使用Microsoft Entra ID SAML SSO配置ISE保证人门户

目录

简介

先决条件

- 要求
- 使用的组件

高级流程图

配置

- 步骤1.在ISE上配置SAML身份提供程序和发起人门户
  - 添加SAML身份提供程序
  - 将发起人门户配置为idP
  - 导出服务提供商信息
- 步骤2.配置Microsoft Entra ID
  - 创建Azure AD用户
  - 2.创建组并添加用户
  - 3.创建Entra Enterprise应用程序
  - 4.将组（或用户）分配给应用程序
- 步骤3.在Entra ID中配置SAML单点登录
  - 2.配置Entra组属性
  - 3.下载联合元数据XML文件
- 步骤4.将元数据从Entra上传到ISE
  - 导入联合元数据
  - 在ISE上配置SAML组
- 步骤5.在ISE上配置发起人组映射

验证

故障排除

- 问题2 — 用户未分配到应用(AADSTS50105)
- 问题3 — 注销失败（“SSO注销失败”）
- 问题4 — 已轮换签名证书（“身份验证失败”）
- 问题5 — 会话快速过期
- 客户端故障排除
- ISE故障排除
- 数据包捕获分析
  - TLS客户端Hello — 其中门户名称可见
  - 客户端上捕获的相同登录

简介

本文档介绍如何将Microsoft Entra ID配置为Cisco ISE保证人门户的SAML身份提供程序。

先决条件

要求

Cisco 建议您了解以下主题：

- Microsoft Entra ID
- 思科身份服务引擎(ISE)3.0
- 安全断言标记语言(SAML)单点登录(SSO)部署基础知识

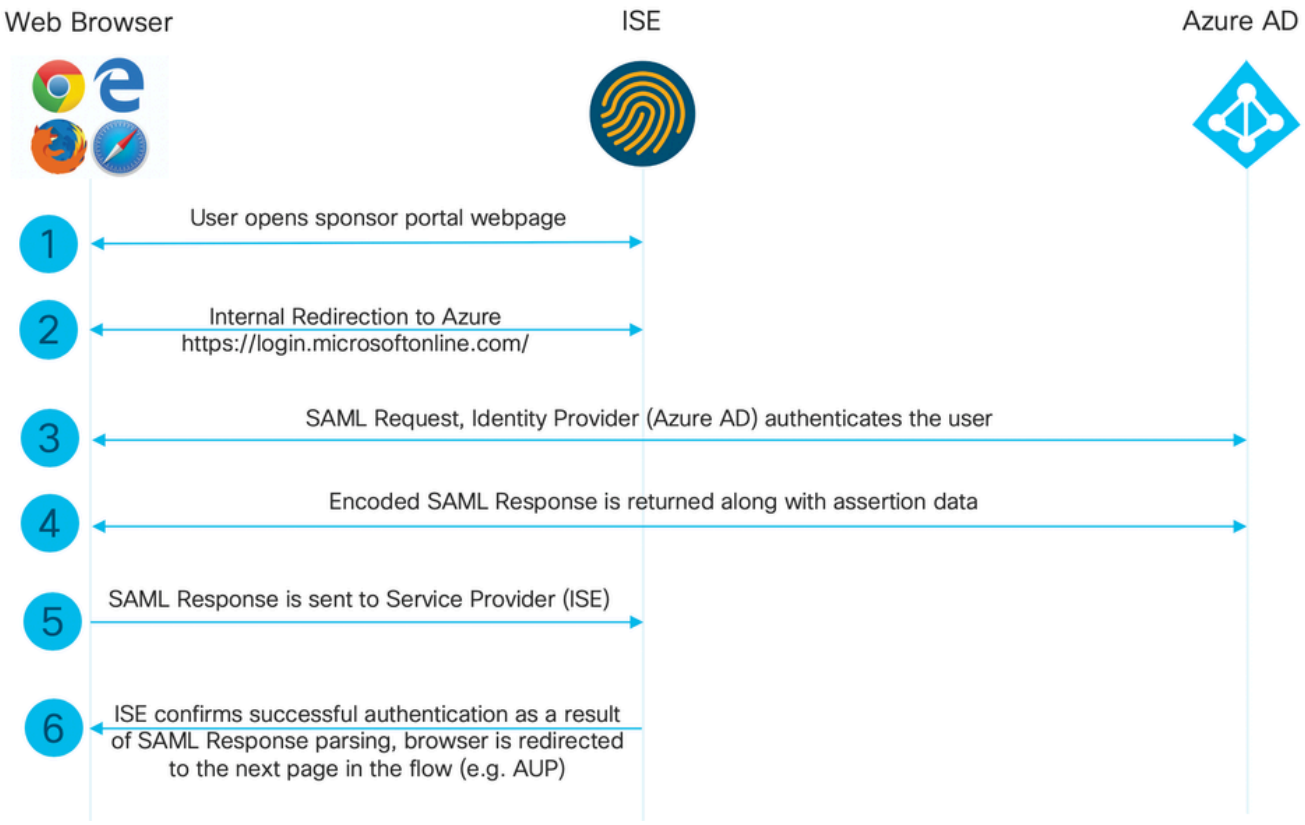
使用的组件

本文档中的信息基于下列硬件和软件版本：

- Cisco ISE 3.4（此过程适用于Cisco ISE 3.1及更高版本）
- Microsoft Entra ID

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

高级流程图



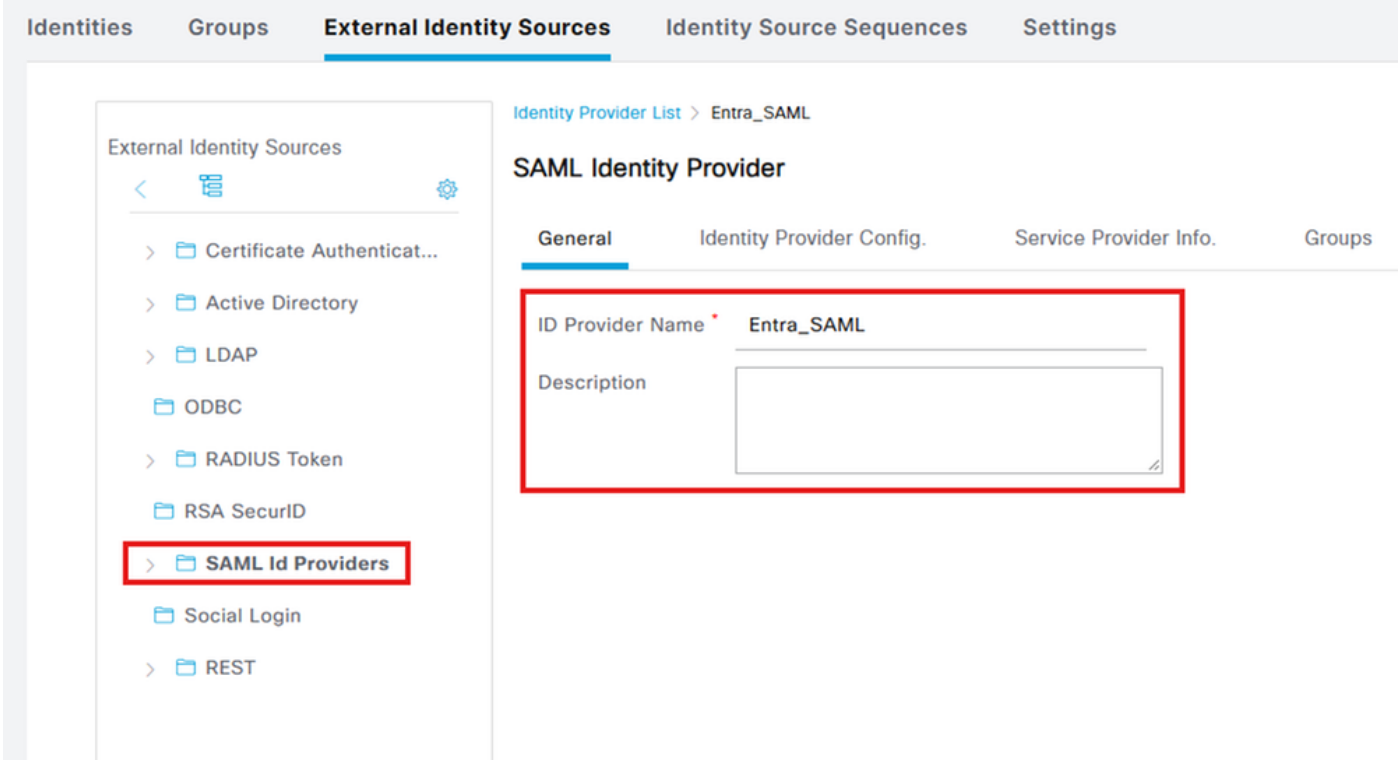
配置

步骤1.在ISE上配置SAML身份提供程序和发起人门户

添加SAML身份提供程序

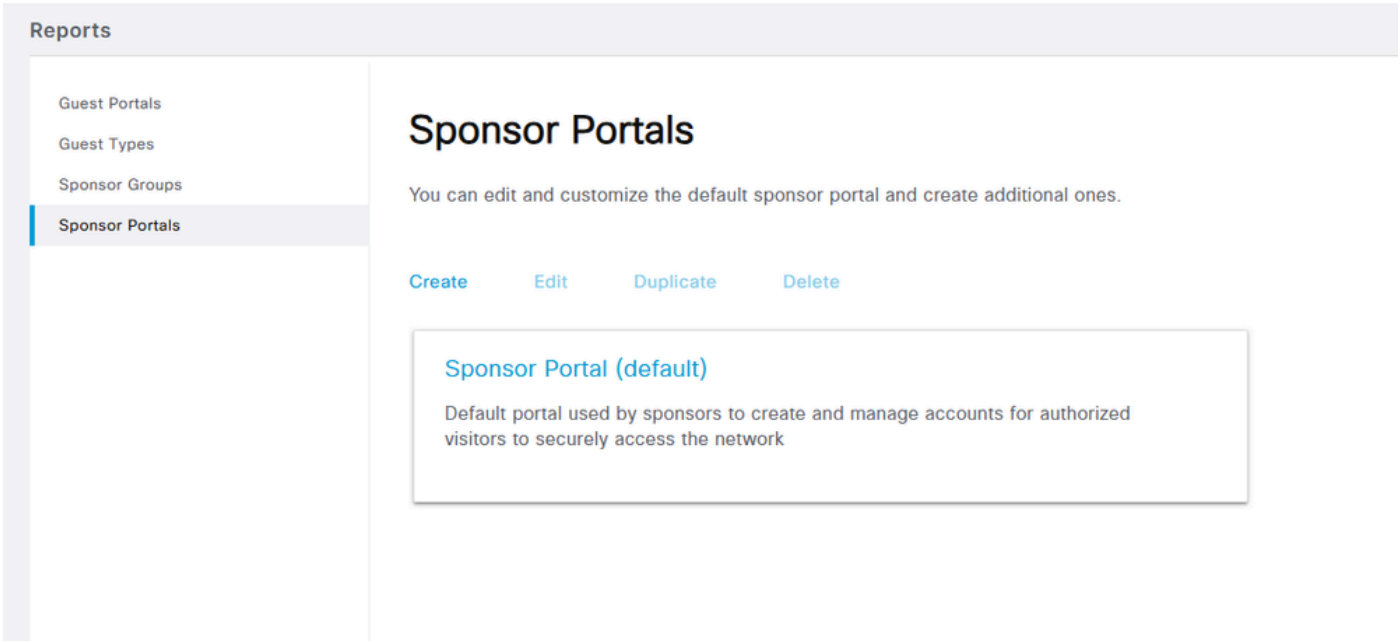
1.在ISE上，导航到管理>身份管理>外部身份源 > SAML Id提供程序，然后点击添加按钮。

