是SAML Response或者断言的算法摘要算法，可在下拉框选择。
断言加密	是	默认为否。是否对断言进行加密。
验证请求签名	是	默认为是。用来对SAML Request签名进行验证，对应SP元数据文件中“AuthnRequestsSigned”值。
验证签名证书	是	SP公钥证书，用来验证SAML request的签名，对应SP元数据文件中use="signing"证书内容。

----结束

在 OneAccess 中配置映射并授权用户

- 映射配置，即在OneAccess中配置认证成功后需要返回给应用的属性，以建立OneAccess与应用端属性的映射关系。

  说明

  如果在**在OneAccess中配置元数据文件**的“Name ID”已设置你所需要的映射关系，可以选择跳过映射配置。

  在认证配置页面，选择“映射配置”页签，单击“添加映射”，建立OneAccess与应用端属性的映射。

表 3-3 映射参数

参数	说明
应用系统属性名	必填。认证成功后，OneAccess返回给应用的用户属性。
映射类型	必填。不同的映射类型决定不同接口返回属性的属性值，可在下拉框按需选择。
Friendly Name	必填。与**应用系统属性名**一致。
Attr Name Format	必填。SAML协议返回的一种数据格式。

- 授权用户，即在OneAccess中授权访问应用的用户，确保用户具有访问应用的权限。

  选择左侧的“授权管理 > 应用账号”，单击“添加账号”，授权访问应用的账号。如需根据策略给用户授权，请参考：**配置应用**中应用账号的授权策略。

  说明

  登录配置、访问控制、对象模型等设置请参考**配置应用**。

建立 SP 对 OneAccess 的信任关系

在SP中配置OneAccess的元数据文件，以建立SP对OneAccess的信任。

步骤1 下载OneAccess系统的元数据文件（metadata文件）。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”进入服务配置页面。
3. 单击“IDP配置”。
4. 在弹出的IDP配置页面，单击右上角的“下载IDP元数据”，数据会自动保存。

步骤2 将上述文件上传到企业SP服务器上，上传方法请参见SP提供商的帮助文档。

步骤3 获取企业SP的元数据文件。获取方法请参见SP提供商的帮助文档。

----结束

OneAccess 用户登录验证

使用**授权用户**中的已授权用户访问用户门户，成功登录以后，单击目标应用即可进入企业应用。

3.3 通过 OAuth2.0 协议单点登录至应用

概述

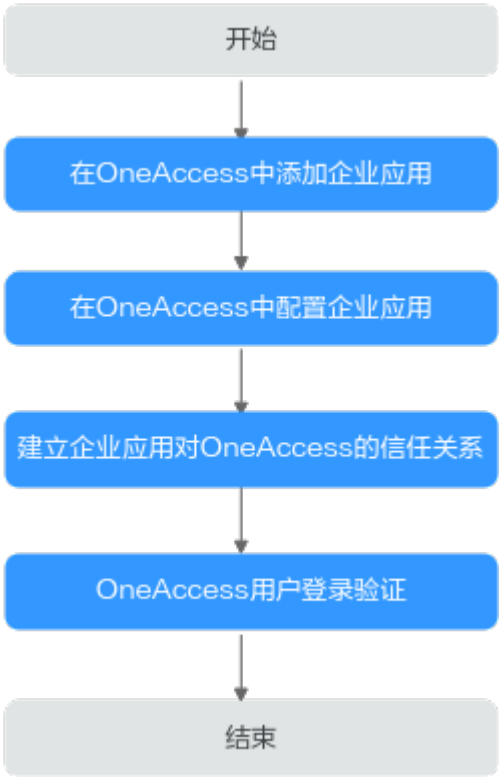
OAuth2.0（开放授权）是一个开放标准，允许用户授权第三方应用访问其存储在资源服务器上的信息，而不需要将用户名和密码提供给第三方应用。

基于该协议进行授权的整体流程为：

1. 用户访问第三方应用系统，第三方应用系统向OneAccess发起授权登录请求，用户同意授权第三方应用系统后，OneAccess将携带授权码code，重定向到第三方应用系统。
2. 第三方应用系统使用授权码code调用OneAccess的API接口换取授权令牌access_token。
3. 第三方应用系统使用授权令牌access_token（access_token有效且未超时）调用OneAccess的API接口获取用户信息。

本文主要介绍OneAccess以OAuth协议集成应用的方法。

配置流程



前提条件

请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中添加企业应用

在OneAccess管理门户中添加企业应用，通过配置认证信息，可以建立OneAccess对企业应用的信任关系。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

----结束

在 OneAccess 中配置企业应用

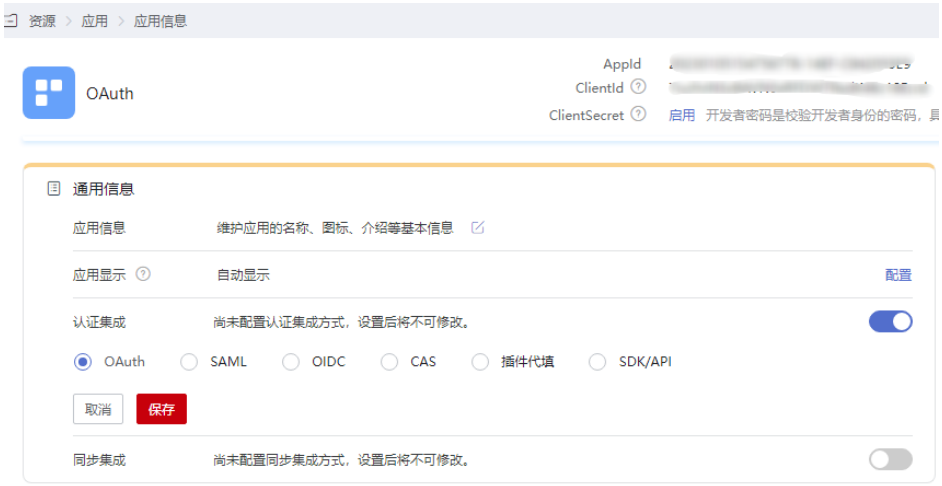
在OneAccess中配置应用的信息，确保用户可以通过OneAccess登录企业应用。包括认证配置、 映射配置、授权用户。

- 认证配置
  a. 单击**在OneAccess中添加企业应用**中添加的企业应用，在应用信息页面单击应用图标。
  b. 在通用信息模块，单击“认证集成”后的  打开认证集成设置，此处选择“OAuth”协议，单击“保存”。

  说明

  应用认证集成协议一旦设置不可修改。

  图 3-3 设置认证协议

  c. 在通用信息模块，单击“认证集成”后的“配置”，进入“认证集成（OAUTH）”的“参数配置”页签。

  说明

  配置参数会明文展示所输入的信息，请防止信息泄露。

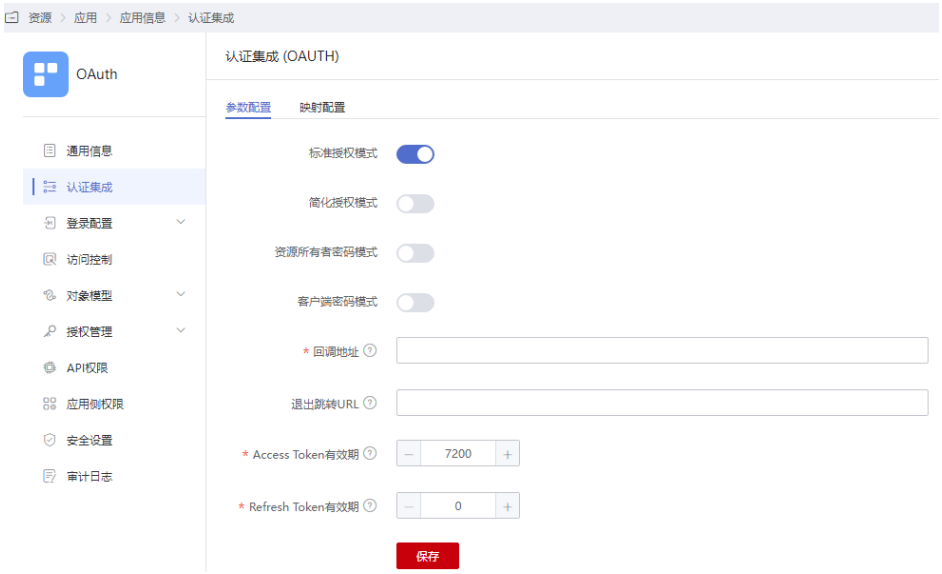


表 3-4 认证参数

参数	说明
标准授权模式	默认开启。是最常用，安全性也最高的一种认证模式，适用于有后端的Web应用。该模式下，授权码通过前端传送，令牌存储在后端，可以避免令牌泄漏，而且所有与资源服务器的通信都在后端完成。具体的标准授权模式可参考**概述**。
简化授权模式	默认关闭。适用于没有后端的Web应用，必须将令牌存储在前端，用于一些对安全要求不高的场景。与标准授权模式相比，省略了获取授权码code环节。
资源所有者密码模式	默认关闭。适用于用户对客户端高度信任的场景，用户将用户名和密码提供给客户端，由客户端申请令牌。
客户端密码模式	默认关闭。适用于没有前端的应用，由客户端发起申请令牌请求。
回调地址	必填。成功授权后的回调地址，必须在可信域名范围内（多个域名以逗号分隔），建议设置为应用首页。如https://example.com。
退出跳转URL	可选。应用退出地址。用户在OneAccess注销会话后返回绑定的地址。
Access Token有效期	授权令牌的有效期，默认2小时，以秒为单位。
Refresh Token有效期	刷新令牌的有效期，默认0，即不支持Refresh Token。当Access Token过期后，用户可通过Refresh Token实现自动更新令牌。 **说明** 实现自动更新令牌的前提是设置Refresh Token有效期大于Access Token的有效期。

- （可选）映射配置

  在认证配置页面，选择“映射配置”页签，单击“添加映射”，建立OneAccess与应用端属性的映射。

  表 3-5 映射参数

参数	说明
应用系统属性名	必填。认证成功后，OneAccess返回给应用的用户属性。
映射类型	必填。不同的映射类型决定不同接口返回属性的属性值，可在下拉框按需选择。

- 授权用户

  选择左侧的“授权管理 > 应用账号”，单击“添加账号”，授权访问应用的账号。如需根据策略给用户授权，请参考**配置应用**中应用账号的授权策略。

  说明

  登录配置、访问控制、对象模型等设置请参考**配置应用**。

建立企业应用对 OneAccess 的信任关系

在企业应用中配置OneAccess的授权信息，以建立企业应用对OneAccess的信任。

步骤1 获取OneAccess侧的ClientId和ClientSecret。

单击**在OneAccess中添加企业应用**中添加的企业应用，在应用信息页面单击应用图标，在应用详情页面获取ClientId和ClientSecret。

说明

- ClientSecret需单击“启用”生成。
- ClientSecret是校验开发者身份的密码，具备高安全性，切勿将其直接提供给第三方开发者或直接存储在代码中。
- 重置后的ClientSecret即时生效，所有使用原ClientSecret的接口将全部失效，请谨慎重置。
- OneAccess不存储ClientSecret，当获取ClientSecret后，请妥善保管。

图 3-4 获取 ClientId 和 ClientSecret

步骤2 获取OneAccess侧的认证信息。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”进入服务配置页面。
3. 单击“OIDC”。
4. 在弹出的OIDC页面，查看认证地址。

步骤3 获取企业应用的授权信息。获取方法请参见应用提供商的帮助文档。

----结束

OneAccess 用户登录验证

使用**授权用户**中的已授权用户访问用户门户，成功登录以后，单击目标应用即可进入企业应用。

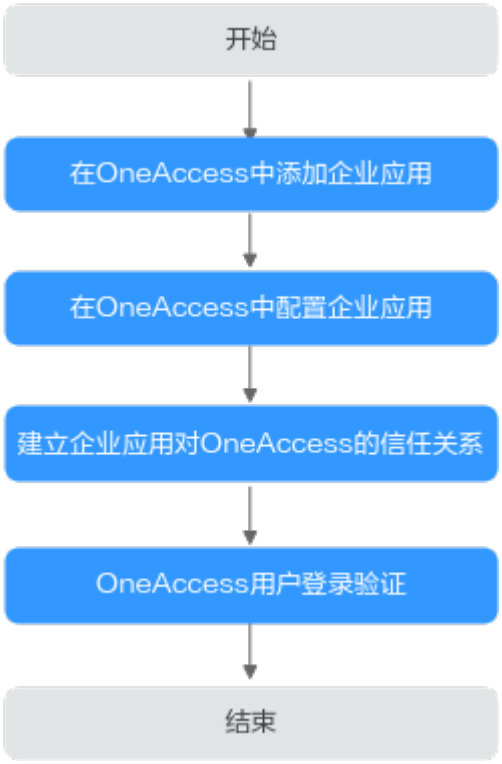
3.4 通过 OIDC 协议单点登录至应用

概述

OIDC是OpenID Connect的简称，是一个基于OAuth 2.0协议的身份认证标准协议。关于OIDC的详细描述请参见**欢迎使用OpenID Connect**。

本文主要介绍OneAccess以OIDC协议集成应用的方法。

配置流程



前提条件

请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中添加企业应用

在OneAccess管理门户中添加企业应用，通过配置认证信息，可以建立OneAccess对企业应用的信任关系。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

----结束

在 OneAccess 中配置企业应用

在OneAccess中配置应用的信息，确保用户可以通过OneAccess登录企业应用。包括认证配置、映射配置、 授权用户。

- 认证配置
  a. 单击**在OneAccess中添加企业应用**中添加的企业应用，在应用信息页面单击应用图标。
  b. 在通用信息模块，单击“认证集成”后的 打开认证集成设置，此处选择OIDC协议，单击“保存”。

说明

应用认证集成协议一旦设置不可修改。

图 3-5 设置认证协议

c. 在通用信息模块，单击“认证集成”后的“配置”，进入“参数配置”页签。

说明

配置参数会明文展示所输入的信息，请防止信息泄露。

表 3-6 认证参数

参数	说明
Redirect URL	必填。成功授权后的回调地址，必须在可信域名范围内（多个域名以逗号分隔），可以接收并处理授权的地方，建议为应用首页，如https://example.com。
Logout URL	可选。应用退出地址。用户在OneAccess注销会话后返回绑定的地址。
授权码模式	默认开启。是使用最广泛的一种认证模式，适用于前后端分离的应用。具体的授权码模式可参考**概述**。
隐式授权模式	默认关闭。适用于没有后端的应用，与授权码模式相比，省略了获取授权码code环节。
TOKEN签名算法	默认为RS256，对Token签名的算法，可在下拉框选择。用户需要与自身系统中使用的加密算法进行匹配。
Access Token有效期	授权令牌的有效期，默认2小时，以秒为单位。

参数	说明
Refresh Token有效期	刷新令牌的有效期，默认0，即不支持Refresh Token。当Access Token过期后，用户可通过Refresh Token实现自动更新令牌。 **说明** 实现自动更新令牌的前提是设置Refresh Token有效期大于Access Token的有效期。

- （可选）映射配置

  在认证集成页面，选择“映射配置”页签，单击“添加映射”，建立OneAccess与应用端属性的映射。

  表 3-7 映射参数

参数	说明
应用系统属性名	必填。认证成功后，OneAccess返回给应用的用户属性。
映射类型	必填。不同的映射类型决定不同接口返回属性的属性值，可在下拉框按需选择。

- 授权用户

  选择左侧的“授权管理 > 应用账号”，单击“添加账号”，授权访问应用的账号。如需根据策略给用户授权，请参考**配置应用**中应用账号的授权策略。

  说明

  登录配置、访问控制、对象模型等设置请参考**配置应用**。

建立企业应用对 OneAccess 的信任关系

在企业应用中配置OneAccess的授权信息，以建立企业应用对OneAccess的信任。

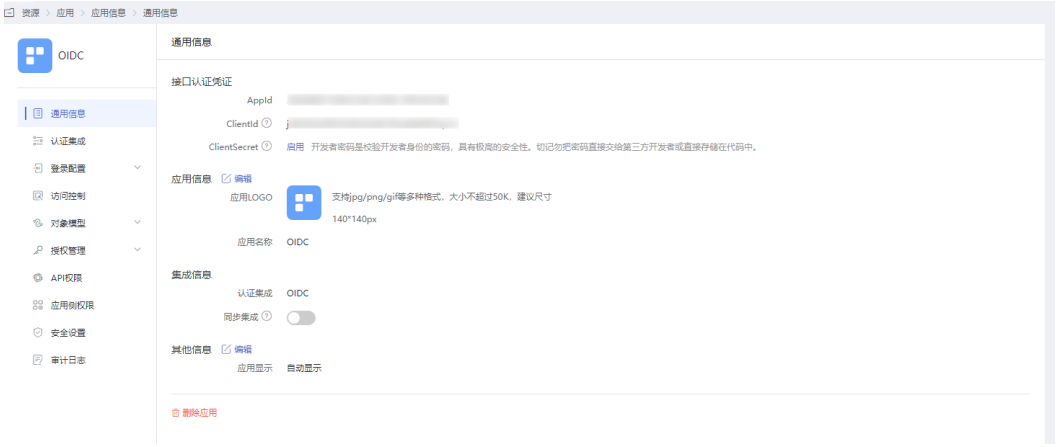
步骤1 获取OneAccess侧的ClientId 和 ClientSecret。

单击**在OneAccess中添加企业应用**中添加的企业应用，在应用信息页面单击应用图标，在应用详情页面获取 ClientId 和 ClientSecret。

说明

- ClientSecret需单击“启用”生成。
- ClientSecret是校验开发者身份的密码，具备高安全性，切勿将其直接提供给第三方开发者或直接存储在代码中。
- 重置后的ClientSecret即时生效，所有使用原ClientSecret的接口将全部失效，请谨慎重置。
- OneAccess不存储ClientSecret，当获取ClientSecret后，请妥善保管。

图 3-6 获取 ClientId 和 ClientSecret



步骤2 获取OneAccess侧的认证信息。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”进入服务配置页面。
3. 单击“OIDC”
4. 在弹出的OIDC页面，查看认证地址，单击右上角的“OIDC设置”可以查看配置认证参数。

步骤3 获取企业应用的授权信息。获取方法请参见应用提供商的帮助文档。

----结束

OneAccess 用户登录验证

使用**授权用户**中的已授权用户访问用户门户，成功登录以后，单击目标应用即可进入企业应用。

3.5 通过 CAS 协议单点登录至应用

概述

CAS是一个基于HTTP2、HTTP3的协议，要求每个组件都可以通过特定的URL访问。通过CAS协议将OneAccess作为身份服务提供商，使第三方应用可以读取OneAccess的用户账号数据。支持CAS1.0、CAS2.0、CAS3.0三种协议。

从抽象的角度来看，主要包括CAS协议和授权流程。

- CAS协议

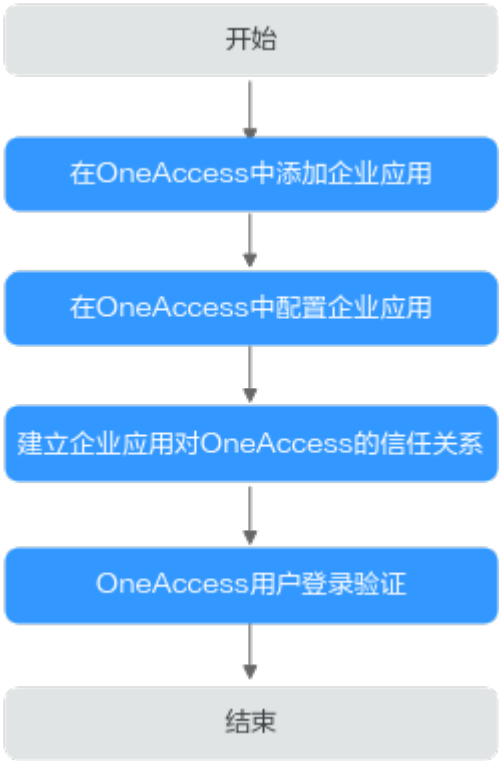
  CAS 协议涉及两个主体，两个主体通过用户浏览器进行信息交换。如CAS Client可以返回带参数的重定向，将信息转发给CAS Server。登录验证成功后 CAS Server会返回CAS Client一个包含用户信息的XML， CAS Client验证用户信息后会返回给用户访问资源。

  - CAS Server： CAS服务端，身份认证提供方，如OneAccess认证服务。
  - CAS Client： CAS客户端，资源提供方，如第三方应用。
- 授权流程

a. 用户登录CAS Client 提供的应用。
b. CAS Client分析该Http请求中是否包含认证票据ST，如果没有，则说明当前用户尚未认证，于是重定向CAS Server ，并传递Service （目的资源地址）。
c. 用户输入认证信息，如登录成功，CAS Server随机产生一个相当长度、唯一、不可伪造的票据ST，然后附带生成的ST重定向到CAS client。
d. CAS Client收到Service和新产生的ST后，通过后台与CAS Server进行交互验证。
e. CAS Server根据请求参数Service和ST进行身份核实，以确保ST的合法性，并返回一段指定格式的XML（包含用户信息）给CAS Client。
f. CAS Client和CAS Server之间完成了一个对用户的身份核实，返回给用户CAS Client访问资源。

本文主要介绍OneAccess以CAS协议集成应用的方法。

配置流程



前提条件

请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中添加企业应用

在OneAccess管理门户中添加企业应用，通过配置认证信息，可以建立OneAccess对企业应用的信任关系。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