2.输入ID提供方名称，然后单击提交以保存它。ID提供程序名称仅对ISE有效，如图所示。

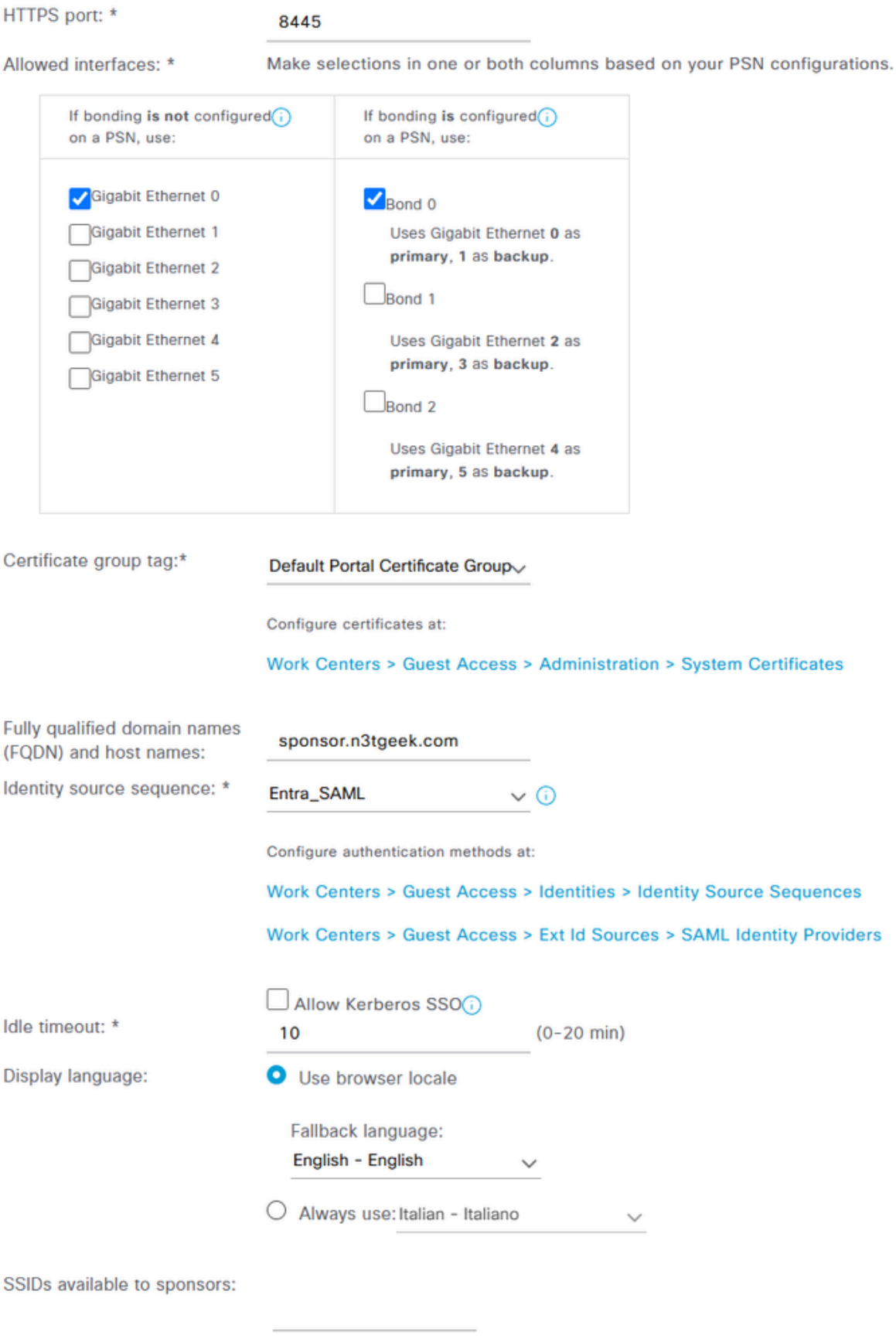


将发起人门户配置为idP

1.定位至工作中心>访客访问>门户和组件>发起人门户，然后选择发起人门户。在本示例中，使用保证人门户（默认）。



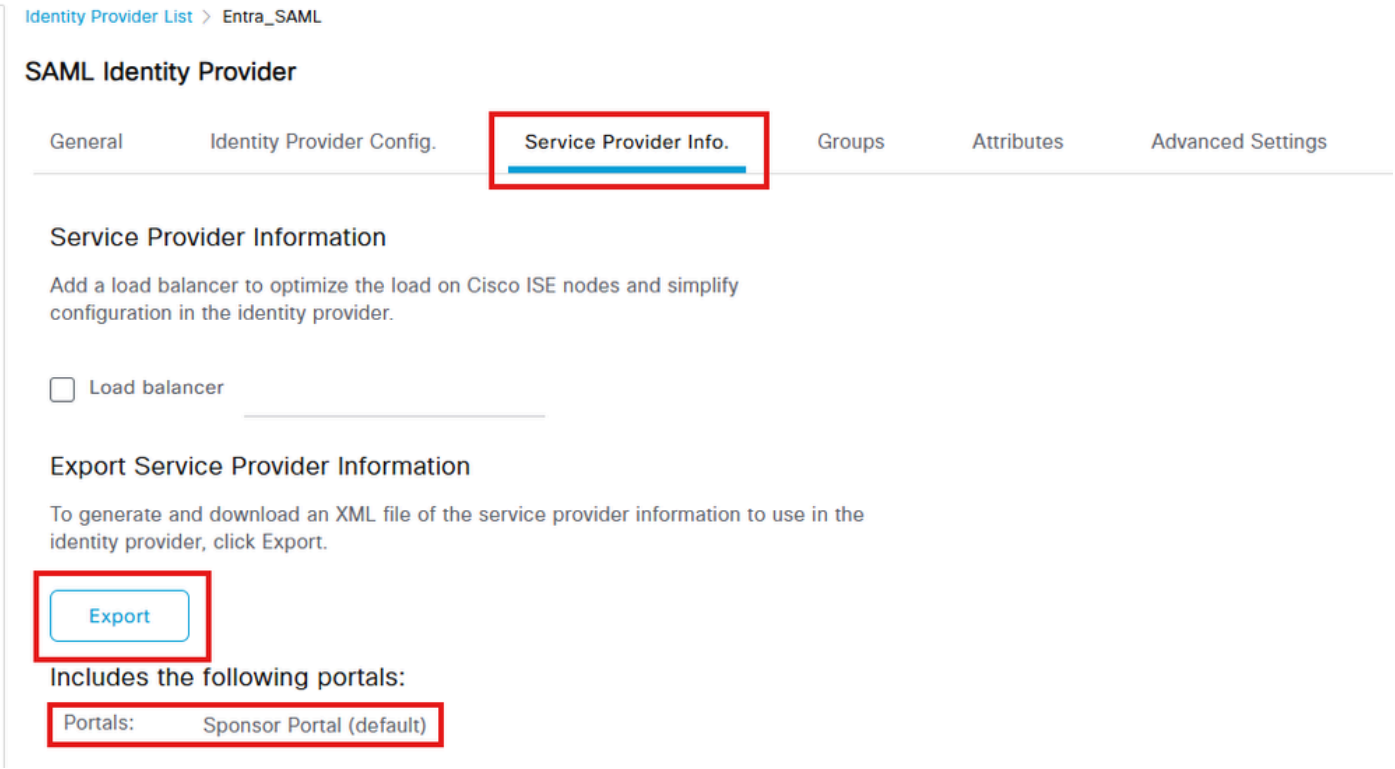
2.展开Portal Settings，然后在Identity Source Sequence中选择新的SAML身份提供程序。配置发起人门户的完全限定域名(FQDN)，并注意HTTPS端口（8445是发起人门户的默认值）。 Click Save.



导出服务提供商信息

1.导航回SAML提供商，然后打开“服务提供商信息”选项卡。确认发起人门户出现在“包括以下门户

”下 — 在导出之前，门户必须绑定到IdP，或者元数据不包括它。单击Export。



2.从下载的XML中，注意：

- entityID:例如，http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2。
- 每个AssertionConsumerService位置(每个节点名称/IP一个 — 独立节点生成三个；多节点部署产生更多)。
- SingleLogoutService ResponseLocation:保证人门户 — 注销响应

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" ...>
    <md:KeyDescriptor use="signing">
      <ds:X509Certificate>MIIFUDCC...(ISE portal signing certificate)...</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutRequest.action?portal=1f789a0
        ResponseLocation="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutResponse.action"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    ...(additional NameIDFormat entries)...
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action" index="0"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://192.168.1.204:8445/sponsorportal/SSOLoginResponse.action" index="1"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://prox-ise04.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action" index="2"/
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

⚠ 警告：XML还包含SOLogoutRequest.action?portal=...位置属性中的URL。这不是在Entra ID中用作“注销URL”的值 — 使用该值会导致“故障排除”部分中描述的“SSO注销失败”错误。正确的值以SSOLogoutResponse.action结尾。

✎ 注意：无论何时进行以下任何更改，都会重新导出并重新导入此元数据：注册新的ISE节点，节点主机名或IP更改，发起人门户FQDN更改，端口或接口设置更改，或关联负载均衡器。如果IdP保留过时的元数据，则拒绝身份验证请求。导出的ZIP还包含自述文件，其中包含每IdP配置说明。

根据XML文件：

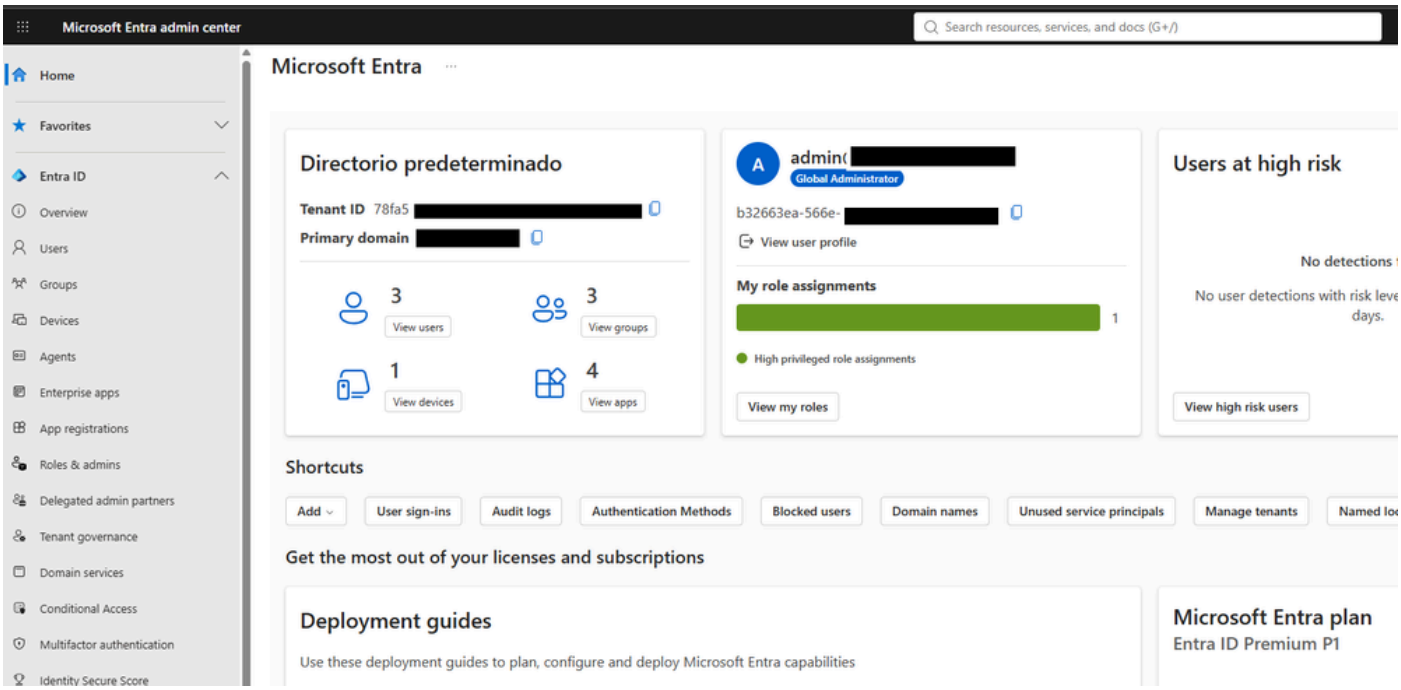
SingleLogoutService
ResponseLocation=https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutResponse.action
entityID="http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2”
AssertionConsumerService
Location="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action"
AssertionConsumerService
Location="https://192.168.1.204:8445/sponsorportal/SSOLoginResponse.action”
AssertionConsumerService Location="https://prox-ise04.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action"

✎ 注意：本实验使用单个ISE节点，因此导出的XML仅包含节点三个AssertionConsumerService条目：发起人门户FQDN、节点IP和节点FQDN。在多节点部署中，XML列出为发起人门户提供服务的每个节点的条目（门户FQDN，以及每个节点的IP和FQDN）。 将所有这些URL添加为Entra ID中的Reply URL，而不仅仅是一个节点的URL。如果回复URL中缺少节点的URL，当用户重定向到该节点时，身份验证失败。

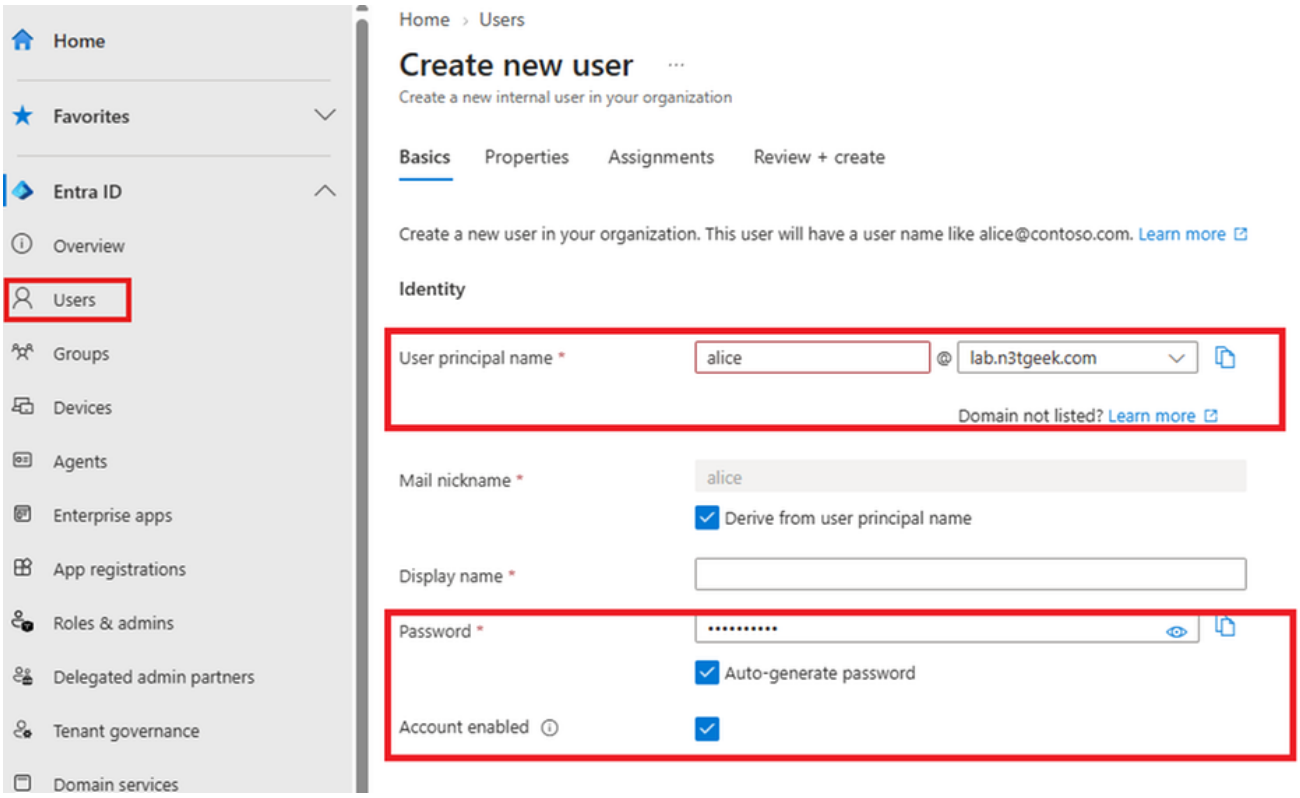
步骤2.配置Microsoft Entra ID

创建Azure AD用户

1.登录到Microsoft Entra管理中心。



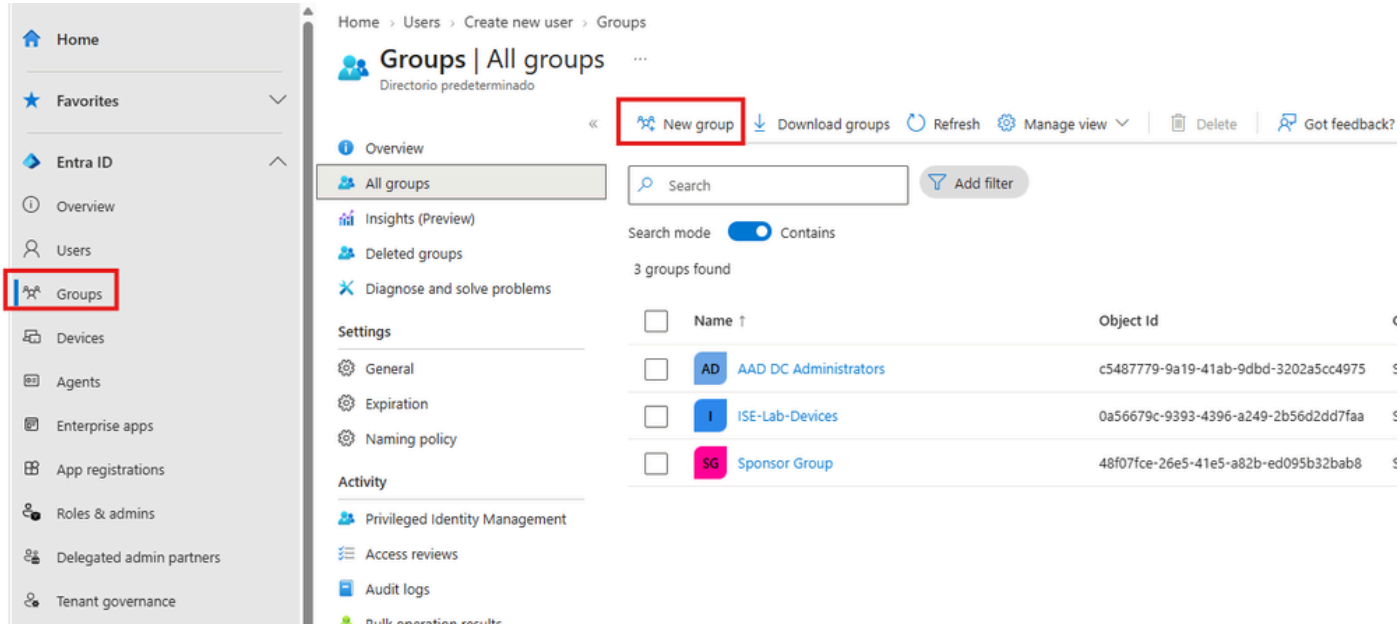
2.定位至Entra ID >用户>新用户>创建新用户，然后创建仅云测试用户。



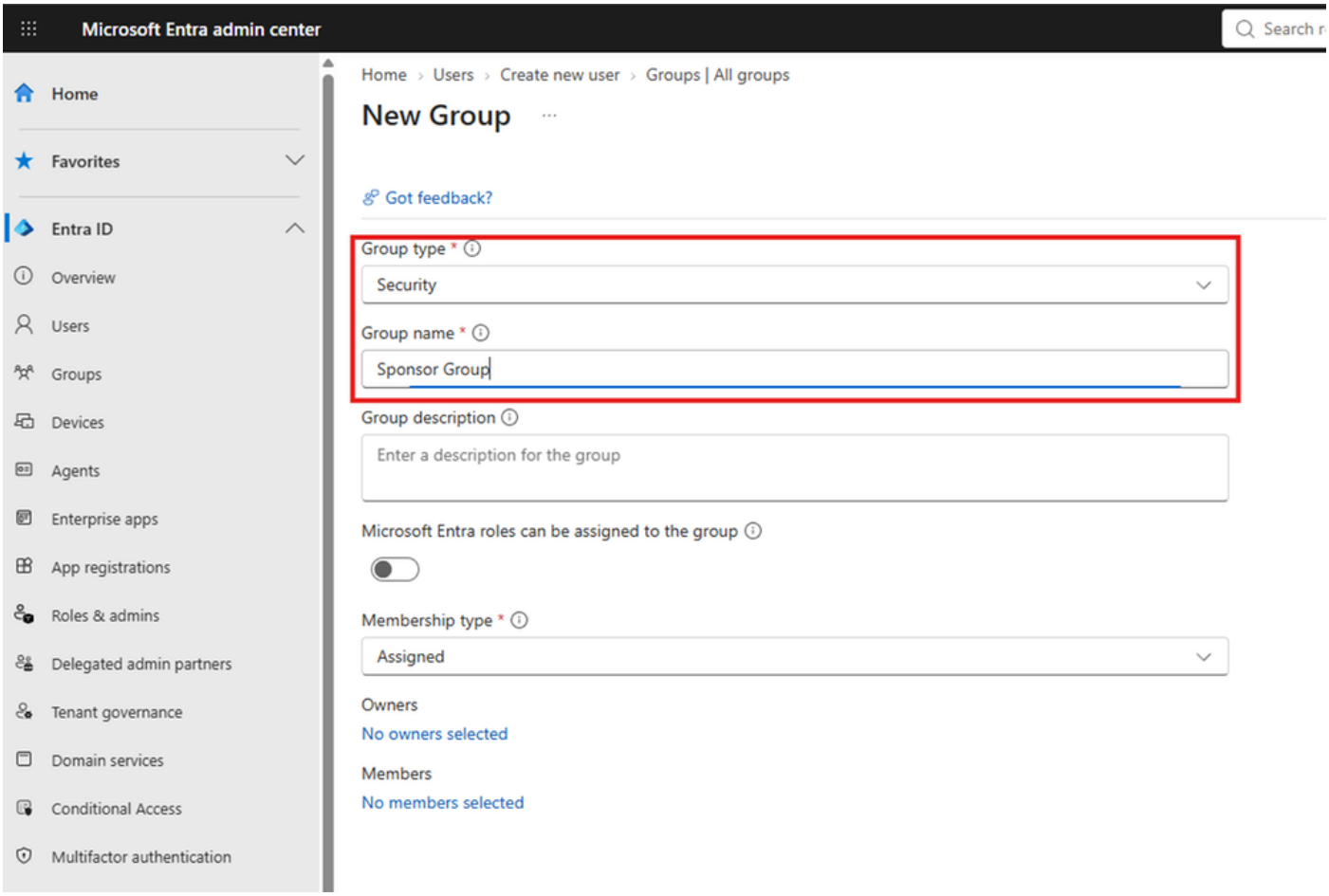
注意：使用仅云成员用户，而不是邀请的访客 — 访客根据他们的主租户进行身份验证，生成的NameID格式会阻止ISE提取用户名。新用户必须在首次登录时更改密码，具有安全默认值的租户也需要MFA注册；在Verify部分之前完成这两项。