----结束

在 OneAccess 中配置企业应用

在OneAccess中配置应用的信息，确保用户可以通过OneAccess登录企业应用。包括认证配置、 映射配置、 授权用户。

- 认证配置
  a. 单击**在OneAccess中添加企业应用**中添加的企业应用，在应用信息页面单击应用图标。

  b. 在通用信息模块，单击“认证集成”后的  打开认证集成设置，此处选择CAS协议，单击“保存”。

  说明

  应用认证集成协议一旦设置不可修改。

  图 3-7 设置认证协议

  c. 在通用信息模块，单击“认证集成”后的“配置”，进入“认证集成（CAS）”的“参数配置”页签。

须知

配置参数会明文展示所输入的信息，请防止信息泄露。

图 3-8 配置认证参数

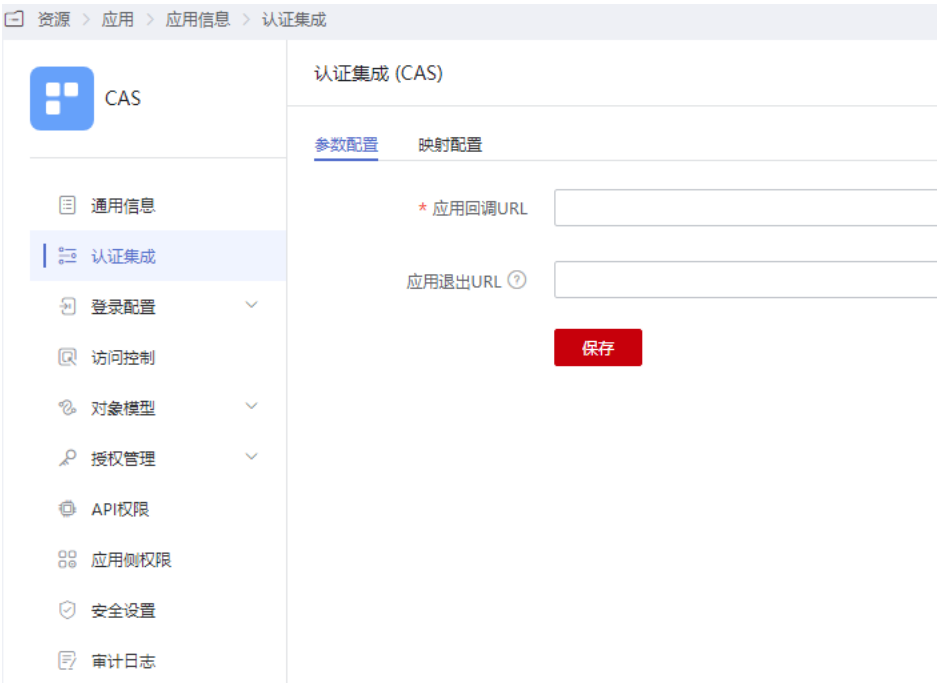


表 3-8 认证参数

参数	说明
应用回调URL	必填。第三方应用的URL，需与CAS接口中service参数值一致，且符合RFC中URL的编码格式。
应用退出URL	选填。应用退出地址，用户在OneAccess注销会话后返回绑定的地址。

- 映射配置

  在认证配置页面，选择“映射配置”页签，单击“添加映射”，建立OneAccess与应用端属性的映射。

图 3-9 添加映射

表 3-9 映射参数

参数	说明
应用系统属性名	必填。认证成功后，OneAccess返回给应用的用户属性。
映射类型	必填。不同的映射类型决定不同接口返回属性的属性值，可在下拉框按需选择。

- 授权用户

  选择左侧的“授权管理 > 应用账号”，单击“添加账号”，授权访问应用的账号。如需根据策略给用户授权，请参考**配置应用**中应用账号的授权策略。

  说明

  登录配置、访问控制、对象模型等设置请参考**配置应用**。

建立企业应用对 OneAccess 的信任关系

在企业应用中配置OneAccess的授权信息，以建立企业应用对OneAccess的信任。

步骤1 获取OneAccess侧的认证信息。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”进入服务配置页面。
3. 单击“CAS配置”。
4. 在弹出的CAS页面，查看认证地址。

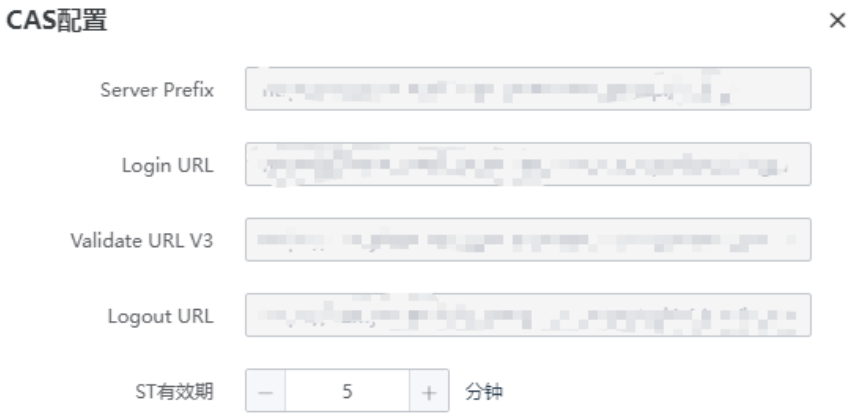


表 3-10 配置参数

参数	说明
Server Prefix	系统自动生成，不可编辑。CAS服务地址的前缀。
Login URL	系统自动生成，不可编辑。CAS服务的请求授权地址。
Validate URL V3	系统自动生成，不可编辑。验证票据，推荐使用V3的地址。

参数	说明
Logout URL	系统自动生成，不可编辑。CAS服务的登出地址。
ST有效期	请求授权返回票据的有效期，建议设置为3~15分钟。

步骤2 获取企业应用的授权信息。获取方法请参见应用提供商的帮助文档。

----结束

OneAccess 用户登录验证

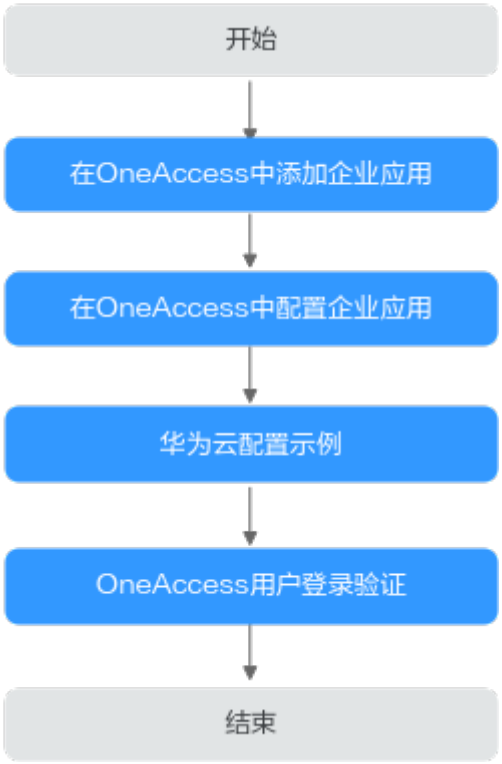
使用**授权用户**中的已授权用户访问用户门户，成功登录以后，单击目标应用即可进入企业应用。

3.6 以插件代填的方式集成应用

OneAccess可在PC端集成不支持标准协议（OAuth2、SAML、OIDC、CAS）且不可改造的应用。

本文主要介绍OneAccess以插件代填的方式集成应用。

配置流程



前提条件

请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中添加企业应用

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

----结束

在 OneAccess 中配置企业应用

配置企业应用包括认证配置、 授权用户。

- 认证配置
  a. 单击**在OneAccess中添加企业应用**中添加的企业应用，在应用信息页面单击应用图标。
  b. 在通用信息模块，单击“认证集成”后的  打开认证集成设置，此处选择插件代填协议，单击“保存”。

  说明

  应用认证集成方式一旦设置不可修改。

  图 3-10 设置认证协议

  c. 单击左侧列表中的“认证配置”，配置认证参数。OneAccess支持多种配置方式，包括简单登录、三字段登录、带Frame的登录、两页面登录。不同的登录方式需配置的参数略有差异。

须知

配置参数会明文展示所输入的信息，请防止信息泄露。

  - 简单登录

    登录页面只有两个输入元素，即用户名和密码，无需其它元素信息即可登录的应用系统。如**图3-11**。

图 3-11 华为云账号登录

  - 三字段登录

    登录页面有三个输入元素，即除用户名和密码外，还需其它输入框或选择框才能登录。如某公司内部系统需员工输入用户名和密码外，还需选择所在部门方可登录。

  - 带Frame的登录

    登录页面嵌套Frame元素，用户名和密码布局在Frame元素内，与整体登录页面隔离。

  - 两页面登录

    登录过程分为两个页面进行，需要在第一个页面跳转至第二个页面。

- 授权用户

  选择左侧的“授权管理 > 应用账号”，单击“添加账号”，授权访问应用的账号。如需根据策略给用户授权，请参考配置应用中应用账号的授权策略。

说明

- 访问控制、对象模型等设置请参考**配置应用**。
- 插件代填的应用不进行用户授权，也可以由用户直接在用户门户中设置。

华为云配置示例

以华为云为例说明简单登录的配置方法。

步骤1 访问**华为云**，打开F12，定位账号输入框，取唯一属性 type。

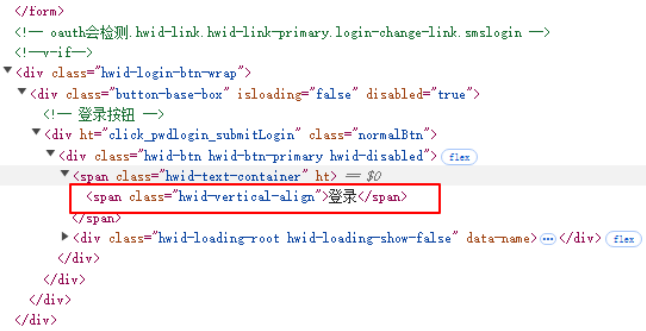
图 3-12 定位账号输入框

步骤2 定位密码输入框，取唯一属性 type。

图 3-13 定位密码输入框

步骤3 定位“登录”按钮，取唯一属性id。

图 3-14 定位登录按钮



步骤4 配置简单登录的参数。CSS选择器可参考**https://www.w3school.com.cn/cssref/css_selectors.asp**。

表 3-11 基本配置

参数	说明
应用地址	应用的访问地址，建议设置为应用首页。
登录页面地址	应用的登录页面地址。选择简单登录、三字段登录、两页面登录时，需配置该参数。
Frame地址	应用的Frame地址。选择带Frame元素登录时，需配置该参数。
用户名输入框	用户名输入框的CSS选择器。
下一步按钮	下一步按钮的CSS选择器。选择两页面登录时，需配置该参数。
密码输入框	密码输入框的CSS选择器。
额外输入框	额外输入框的的CSS选择器。选择三字段登录时，需配置该参数。
额外字段映射	额外字段的映射属性，可选择账号名、名字、密码。选择三字段登录时，需配置该参数。
登录按钮	登录按钮的CSS选择器。
自动提交	表单（用户名、密码等）是否需自动提交。如选择否，只会填充用户名和密码，不会自动提交。 **说明** 涉及人机交互的验证码页面，如手机验证码，不建议勾选自动提交。

表 3-12 账号配置

参数	说明
账号创建人	登录应用的账号归属，可选择管理员、用户。 **说明** 当**账号创建人**为管理员时，需配置“允许用户设置的字段”。如选择密码，只允许用户设置登录应用的密码。

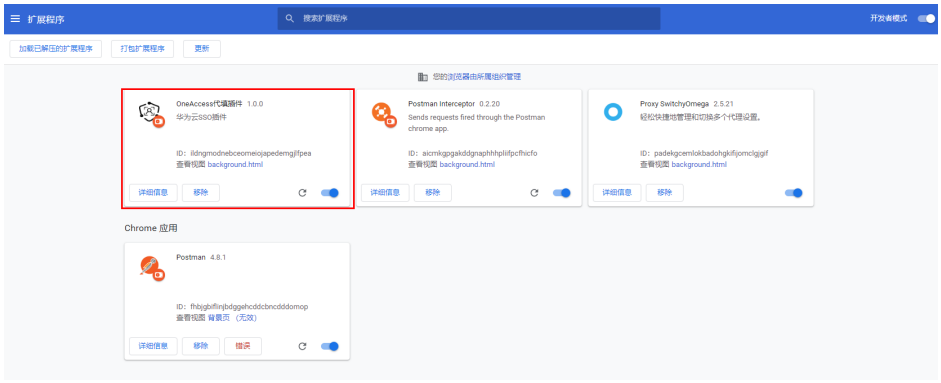
----结束

OneAccess 用户登录验证

步骤1 使用**授权用户**中的已授权用户访问用户门户，成功登录以后，按照页面提示下载插件。

步骤2 解压插件包，将其拖至扩展程序并开启。

图 3-15 添加扩展程序



步骤3 刷新用户门户，单击目标应用，页面弹出输入密码的窗口，输入密码后，单击“登录到 插件代填”，即可进入应用。

说明

若**步骤4**中设置“允许用户设置的字段”为“密码”，则此步只允许用户设置密码。

----结束

4 同步企业数据

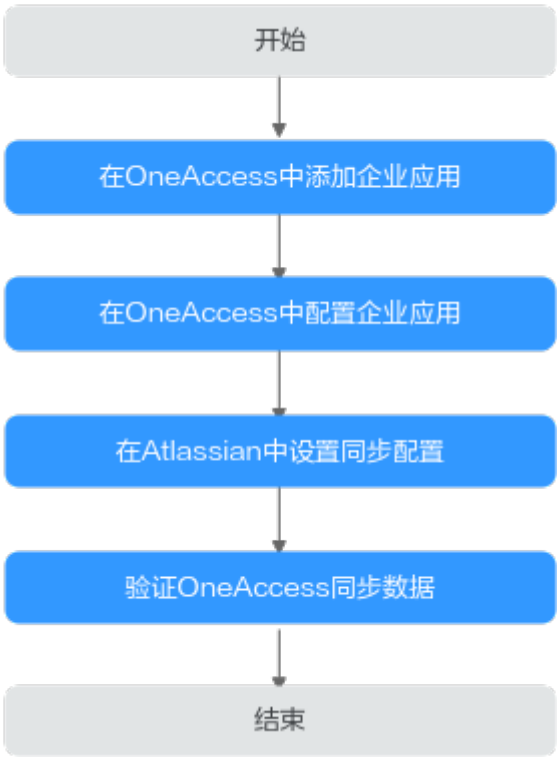
4.1 通过 SCIM 协议同步数据至 Atlassian

概述

SCIM（System for Cross-domain Identity Management），主要用于多租户的云应用身份管理。SCIM 2.0建立在一个对象模型上，所有SCIM对象都继承Resource，它有id、externalId和meta属性，RFC7643定义了扩展公共属性的User、Group和EnterpriseUser。

本文主要介绍OneAccess以SCIM协议同步用户至Atlassian的方法。

配置流程



前提条件

- 请确保您已拥有Atlassian的管理员账号。
- 请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中添加企业应用

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

----结束

在 OneAccess 中配置企业应用

步骤1 单击**在OneAccess中添加企业应用**中添加的企业应用。

步骤2 在通用信息模块，单击“同步集成”后的 打开同步集成设置，此处选择SCIM，单击“保存”。

说明

同步集成协议一旦设置不可修改。

步骤3 在通用信息模块，单击“同步集成”后的“配置”，进入“参数配置”页签。

图 4-1 配置同步参数

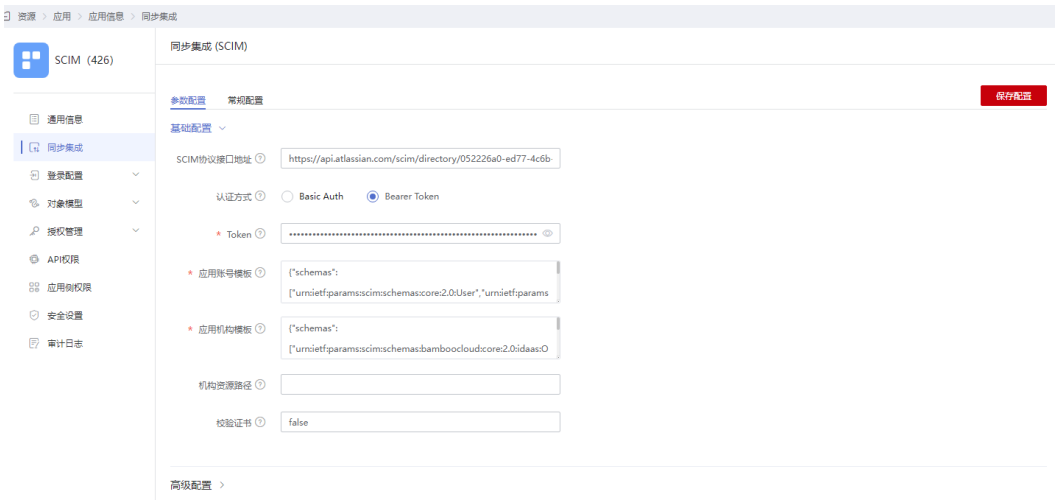


表 4-1 基础配置

参数	是否必填	说明
SCIM协议接口地址	是	目标系统接收SCIM协议数据结构的接口地址，例如 https://example.com/v2。

参数	是否必填	说明
认证方式	是	调用SCIM接口前需要进行授权，如未授权则无法调用相关接口。可选Basic Auth、Bearer Token。OneAccess默认Basic Auth。
认证用户名	是	Basic Auth认证方式对应的认证用户名。当**认证方式**选择**Basic Auth**时，需填写。
认证密码	是	**认证用户名**对应的密码。当**认证方式**选择**Basic Auth**时，需填写。
应用账号模板	是	需要推送给目标系统的用户请求数据模板。系统默认为SCIM2.0标准协议的数据模板，请根据目标系统的SCIM协议填写。
应用机构模板	是	需要推送给目标系统的机构请求数据模板。系统默认为SCIM2.0标准协议的数据模板，请根据目标系统的SCIM协议填写。
机构资源路径	否	SCIM协议机构资源接口路径，例如标准协议中用户路径为User，用户组路径为Group。

表 4-2 高级配置

参数	是否必填	说明
Content-Type	否	请求头部参数，请根据目标系统的要求填写。一般为application/json、application/scim+json。系统默认为application/scim+json。
Accept	否	请求头部参数，请根据目标系统的要求填写。一般为application/json、application/scim+json。
时间格式	否	JSON时间格式的表达式，如果格式为毫秒值，则填timestamp，其他格式则值为格式表达式，如yyyy-MM-dd HH:mm:ss。

步骤4 选择左侧的“对象模型 > 应用账号模型”，在“属性定义”页签单击“添加”，添加属性，配置参数见表4-3。

说明

邮箱属性为SCIM同步Atlassian必填属性，在不添加情况下会同步失败。

表 4-3 属性定义

参数	说明
* 属性名	OneAccess映射至目标应用的属性，如email。

参数	说明
* 显示标签	属性名称的标识，建议与**属性名**对应。
描述	**属性名**的说明。
* 属性类型	属性值的类型，可在下拉框选择。
格式	只有“属性类型”选择文本时才需要设置该参数，用来设置文本的格式。
是否必填	勾选后，同步用户数据至应用时，该属性必须有值，为空时，会提示“{显示标签}为必填属性”。
是否唯一	只有“属性类型”选择“文本”时才需要设置该参数，勾选后，同步用户数据至应用时，该属性的值具有唯一性，重复时，会提示“{显示标签}”已存在。
是否敏感	只有“属性类型”选择“文本”时才需要设置该参数，勾选后，同步用户数据至应用时，数据隐藏展示，单击可以看到数据内容。

步骤5 切换到“映射定义”页签，单击“编辑”，配置映射。

表 4-4 映射定义

参数	说明
用户	OneAccess映射至应用的属性，如邮箱。
转换方式	OneAccess与应用之间属性的映射方式。
脚本表达式	当**转换方式**选择**脚本转换**时，可激活该输入框。
执行方式	OneAccess同步用户数据至目标应用时的方式。
应用账号	应用的账号属性。

步骤6 选择左侧的“授权管理 > 应用账号”，单击“添加账号”，授权访问应用的账号。如需根据策略给用户授权，请参考**配置应用**中应用账号的授权策略。

说明

对象模型、API权限、应用侧权限等设置请参考**配置应用**。

----结束

在 Atlassian 中设置同步配置

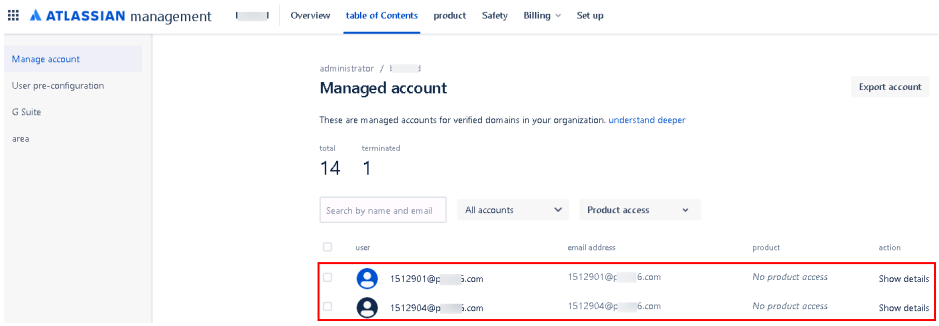
步骤1 **登录Atlassian**。

步骤2 配置并验证邮箱域名，设置API密钥，具体可参考Atlassian平台的帮助文档。

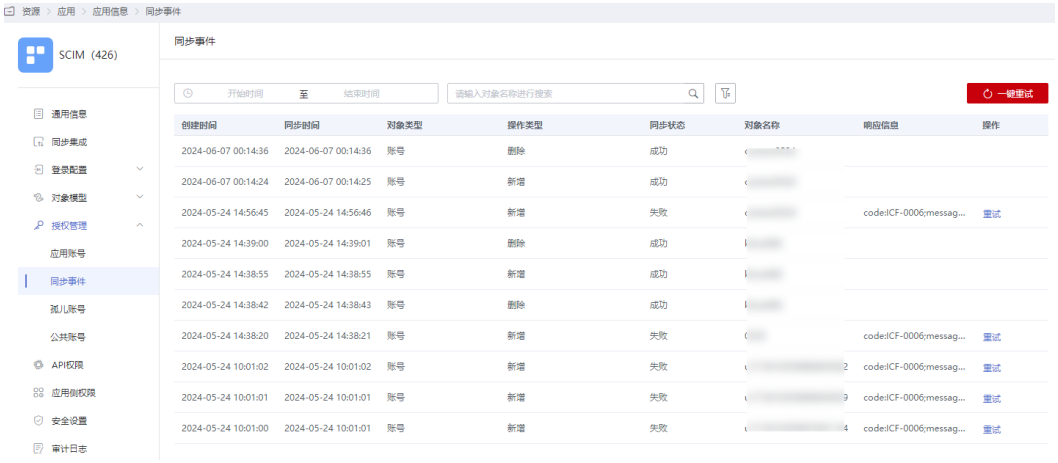
----结束

验证 OneAccess 同步数据

步骤1 Atlassian查看已同步的用户。



步骤2 在同步集成页面，选择“授权管理 > 同步事件”查看同步事件。



----结束

4.2 通过 LDAP 协议同步数据

LDAP（Lightweight Directory Access Protocol）即轻量目录访问协议。它是一种树状结构的组织数据，可以简单理解成一个存储用户和组织信息的树形结构数据库。单点登录是LDAP的主要使用场景之一，即用户只在公司计算机上登录一次后，便可以自动在公司内部网上登录。

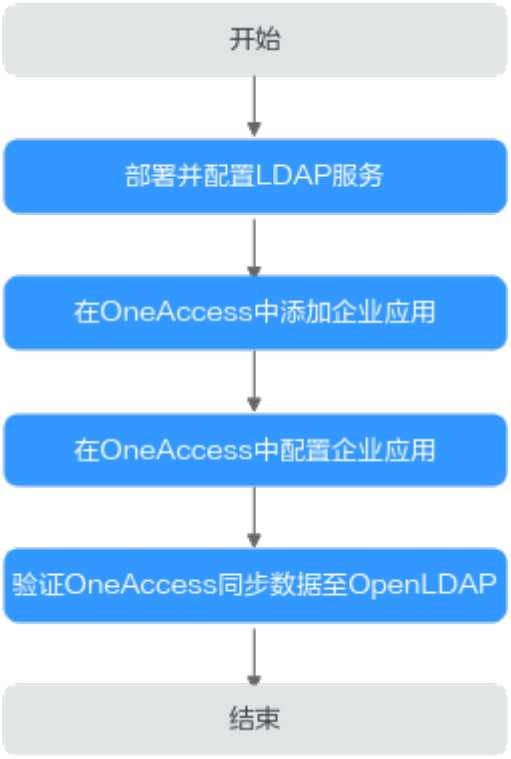
表 4-5 主要术语

术语	说明
ou	全称Organization Unit，组织单位，即容器对象。
dc	全称Domain Component，域名的部分，格式是将完整的域名分成几部分。
sn	全称Surname，即姓。
cn	全称Common Name，公共名称。

术语	说明
dn	全称Distinguished Name，唯一标识名。
uid	全称User ID，用户ID。
rdn	全称Relative dn，相对辨别名，类似文件系统中的相对路径。

本文主要介绍OneAccess以LDAP协议同步组织和用户数据至OpenLDAP的方法。

配置流程



前提条件

请确保您已拥有OneAccess管理门户的访问权限。

部署并配置 LDAP 服务

部署并配置LDAP服务，具体请参考**搭建LDAP服务器**和**配置LDAP连接**。

在 OneAccess 中添加企业应用

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

----结束

在 OneAccess 中配置企业应用

步骤1 单击**在OneAccess中添加企业应用**中添加的企业应用。

步骤2 在通用信息模块，单击“同步集成”后的  打开同步集成设置，此处选择LDAP，单击“保存”。

说明

同步集成协议一旦设置不可修改。

步骤3 在通用信息模块，单击“同步集成”后的“配置”，进入“参数配置”页签。

图 4-2 配置同步参数

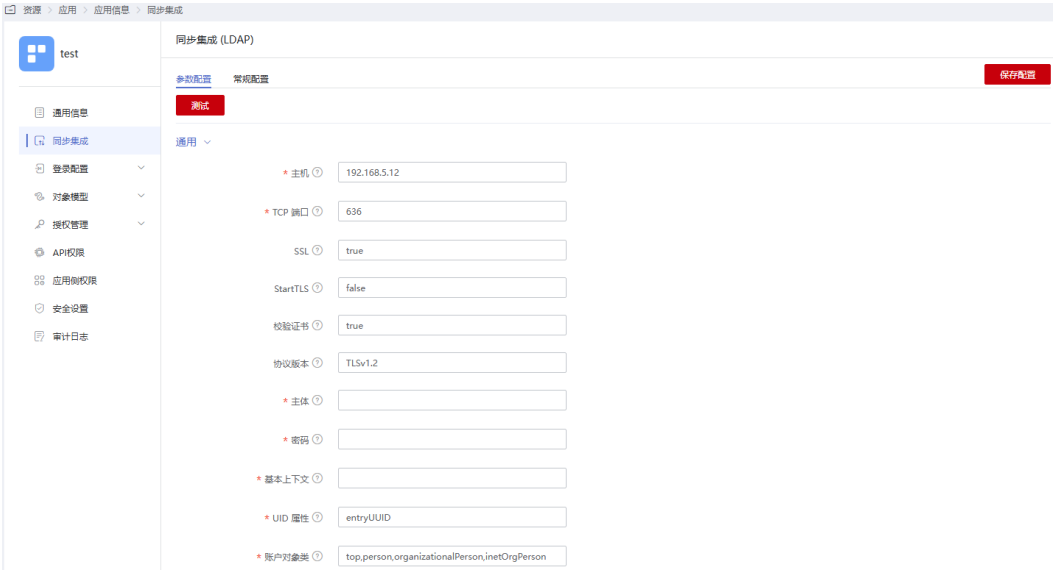


表 4-6 通用参数

参数	说明
* 主机	运行LDAP服务器的主机名称或IP地址。 **说明** OneAccess目前只支持公网访问，LDAP服务器需要提供公网地址。
*TCP端口	与LDAP服务器进行通信的TCP/IP端口号。默认为636。
SSL	系统默认true，即使用SSL连接到 LDAP 服务器。
StartTLS	是否启用startTLS进行加密通信。(true：启用StartTLS，且SSL不能设置为true；false：不启用StartTLS)。 如果是同步数据到AD服务器，则SSL和StartTLS必须开启一个。

参数	说明
校验证书	是否校验证书。仅在SSL为true或者StartTLS为true时有效。true: 校验证书，false: 不校验证书。证书必须是公网认证的证书，自签名证书不可以。
协议版本	系统默认TLSv1.2，推荐使用TLSv1.3、TLSv1.2。
*主体	进行LDAP服务器验证时使用的标识名，如cn=admin，cn=test,cn=com。
*密码	主体的密码。
* 基本上下文	需要同步LDAP目录的根节点。
UID属性	映射到UID属性的LDAP属性的名称。系统默认entryUUID。
账户对象类	在LDAP树中创建新用户对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。系统默认top,person,organizationalPerson,inetOrgPerson。

表 4-7 可选参数

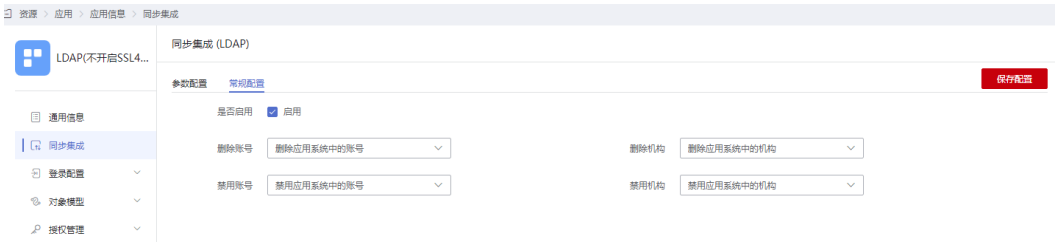
参数	说明
域名	域名存在时，回收的用户名中将该域名排除掉（存在多个域名用","分隔，默认用户名会排除域名）。
账户用户名属性	保存账户用户名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的用户名的LDAP条目。系统默认uid,cn。
机构对象类	在LDAP树中创建新机构对象时将使用的一个或多个对象类。如果输入多个对象类，每一项输入应独占一行；请不要使用逗号或分号来分隔多个对象类。有些对象类可能要求您指定类分层结构中的所有对象类。系统默认top,organizationalUnit。
机构名属性	保存机构名的一个或多个属性。在进行验证时，将使用这些属性查找要验证的机构名的LDAP条目。系统默认ou。
故障转移服务器	列出首选服务器发生故障时将用于故障转移的所有服务器。如果首选服务器发生故障，JNDI将连接到列表中的下一个可用服务器。按照 "ldap://ldap.example.com:389/" 格式（符合 RFC 2255 中所述的标准 LDAP v3 URL）列出所有服务器。只有 URL 的主机和端口部分在此设置中是相关的。
密码属性	用于保存密码的LDAP属性的名称。在更改用户的密码时，会为该属性设置新密码。系统默认userPassword。如果是同步密码到AD服务器，则配置为unicodePwd。
用于检索账户的LDAP过滤器	用于控制从LDAP资源返回的账户的可选LDAP过滤器。如果未指定任何过滤器，则只返回包含所有指定对象类的账户。

参数	说明
密码散列算法	指出Identity System对密码执行散列时应使用的算法。目前支持的值为SSHA、SHA、SMD5和MD5。空值表示系统不会对密码执行散列。除非LDAP服务器执行散列（Netscape Directory Server 和 iPlanet Directory Server 执行散列），否则这将导致明文密码存储在LDAP中。
优先处理资源密码策略重置后更改	如果在登录模块中指定此资源（即，此资源是传递验证目标），并且将资源的密码策略配置为在重置后更改，则以管理方式重置了资源账户密码的用户需要在成功验证后更改该密码。系统默认“false”。
使用VLV控件	指定是否在标准LDAP控件上强制使用VLV控件。默认为“false”。
VLV排序属性	指定用于资源上 VLV 索引的排序属性。系统默认uid。
读取模式	如果为true，连接器将从服务器中读取模式。如果为false，连接器将根据配置中的对象类提供一个默认模式。要使用扩展对象类，该属性必须为true。系统默认 true。
要同步的基本上下文	LDAP树中用于确定是否应同步更改的一个或多个起始点。如果未设置此属性，则将使用基本上下文属性来同步更改。
用同步的对象类	要同步的对象类。更改日志针对所有对象；它会根据所列出的对象类来对更新进行过滤。除非您要将对象与任何超类值同步，否则不应列出对象类的超类。例如，如果仅应同步 "inetOrgPerson" 对象，但应过滤掉 "inetOrgPerson" 的超类（"person"、"organizationalperson" 和 "top"），则此处仅应列出 "inetOrgPerson"。LDAP中的所有对象都是 "top" 的派生子类。因此，绝不应列出 "top"，否则将无法过滤任何对象。系统默认inetOrgPerson。
要同步的属性	要同步的属性的名称。设置此项后，如果更改日志中的更新没有对任何命名属性进行更新，则会忽略这些更新。例如，如果仅列出 "department"，则只处理影响 "department" 的更改。而忽略所有其他更新。如果将其留空（默认设置），则处理所有更改。
要同步的账户的LDAP过滤器	同步对象时使用的可选LDAP过滤器。由于更改日志适用于所有对象，因此此过滤器只更新符合指定过滤器条件的对象。如果指定了过滤器，则只有在对象符合过滤器条件并且包含已同步的对象类时，才会对其进行同步。
更改日志块大小	每个查询获取的更改日志条目数。系统默认100。
更改编号属性	更改日志条目中的更改编号属性的名称。系统默认changeNumber。
使用OR而不是AND进行过滤	通常，用于获取更改日志条目的过滤器是基于AND条件检索一段时间间隔内的更改条目。如果设置了此属性，则过滤器将改用OR条件配合所需的更改数量进行过滤。系统默认false。

参数	说明
从过滤器中删除日志条目对象类	如果设置了此属性（默认设置），用于获取更改日志条目的过滤器不会包含 “changeLogEntry”对象类，因为更改日志中应该不包含其他对象类型的条目。系统默认true。
要同步的密码属性	在执行密码同步时要同步的密码属性的名称。
状态管理类	用于管理启用/禁用状态的类。 如果未指定类，则无法进行身份状态管理。
是否搜索密码	搜索时是否检索用户密码。 默认值为false。
DN属性	条目DN属性名称。默认值entryDN。
LDAP过滤器	一个可选的LDAP过滤器，用于控制从LDAP资源返回的组。 如果未指定过滤器，则仅返回包含所有指定对象类的组。
读超时	等待接收响应的时间。如果在指定的时间内没有响应，读取尝试将被中止。值为0或小于0表示没有限制。系统默认30000。
连接超时	打开新服务器连接时的等待时间。 值0表示将使用TCP网络超时，可能是几分钟。 值小于0表示没有限制。系统默认6000。
账号DN前缀	当该值为空时，默认为cn，也可以为uid等其它用于dn前缀的属性名。

步骤4 配置完成后，单击“保存配置”。单击“测试”可以对连接状态进行测试。

步骤5 单击“常规配置”，在“常规配置”页签，勾选“是否启用”则此处设置的同步数据处理逻辑生效，同步数据处理逻辑可通过在删除账号、删除机构、禁用账号下拉框中选择的处理逻辑来设置。



步骤6 如果需要同步用户的其他属性， 选择左侧的“对象模型 > 应用账号模型”，在“属性定义”页签单击“添加”，添加属性参数见表4-8。下面以employeeNumber为例。

说明

- 系统内置属性，可修改，不支持删除。
- 非内置属性，支持修改和删除，单击待操作属性操作列的“更新”或“删除”进行相应操作。

表 4-8 属性定义

参数	说明
* 属性名	输入应用系统的账号属性，如employeeNumber。

参数	说明
* 显示标签	属性名称的标识，建议与**属性名**对应。
描述	**属性名**的说明。
* 属性类型	属性值的类型，可在下拉框选择。
格式	只有“属性类型”选择文本时才需要设置该参数，用来设置文本的格式。
是否必填	勾选后，同步用户数据至应用时，该属性必须有值，为空时，会提示“{显示标签}为必填属性”。
是否唯一	只有“属性类型”选择“文本”时才需要设置该参数，勾选后，同步用户数据至应用时，该属性的值具有唯一性，重复时，会提示“{显示标签}”已存在。
是否敏感	只有“属性类型”选择“文本”时才需要设置该参数，勾选后，同步用户数据至应用时，数据隐藏展示，单击可以看到数据内容。

步骤7 单击“保存”。

步骤8 切换到“映射定义”页签，单击“编辑”，配置属性映射。

表 4-9 映射定义

参数	说明
系统用户	OneAccess映射至应用的属性，如手机号。
转换方式	OneAccess与应用之间属性的映射方式。
脚本表达式	当**转换方式**选择**脚本转换**时，可激活该输入框。映射脚本请参考**如何开发映射脚本**。
执行方式	OneAccess同步用户数据至目标应用时的方式。
应用账号	应用的账号属性。

步骤9 如果需要同步机构， 选择左侧的“对象模型 > 应用机构模型”，单击 开启应用机构。应用机构开启后不支持关闭。

说明

- 系统内置属性可修改，不支持删除。
- 非内置属性支持修改和删除，单击目标属性操作列的“更新”或“删除”进行相应操作。

步骤10 如果需要同步机构的其他属性， 选择左侧的“对象模型 > 应用机构模型”，在“属性定义”页签单击“添加”，添加机构属性，配置参数请参见**表4-10**。

表 4-10 属性定义

参数	说明
* 属性名	应用机构的属性名称。
* 显示标签	属性名称的标识，建议与**属性名**对应。
描述	**属性名**的说明。
* 属性类型	属性值的类型，可在下拉框选择。
格式	只有“属性类型”选择文本时才需要设置该参数，用来设置文本的格式。
是否必填	勾选后，同步机构数据至应用时，该属性必须有值，为空时，会提示“{显示标签}为必填属性”。
是否唯一	只有“属性类型”选择“文本”时才需要设置该参数，勾选后，同步机构数据至应用时，该属性的值具有唯一性，重复时，会提示“{显示标签}”已存在。
是否敏感	只有“属性类型”选择“文本”时才需要设置该参数，勾选后，同步机构数据至应用时，数据隐藏展示，单击可以看到数据内容。

步骤11 单击“保存”。

步骤12 切换到“映射定义”页签，单击“编辑”，配置属性映射，配置参数请参见表4-11。

表 4-11 映射定义

参数	说明
组织	OneAccess映射至应用的组织属性。
转换方式	OneAccess与应用之间属性的映射方式。
脚本表达式	当**转换方式**选择**脚本转换**时，可激活该输入框。映射脚本请参考**如何开发映射脚本**。
执行方式	OneAccess同步组织数据至目标应用时的方式。
应用机构	应用的机构属性。

----结束

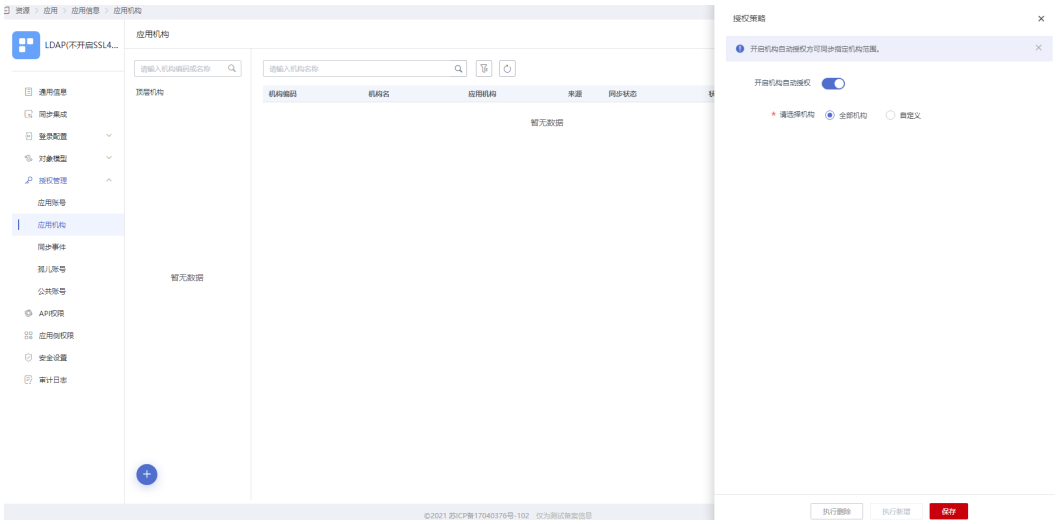
验证 OneAccess 同步数据至 OpenLDAP

步骤1 在应用详情页面，选择左侧的“授权管理 > 应用机构”，单击“授权策略”，开启机构自动授权，选择需要同步的机构，单击“保存”后，单击“执行新增”。

说明

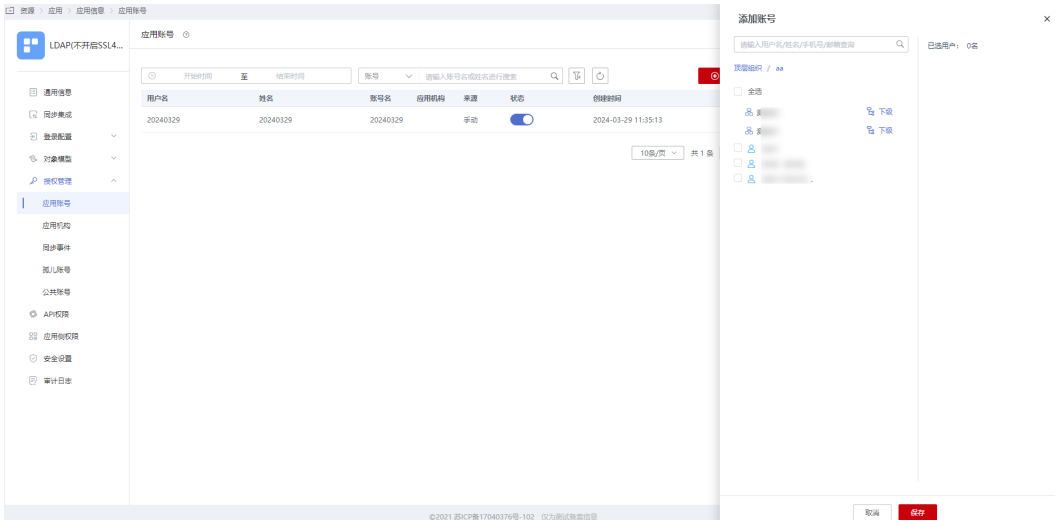
- 如果需要删除已同步的部分机构，取消勾选目标机构，单击“保存”后，单击“执行删除”。
- 单击页面的，即可添加虚拟机构。

图 4-3 授权机构



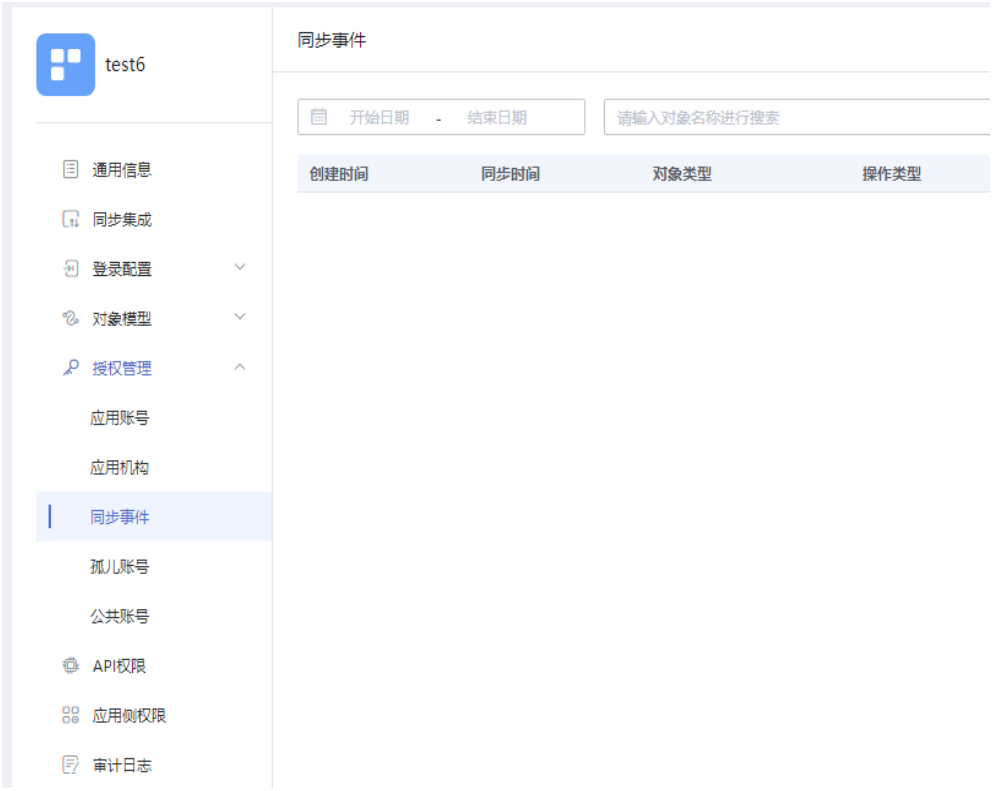
步骤2 选择左侧的“授权管理 > 应用账号”，单击“添加账号”，勾选需要同步的用户。如需根据策略给用户授权，请参考**配置应用**中应用账号的授权策略。