2.创建组并添加用户

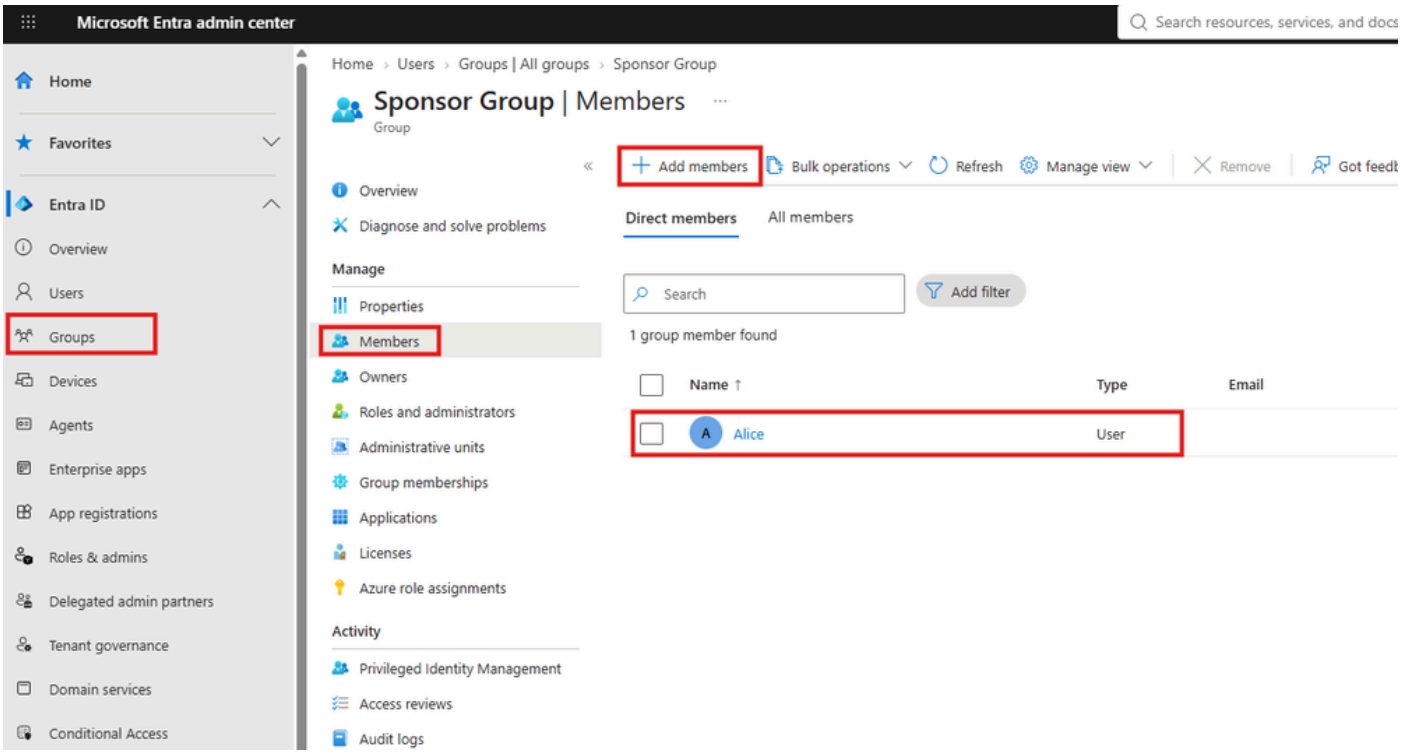
1.定位至Entra ID >“组”>“新建组”。



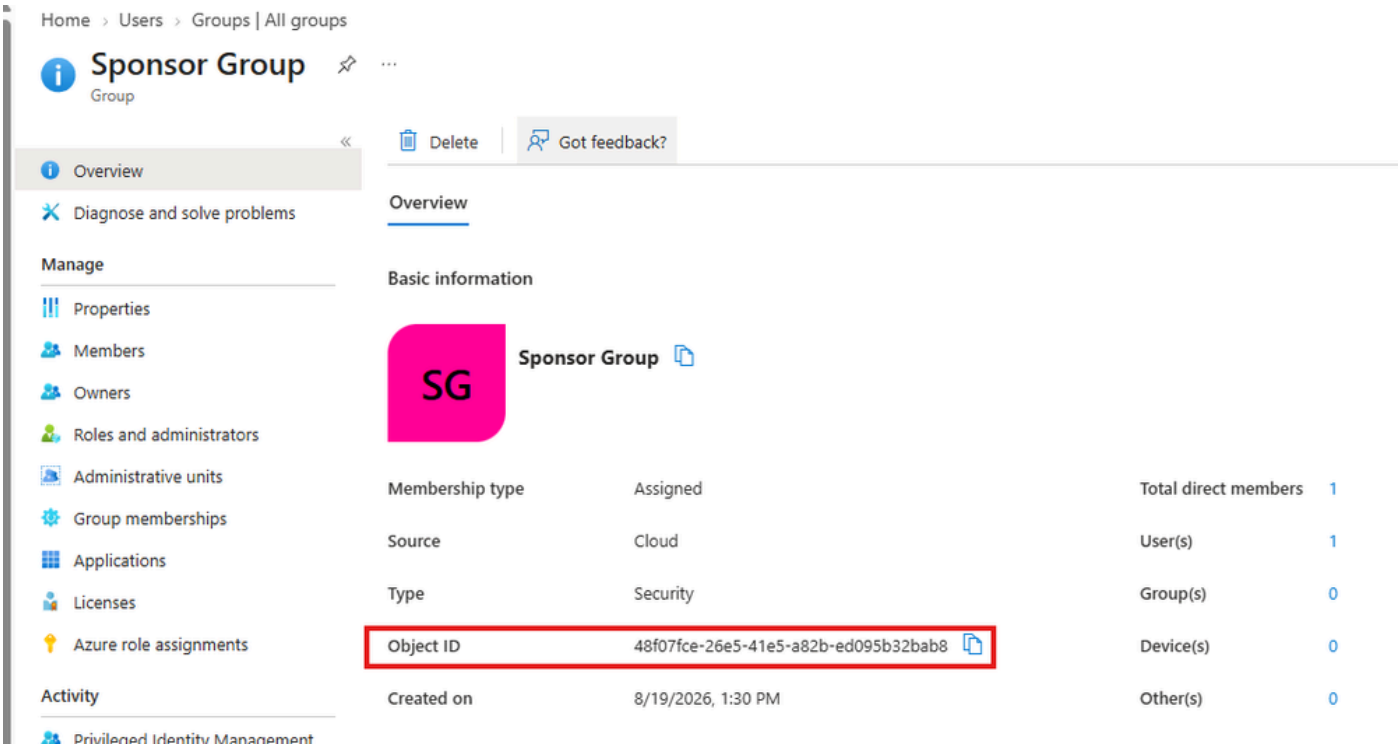
2.将组类型保留为Security。配置组名称，如图所示：



3.打开“组成员”页，单击“添加成员”，搜索测试用户，选择它，然后单击选择。

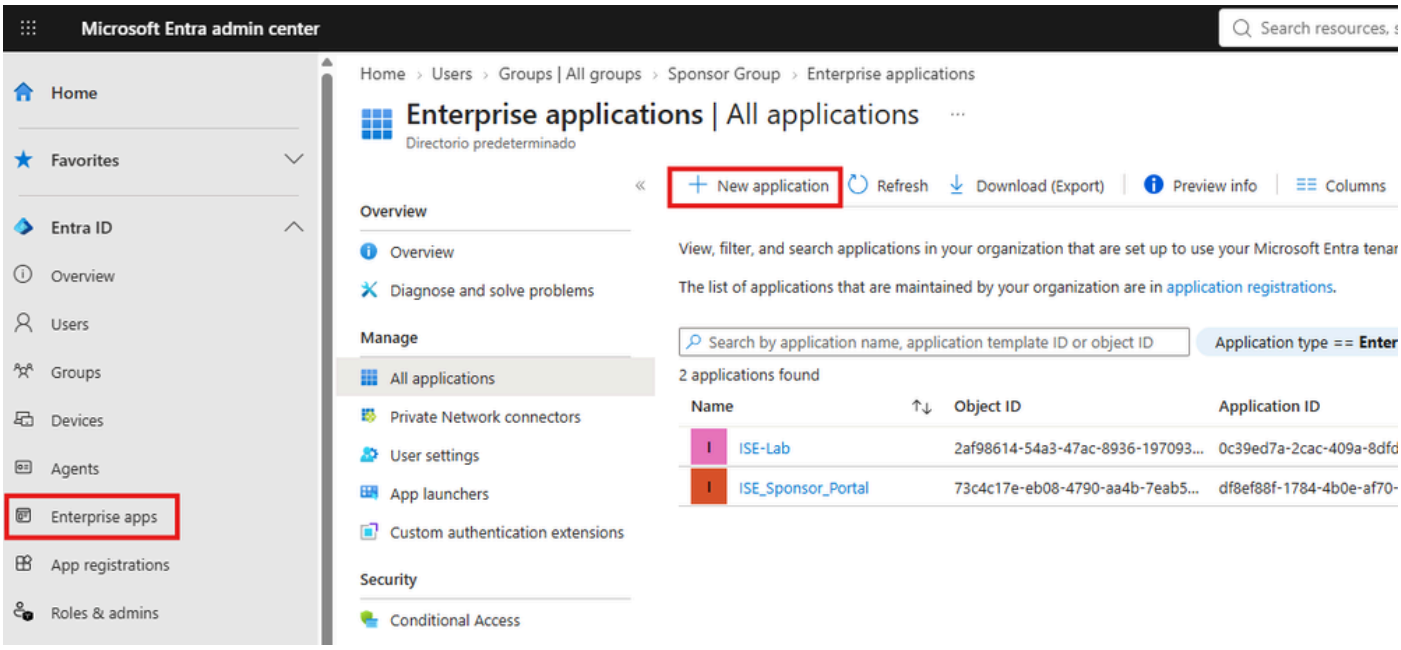


4.记下Group Object ID，在此屏幕中，发起人组的值为48f07fce-26e5-41e5-a82b-ed095b32bab8。

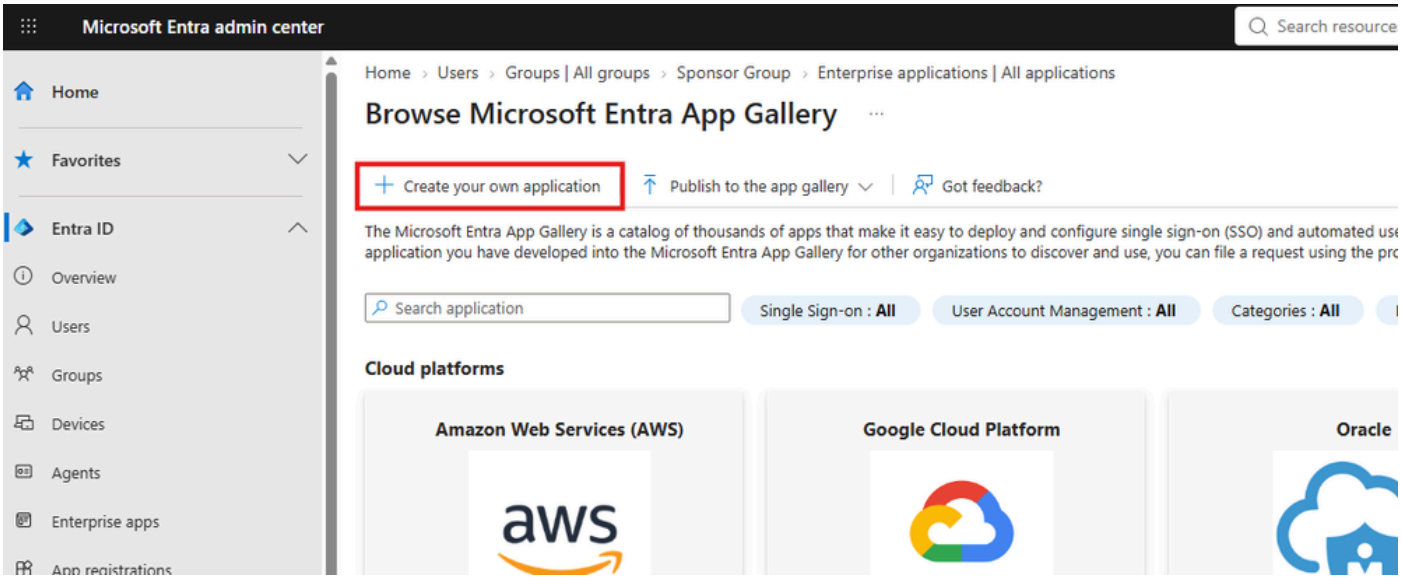


3.创建Entra Enterprise应用程序

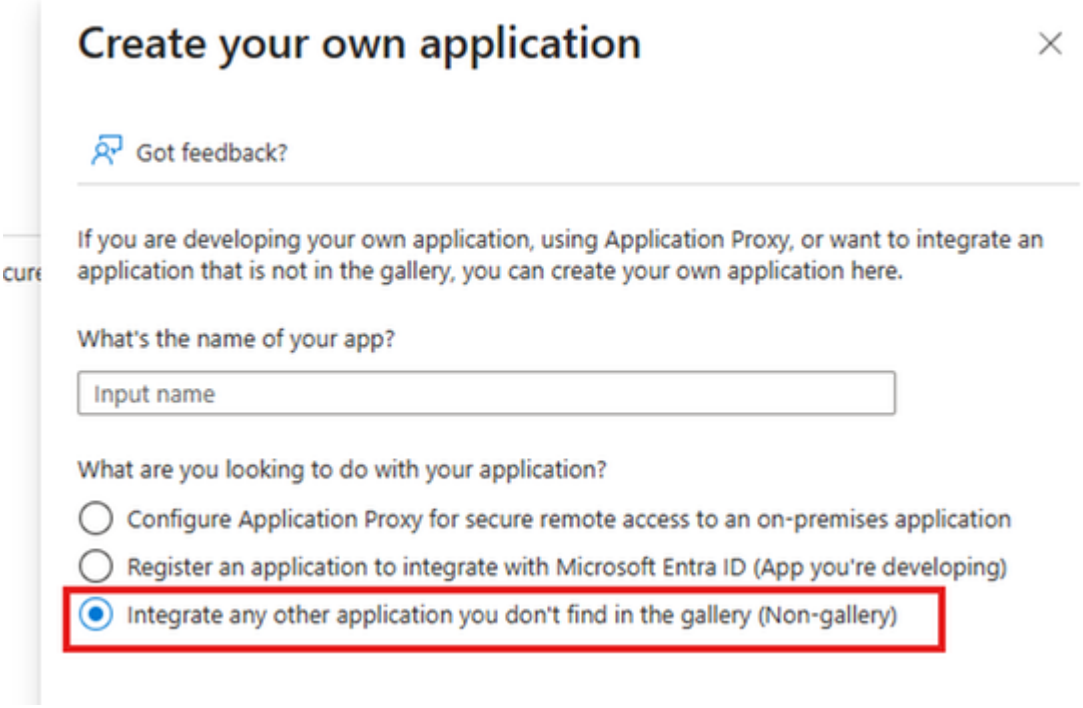
1.定位至Entra ID >企业应用>所有应用>新应用。



2.选择“创建自己的应用程序”。

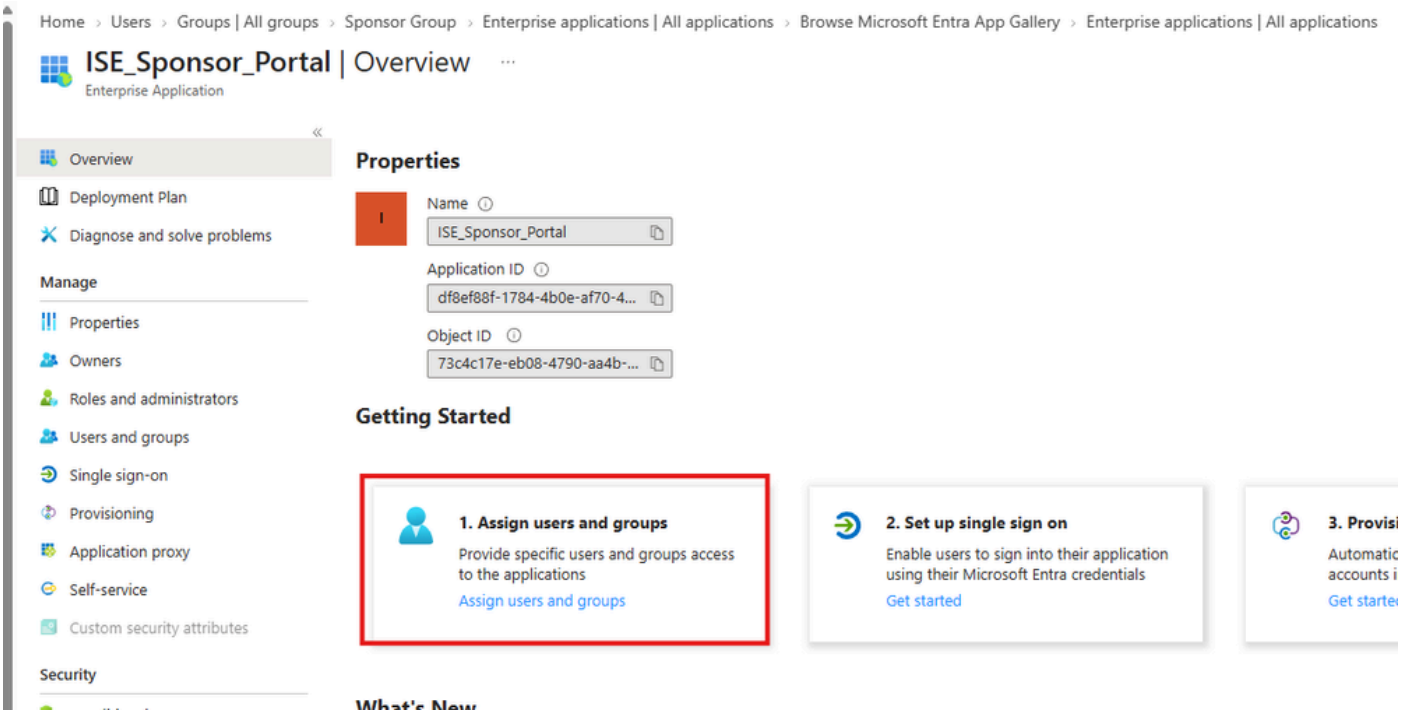


3.输入名称，选择“集成未在库（非库）中找到的任何其它应用程序”，然后单击“创建”。



4.将组（或用户）分配给应用程序