图 4-4 添加账号

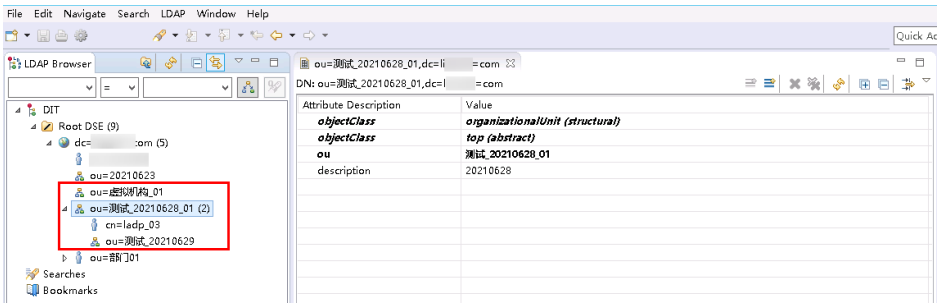


步骤3 选择左侧的“授权管理 > 同步事件”，可以查看上述的同步记录。同时，对于组织、用户的编辑和删除等操作，也可以进行查看并过滤。

图 4-5 查看同步事件



步骤4 在LDAP中查看上述已同步的数据。



----结束

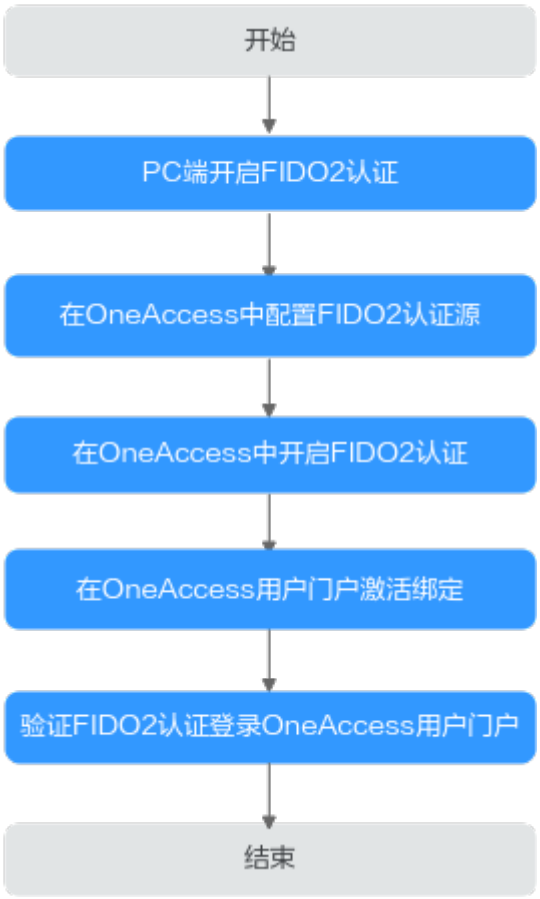
5 集成认证源

5.1 内置认证源

概述

本文为您介绍通过FIDO2认证源（人脸、指纹等生物认证）来登录OneAccess平台集成的应用系统。您可以在OneAccess平台中配置FIDO2认证源，在登录页面选择FIDO2登录方式登录各应用系统，从而实现单点登录的效果，在给用户带来更简易便捷的登录方式的同时提供更安全可靠的登录体验。

配置流程



说明

该配置流程以用户PC端访问用户门户为例，您可以按需选择应用和配置应用的认证方式，配置流程类似。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 用户PC端设备拥有安全密钥 (USB或蓝牙) 或生物识别身份验证器 (WindowsHello、Touch ID等)。

PC 端开启 FIDO2 认证

在用户PC端设备上开启安全密钥 (USB或蓝牙) 或生物识别身份验证器 (WindowsHello、Touch ID等)。下文以开启WindowsHello为例。

在 OneAccess 中配置 FIDO2 认证源

在OneAccess中添加FIDO2认证源，并配置应用的信息，确保用户可以通过FIDO2方式登录OneAccess用户门户。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理 > 内置认证源 > FIDO2”。

步骤3 配置需要填写的认证源参数信息。

图 5-1 配置 FIDO2 认证源

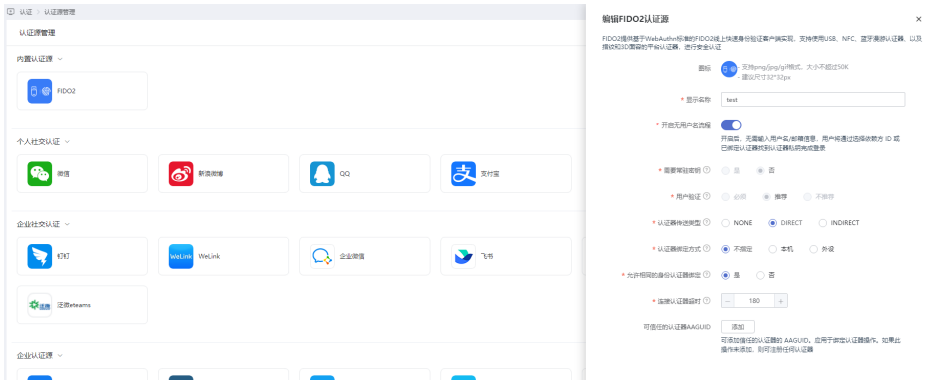


表 5-1 配置参数

参数	说明
图标	可自定义图标。

参数	说明
显示名称	自定义认证源显示名称。
开启无用户名流程	开启后，无需输入用户名/邮箱信息，用户将通过选择依赖方ID或已绑定认证器找到认证器私钥完成登录。
需要常驻密钥	认证器生成Public Key Credential作为Client-side-resident Public Key Credential Source。默认设置为 “否” ，当开启无用户名流程时，此参数同步调整为 “是” 。
用户验证	认证器确认实际验证用户，应用于注册和认证操作。默认值为 “推荐” ，当开启无用户流程，此参数同步调整为 “必须” 。
认证器传送类型	WebAuthn API实现如何生成证明声明的首选项。应用于注册操作。默认值为 “DIRECT” 。
认证器绑定方式	WebAuthn客户端可接受的验证器附件模式。应用于注册操作。默认值为不指定。
允许相同的身份认证器注册	允许重新注册同类型身份验证器。默认值为 “是” 。
连接认证器超时	用于绑定和认证操作时连接身份认证器的超时设置，默认为 180 秒。
可信任的认证器AAGUID	可添加信任的认证器的 AAGUID。应用于绑定认证器操作。如果此操作未添加，则可注册任何认证器。

----结束

在 OneAccess 中开启 FIDO2 认证

步骤1 登录OneAccess管理门户。

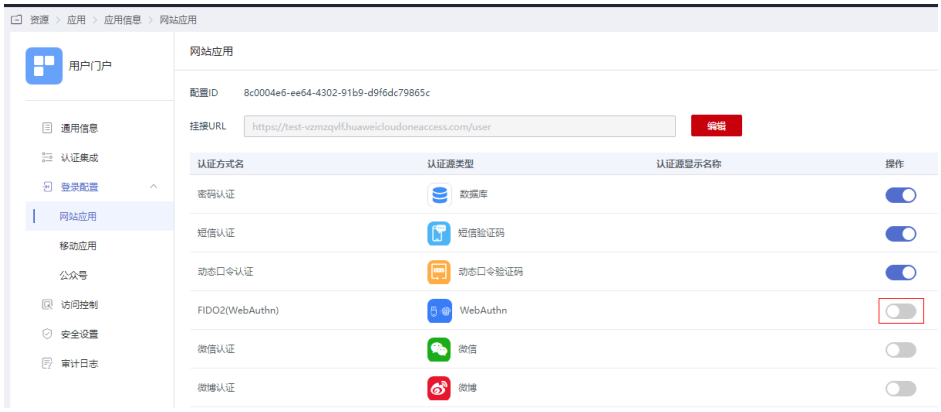
步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击“用户门户”。

步骤4 在“应用信息”页面，单击“用户门户”应用图标。

步骤5 选择“登录配置 > 网站应用”，单击认证方式名为“FIDO2(WebAuthn)”操作列的 开启FIDO2认证。

图 5-2 开启 FIDO2 认证



----结束

在 OneAccess 用户门户激活绑定

步骤1 登录OneAccess用户门户，鼠标放置在右上角的用户名上，单击 "账号设置"。

步骤2 选择 “账号安全”，单击此前添加的安全密钥或生物识别身份验证器后的“绑定”。

说明

- 未添加安全密钥或生物识别身份验证器时，无法绑定，“绑定”按钮为不可用状态。
- 添加多种验证器时可绑定多个，如需修改则可选择移除已添加的认证重新添加。

----结束

验证 FIDO2 认证登录 OneAccess 用户门户

用户访问用户门户，选择FIDO2认证方式登录，弹出安全密钥或生物识别身份认证器，通过相关验证后，成功登录。

图 5-3 选择 FIDO2 认证

说明

在无痕浏览器下无法绑定生物识别身份认证器，即无法使用FIDO2认证登录。

5.2 标准协议认证源

5.2.1 SAML 认证登录

5.2.1.1 配置 SAML 认证源

概述

为方便企业用户的认证登录，OneAccess平台支持配置SAML协议作为认证源，用户可以通过SAML协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。

本章节为您介绍配置SAML认证源的相关操作。

基本概念

- 身份提供商（Identity Provider，简称IdP），负责收集、存储用户身份信息，如用户名、密码等，在用户登录时负责认证用户的服务。在企业与OneAccess身份认证的过程中，身份提供商指企业自身的身份提供商。
- 服务提供商（Service Provider，简称SP），服务提供商通过与IdP建立信任关系，使用IdP提供的用户信息，为用户提供具体的服务。在企业与OneAccess身份认证的过程中，服务提供商指OneAccess。
- 单点登录（Single Sign-On，简称SSO），用户在企业IdP系统登录后，就可以通过跳转链接访问已建立互信关系的SP系统，这一过程称之为单点登录。如企业IdP与OneAccess建立互信关系后，企业IdP中的用户通过OneAccess提供的登录入口，使用已有的账号密码在企业IdP中登录后，即可跳转访问OneAccess。
- SAML2.0，安全断言标记语言（Security Assertion Markup Language 2.0，缩写为SAML 2.0）是一个由一组协议组成，用来传输安全声明的XML框架。SAML2.0是由标准化组织OASIS提出的用于安全操作的标准，是很多身份提供商（IdP）使用的一种开放标准，关于SAML2.0的详细描述请参见**SAML 2.0技术概述**。OneAccess支持使用SAML2.0协议进行身份认证，因此与OneAccess建立身份认证的企业IdP必须支持SAML2.0协议。

本文主要介绍OneAccess以SAML集成第三方认证源的方法。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您拥有第三方身份提供商（IDP）的应用系统权限，且该身份提供商支持SAML认证。

建立 IdP 对 OneAccess 的信任关系

在IdP中配置OneAccess的元数据文件，以建立IdP对OneAccess的信任。

步骤1 下载OneAccess系统的元数据文件（metadata文件）。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“认证 > 认证源管理 > 企业认证源 > SAML”。
3. 在SAML认证源页面，单击右上方的“SP元数据”，数据会自动下载到本地。

步骤2 将**步骤1.3**获取的文件上传到企业IdP服务器上，不同企业idP服务器，上传方法不同，具体请参考相应IdP提供商的帮助文档。

步骤3 获取企业IdP的元数据文件。不同企业idP服务器，获取元数据方法不同，具体请参考相应IdP提供商的帮助文档。

----结束

在 OneAccess 中添加 SAML 认证源

在OneAccess中添加SAML认证源，配置身份提供商的元数据文件后，可以在OneAccess中建立对IdP的信任关系，使得企业用户可以通过idp访问OneAccess用户门户。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理 > 企业认证源 > SAML”。

步骤3 在SAML认证源页面，单击右上方“添加认证源”，配置参数。

图 5-4 配置参数

表 5-2 配置参数

参数	是否必选	说明
图标	否	支持png/jpg/gif 格式的图片，且图片大小不超过50K。建议尺寸32*32px。
显示名称	是	认证源的显示名称，支持自定义。如SAML认证。
entityId	是	对应IdP元数据文件中“entityID”的值。
签名证书	是	IdP的签名证书，可从IdP的元数据文件中获取。 签名证书是一份包含公钥用于验证签名的证书。OneAccess通过元数据文件中的签名证书来确认用户身份认证过程中断言消息的可信性、完整性。
绑定类型	是	对应IdP元数据文件中“SingleSignOnService”地址支持的绑定类型。 用户登录过程中发送SAML请求的方式。元数据文件中的“SingleSignOnService”需要支持HTTP Redirect或HTTP POST方式。
SSO URL	是	对应IdP元数据文件中“SingleSignOnService”的值。
Logout URL	否	对应IdP元数据文件中“SingleLogoutService” 的值。 服务提供商提供会话注销功能，用户在OneAccess注销会话后返回绑定的地址。
关联源属性	是	SAML断言中用户唯一属性名，需与应用映射配置中的应用系统属性名一致。如NameId。
关联用户属性	是	SAML认证源对接OneAccess的映射属性。如用户ID，可在下拉框选择。
未关联用户时	是	当用户使用SAML认证源登录成功后，如未关联到系统用户时，可以根据该设置进行操作，如自动创建用户，可在下拉框选择。

如果您需要同时映射其他属性，如用户名，可以设置“**未关联用户时**”为“**自动创建用户**”，设置是否更新已存在属性，通过单击“添加映射”完成。可参考**表5-3**。

表 5-3 映射参数

参数	说明
用户属性名	SAML应用对接OneAccess的映射属性，可在下拉框选择，如用户名。

参数	说明
映射类型	OneAccess与SAML应用之间用户属性的映射方式，可在下拉框选择，如认证源属性。 **说明** • 当选择“映射类型”为“认证源属性”时，需要同时输入“认证源属性名”。 • 当选择“映射类型”为“固定属性值”时，需要同时输入“固定属性值”。 • 当选择“映射类型”为“脚本转换”时，需要同时输入“脚本内容”。

----结束

5.2.1.2 配置 SAML 认证登录

概述

本章节以OneAccess用户门户为例为您介绍SAML认证功能的配置过程，在OneAcces平台配置集成SAML认证源后，参考本模块配置SAML认证登录各应用系统。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已在OneAccess实现SAML认证源配置，如需配置，请参考**配置SAML认证源**。

在 OneAccess 中开启 SAML 认证

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击“用户门户”。

步骤4 在“应用信息”页面，单击“用户门户”应用图标。

步骤5 选择“登录配置 > 网站应用”，单击认证方式名为“SAML认证”操作列的 开启SAML认证，并关联**在OneAccess中添加SAML认证源**中添加的认证源。

----结束

验证 SAML 认证登录 OneAccess 用户门户

步骤1 用户访问用户门户，选择SAML登录，输入idp侧的账号和密码即可进入OneAccess用户门户。

图 5-5 选择 SAML 登录

步骤2 登录成功以后，在OneAccess的“用户 > 组织与用户”处可查看自动创建的用户。

说明

- 当授权用户未关联系统用户时，在系统自动创建用户的前提是“**未关联用户时**”设置为“**自动创建用户**”。可参考**表5-2**。
- 自动创建的用户默认属于SP侧的第一个根机构。

----结束

5.2.2 OIDC 认证登录

5.2.2.1 配置 OIDC 认证源

概述

为方便企业用户的认证登录，OneAccess平台支持配置OIDC协议作为认证源，用户可以通过OIDC协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。

OIDC是OpenID Connect的简称，是一个基于OAuth 2.0协议的身份认证标准协议。关于OIDC的详细描述请参见**欢迎使用OpenID Connect**。

本文主要介绍OneAccess以OIDC协议集成第三方认证源的方法。以Okta为例。

前提条件

- 请确保您已拥有Okta平台的管理员权限。具体可参考Okta平台的帮助文档。
- 请确保您已拥有OneAccess管理门户的访问权限。

在 Okta 平台上创建应用

在Okta平台上创建应用，并配置OneAccess的授权信息，可以建立Okta对OneAccess的信任。

步骤1 登录Okta平台。

步骤2 在Okta平台，选择“Applications > Add Application > Create New App”，设置参数，创建应用。具体可参考Okta开放平台的帮助文档。

说明

配置应用时，Login redirect URIs填写OneAccess添加认证源时自动生成的调用地址，可参考**表5-4**。示例：https://xxx.huaweioneaccess.com/api/v1/oidc/sso/2***71-8***-D***1。

图 5-6 配置参数

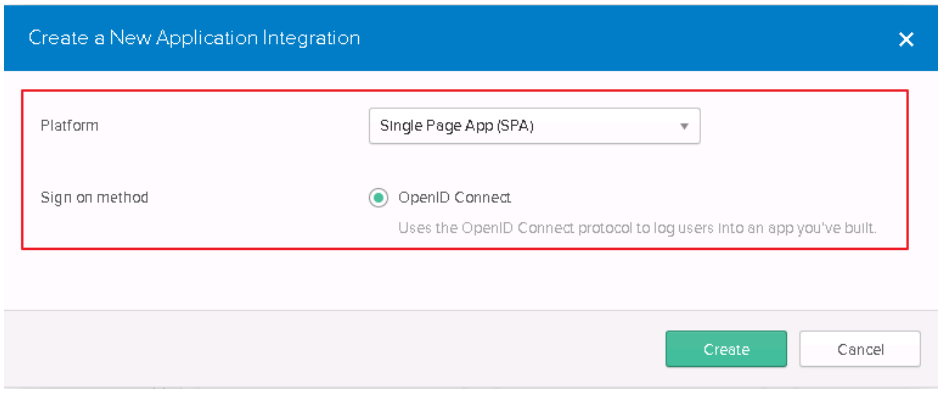
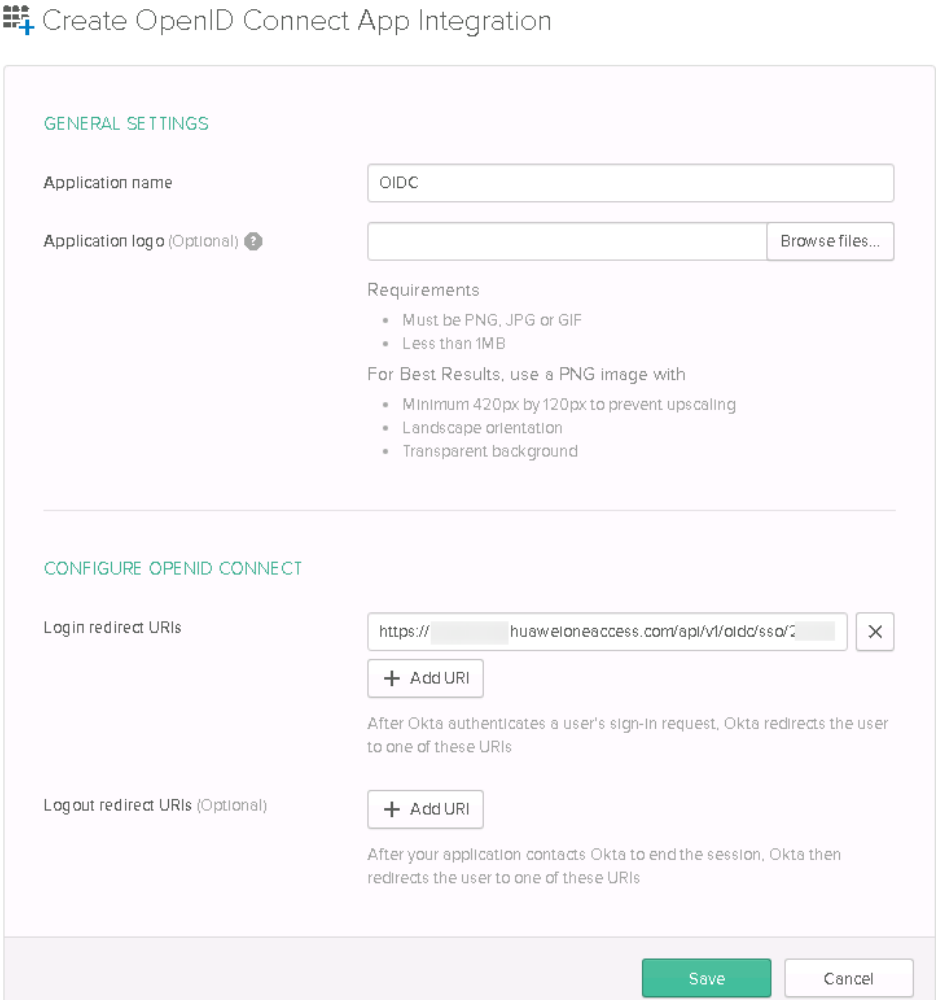


图 5-7 配置 Login redirect URIs



步骤3 配置应用参数，授权用户 。具体可参考Okta平台的帮助文档。

图 5-8 配置应用参数

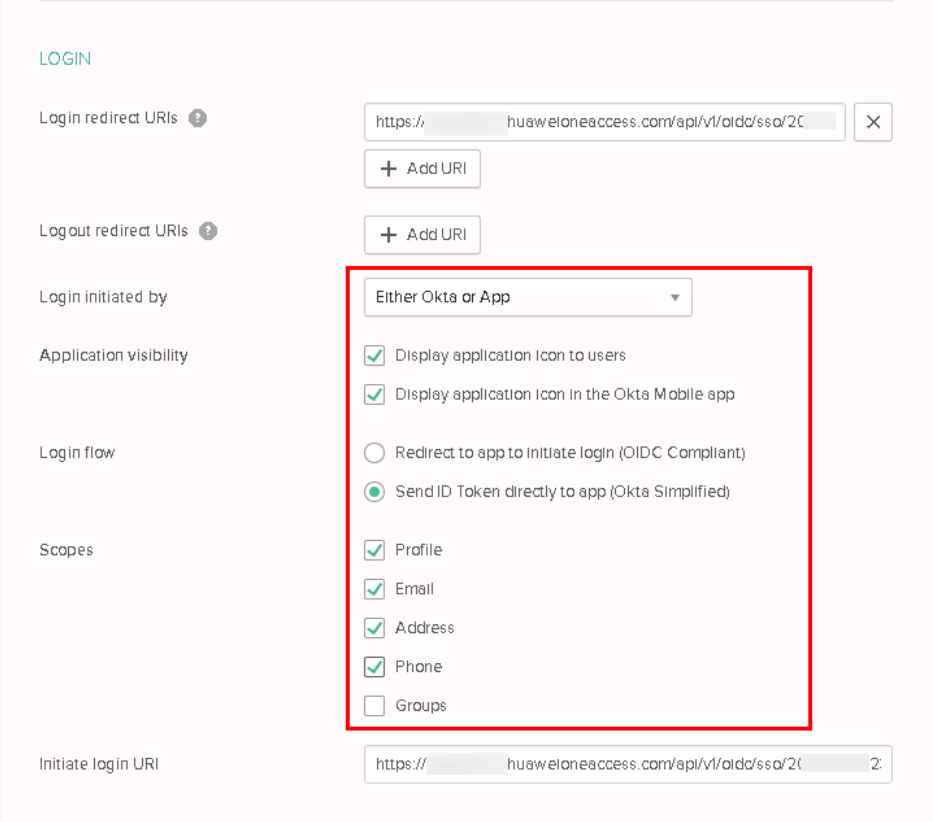
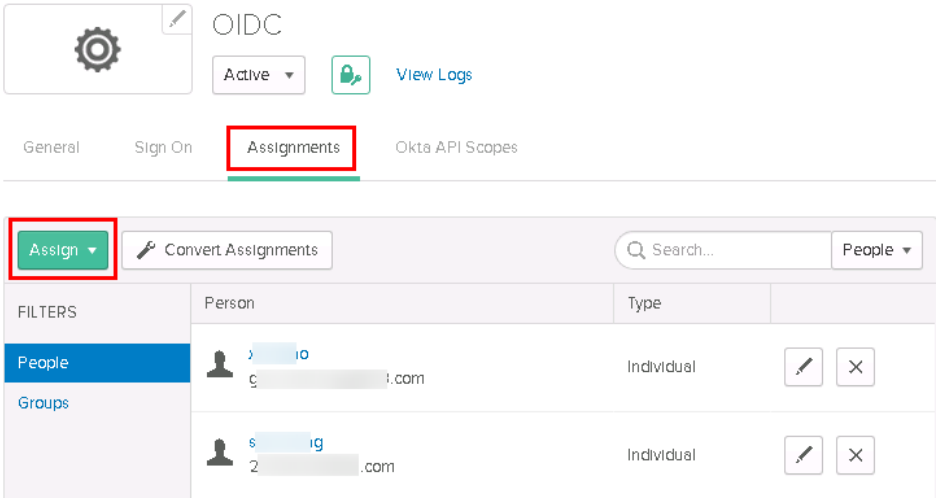