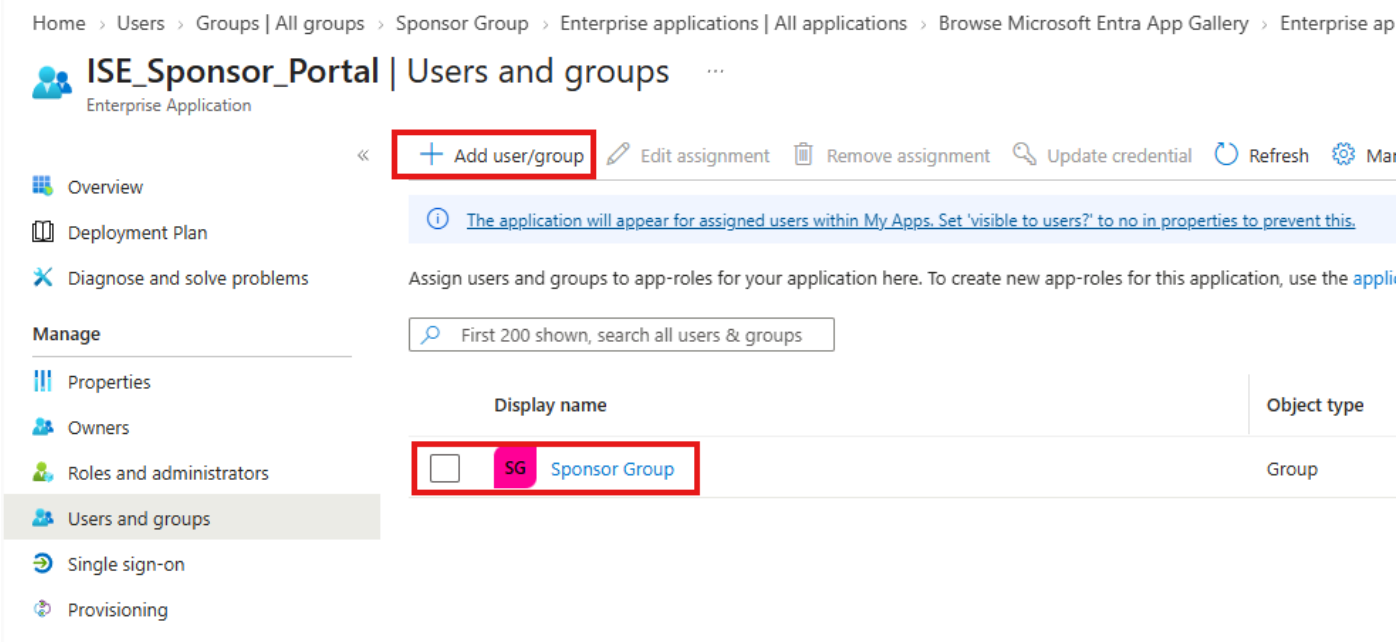
1.在应用程序中，导航到用户和组>添加用户/组，然后分配之前创建的组。



添加用户/组：

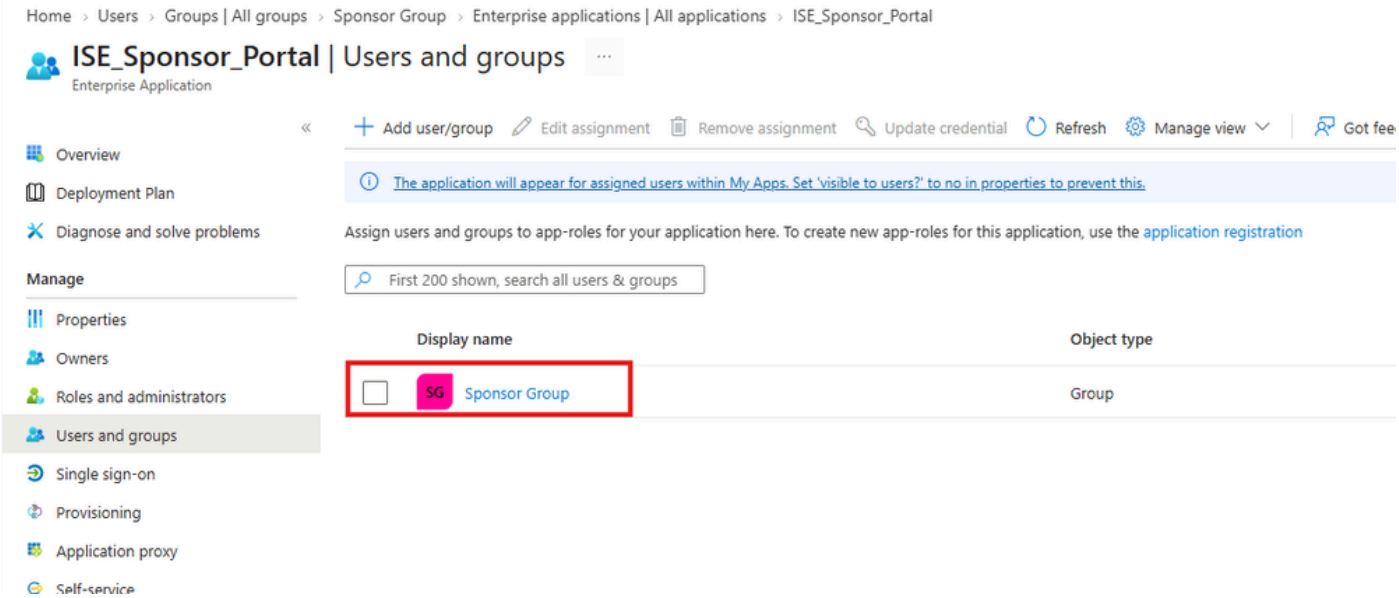
注意：如果您的租户在Microsoft Entra ID Free上，则组分配不可用 — 改为直接分配测试用户

；其他每个步骤都是相同的。



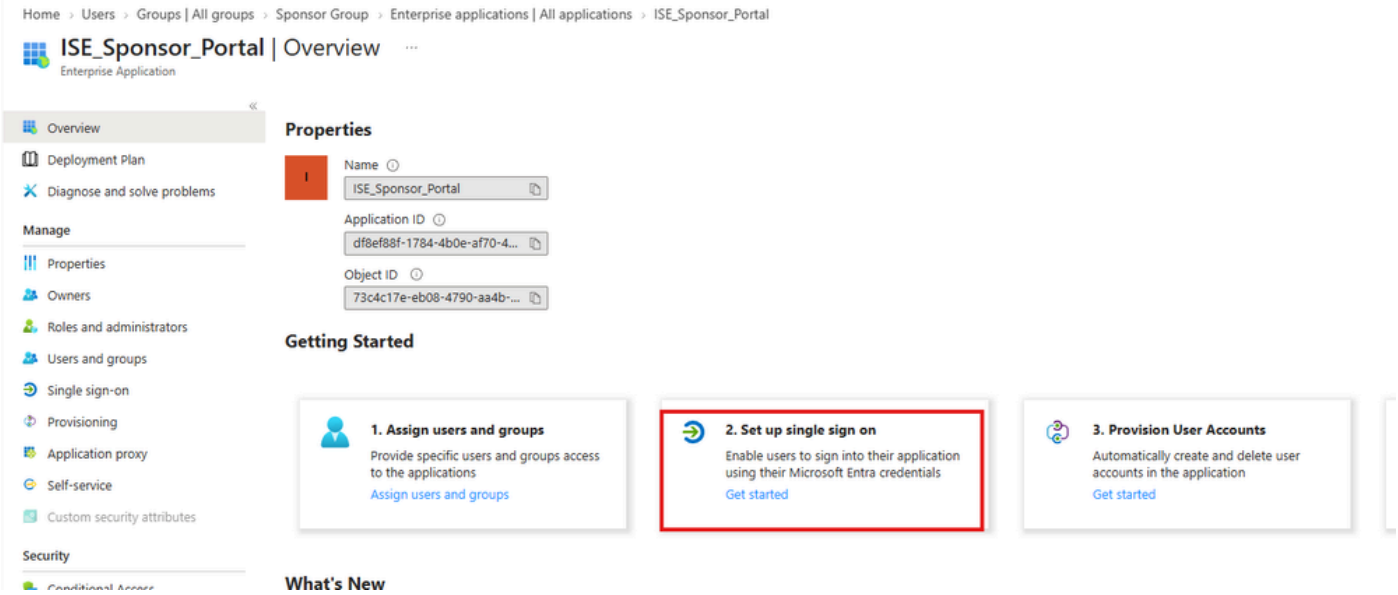
注意：您应选择要应用访问权限的正确用户或组。

1.因此，应用程序的“用户和组”菜单必须填写所选组。

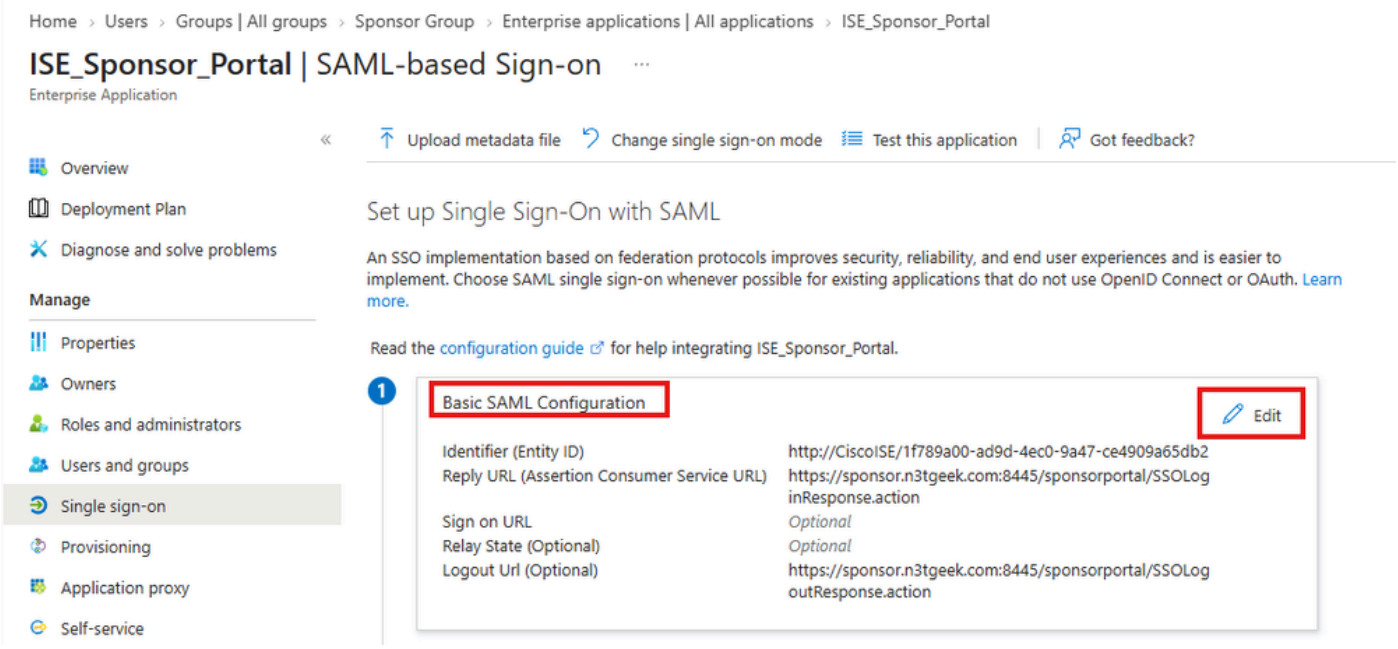


步骤3.在Entra ID中配置SAML单点登录

1.在应用程序中，导航至设置单点登录。



2.选择SAML，然后单击基本SAML配置旁边的编辑。



3.使用ISE SP元数据XML中的entityID值填充标识符（实体ID），并使用其中列出的每个AssertionConsumerService位置填充回复URL。对于Logout Url，请使用SingleLogoutService ResponseLocation值。将Sign-on URL（登录URL）和Relay State（中继状态）留空，然后单击Save。

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2	☑

Add identifier

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://prox-ise04.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action		☐
https://192.168.1.204:8445/sponsorportal/SSOLoginResponse.action		☐
https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action		☑

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

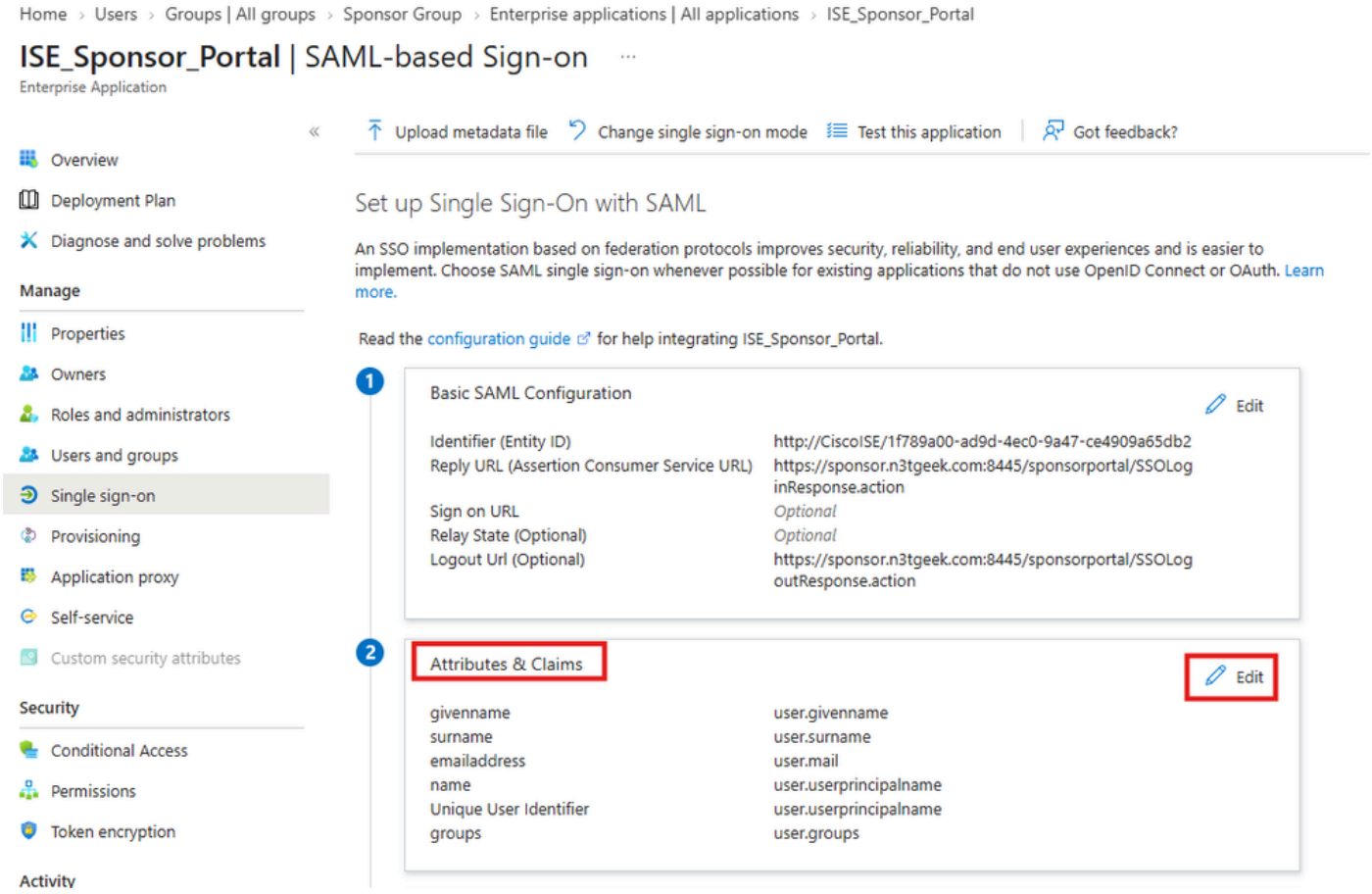
This URL is used to send the SAML logout response back to the application.

https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutResponse.action

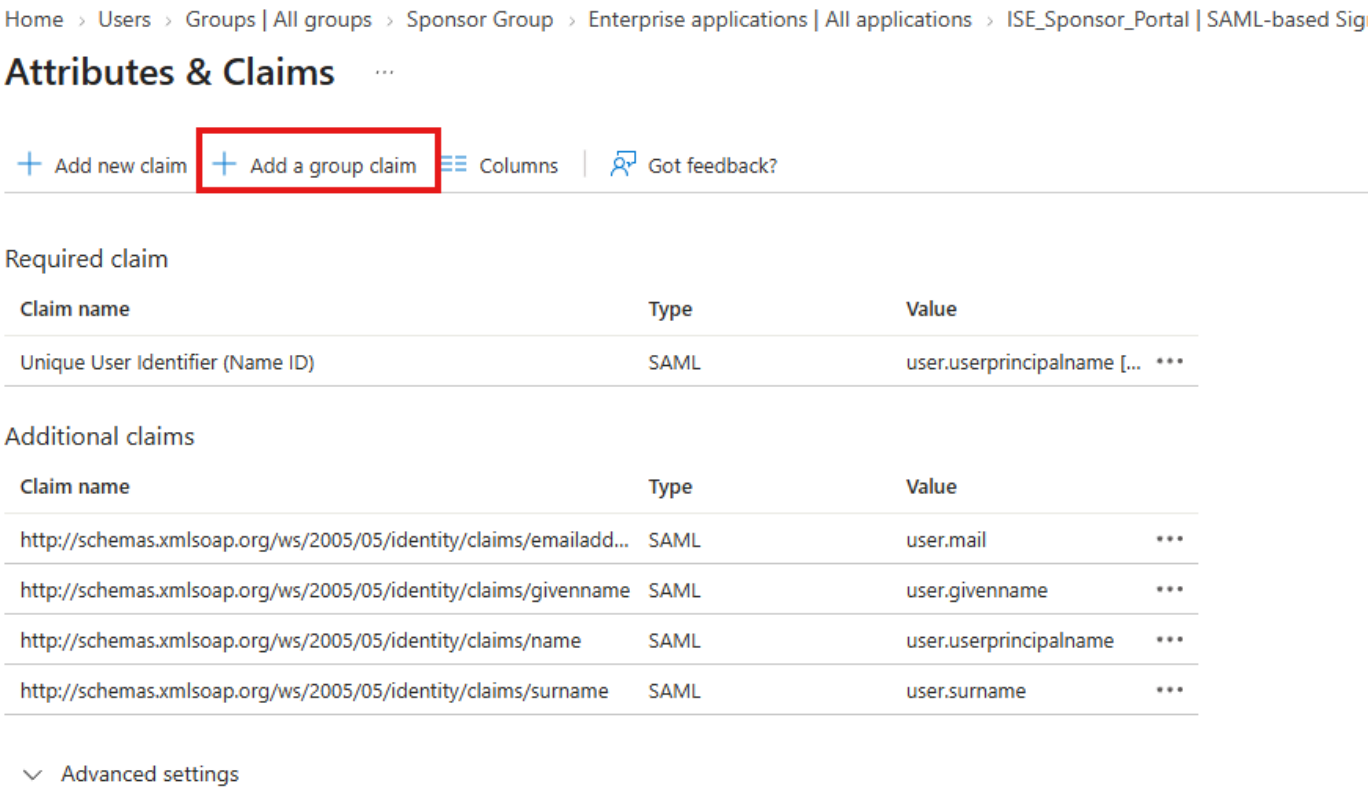
注意：回复URL用作传递列表，允许某些URL在重定向到IdP页面时用作源。

2.配置Entra组属性

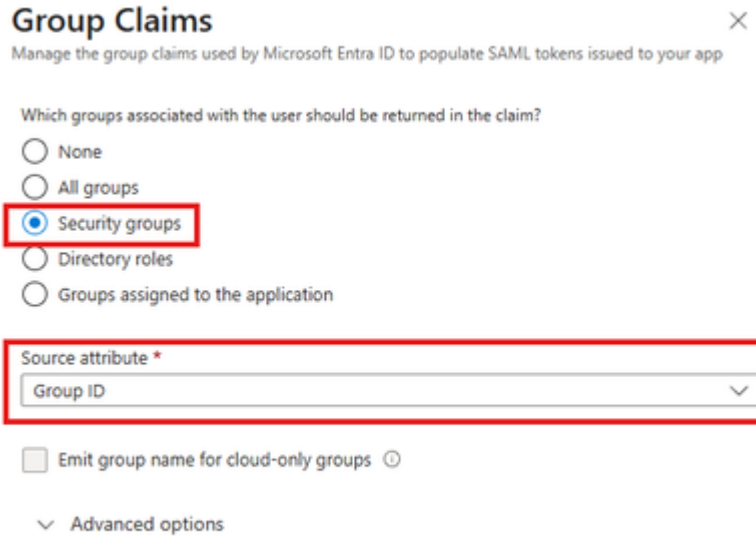
1.点击属性和领款申请旁边的编辑。



2.然后添加组声明。

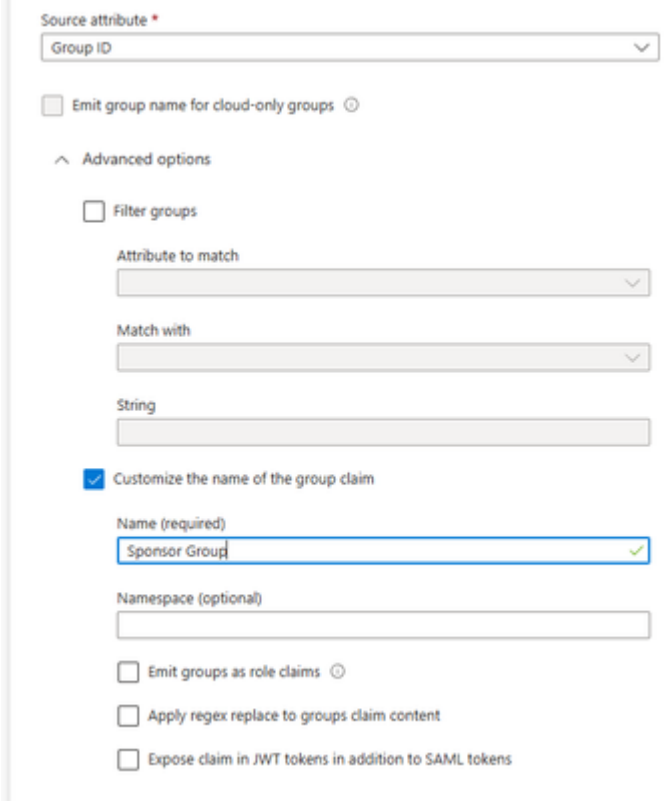


3.选择Security groups和Source attribute Group ID，然后单击Save。保留其他所有项目为默认值。

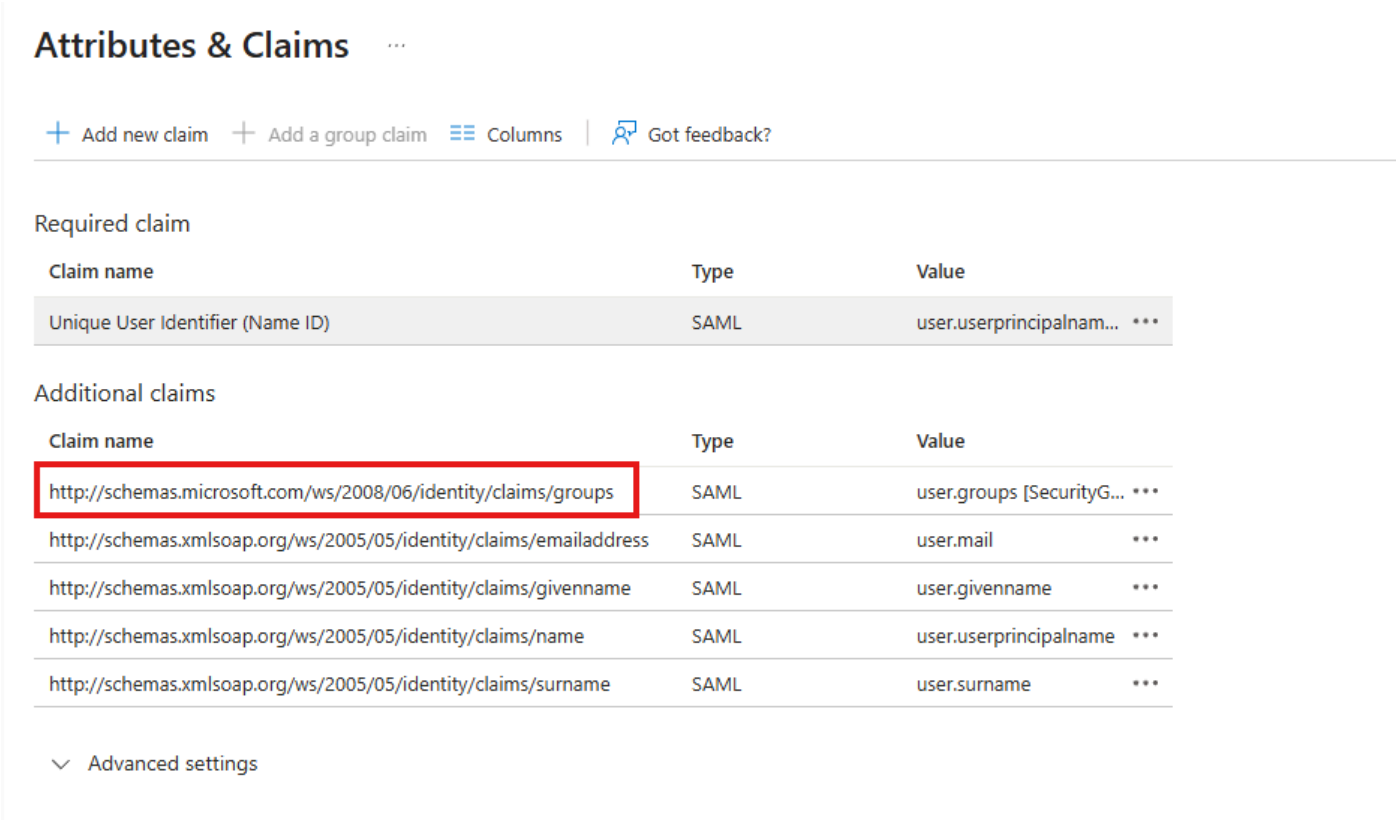


⚠ 警告：不要选中“自定义组声明的名称”。 重命名声明需要在ISE组成员资格属性字段中使用相同的自定义名称，本文档的其余部分采用默认声明名称。

4.如果仍要自定义它，则可以，但必须在ISE的“组成员属性”字段中输入相同的自定义名称。例如，如果您在Entra ID中输入Sponsor Group，则ISE字段必须正好包含Sponsor Group。在Entra ID中，设置如下所示：