图 5-9 授权用户



----结束

在 OneAccess 中添加 OIDC 认证源

在OneAccess中添加OIDC认证源，并配置应用的信息，确保用户可以通过OIDC登录OneAccess用户门户。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理 > 企业认证源 > OIDC”，配置参数。

步骤3 在OIDC认证源页面，单击右上方“添加认证源”，配置参数。

图 5-10 配置参数

表 5-4 配置参数

参数	是否必选	说明
图标	否	支持png/jpg/gif 格式的图片，且图片大小不超过50K。建议尺寸32*32px。
显示名称	是	认证源的显示名称，支持自定义。如OIDC认证。
认证方式	是	认证用户的方式，选择**主动发起认证**。 **说明** • 认证方式确认后不支持修改。 • 如果需要从应用侧发起认证，请选择认证源发起认证。
公钥格式	是	根据应用选择相应的公钥格式。
公钥	是	在OIDC的jwks_uri中获取或由认证源管理员提供，与公钥格式相匹配。 • 公钥格式为**JWKURL**时，公钥为 https://{Okta域名}/oauth2/v1/keys。 • 公钥格式为**JSON格式公钥**时，公钥为 https://{Okta域名}/oauth2/v1/keys 中的value值。
签名算法	是	默认为RS256。
Audience	是	当**认证方式**选择**认证源发起认证**时，该参数对应**步骤1**中创建应用生成的Audience的值。
流程类型	是	根据应用配置选择对应的流程类型，如授权码模式，可在下拉框选择。
response Type	是	默认为code。
Scope	是	对应OIDC认证源端scopes的配置，必须包含“openid”，如openid email。
AuthrozationUrl	是	对应OIDC认证源端“EMBED LINK”的值。
Clientld	是	对应OIDC认证源端“Client ID”的值。
PKCE	是	默认禁用，根据应用配置选择是否启用。如**认证方式**选择**主动发起认证**，则开启。
TokenUrl	是	Token地址，在OIDC的token_endpoint中获取，格式为https://{Okta域名}/api/v1/oauth2/token。
LogoutUrl	否	应用的全局退出地址，在应用端获取。
调用地址	是	系统默认生成。对应应用的Login redirect URIs 参数。
关联源属性	是	OIDC认证源端用户的唯一属性。如email。

参数	是否必选	说明
关联用户属性	是	OIDC认证源对接OneAccess的映射属性。如邮箱，可在下拉框选择
未关联用户时	是	当用户使用OIDC认证源登录成功后，如未关联到系统用户时，可以根据该设置进行操作，如自动创建用户，可在下拉框选择。

如果您需要同时映射其他属性，如姓名，可以设置“**未关联用户时**”为“**自动创建用户**”，通过单击“添加映射”完成。可参考**表5-5**。

表 5-5 映射参数

参数	说明
用户属性名	OIDC应用对接OneAccess的映射属性，可在下拉框选择，如姓名。
映射类型	OneAccess与OIDC应用之间用户属性的映射方式，可在下拉框选择，如认证源属性。 **说明** • 当选择“映射类型”为“认证源属性”时，需要同时输入“认证源属性名”。 • 当选择“映射类型”为“固定属性值”时，需要同时输入“固定属性值”。 • 当选择“映射类型”为“脚本转换”时，需要同时输入“脚本内容”。

----结束

5.2.2.2 配置 OIDC 认证登录

概述

本章节以OneAccess用户门户为例为您介绍OIDC认证功能的配置过程，在OneAcces平台配置集成OIDC认证源后，参考本模块配置OIDC认证登录各应用系统。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已在OneAccess实现OIDC认证源配置，如需配置，请参考**配置OIDC认证源**。

在 OneAccess 中开启 OIDC 认证

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击“用户门户”。

步骤4 在“应用信息”页面，单击“用户门户”应用图标。

步骤5 选择“登录配置 > 网站应用”，单击认证方式名为“OIDC认证”操作列的 开启OIDC认证，并关联**在OneAccess中添加OIDC认证源**中添加的认证源。

----结束

验证 OIDC 认证登录 OneAccess 用户门户

步骤1 用户访问用户门户，选择OIDC登录，输入**步骤3**中授权用户的用户名密码登录，可进入OneAccess侧的用户门户。

图 5-11 OIDC 认证登录

步骤2 登录成功以后，在OneAccess的“用户 > 组织与用户”处可查看自动创建的用户。

说明

- 当授权用户未关联系统用户时，在系统自动创建用户的前提是“**未关联用户时**”设置为“**自动创建用户**”。可参考表5-4。
- 当用户email属性唯一时，自动创建的用户默认属于OneAccess侧的第一个根机构。

----结束

5.2.3 CAS 认证登录

5.2.3.1 配置 CAS 认证源

概述

CAS是一个基于HTTP2、HTTP3的协议，要求每个组件都可以通过特定的URL访问。通过CAS协议将OneAccess作为服务提供商，使第三方应用的用户账号数据可以访问OneAccess。支持CAS1.0、CAS2.0、CAS3.0三种协议。

CAS 协议涉及两个主体。两个主体通过用户浏览器进行信息交换。如 CAS Client可以返回带参数的重定向，将信息转发给CAS Server。登录验证成功后CAS Server会返回CAS Client一个包含用户信息的XML， CAS Client验证用户信息后会返回给用户访问资源。

- CAS Client：CAS客户端，资源提供方，如第三方应用。
- CAS Server：CAS服务端，身份认证提供方，如OneAccess认证服务。

为方便企业用户的认证登录，OneAccess平台支持配置CAS协议作为认证源，用户可以通过CAS协议认证登录各应用系统以及实现应用系统间单点登录效果，为企业用户带来更简易便捷的登录方式和更好的用户体验。

本文主要介绍OneAccess以CAS协议集成第三方认证源的方法。

前提条件

请确保您已拥有OneAccess管理门户的访问权限。

建立企业应用对 OneAccess 的信任关系

在企业应用中配置OneAccess的授权信息，以建立企业应用对OneAccess的信任。

步骤1 获取OneAccess侧的认证信息。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置”。
3. 单击“CAS配置”。
4. 在弹出的CAS页面，查看认证地址。

图 5-12 查看 CAS 配置

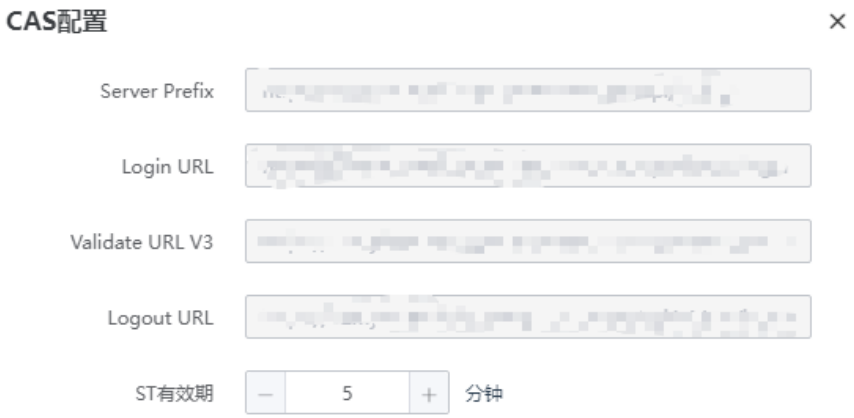


表 5-6 配置参数

参数	说明
Server Prefix	系统自动生成，不可编辑。CAS服务地址的前缀。
Login URL	系统自动生成，不可编辑。CAS服务的请求授权地址。
Validate URL V3	系统自动生成，不可编辑。验证票据，推荐使用V3的地址。
Logout URL	系统自动生成，不可编辑。CAS服务的登出地址。
ST有效期	请求授权返回票据的有效期，建议设置为3~15分钟。

步骤2 获取OneAccess侧的服务地址，可参考**表5-7**。

步骤3 在企业应用中配置上述信息。配置方法请参见应用提供商的帮助文档。

步骤4 获取企业应用的授权信息。获取方法请参见应用提供商的帮助文档。

----结束

在 OneAccess 中添加 CAS 认证源

在OneAccess中添加CAS认证源，并配置应用的信息，确保用户可以通过CAS登录OneAccess用户门户。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理”。

步骤3 选择“企业认证源 > CAS”。

步骤4 在CAS认证源页面，单击右上方“添加认证源”，配置参数。

表 5-7 配置参数

参数	是否必选	说明
图标	否	支持png/jpg/gif 格式的图片，且图片大小不超过50K。建议尺寸32*32px。
显示名称	是	认证源的显示名称，支持自定义。如CAS认证。

参数	是否必选	说明
登录地址	是	应用的登录地址。请以http或https开头，如https://xxx.xxx.xxx/login。
退出地址	是	应用的退出地址，请以http或https开头，如https://xxx.xxx.xxx/logout。
验证地址	是	应用的验证地址，不同的协议版本对应的验证地址不同，请以http或https开头。 CAS1.0对应的验证地址为：https://xxx.xxx.xxx/validate，具体可参考**验证票据(CAS1.0)**。 CAS2.0对应的验证地址为：https://xxx.xxx.xxx/serviceValidate，具体可参考**验证票据(CAS2.0)**。 CAS3.0对应的验证地址为：https://xxx.xxx.xxx/p3/serviceValidate，具体可参考**验证票据(CAS3.0)**。
请求类型	是	http请求发起的方式，支持GET和POST方式。
服务地址	是	系统默认生成，不可编辑。配置企业应用时，可从该处获取。
CAS协议版本	是	应用侧支持的协议版本，其中，CAS1.0和CAS2.0协议不支持具体用户属性传值。
认证源属性	是	CAS Server认证成功后返回的用户属性名，需与应用系统的属性名一致。
关联用户属性	是	CAS认证源对接OneAccess的映射属性。如用户名，可在下拉框选择。
未关联用户时	是	当用户使用CAS认证源登录成功后，如未关联到系统用户时，可以根据该设置进行操作，如自动创建用户，可在下拉框选择。

如果您需要同时映射其他属性，如邮箱，可以设置“**未关联用户时**”为“**自动创建用户**”，通过单击“添加映射”完成。可参考**表5-8**。

表 5-8 映射参数

参数	说明
用户属性名	CAS应用对接OneAccess的映射属性，可在下拉框选择，如手机号。
映射类型	OneAccess与CAS应用之间用户属性的映射方式，可在下拉框选择，如认证源属性。 **说明** • 当选择“映射类型”为“认证源属性”时，需要同时输入“认证源属性名”。 • 当选择“映射类型”为“固定属性值”时，需要同时输入“固定属性值”。 • 当选择“映射类型”为“脚本转换”时，需要同时输入“脚本内容”。

----结束

5.2.3.2 配置 CAS 认证登录

概述

本章节以OneAccess用户门户为例为您介绍CAS认证功能的配置过程，在OneAcces平台配置集成CAS认证源后，参考本模块配置CAS认证登录各应用系统。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已在OneAccess实现CAS认证源配置，如需配置，请参考**配置CAS认证源**。

在 OneAccess 中开启 CAS 认证

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击“用户门户”。

步骤4 在“应用信息”页面，单击“用户门户”应用图标。

步骤5 选择“登录配置 > 网站应用”，单击认证方式名为“CAS认证”操作列的  开启CAS认证，并关联**在OneAccess中添加CAS认证源**中添加的认证源。

----结束

验证 CAS 认证登录 OneAccess 用户门户

步骤1 用户访问用户门户，选择CAS登录，输入应用侧的账号和密码即可进入OneAccess用户门户。

图 5-13 选择 CAS 登录

步骤2 登录成功以后，在OneAccess侧的“用户 > 组织与用户”处可查看自动创建的用户。

说明

- 当授权用户未关联系统用户时，在系统自动创建用户的前提是“**未关联用户时**”设置为“**自动创建用户**”，可参考**表5-7**。
- 自动创建的用户默认属于OneAccess侧的第一个根机构。

----结束

5.2.4 OAuth 认证登录

5.2.4.1 配置 OAuth 认证源

OAuth（开放授权）是一个开放标准，允许用户授权第三方应用访问其存储在资源服务器上的信息，而不需要将用户名和密码提供给第三方应用。

为方便企业用户的认证登录，OneAccess平台支持配置OAuth协议作为认证源，用户可以通过OAuth协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。

本章节为您介绍配置OAuth认证源的相关操作。

前提条件

请确保您已拥有OneAccess管理门户的访问权限。

建立企业应用对 OneAccess 的信任关系

在企业应用中配置OneAccess的授权信息，以建立企业应用对OneAccess的信任。

步骤1 获取OneAccess侧的认证信息。

1. 登录OneAccess管理门户。
2. 在导航栏中，选择“设置 > 服务配置 ”。
3. 单击“OIDC”。
4. 在弹出的OIDC页面，查看认证地址。单击右上角的“OIDC设置”,可以查看配置认证参数。

步骤2 获取OneAccess侧的回调地址，可参考**表5-9**。

步骤3 在企业应用中配置上述信息。配置方法请参见应用提供商的帮助文档。

步骤4 获取企业应用的授权信息。获取方法请参见应用提供商的帮助文档。

----结束

在 OneAccess 中添加 OAuth 认证源

在OneAccess中添加OAuth认证源，并配置应用的信息，确保用户可以通过OAuth登录OneAccess用户门户。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理 ”。

步骤3 选择“企业认证源 > OAuth”。

步骤4 在OAuth认证源页面，单击右上方“添加认证源”，配置参数。

图 5-14 配置参数

表 5-9 配置参数

参数	是否必选	说明
图标	否	支持 png/jpg/gif 格式的图片，且图片大小不超过50K。建议尺寸32*32px。
显示名称	是	认证源的显示名称。如OAuth认证。
clientId	是	企业应用的接口认证凭证ID。从企业应用处获取。
clientSecret	是	企业应用的接口认证凭证密钥。从企业应用处获取。
认证模式	是	系统默认authorization_code。
client信息传递方式	是	支持basic和post方式。
token传递方式	是	系统默认Bearer。
scope	否	授权范围，多值以“,”分隔。
认证授权 Url	是	企业应用的认证授权地址。从企业应用处获取。
获取token Url	是	获取token的地址。从企业应用处获取。
UserInfo Url	是	获取用户信息的地址。从企业应用处获取。
回调地址	是	系统默认生成，不可编辑。配置企业应用时，可从该处获取。
关联源属性	是	服务端认证成功后返回的用户属性名，需与应用系统的属性名一致。
关联用户属性	是	OAuth认证源对接OneAccess的映射属性。如用户名，可在下拉框选择。
未关联用户时	是	当用户使用OAuth认证源登录成功后，如未关联到系统用户时，可以根据该设置进行操作，如自动创建用户，可在下拉框选择。
更新已存在属性	是	默认为否。认证源登录时如果关联到了用户，可以通过该选项来更新已存在的用户属性值。

如果您需要同时映射其他属性，如姓名，可以设置“**未关联用户时**”为“**自动创建用户**”，通过单击“添加映射”完成。可参考**表5-10**。

表 5-10 映射参数

参数	说明
用户属性名	OAuth应用对接OneAccess的映射属性，可在下拉框选择，如姓名。

参数	说明
映射类型	OneAccess与OAuth应用之间用户属性的映射方式，可在下拉框选择，如认证源属性。 **说明** • 当选择“映射类型”为“认证源属性”时，需要同时输入“认证源属性名”。 • 当选择“映射类型”为“固定属性值”时，需要同时输入“固定属性值”。 • 当选择“映射类型”为“脚本转换”时，需要同时输入“脚本内容”。

----结束

5.2.4.2 配置 OAuth 认证登录

概述

本章节以OneAccess用户门户为例为您介绍OAuth认证功能的配置过程，在OneAcces平台配置集成OAuth认证源后，参考本模块配置OAuth认证登录各应用系统。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已在OneAccess实现OAuth认证源配置，如需配置，请参考**配置OAuth认证源**。

在 OneAccess 中开启 OAuth 认证

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击“用户门户”。

步骤4 在“应用信息”页面，单击“用户门户”应用图标。

步骤5 选择“登录配置 > 网站应用”，单击认证方式名为“OAuth认证”操作列的  开启OAuth认证，并关联**在OneAccess中添加OAuth认证源**中添加的认证源。

----结束

验证 OAuth 认证登录 OneAccess 用户门户

步骤1 用户访问用户门户，选择OAuth登录，应用侧的账号和密码即可进入OneAccess用户门户。

图 5-15 选择 OAuth 登录

步骤2 登录成功以后，在OneAccess侧的**组织与用户**处可查看自动创建的用户。

说明

- 当授权用户未关联系统用户时，在系统自动创建用户的前提是“**未关联用户时**”设置为“**自动创建用户**”。可参考**表5-9**。
- 自动创建的用户默认属于OneAccess侧的第一个根机构。

----结束

5.2.5 Kerberos 认证登录

5.2.5.1 配置 Kerberos 认证源

Kerberos是一种计算机网络认证协议，它允许某实体在非安全网络环境下通信，向另一个实体以一种安全的方式证明自己的身份。具体请参考**https://web.mit.edu/kerberos**。

AD（Active Directory），即活动目录。您可以将AD简单理解成一个数据库，其存储有关网络对象的信息，方便管理员和用户查找所需信息。

SPN（Service Principal Name），即服务主体名称。是服务实例的唯一标识符。

在Kerberos认证过程中，使用SPN将服务实例与服务登录账号关联。所以，必须在内置计算机账户或用户账户下为服务器注册SPN。对于内置账户，SPN会自动注册。如果需要在域用户账户下运行服务，必须要为使用的账户手动注册SPN。

为方便企业用户的认证登录，OneAccess平台支持配置Kerberos协议作为认证源，用户可以通过Kerberos协议认证登录各应用系统，为企业用户带来更简易便捷的登录方式和更好的用户体验。

本章节为您介绍配置Kerberos认证源的相关操作。

搭建 AD 服务器

以windows server 2012 r2搭建域服务器为例。具体请参考**搭建AD服务器**。

创建 AD 用户

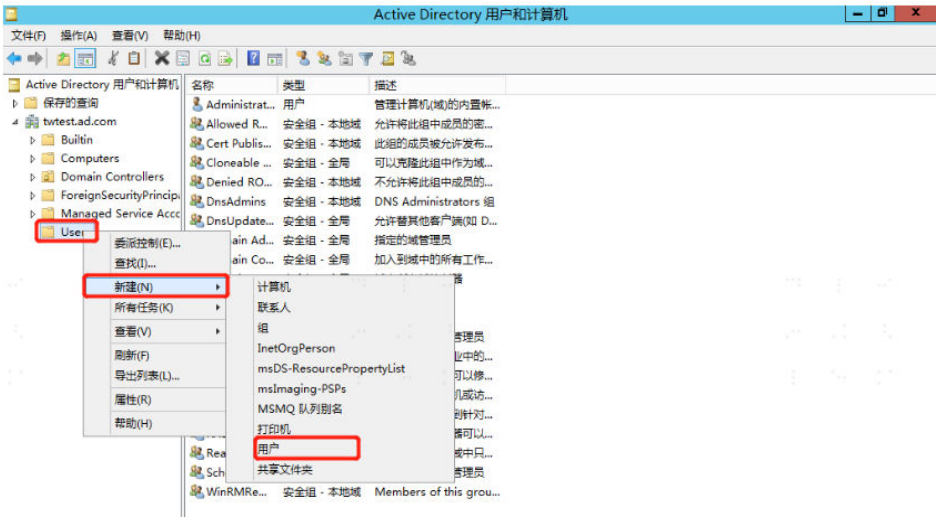
在已搭建好的AD域中创建AD用户。

步骤1 进入Active Directory 管理中心。

步骤2 右键目标域，选择“新建 > 用户”，输入用户信息，单击“确定”。

说明

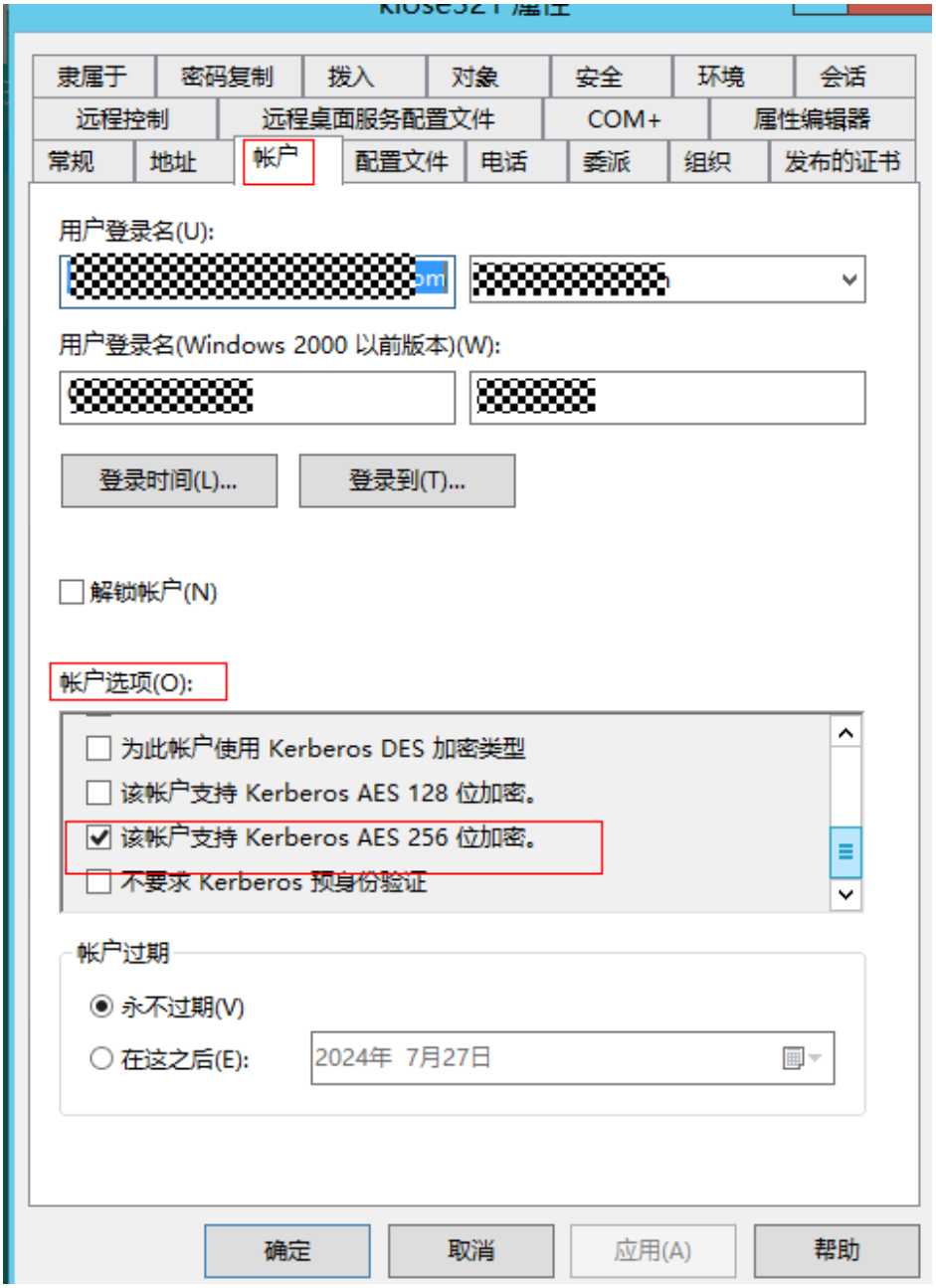
建议设置该用户密码为“密码永不过期”，避免后续登录异常。



说明

每个需要免密登录的AD用户都需要检查是否开启对AES 256位加密的支持，具体操作步骤如下：

在AD服务器中右击用户打开属性框，找到账户属性，确保账户选项中的“该账户支持Kerberos AES 256 位加密”被勾选。



----结束

配置 AD 服务器

步骤1 在AD服务器中生成SPN。

在AD服务器的DOS窗口中执行命令：setspn -A HTTP/{租户域名} {AD用户名}，如setspn -A HTTP/xxxxxx.huaweioneaccess.com Appointer。