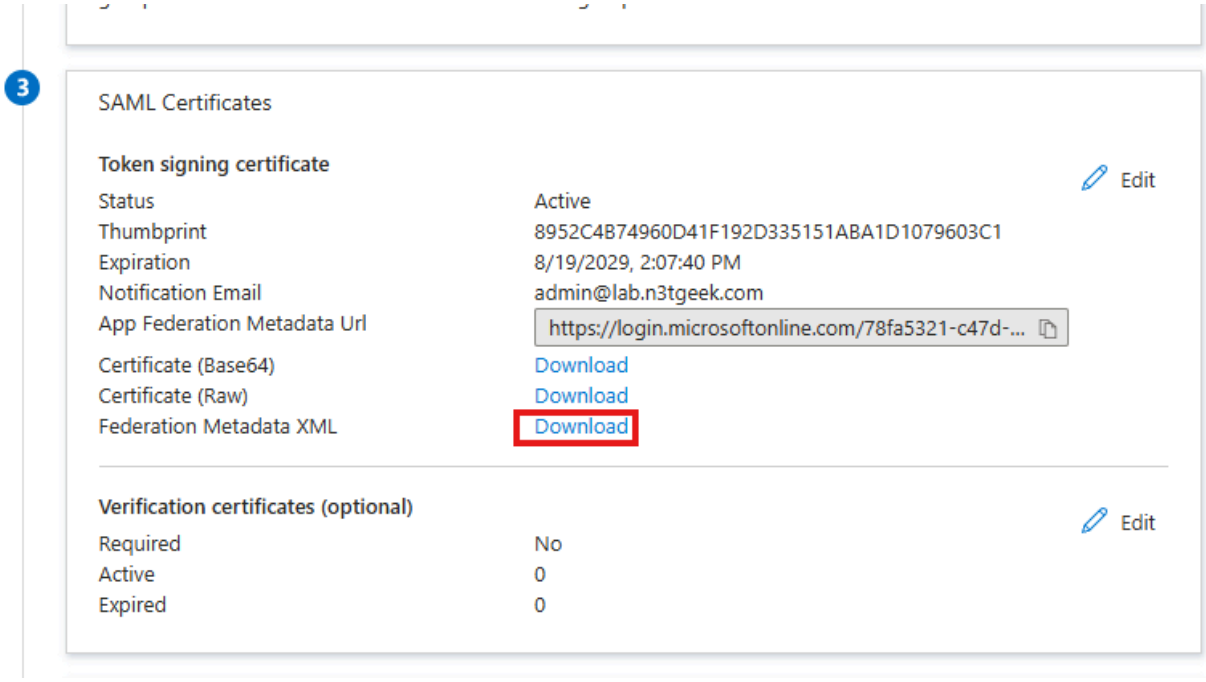


5.记录该组的索赔申请名称。



3.下载联合元数据XML文件

1.在SAML签名证书中单击Download对联合元数据XML。



2.下载的联盟元数据由Microsoft签名并包含ISE所需的所有内容；idP实体ID、SSO/SLO终端和令牌签名证书（缩写如下）：

```
    ...(signed by Microsoft)...

 ...(WS-Fed RoleDescriptor sections – not used by ISE)...

      MIIC8DCC...(Entra ID token signing certificate)...
```

3.在导入时（第4步），这些字段将成为单点登录/注销URL和“身份提供程序配置”选项卡中的签名证书条目。

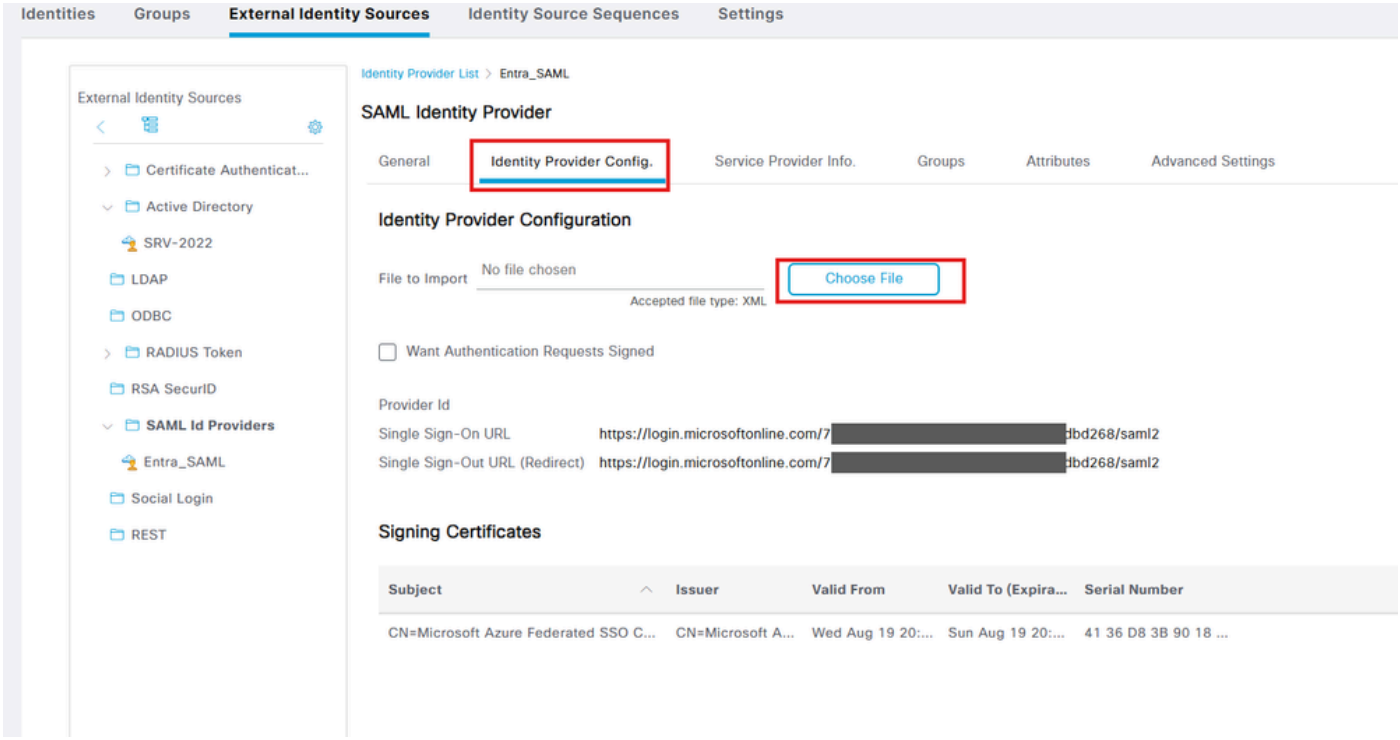
注意：Entra ID令牌签名证书的有效期为三年。当它旋转时，请再次下载联合元数据XML并将其重新导入到ISE中，或SSO突然停止工作。在证书上配置通知邮件以获取过期警告。

步骤4.将元数据从Entra上传到ISE

导入联合元数据

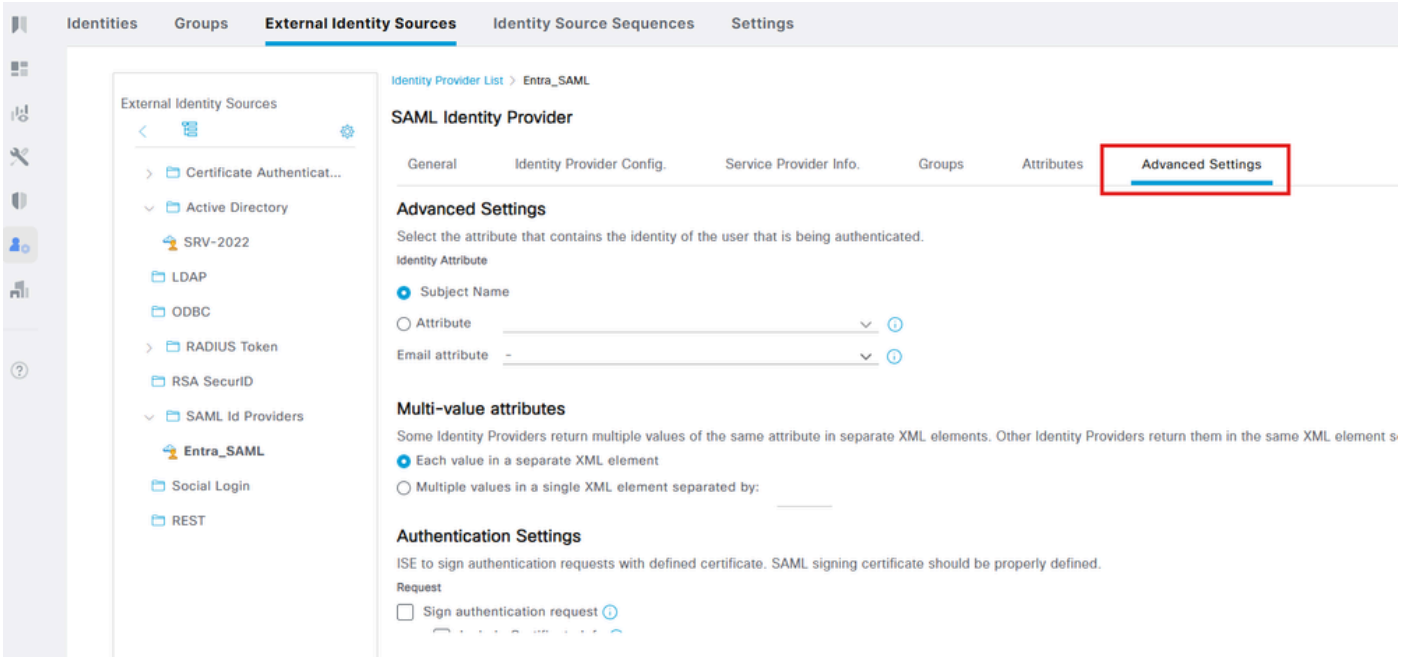
1.导航到管理>身份管理>外部身份源> SAML Id提供程序> [您的提供程序]，打开身份提供程序配置选项卡，单击选择文件，选择联合元数据XML，然后单击保存。系统将填充单点登录/注销URL和签名证书。

注意：即使导入并保存元数据文件，此选项卡中的提供程序ID字段仍留空。这是Cisco Bug ID CSCvv74517跟踪的仅显示问题。IdP实体ID存储正确并在运行时使用，并且可以在ise-psc.log调试输出中确认为strong>IdP URI。



注意：当前ISE版本导出的SP元数据声明WantAssertionsSigned="false"（旧版本声明为true）；该属性现在位于Advanced Settings选项卡中的Require Assertions Signed复选框（默认情况下未选中）。这并不意味着接受未签名的断言。ISE始终在SAML响应或断言上至少需要一个签名，即使这两个复选框均未选中。

可选的高级设置选项卡:身份属性(默认：Subject Name)选择提取用户名的位置；如果发起人过滤待审批的访客列表，则必须配置Email属性；Sign Authentication Request控制请求签名，并优先于上一个选项卡的只读“Want Authentication Requests Signed”复选框。

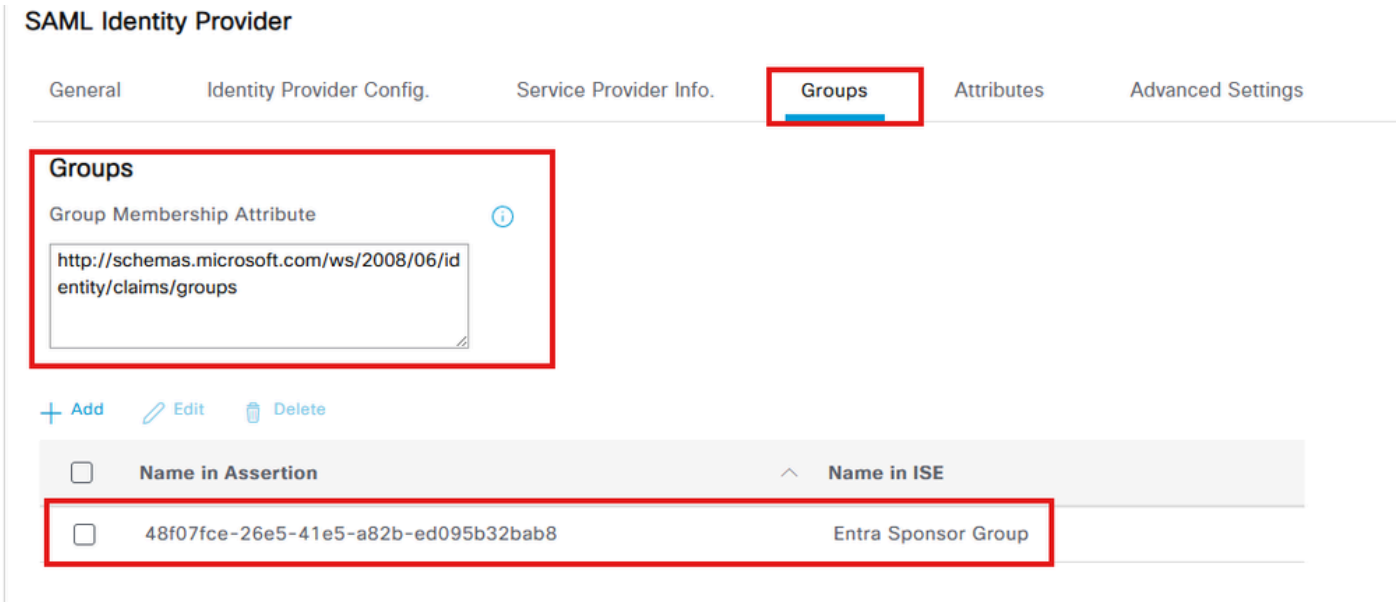


在ISE上配置SAML组

1.打开Groups选项卡，在Group Membership Attribute中，粘贴第3步中的声明名称：

```
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
```

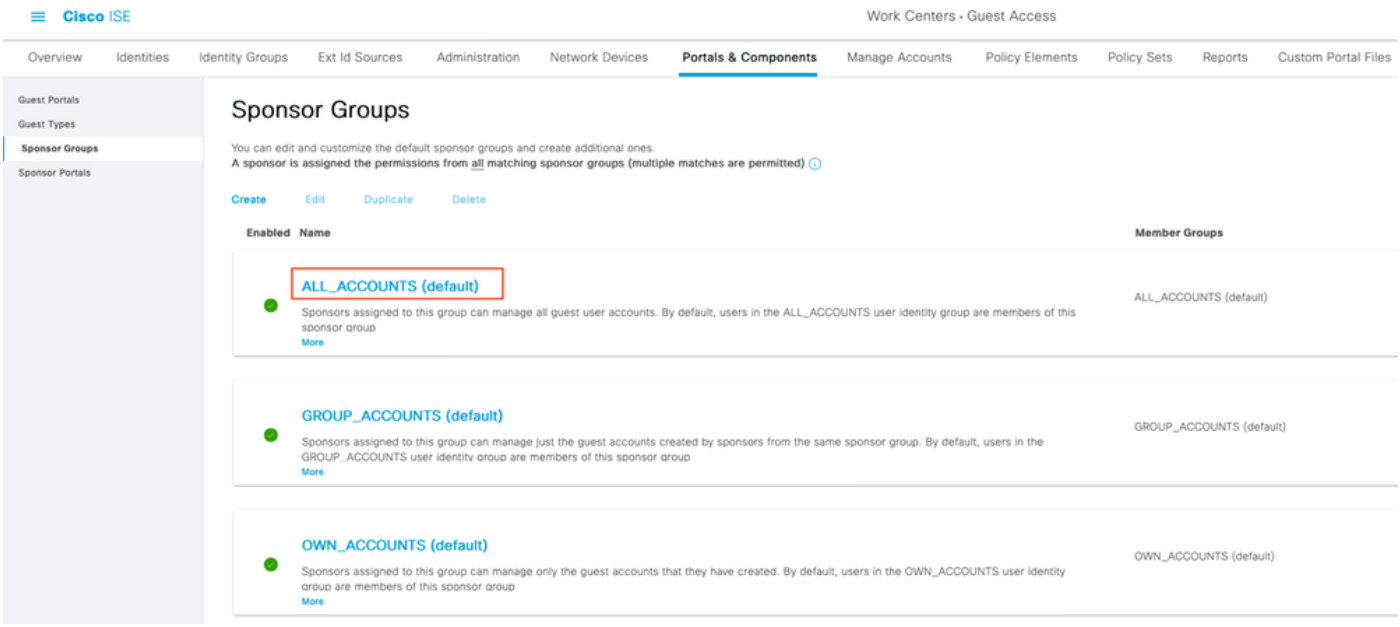
2.单击Add。在Name in Assertion中，输入第2步中捕获的组Object ID（该值必须完全匹配）。 在ISE的名称中，输入任何有意义的本地标签（仅在ISE菜单内使用的自由格式别名）。 单击OK，然后单击Save。