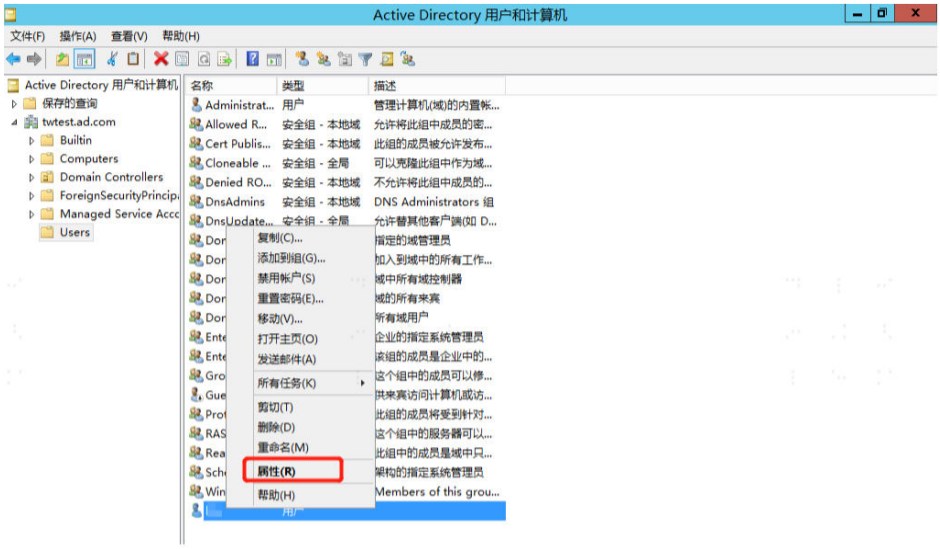
步骤2 在AD服务器中生成Keytab文件。

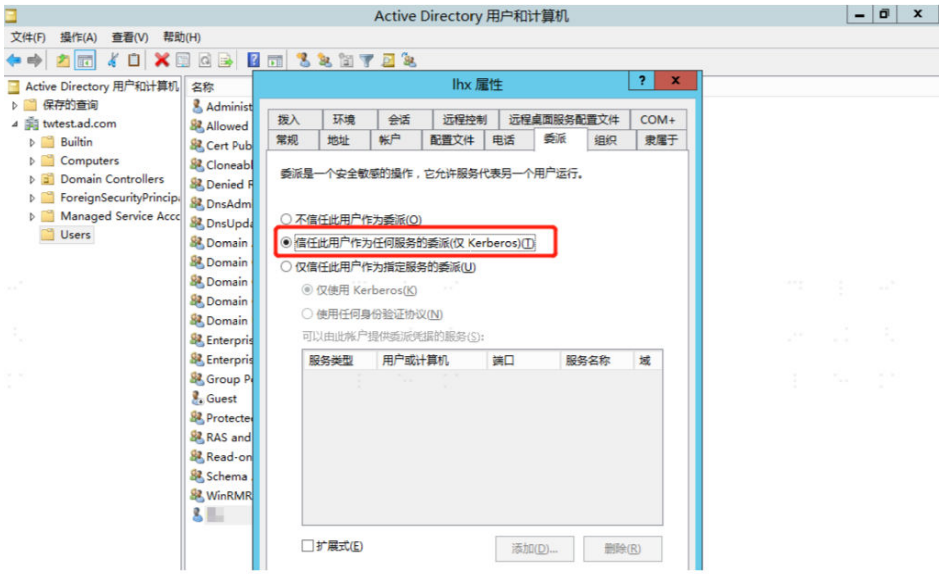
在AD服务器的DOS窗口中执行命令：ktpass /out {keytab文件地址} /mapuser {AD用户名} /princ HTTPS/{租户域名}@{AD域名} /pass {AD用户密码} /ptype KRB5_NT_PRINCIPAL /crypto AES256-SHA1，如ktpass /out c:\Appointer.keytab /mapuser Appointer /princ HTTPS/xxxxxx.huaweioneaccess.com@ONEACCESS.COM /pass {AD用户密码} /ptype KRB5_NT_PRINCIPAL /crypto AES256-SHA1。

```
C:\Users\Administrator.ECS-ONEACCESS-T>setspn -A HTTP/                    .huawei
oneaccess.com Appointer
        DC=oneaccess,DC=com

        CN=Appointer,DC=oneaccess,DC=com       ServicePrincipalNames
                HTTP/                    .huaweioneaccess.com


C:\Users\Administrator.ECS-ONEACCESS-T>
C:\Users\Administrator.ECS-ONEACCESS-T>ktpass /out c:\Appointer.keytab /mapuser
Appointer /princ HTTPS/                    .huaweioneaccess.com@ONEACCESS.COM /pa
ss                 /ptype KRB5_NT_PRINCIPAL /crypto ALL
Targeting domain controller:                          -0002.oneaccess.com
Using legacy password setting method
Successfully mapped HTTPS/                    .huaweioneaccess.com to Appointer.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to c:\Appointer.keytab:
Keytab version: 0x502
keysize 86 HTTPS/                    .huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x1 (DES-CBC-CRC) keylength 8 (0x405886a8ce8962ea
)
keysize 86 HTTPS/                    .huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x3 (DES-CBC-MD5) keylength 8 (0x405886a8ce8962ea
)
keysize 94 HTTPS/                    .huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x17 (RC4-HMAC) keylength 16 (0x6de00c52dbabb0e95
c074e3006fcf36e)
keysize 110 HTTPS/                    .huaweioneaccess.com@ONEACCESS.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 4 etype 0x12 (AES256-SHA1) keylength 32 (0xab9432e6a5f60
c5fa5467250e119b82b4d1f4b5ce894c2721645ab62b3304fcd)
keysize 94 HTTPS/                    .huaweioneaccess.com@ONEACCESS.COM ptype 1 (
KRB5_NT_PRINCIPAL) vno 4 etype 0x11 (AES128-SHA1) keylength 16 (0xd2233b57be1451
ea6f4f114d2d8822aa)
```

步骤3 在AD服务器中设置委派。

1. 选择**创建AD用户**中创建的用户，右键选择“属性”，设置委派。





----结束

配置客户端浏览器

- IE浏览器

  访问IE浏览器，选择“工具 > Internet选项 > 安全 > 本地 Intranet > 站点 > 高级 > 添加https://{租户域名}”。

- 谷歌浏览器

  与IE浏览器共用配置，即IE浏览器配置后，谷歌浏览器可以直接使用无需额外配置。

- 火狐浏览器
  a. 访问火狐浏览器，在地址栏输入“about:config”，单击“接受风险并继续”。
  b. 在配置项页面，输入“network.negotiate-auth-trusted-uris”，设置其值为https://{租户域名}。

在 OneAccess 中添加 Kerberos 认证源和用户

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理 > 企业认证源 > Kerberos”，进入Kerberos认证源页面，单击右上方“添加认证源”，配置参数添加认证源。

图 5-16 添加认证源

表 5-11 配置参数

参数	说明
* 显示名称	认证源的显示名称，支持自定义。如Kerberos认证。
* AD域名	大写的AD域名。如ONEACCESS.COM。
* KeyTab文件	步骤2中生成的文件。
* 关联用户属性	关联系统用户的唯一属性，如用户ID。
未关联用户时	通过“关联用户属性”认证失败时，登录失败。

步骤3 在导航栏中，选择“用户 > 组织与用户”，选择目标组织，单击“添加用户”，输入用户信息。用户名需与AD域中的登录用户名一致。

----结束

5.2.5.2 配置 Kerberos 认证登录

概述

本章节以OneAccess用户门户为例为您介绍Kerberos认证功能的配置过程，在OneAcces平台配置集成Kerberos认证源后，参考本模块配置Kerberos认证登录各应用系统。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已在OneAccess实现Kerberos认证源配置，如需配置，请参考**配置Kerberos认证源**。

在 OneAccess 中开启 Kerberos 认证源

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击“用户门户”。

步骤4 在应用信息页面，单击用户门户图标。

步骤5 选择“登录配置 > 网站应用”，单击认证方式名为“Kerberos认证”操作列的 开启Kerberos认证，并关联**在OneAccess中添加Kerberos认证源和用户**中添加的认证源。

说明

当开启Kerberos认证后，访问用户门户时，优先使用该认证方式。如果需要使用其他认证方式，需关闭Kerberos认证。

----结束

验证 Kerberos 认证登录 OneAccess 用户门户

步骤1 用户登录AD域。

步骤2 通过浏览器访问用户门户，即可免密进入。该用户即为**创建AD用户**中登录AD域的用户。

----结束

5.2.6 AD 认证登录

5.2.6.1 配置 AD 认证源

AD全称Active Directory，即活动目录。您可以将AD简单理解成一个数据库，其存储有关网络对象的信息，方便管理员和用户查找所需信息。

为方便企业用户的认证登录，OneAccess通过LDAP协议把认证指向AD域，AD通过认证后，根据AD返回的用户属性与OneAccess用户关联属性做匹配校验，验证通过即可登录OneAccess。

本章节为您介绍配置AD认证源的相关操作。

前提条件

请确保您已拥有OneAccess管理门户的访问权限。

搭建 AD 服务器

以windows server 2012 r2搭建域服务器为例。

步骤1 打开服务管理器，选择右上方“管理 > 添加角色和功能”。

步骤2 单击“下一步”，直到“选择服务器角色”页面，勾选“Active Directory域服务”选项，并在弹框中单击“确认添加”。

步骤3 单击“下一步”，直到“安装”页面，单击“安装”，启动角色安装流程。

步骤4 安装成功以后，单击右上方黄色三角提示标，单击“将此服务器提升为域控制器”，进入Active Directory域服务配置向导。

图 5-17 单击将此服务器提升为域控制器

步骤5 在“部署配置”页面，选择“添加新林”，并设置域名（如：oneaccess.com）。

步骤6 单击“下一步”，配置域服务器参数，输入DSRM的密码（非域用户）。

步骤7 单击“下一步”，直到“安装”页面，单击“安装”，开始安装AD域服务器，安装完成后会自动重启。

----结束

创建域账号

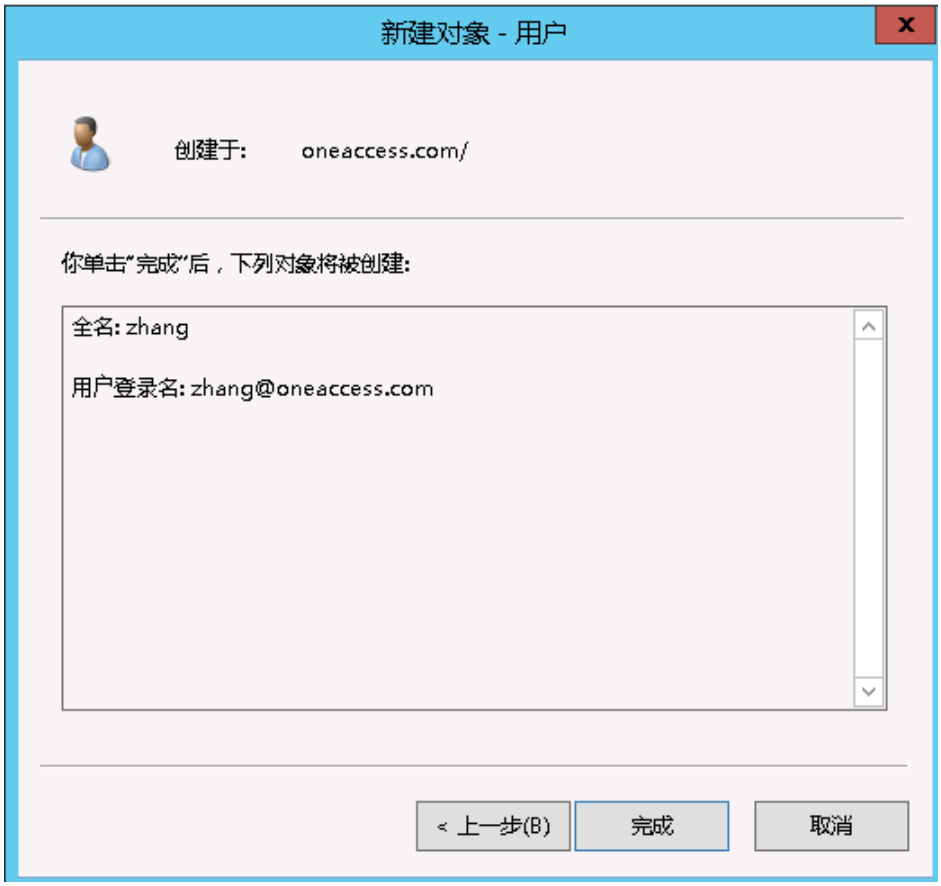
步骤1 选择右上方“工具 > Active Directory用户和计算机”。

步骤2 右键目标域，选择“新建 > 用户”，输入用户名称，单击“下一步”。

步骤3 输入“姓氏”和“用户登录名”，单击“下一步”。如zhang@oneaccess.com。

步骤4 填写域账号密码和确认密码。取消所有勾选框的检查（第一次登录时不需要更改密码）。

图 5-18 创建对象



----结束

配置 LDAP 连接 AD

步骤1 下载并安装ApacheDirectoryStudio（LDAP客户端工具）。

步骤2 选择“LDAP > New Connection”，填写连接参数。连接成功后，可以看到AD里的用户组织信息。

图 5-19 创建 Connection

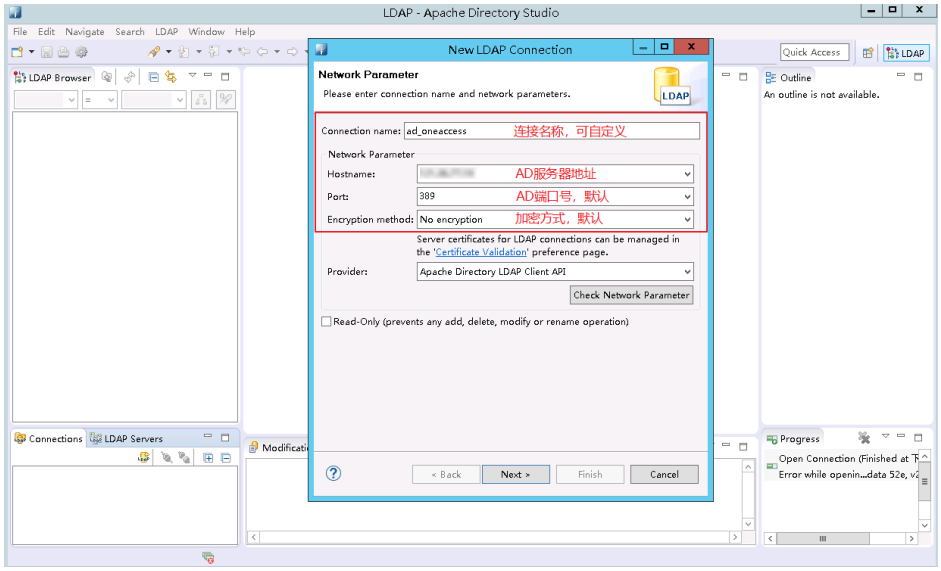


图 5-20 配置参数

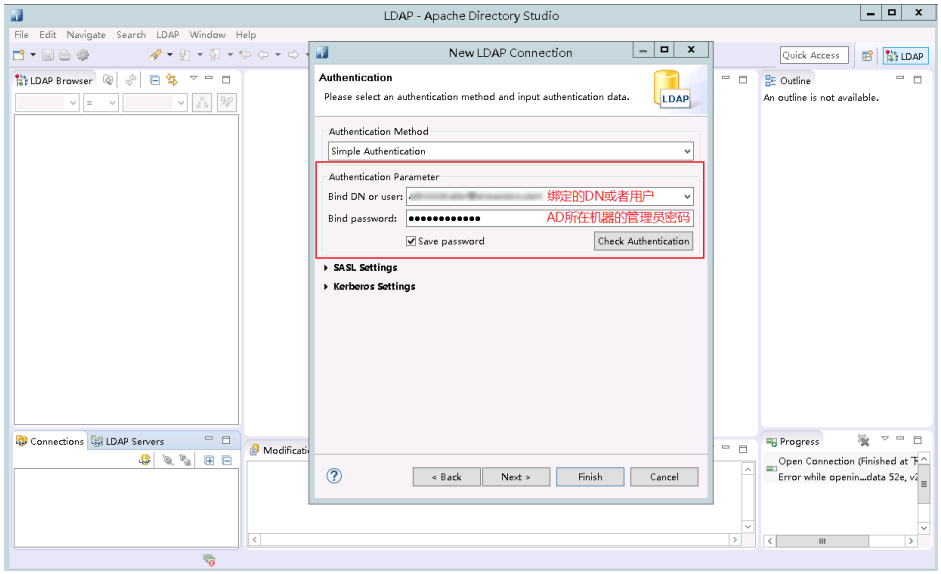
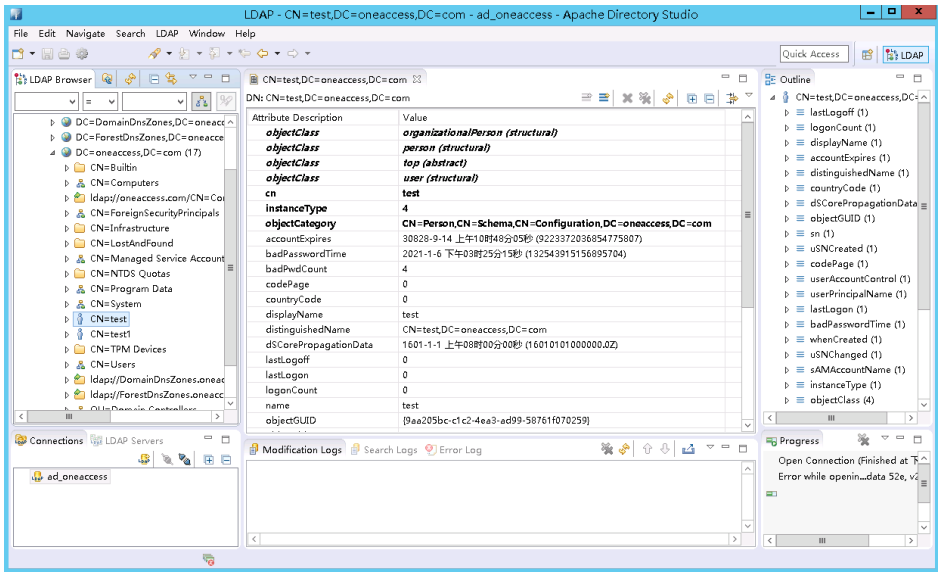