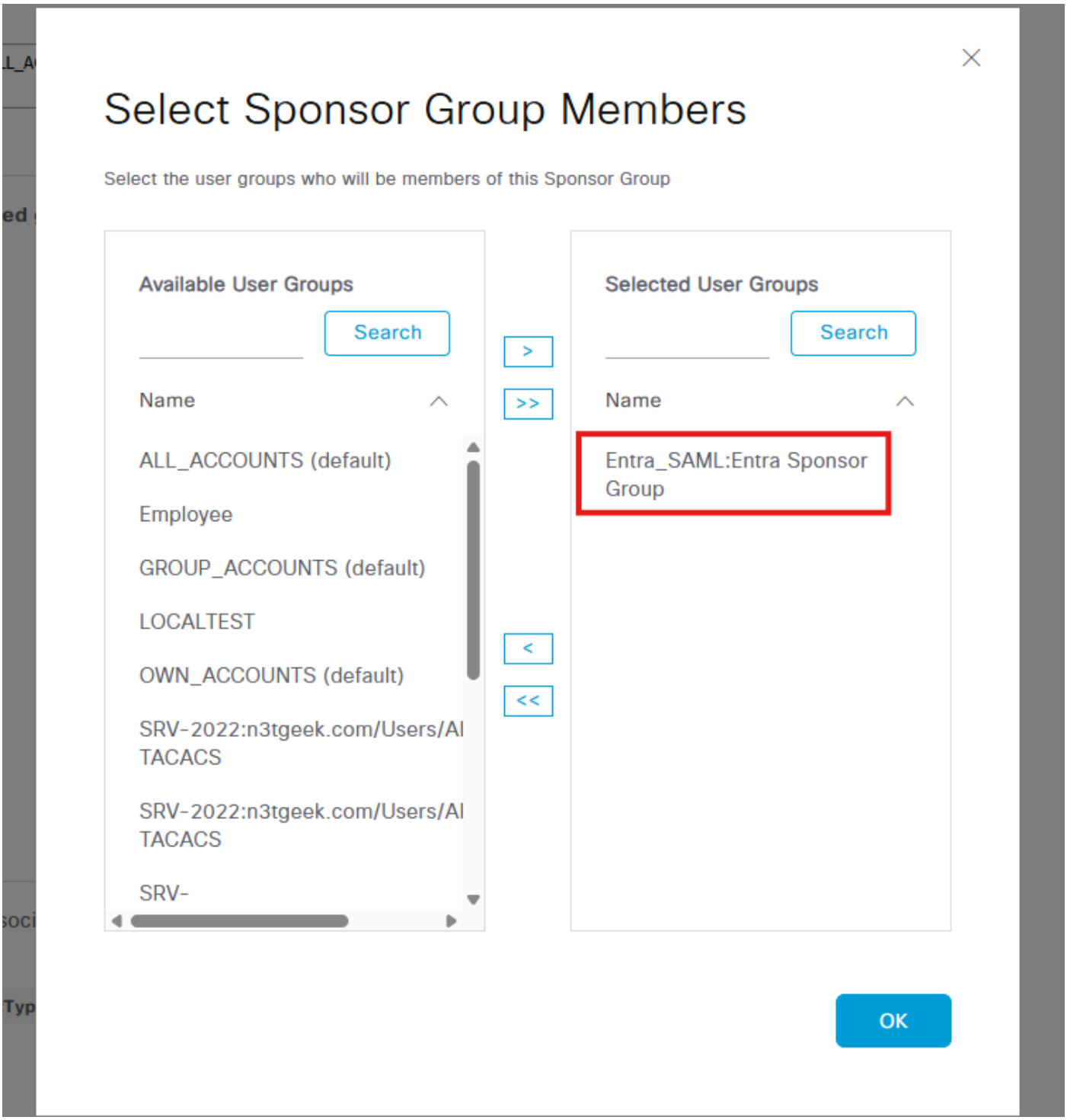
3.这将创建Entra中的组与可在ISE上使用的组名称之间的映射。

步骤5.在ISE上配置发起人组映射

1.定位至工作中心>访客访问>门户和组件>保证人组，然后选择要映射的保证人组。在本示例中，ALL_ACCOUNTS（默认）。



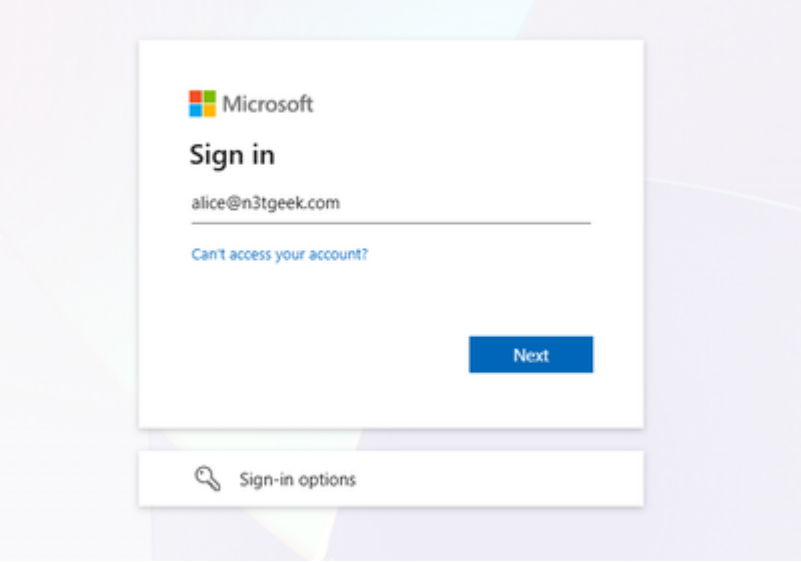
2.单击成员……，将ISE条目中的IdP:Name移动到Selected User Groups，单击OK,然后Save。



注意：为保证人分配所有匹配保证人组的权限。将Entra ID组映射到单个发起人组，除非需要累积权限。

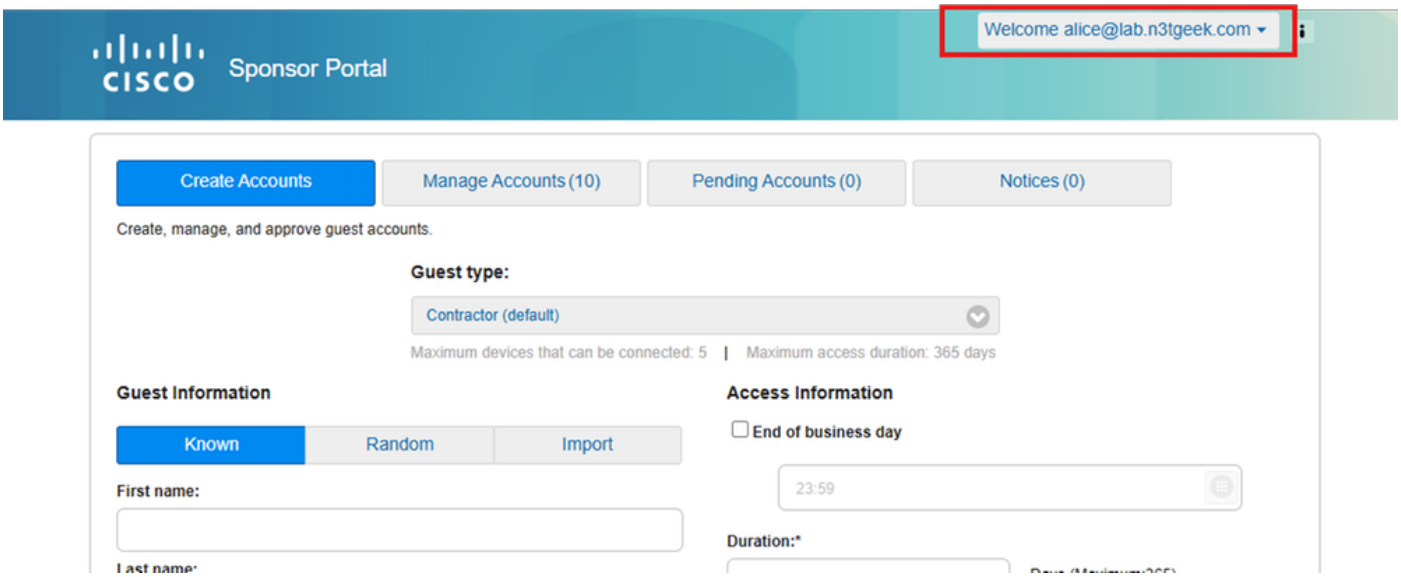
验证

1.从Portal Test URL（门户测试URL）链接启动Sponsor Portal。ISE重定向到Microsoft登录页面；使用测试用户凭证进行身份验证。

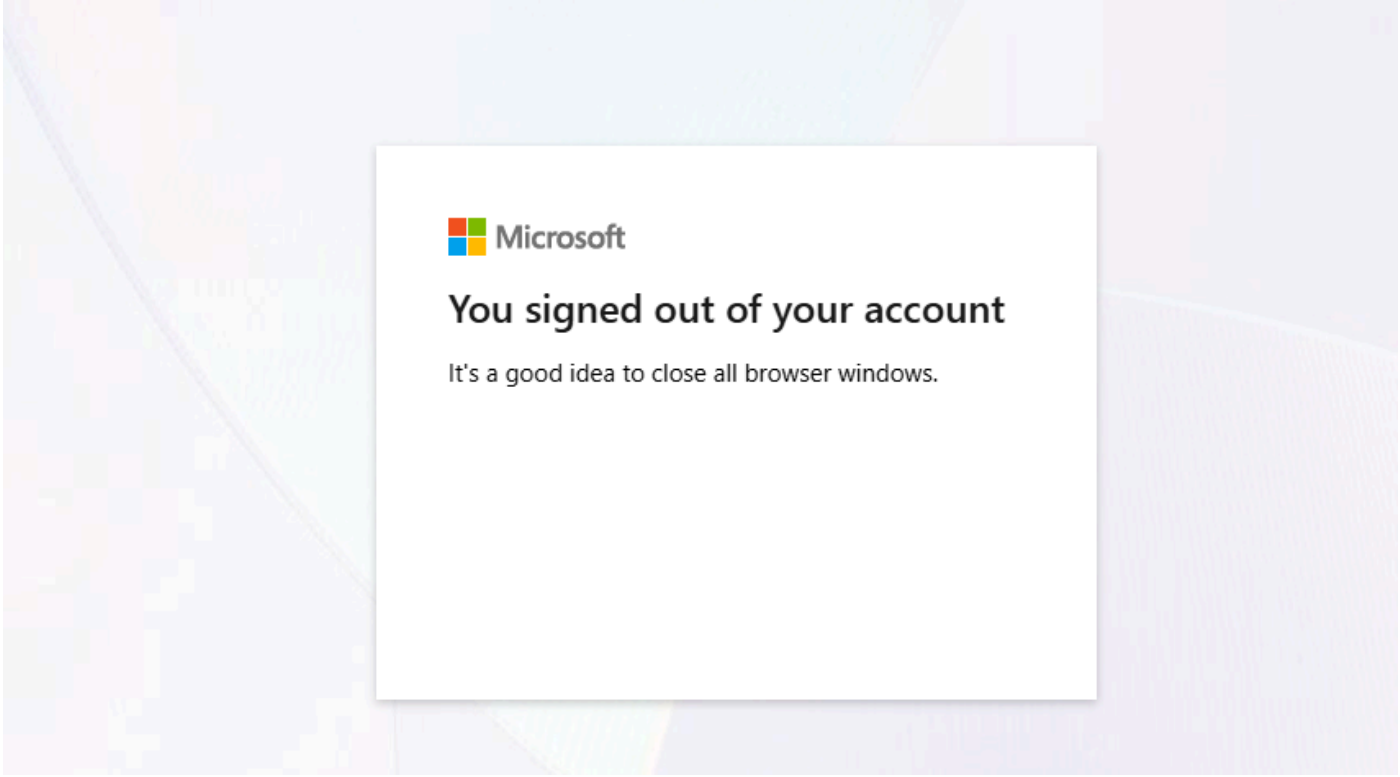


注意：新用户在首次登录时被迫更改用户密码。并且接受AUP验证步骤未涵盖此内容。验证包括用户首次登录后发起人(alice)已接受一次AUP的场景。

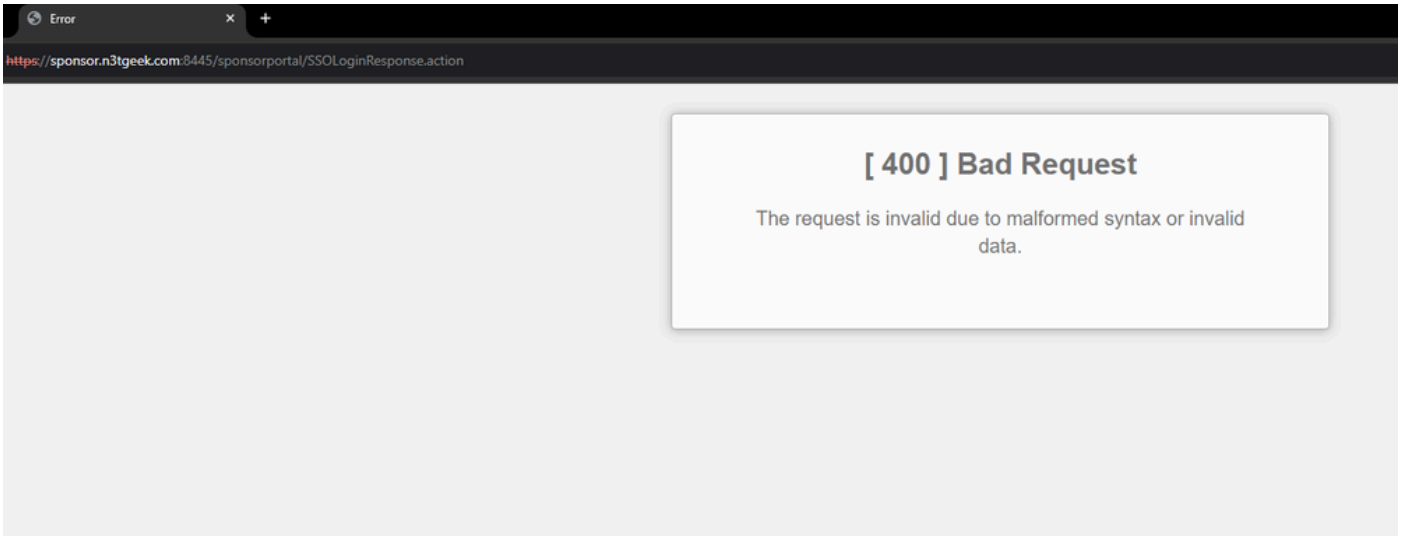
2.身份验证后，浏览器返回门户并显示AUP。接受后，发起人具有映射的发起人组权限。



3.从“欢迎使用”菜单注销将门户会话和SSO会话干净结束。



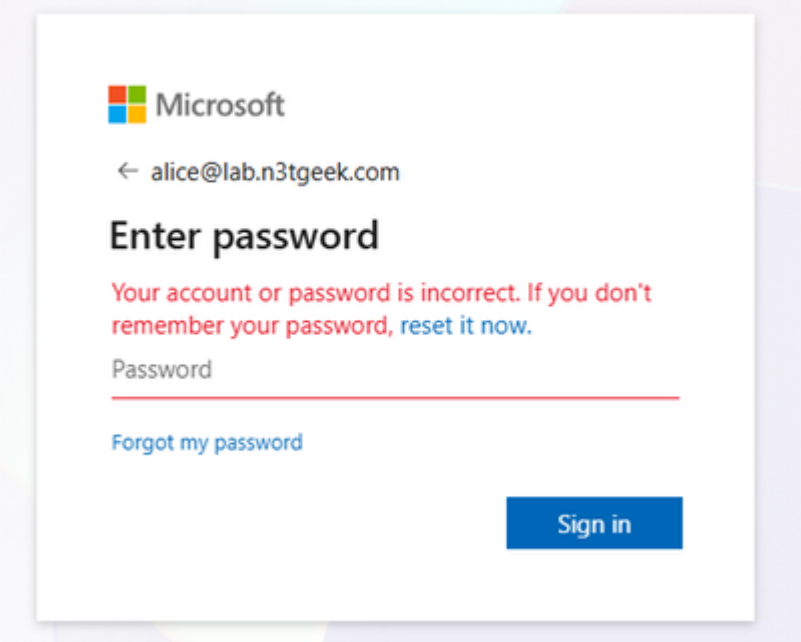
不支持IdP发起的SSO:思科ISE不支持IdP发起的SAML。Microsoft Entra ID中的Test Single Sign-On按钮(“Test this application”)始终无法进行此集成 — IdP启动的POST到达SOLoginResponse.action，门户返回HTTP [400] Bad Request (“由于语法格式错误或数据无效，请求无效”) 。 这是预期行为，不是配置错误。始终从发起人门户端进行验证。



故障排除

SAML身份验证发生在浏览器和Microsoft Entra ID之间；在涉及ISE之前，可直接从IdP显示错误。

问题1 — 密码错误



错误出现在Microsoft登录页面上；没有用户数据到达ISE。在ISE端，日志仅显示出站段，然后不显示任何内容。在guest.log中，门户流到达SSO_LOGIN，生成SAML请求，将浏览器重定向到IdP，会话从不返回：