图 5-21 查看数据



----结束

在 OneAccess 中添加 AD 认证源

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理。

步骤3 选择“企业认证源 > AD”。

步骤4 在AD认证源页面，单击右上方“添加认证源”，配置参数。

图 5-22 配置参数

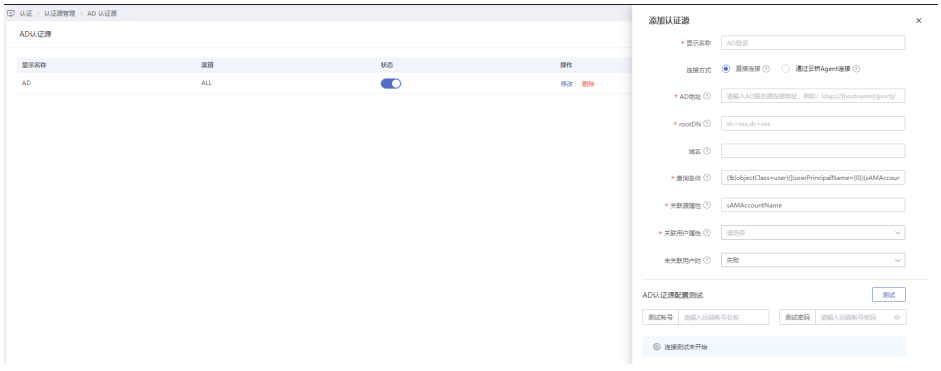


表 5-12 配置参数

参数	说明
显示名称	必填。认证源的显示名称，支持自定义。如AD认证。
连接方式	可选直接连接或通过云桥Agent连接。默认为直接连接。

参数	说明
AD地址	必填。AD连接地址。格式为ldap://{hostname}:{port}/，其中，{hostname}为AD服务器地址，端口为默认端口389。可参考**配置LDAP连接AD**。
rootDN	必填。AD中的节点，会到该节点下认证用户。 格式为dc=,dc=。可参考**配置LDAP连接AD**。
域名	选填。搭建AD服务器时设置的域名。如果填写，则将自动拼接登录名+@+域名作为查询条件，反之，只将登录名作为查询条件。可参考**步骤5**。
查询条件	必填。根据对象类和用户登录名进行查找，userPrincipalName可根据实际情况调整，占位符为{0}时，指带域名查询，页面输入值+域名，如zhangsan@companya.cn，无域名时，获取认证源域名属性值拼接后查询；占位符为{1}时，指原值查询，以页面输入值查询，如zhangsan。
关联源属性	必填。关联用户登录名AD用户的属性。如userPrincipalName。可在**配置LDAP连接AD**中获取。
关联用户属性	必填。AD在系统中映射的用户属性，唯一且为文本类型。
未关联用户时	必填。登录成功后，如未关联到系统用户，可以根据该配置操作。

说明

您可以按需定义用户属性，要求属性唯一且为文本类型。具体请参考**添加扩展属性**。

----结束

在 OneAccess 中开启 AD 认证

步骤1 在导航栏中，选择“资源 > 应用 ”进入应用页面。

步骤2 在应用页面，单击“用户门户”进入应用信息页面。

步骤3 单击用户门户图标进入通用信息页面。

步骤4 选择“登录配置 > 网站应用”，单击认证方式名为“AD认证”操作列的 开启AD认证，并关联**在OneAccess中添加AD认证源**中添加的认证源。

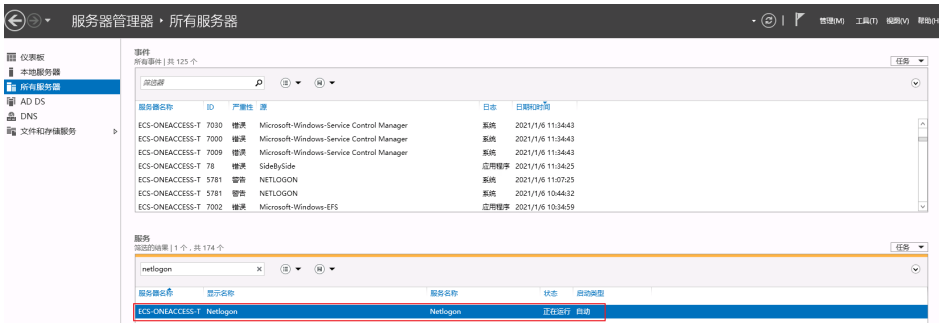
说明

开启AD认证时会占用密码登录方式的输入框，需要单击认证方式名为“密码认证”操作列 禁用数据库认证方式。如果已开启LDAP认证，同时需要单击认证方式名为“LDAP认证”操作列 禁用LDAP认证方式。

----结束

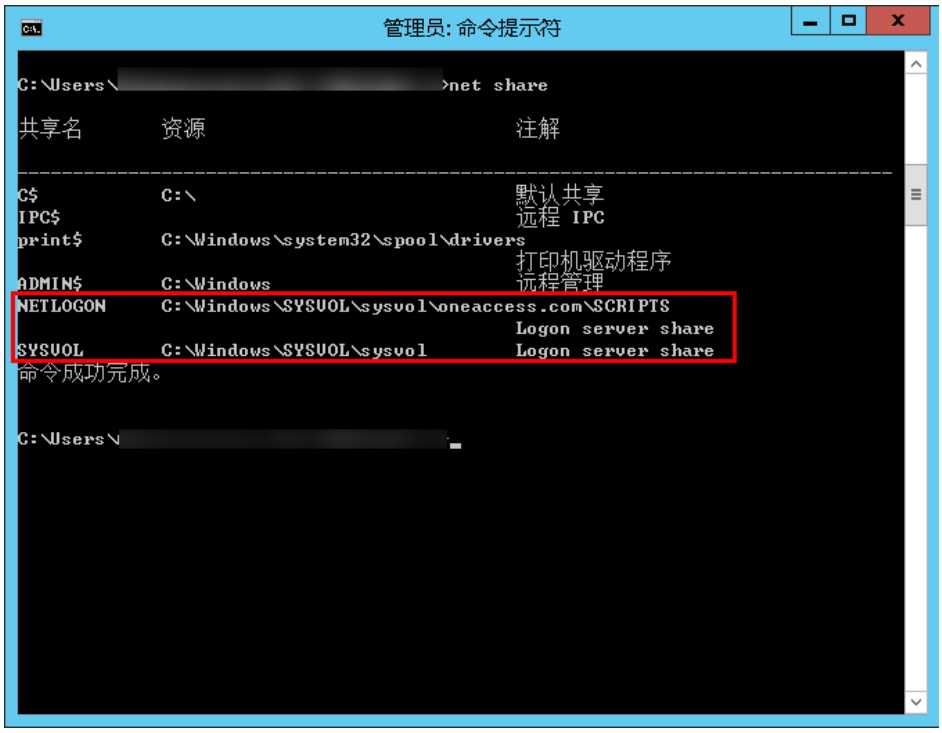
FAQ

1. 创建域账号时，用户AD活动目录无法打开，提示域不存在或无法联系。
   a. 检查Netlogon和DFS服务是否已经启动。



   b. 运行**net share**命令，查看共享是否正常。

   如果异常，可将注册表中HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters中SysvolReady的键值改为1。再次运行**net share**命令，共享正常。



   c. 对于AD域的问题，主要还是查看事件查看器日志并通过DcDiag工具查询错误信息。

2. 配置LDAP连接AD时，如果提示 [LDAP：error code 49-80090308:LdapErr:…… AcceptSecurityContext error.data.52e.vece]。

   密码或凭证无效，用户名的格式为{用户名}@{域名}。

5.2.6.2 配置 AD 账号密码登录

概述

本章节以OneAccess用户门户为例为您介绍AD认证功能的配置过程，在OneAcces平台配置集成AD认证源后，参考本模块配置AD认证登录各应用系统。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已在OneAccess实现AD认证源配置，如需配置，请参考**配置AD认证源**。

验证 AD 认证登录 OneAccess 用户门户

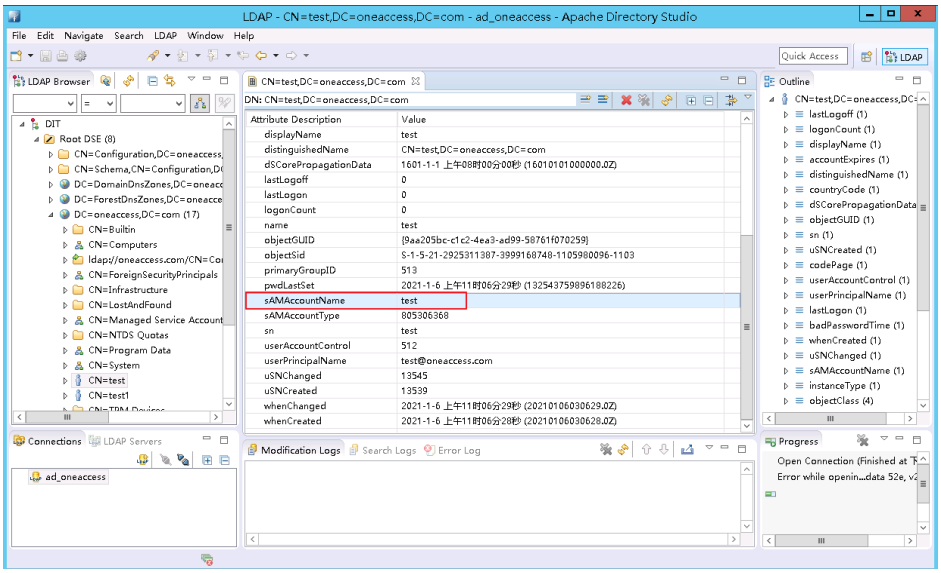
1. 用户访问用户门户，选择“AD”登录，输入AD账号和密码登录，可进入用户门户。

   图 5-23 选择 AD 登录

2. 用户登录成功以后，可在管理门户的“用户 > 组织与用户”处查看自动创建的用户。

3. 当AD中的用户未关联OneAccess用户，且图5-22中“未关联用户时”设置为“失败时，此时，如果需要通过AD成功访问用户门户时，需在OneAccess中创建与AD中同名的用户。

图 5-24 查看 AD 用户



5.2.7 LDAP 认证登录

5.2.7.1 配置 LDAP 认证源

概述

LDAP（Lightweight Directory Access Protocol），即轻量目录访问协议。

它是一种树状结构的组织数据，可以简单理解成一个存储用户和组织信息的树形结构数据库。单点登录是LDAP的主要使用场景之一，即用户只在公司计算机上登录一次后，便可以自动在公司内部网上登录。

表 5-13 主要术语

术语	说明
ou	全称 Organization Unit，组织单位，即容器对象。
dc	全称 Domain Component，域名的部分，格式是将完整的域名分成几部分。
sn	全称 Surname，姓。
cn	全称 Common Name，公共名称。
dn	全称 Distinguished Name，唯一标识名。
uid	全称 User ID，用户ID。
rdn	全称 Relative dn，相对辨别名，类似文件系统中的相对路径。

为方便企业用户的认证登录，OneAccess通过LDAP协议把认证指向LDAP，LDAP通过认证后，根据LDAP返回的用户属性与IDaaS用户关联属性做匹配校验，验证通过即可登录OneAccess。

本章节为您介绍配置LDAP认证源的相关操作。

前提条件

请确保您已拥有OneAccess管理门户的访问权限。

搭建 LDAP 服务器

步骤1 通过**ForgeRock官网**下载Directory Services安装包。

步骤2 部署LDAP服务，具体可参考ForgeRock平台的帮助文档。

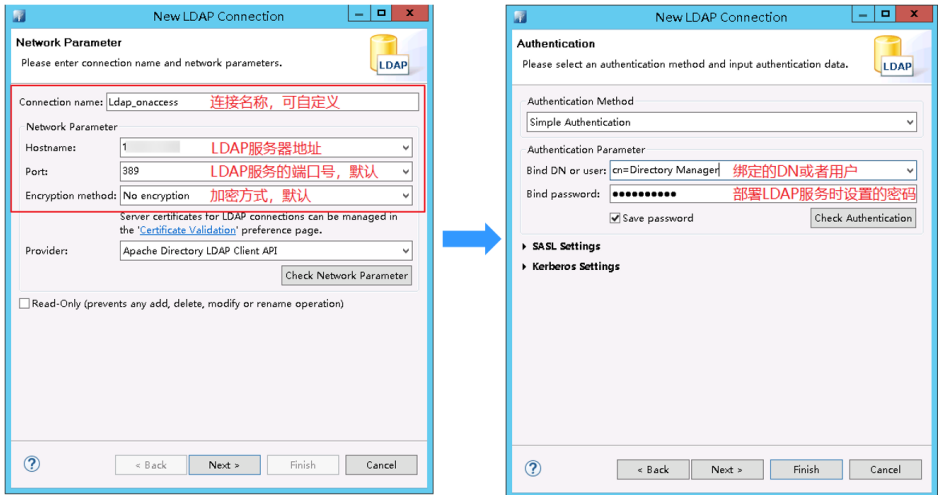
----结束

配置 LDAP 连接

步骤1 下载并安装ApacheDirectoryStudio（LDAP客户端工具）。

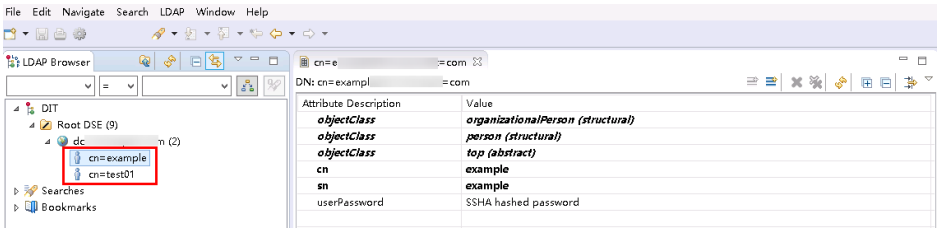
步骤2 选择“LDAP > New Connection”，创建连接并填写参数。

图 5-25 创建 Connection



步骤3 LDAP添加账号。

图 5-26 查看用户



----结束

在 OneAccess 中添加 LDAP 认证源

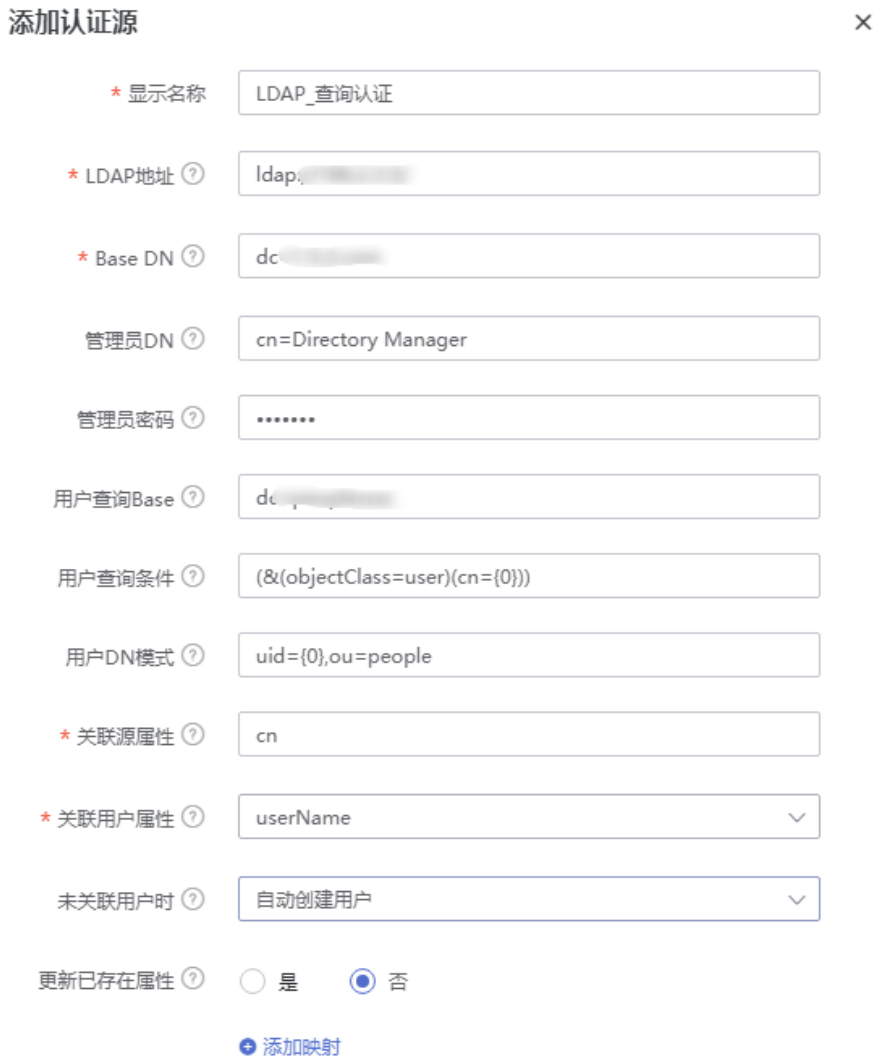
LDAP主要有三种认证模式，包括DN认证模式、查询认证模式和组合模式。

- DN认证模式：选择该模式代表清楚用户的DN规则，如（uid=**，ou=people，dc=example，dc=com），只需配置用户DN模式即可。

图 5-27 DN 认证模式

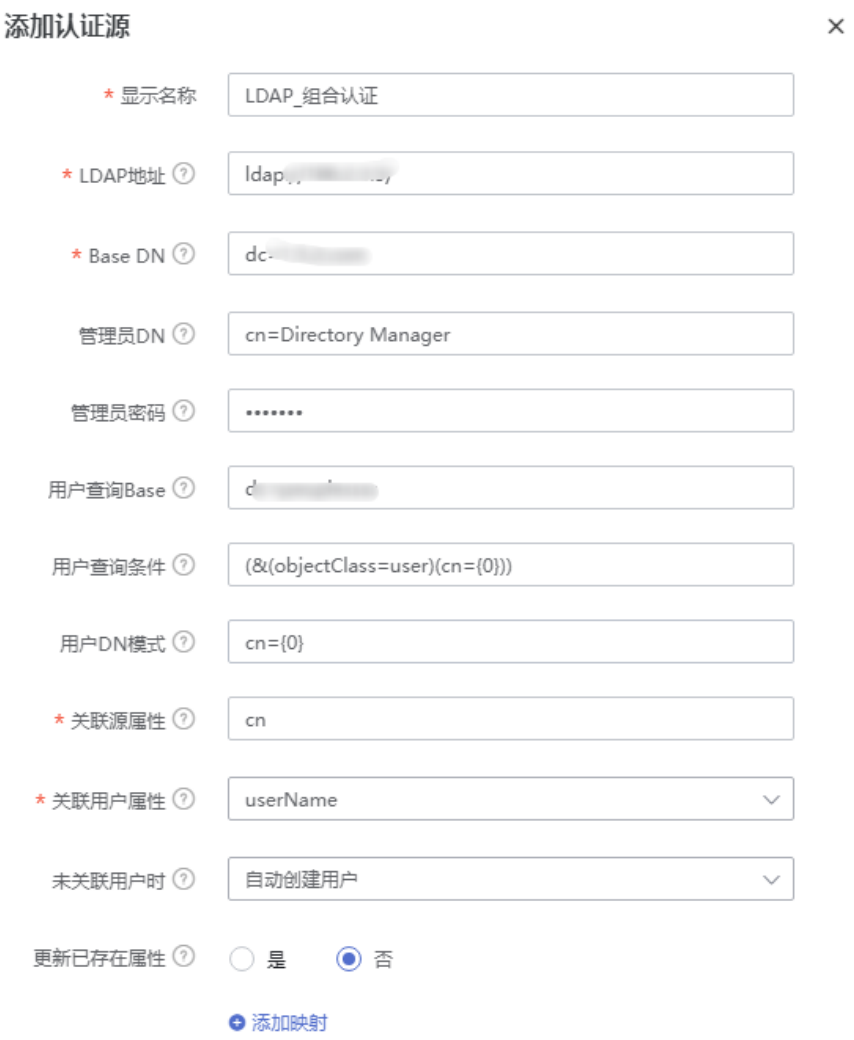
- 查询认证模式：选择该模式，需配置LDAP的管理员账号和密码，并且配置查询条件。认证时，使用LDAP管理员账号，根据配置的查询条件和输入的用户名查询用户，查到用户后，取用户的DN，在LDAP中验证用户的DN和密码。

图 5-28 查询认证模式



- 组合模式：该模式是DN认证模式+查询认证模式的组合，该模式下DN模式优先。

图 5-29 组合模式



以下主要介绍配置LDAP组合认证模式的方法。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“认证 > 认证源管理”。

步骤3 选择“企业认证源 > LDAP”。

步骤4 在LDAP认证源页面，单击右上方“添加认证源”，配置参数。

表 5-14 配置参数

参数	是否必填	说明
显示名称	是	认证源的显示名称，支持自定义。如LDAP认证。
LDAP地址	是	LDAP连接地址。格式为ldap://{hostname}:{port}/，其中，{hostname}为LDAP服务器地址，{port}为LDAP端口号，默认为389。可参考**搭建LDAP服务器**。

参数	是否必填	说明
Base DN	是	LDAP目录的根节点，会到该节点下认证用户。 格式为dc=,dc=。可参考**搭建LDAP服务器**。
管理员DN	否	管理员的标识名，默认cn=Directory Manager。
管理员密码	否	LDAP服务中管理员账户的密码。
用户查询Base	否	用户的baseDN，系统默认“ou=People”。
用户查询条件	否	LDAP中匹配系统用户的过滤条件，系统默认“(&(objectClass=user)(uid={0}))”，详细请参考**LDAP过滤器**。基于条件的查询优先级低于基于DN的查询。
用户DN模式	否	LDAP用户的搜索路径，系统默认“uid={0},ou=people”。用户DN模式查询优先。
关联源属性	是	LDAP用户名属性，系统默认“uid”，可在**步骤3**中获取。
关联用户属性	是	LDAP在系统中映射的用户属性，唯一且为文本类型。可在下拉框选择。
未关联用户时	是	登录成功后，如未关联到系统用户，可以根据系该配置操作。

如果您需要同时映射其他属性，如用户名，可以设置“**未关联用户时**”为“**自动创建用户**”，通过“添加映射”完成。可参考**表5-15**。

表 5-15 映射参数

参数	说明
用户属性名	LDAP对接OneAccess的映射属性，可在下拉框选择。
映射类型	OneAccess与LDAP之间用户属性的映射方式，可在下拉框选择。 **说明** • 当选择“映射类型”为“认证源属性”时，需要同时输入“认证源属性名”。 • 当选择“映射类型”为“固定属性值”时，需要同时输入“固定属性值”。 • 当选择“映射类型”为“脚本转换”时，需要同时输入“脚本内容”。

----结束

5.2.7.2 配置 LDAP 账号密码登录

概述

本章节以OneAccess用户门户为例为您介绍LDAP认证功能的配置过程，在OneAcces平台配置集成LDAP认证源后，参考本模块配置LDAP认证登录各应用系统。

前提条件

- 请确保您已拥有OneAccess管理门户的访问权限。
- 请确保您已在OneAccess实现LDAP认证源配置，如需配置，请参考**配置LDAP认证源**。

在 OneAccess 中开启 LDAP 认证

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在应用页面，单击“用户门户”。

步骤4 在“应用信息”页面，单击“用户门户”应用图标。

步骤5 选择“登录配置 > 网站应用”，单击认证方式名为“LDAP认证”操作列的 开启LDAP认证，并关联**在OneAccess中添加LDAP认证源**中添加的认证源。

说明

开启LDAP认证时会占用密码登录方式的输入框，需要单击认证方式名为“密码认证”操作列 禁用数据库认证方式。如果已开启AD认证，同时需要单击认证方式名为“AD认证”操作列 禁用AD认证方式。

----结束

验证 LDAP 认证登录 OneAccess 用户门户

1. 用户访问用户门户，选择“LDAP”登录，输入LDAP账号和密码登录，可进入用户门户。

图 5-30 选择 LDAP 登录

2. 用户登录成功以后，可在管理门户的“用户 > 组织与用户”处查看自动创建的用户。

   说明

   - 当授权用户未关联系统用户时，在系统中自动创建用户的前提是“**未关联用户时** ”设置为“**自动创建用户**”，可参考**表5-14**。
   - 自动创建的用户默认属于管理门户中的第一个根机构。

6 授权 IAM 用户访问 OneAccess 实例管理门户

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助您安全地控制华为云服务和资源的访问权限。IAM无需付费即可使用。

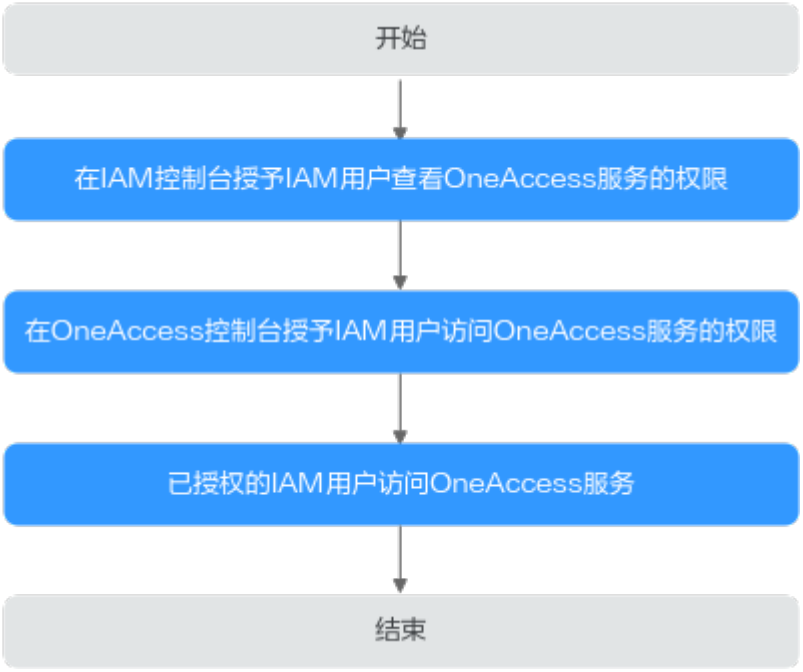
IAM用户是账号在IAM中创建的用户，是云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据账号授予的权限使用资源。

如果您需要通过OneAccess单点登录华为云，请参考**通过OneAccess免密登录单个华为云账号（SAML-虚拟用户SSO）**。

OneAccess支持IAM用户通过华为云访问服务实例，方便企业管理员安全的控制OneAccess服务和资源的访问权限。

本文主要介绍授权IAM用户访问OneAccess实例管理门户的方法。

配置流程



前提条件

请确保您已拥有华为云账号，并且该账号已购买OneAccess实例。如需购买请参考**购买实例**。

在 IAM 控制台授予 IAM 用户查看 OneAccess 服务的权限

在IAM控制台创建用户组并授权、创建用户并添加至用户组中，用户就继承了用户组的权限。

步骤1 参考**创建用户组并授权**在IAM控制台创建用户组，并授予OneAccess服务的只读权限“OneAccess ReadOnlyAccess”。

步骤2 参考**创建用户并加入用户组**在IAM控制台创建用户，并将其加入**步骤1**中创建的用户组。

步骤3 参考**用户登录**登录控制台，验证OneAccess服务的只读权限。

----结束

在 OneAccess 控制台授权 IAM 用户访问 OneAccess 服务的权限

在应用身份管理服务控制台“实例授权”IAM用户，确保IAM用户可以访问OneAccess服务。

步骤1 使用管理员登录应用身份管理服务控制台。

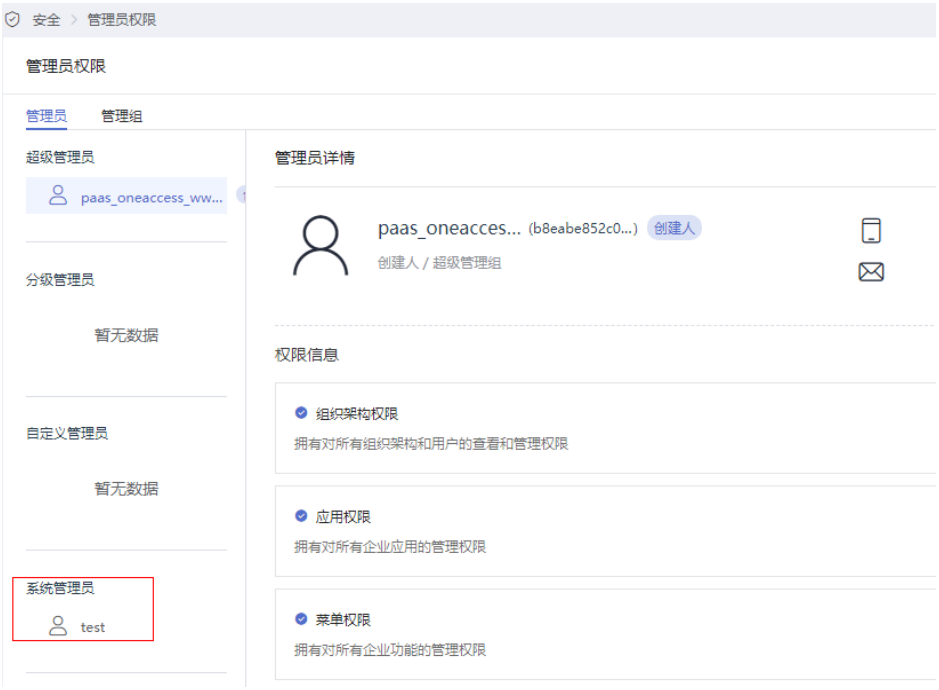
步骤2 在应用身份管理服务控制台页面，单击“实例授权”。

步骤3 在实例授权页面，单击“新增授权”，选择**步骤2**中创建的用户，单击“是”，即可授权IAM用户访问OneAccess服务的权限。

说明

OneAccess“实例授权”可支持授权50个IAM用户访问OneAccess服务的权限。

步骤4 当授权IAM用户后，可在OneAccess管理门户的管理员权限处查看已自动生成的系统管理员。



----结束

已授权的 IAM 用户访问 OneAccess 服务

当授予IAM用户访问OneAccess服务的权限后，该IAM用户可通过华为云进入OneAccess管理门户。

步骤1 IAM用户登录华为云，具体可参考**IAM用户登录**。如您需要使用扫码登录，请参考**扫码登录**。

步骤2 在服务列表中选择“管理与监管 > 应用身份管理服务 OneAccess”，进入应用身份管理服务控制台。

步骤3 在控制台页面，单击要访问的“实例名称”，进入OneAccess管理门户。

说明

- IAM用户进入OneAccess管理门户后，无“安全>管理员权限”页签的查看权限。其他操作可参考**企业管理员指南**。
- 如需IAM用户拥有OneAccess服务的所有权限，请授予“OneAccess FullAccess”权限。具体可参考**步骤1**。

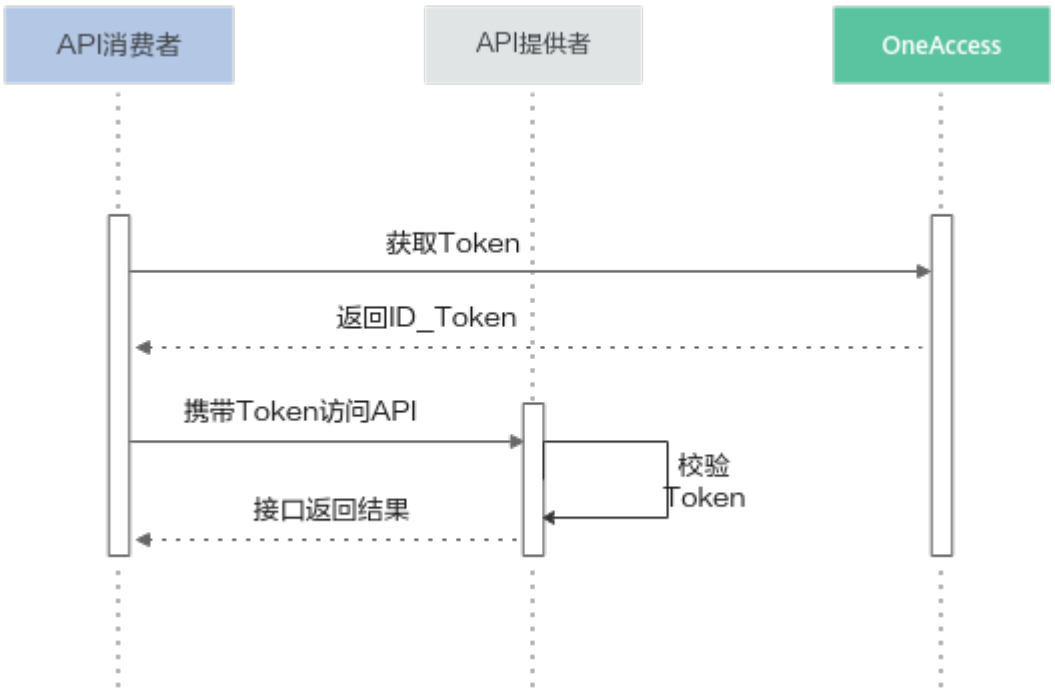
----结束

7 企业 API 使用

场景简介

OneAccess提供第三方API的授权管理功能，API提供者将API配置到OneAccess之后，API消费者在使用API之前需要先到OneAccess获取鉴权Token，在使用API时携带该鉴权Token，API提供者根据鉴权Token判断是否可以提供服务，用以实现API的授权管理功能。

图 7-1 场景简介图



前提条件

请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中添加企业应用

在OneAccess管理门户中添加企业应用，提供给API使用者获取鉴权Token信息。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 在企业应用页面，单击自建应用下的“添加自建应用”，设置Logo和名称，单击“保存”。

步骤4 获取的ClientId和ClientSecret。

在应用信息页面单击应用图标，在应用详情页面获取ClientId和ClientSecret（此信息需要提供给API使用者）。

说明

- ClientSecret需单击“启用”生成。
- ClientSecret是校验开发者身份的密码，具备高安全性，切勿将其直接提供给第三方开发者或直接存储在代码中。
- 重置后的ClientSecret即时生效，所有使用原ClientSecret的接口将全部失效，请谨慎重置。
- OneAccess不存储ClientSecret，当获取ClientSecret后，请妥善保管。

----结束

在 OneAccess 中添加企业 API

OneAccess管理员在OneAccess管理门户中添加企业需要的自定义API产品。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 企业API”。

步骤3 在企业API页面，单击自定义API产品下的“添加自定义API产品”。

步骤4 在“添加企业API”页面，上传产品LOGO，填写产品名称和描述，单击“确定”，自定义API产品添加完成，自定义API产品页面显示已添加的API产品。

步骤5 单击新建的自定义API产品，切换到“应用授权”页签，单击**在OneAccess中添加企业应用**中新建的应用后的“授权”，完成API对应用的授权使用。

步骤6 切换到“权限信息”页面，添加API权限信息。

----结束

在 OneAccess 应用中授权相应 API 权限

在OneAccess的应用中，授权具体自定义API的权限。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，单击“资源 > 应用”。

步骤3 单击**在OneAccess中添加企业应用**中新建的应用，单击应用图标，进入通用信息页面。

步骤4 选择“API权限 ”，在API权限页面，单击某一权限代码右侧“操作”列的“授权”则授权成功。

----结束

在 OneAccess 中获取签名公钥和算法密钥

OneAccess颁发的鉴权Token是经过加密和签发的，需要获取签名公钥和算法密钥给API提供者进行解密。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“设置 > 服务配置”，单击“API认证配置”，获取签名公钥和算法密钥，提供给API提供者。

说明

OneAccess不展示算法密钥，当重置算法密钥后，请妥善保管。

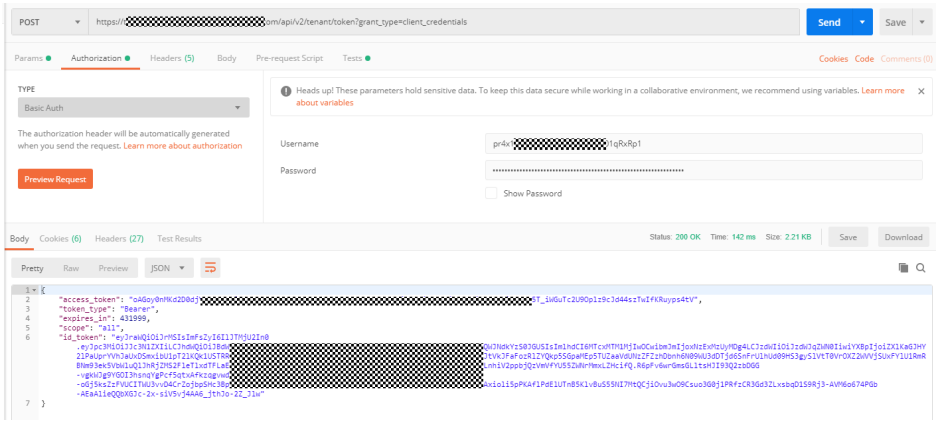
----结束

API 使用者从 OneAccess 获取鉴权 Token

API使用者调用OneAccess鉴权接口获取鉴权Token。

访问接口：https://访问域名/api/v2/tenant/token?grant_type=client_credentials。

PostMan调用示例：



说明

- 访问域名为用户访问域名。可在OneAccess实例详情页获取。。
- 使用POST访问，使用Basic认证，Basic认证的用户名和密码为**步骤4**中获取的ClientId和ClientSecret。
- 返回的id_token可以由API使用者使用对应API时传递给API提供者做身份认证和授权，其中包含签名信息以及对应的API权限信息。可以使用header来传递。建议使用标准的Authorization Header传递。
- 返回的id_token有有效期，有效期之内，此id_token可以重复使用，有效期的期限由应用中配置决定。

API 提供者校验 Token

API使用者调用API提供者的接口时，携带从OneAccess获取的id_token，API提供者在收到API使用者的消息时需要校验该Token，主要校验两个内容：

- Token的签名信息是否正确，保证Token是OneAccess颁发的。
- 校验Token中申明的权限是否包含当前访问当前的API。

下面是java示例代码：

```
import com.alibaba.fastjson.JSON;
import lombok.Data;
import org.apache.commons.codec.binary.Base64;
import org.jose4j.jwa.AlgorithmConstraints;
import org.jose4j.jwe.ContentEncryptionAlgorithmIdentifiers;
import org.jose4j.jwe.JsonWebEncryption;
import org.jose4j.jwe.KeyManagementAlgorithmIdentifiers;
import org.jose4j.jwk.JsonWebKey;
import org.jose4j.jwt.JwtClaims;
import org.jose4j.jwt.consumer.InvalidJwtException;
import org.jose4j.jwt.consumer.JwtConsumer;
import org.jose4j.jwt.consumer.JwtConsumerBuilder;
import org.jose4j.lang.JoseException;

import java.io.ByteArrayInputStream;
import java.io.InputStream;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.security.interfaces.RSAPublicKey;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

/**
 * @author : bsong
```

```
**/
public class JWTTest {
    public static final String BEGIN_CERT = "-----BEGIN CERTIFICATE-----";
    public static final String END_CERT = "-----END CERTIFICATE-----";

    public static void main(String[] args) throws CertificateException, InvalidJwtException, JoseException {
        //id token由API调用者传递
        String idToken = "";
        // 算法密钥在OneAccess中设置
        String aesKey = "0123**********789abc";
        //证书在OneAccess管理门户配置中获取
        String certificate = "-----BEGIN CERTIFICATE-----\n" +
                "MIIC2jCCAcKgAwI.....QEBCwUAMC4xLDAqBgNVBAMM\n" +
                "I2Jzb25nLmlkYWF.....GUuY29tMB4XDTIyMDExNDA3\n" +
                "MDY1NVoXDTMyMDE.....wwjYnNvbmcuaWRhYXMtdGVz\n" +
                "dC1hbHBoYS5iY2N.....Ib3DQEBAQUAA4IBDwAwggEK\n" +
                "AoIBAQCJ7bfMCVX.....GnE3W9uiSYk3WFkYFK8vh16\n" +
                "efVuvccAULE+xqi.....652lsIBNOAC5YPy7J47z4iw\n" +
                "1GiAVYXxwyehgRe3.....e0eJDKy6Ew5S+TUq72hqSD7\n" +
                "zrtQA3szqSK1pgFB.....J8rMh9WiF2qUqzCdNRqkQRC\n" +
                "smGGj+PqD86otiif.....0OPH5UOhR2OEve1cT9dgAlS\n" +
                "Vt1tKbE0l+iUTQqi.....oZIhvcNAQELBQADggEBAEP8\n" +
                "EmkyoaWjngk3Tn5u.....cJEDGTbuYO55wKap0BTetu6\n" +
                "cvGFxJYMQYefsx0.....xn8N4ZgWvwgwDQVQx5WPgAT\n" +
                "QKunLWz30W4GYUE.....QJZ7ift2sqoBLmkmjfcyqW0\n" +
                "jU1+7/e/ea5XAC3.....DtVHqufwP4R/TALg1muaNyJ\n" +
                "f7obOcMHAb/OcbP.....FSAwkVYsxSC9LEEUPhCONvX\n" +
                "KCWoeQoX/qkZH/nBvXU=\n" +
                "-----END CERTIFICATE-----";

        RSAPublicKey publicKey = getPublicKeyByCertificate(certificate);
        JsonWebKey jsonWebKey = getJsonWebKey(aesKey);
        JwtClaims jwtClaims = validateIDToken(publicKey, idToken);
        String apiPermission = jwtClaims.getClaimValue("api").toString();
        String permissionString = decryptionIDToken(jsonWebKey, apiPermission);
        System.out.println(permissionString);
        Map<String, List<String>> permissions = getPermissionsFromIdToken(permissionString);
        System.out.println(permissions);
    }

    public static Map<String, List<String>> getPermissionsFromIdToken(String permissionString) throws
JoseException {
        Map<String, List<String>> result = new HashMap<>();
        Permission permission = JSON.parseObject(permissionString,Permission.class);
        permission.getAuz().stream().forEach(p ->{
            p.entrySet().forEach(e->{
                result.put(e.getKey(),e.getValue());
            });
        });
        return result;
    }

    @Data
    public static class Permission{
        List<Map<String, List<String>>> auth_method;
        List<Map<String, List<String>>> auz;
    }

    public static RSAPublicKey getPublicKeyByCertificate(String certificate) throws CertificateException {
        CertificateFactory fact = CertificateFactory.getInstance("X.509");
        byte[] decoded = Base64.decodeBase64(certificate.replace(BEGIN_CERT, "").replace(END_CERT, ""));
        InputStream input = new ByteArrayInputStream(decoded);
        X509Certificate cert = (X509Certificate) fact.generateCertificate(input);
        return (RSAPublicKey) cert.getPublicKey();
    }

    public static JsonWebKey getJsonWebKey(String key) throws JoseException {
        Map<String,Object> map = new HashMap<>();
        map.put("kty","oct");
```

```
        map.put("k",key);
        String jwkJson = JSON.toJSONString(map);
        return JsonWebKey.Factory.newJwk(jwkJson);
    }

    public static JwtClaims validateIDToken( RSAPublicKey publicKey,String idToken) throws
InvalidJwtException {
        JwtConsumer jwtConsumer = new JwtConsumerBuilder()
                .setRequireExpirationTime()                 // JWT必须具有到期时间
                .setAllowedClockSkewInSeconds(300)          //允许在验证基于时间的声明时留有余地以解决时钟偏
移
                .setRequireSubject()                        // JWT必须具有主题声明
                .setExpectedIssuer("Issuer")                //谁JWT需要已被发出
                .setExpectedAudience("Audience")            // JWT的目标对象
                .setVerificationKey(publicKey)
                .build();
        return jwtConsumer.processToClaims(idToken);
    }

    public static String decryptionIDToken(JsonWebKey jwk, String idToken) throws JoseException {
        JsonWebEncryption jsonWebEncryption = new JsonWebEncryption();
        jsonWebEncryption.setAlgorithmConstraints(new
AlgorithmConstraints(AlgorithmConstraints.ConstraintType.PERMIT,
KeyManagementAlgorithmIdentifiers.DIRECT));
        jsonWebEncryption.setContentEncryptionAlgorithmConstraints(new
AlgorithmConstraints(AlgorithmConstraints.ConstraintType.PERMIT,
ContentEncryptionAlgorithmIdentifiers.AES_128_CBC_HMAC_SHA_256));
        jsonWebEncryption.setCompactSerialization(idToken);
        jsonWebEncryption.setKey(jwk.getKey());
        return jsonWebEncryption.getPlaintextString();
    }
}
```

8 用户登录二次认证配置

OneAccess支持用户登录时进行二次认证的功能，提供更为安全的保障，本文以用户门户为例，为您介绍如何实现二次认证的配置以及使用。

前提条件

请确保您已拥有OneAccess管理门户的访问权限。

在 OneAccess 中开启应用二次认证功能

在OneAccess管理门户中开启并配置应用的二次认证功能。

步骤1 登录OneAccess管理门户。

步骤2 在导航栏中，选择“资源 > 应用”。

步骤3 在企业应用页面（以用户门户为例），单击预集成应用下的“用户门户”，进入用户门户信息页面。

步骤4 单击“访问控制”区域的  ，在弹出的“开启访问控制策略”页面，在“默认策略”处选择“二次认证”，选择“二次认证频率”和“二次认证方式”，单击“保存”。

说明

- 只有打开认证集成，才可以配置访问控制。
- 二次认证方式支持多选，当勾选多个后，用户登录二次认证时，可选择二次认证方式。
- 如果二次认证方式选择“FIDO2”方式，需要配置FIDO认证源，具体配置可以参考**内置认证源**。

步骤5 单击“添加策略”，在弹出的“添加策略”页面，配置访问控制参数，单击“保存”添加策略完成，具体配置参数可以参考**访问控制**。

----结束

访问用户门户

用户访问用户门户，登录成功之后，进入二次认证页面，认证成功后进入用户门户。