<#root>

```
01:20:46 DEBUG StepExecutor          -- StepTran for Step=INIT => tranEnum=PROCEED_SSO, toStep=SSO_LOGI
01:20:46 DEBUG SSOLoginConfigHandler -- Redirect to IDP:
    https://login.microsoftonline.com/




     /saml2?SAMLRequest=jZNRc6IwFIX...
01:20:46 INFO  ISEPortalControllerUtils -- forwarding to: pages/ssoLoginRequest.jsp
(the portal session ends here --



no SSOLoginResponse is ever POSTed back

)
```

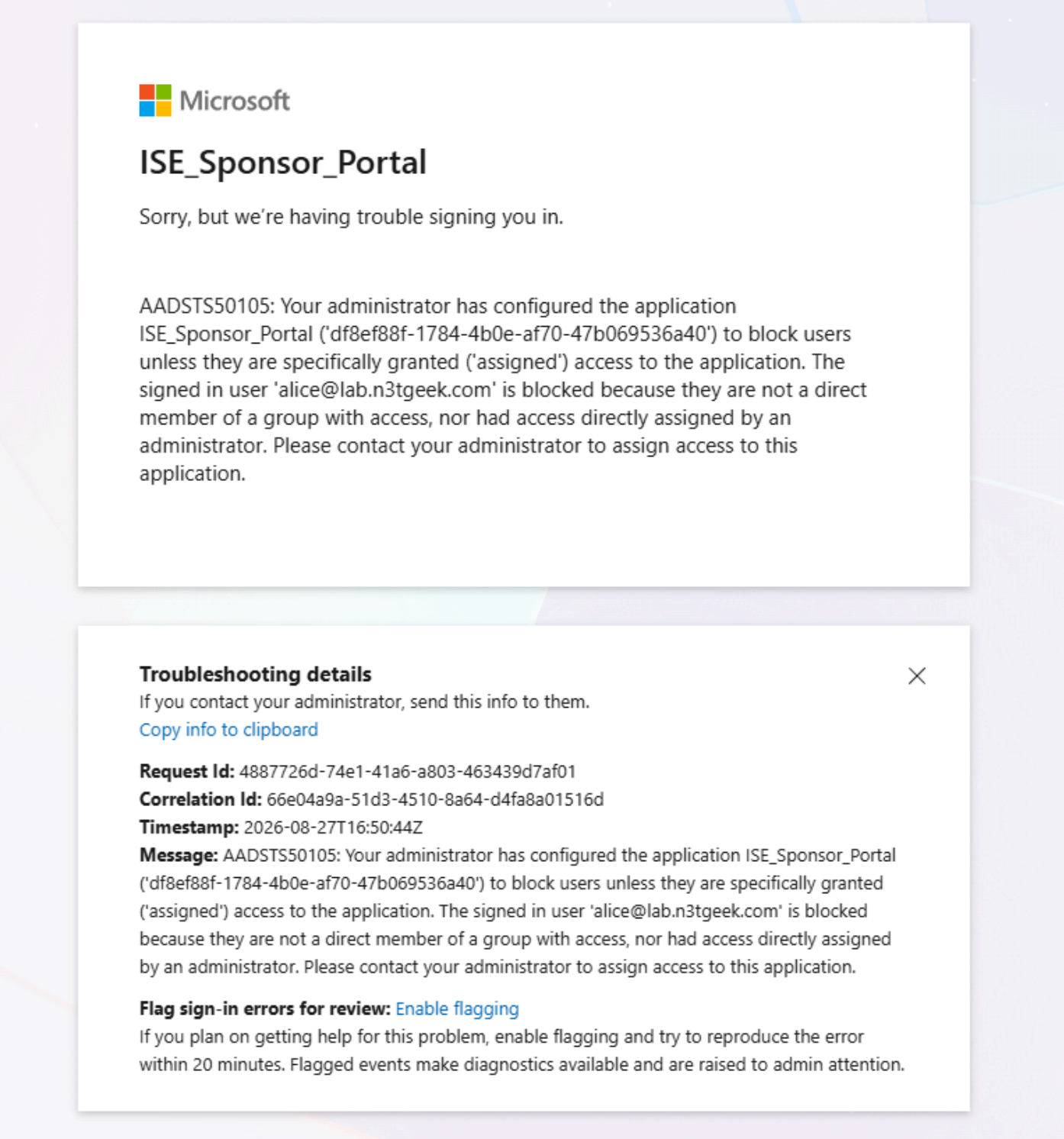
ise-psc.log从SAML框架端讲述的是相同的故事：

```
01:20:46 DEBUG SAMLFacadeImpl  -- SAML request - providerId (as should be found in IdP
    configuration): http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2
01:20:46 DEBUG SAMLFacadeImpl  -- SAML request - spUrlToReturnTo:
```

```
    https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action
01:20:46 DEBUG SAMLFacadeImpl  -- SignAuthenRequest configuration is - off
01:20:46 DEBUG MessageComposer -- local cert is null, request won't be signed
(capture ends here -- ISE never receives a SAML response)
```

问题2 — 用户未分配到应用(AADSTS50105)

在发出任何SAML响应之前，Entra ID会阻止登录。



nguest.log仅显示正在准备的重定向，而ise-psc.log则完全不显示SAML活动。故障发生在IdP端：

<#root>

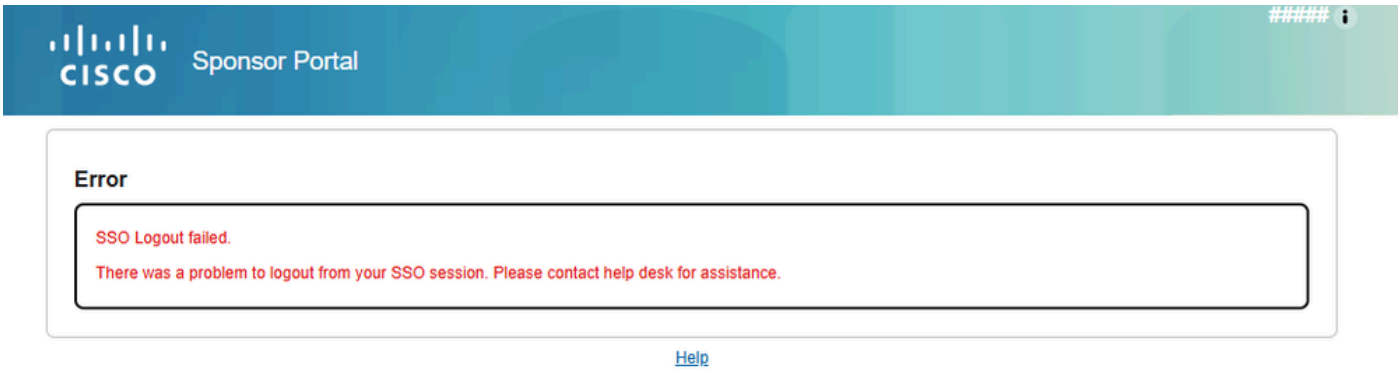
```
16:50:21 INFO  ISEPortalControllerUtils -- forwarding to: pages/ssoLoginRequest.jsp
(nothing follows --
```

the user never returns from the IdP

)

修复程序:将用户或组分配到企业应用程序（第2.4步）。

问题3 — 注销失败（“SSO注销失败”）



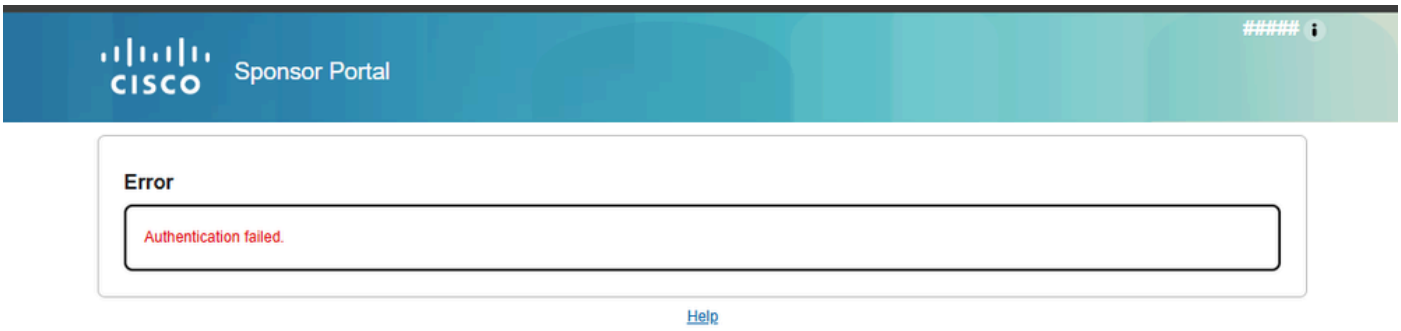
当Entra ID中的注销URL配置了SSOLogoutRequest.action?portal=...时，会发生这种情况。URL而非SSOLogoutResponse.action。在guest.log中，将启动注销，且无法处理返回的响应：

```
16:54:12 INFO  ISEPortalControllerUtils -- forwarding to: /pages/ssoLogoutRequest.jsp
16:54:13 ERROR SponsorSSOLogin -- SAML Response is invalid or subject is NULL!
16:54:13 INFO  ISEPortalControllerUtils -- forwarding to: pages/error.jsp
```

修复程序:更正基本SAML配置中的注销URL。

问题4 — 已轮换签名证书（“身份验证失败”）

当Entra ID令牌签名证书轮转（三年有效期）时，会激活新证书，并且联合元数据XML不会重新导入到ISE中，每次登录都会失败，在门户上使用通用的“身份验证失败”(Authentication failed)，即使两端都没有明显更改。



ise-psc.log明确说明了真正的原因：

```
16:58:30,429 WARN  apache.xml.security.signature.XMLSignature -- Signature verification failed.
16:58:30,430 ERROR cpm.saml.framework.impl.SAMLFacadeImpl -- SAML Response: processing failed:
com.cisco.cpm.saml.exceptions.SAMLException: Assertion signature did not validate
    against the IdP signature certificate
Caused by: org.opensaml.xml.validation.ValidationException: Signature did not validate
    against the credential's key
```

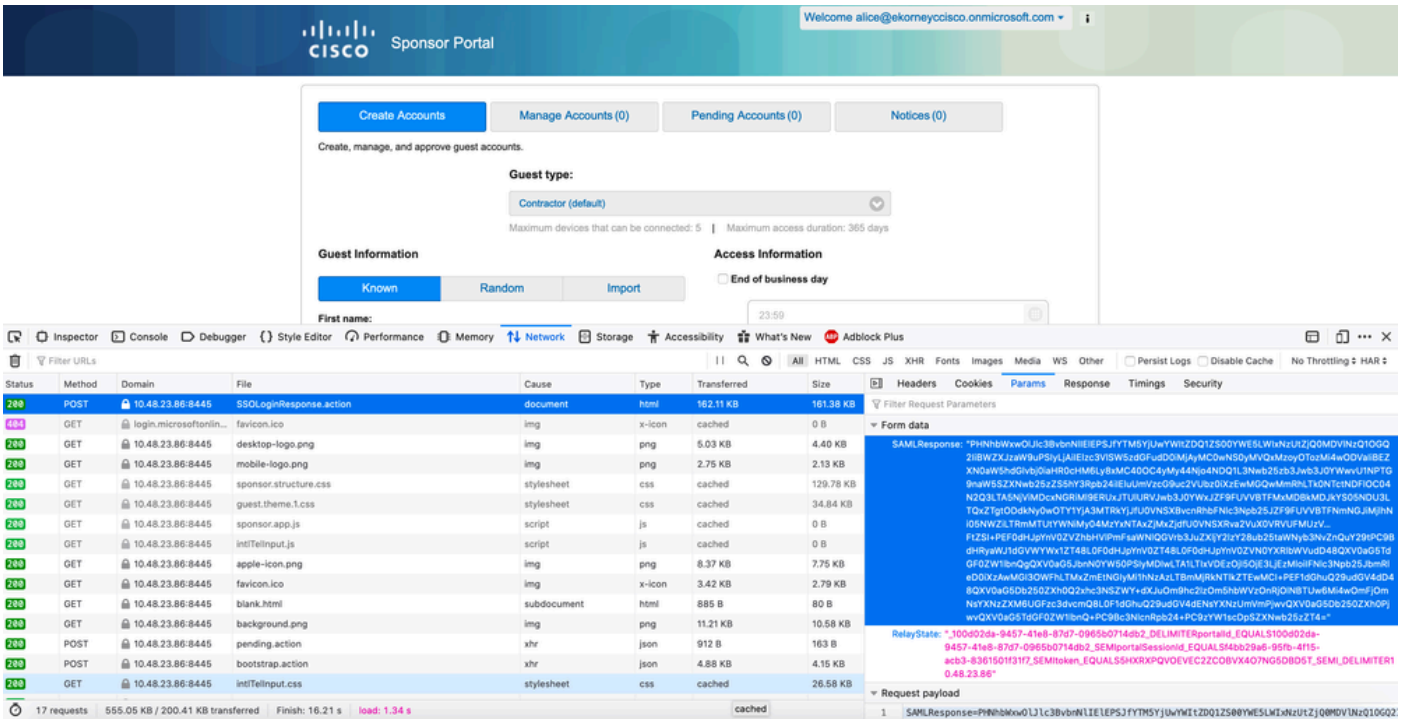
修复程序:从Entra ID重新下载联合元数据XML并将其重新导入到ISE。

问题5 — 会话快速过期

门户SSO会话空闲超时默认为5分钟（每个门户均可配置，本实验使用10分钟）。可以通过可选内容(Optional Content)字段将“再次登录”(Sign On Again)按钮添加到门户“错误”(Error)页面。

客户端故障排除

由于SAML消息通过浏览器传输，因此浏览器开发工具(F12 > Network Tab)显示整个交换。在Network（网络）选项卡打开的情况下重新生成登录，并查找POST到SOLoginResponse.action。浏览器向ISE提供SAML断言的那一刻：



ISE故障排除

必须在ISE上更改组件的日志级别。导航到操作>故障排除>调试向导>调试日志配置。

组件名称	日志级别	日志文件名
访客接入	调试	guest.log
portal-web-action	调试	guest.log
opensaml	调试	ise-psc.log
saml	调试	ise-psc.log

正确执行流时的工作集Debug(ise-psc.log):

1.用户从发起人门户重定向到IdP URL。

```
2026-08-27 01:55:58,021 DEBUG  [admin-http-pool3][[]] guestaccess.apiservices.portal.view.PortalConfigC
 ::::- hostName =sponsor.n3tgeek.com will be applied to URL!
    reqUtl =https://sponsor.n3tgeek.com:8445/sponsorportal/PortalSetup.action
2026-08-27 01:55:58,036 DEBUG  [https-jsse-nio-192.168.1.204-8445-exec-2][[]]
cisco.ise.portalwebaction.utils.PortalSessionUtil -::::- Portal URL:
    https://sponsor.n3tgeek.com:8445/sponsorportal/PortalSetup.action
2026-08-27 01:55:58,037 DEBUG  cisco.ise.portalwebaction.actions.BasePortalAction -::::-
    Action com.cisco.ise.portalwebaction.actions.PortalSetupAction Complete for request /sponsorportal/
```

2.从浏览器收到SAML响应：

```
2026-08-27 01:56:19,384 DEBUG cpm.saml.framework.impl.SAMLFacadeImpl -::::-
    SAML Response: statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
IdP URI: https://sts.windows.net/<Tenant-ID>/
SP URI: http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2
Assertion Consumer URL: https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action
```

3.属性（断言）分析已启动：

```
cpm.saml.framework.validators.SAMLSignatureValidator -::::- no signature in response
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Validating signature of assertion
org.opensaml.xml.signature.SignatureValidator -::::- Signature validated with key from supplied credent
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Assertion signature validated succesfully
cpm.saml.framework.validators.AssertionValidator -::::- Conditions succesfully validated
```

4.从断言中提取用户名和组属性(48f07fce-26e5-41e5-a82b-ed095b32bab8)，身份验证通过：

```
SAMLUtils::getUserNameFromAssertion: username value from Subject is=[alice@lab.n3tgeek.com]
loginInfo: ... format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
[cacheGroupAttr] Adding to cache ExternalGroup values=<48f07fce-26e5-41e5-a82b-ed095b32bab8>
AuthenticatePortalUser - added user groups from SAML response to AuthenticationResult,
    all retrieved groups:[48f07fce-26e5-41e5-a82b-ed095b32bab8]
Authenticate SAML User - result:PASSED
```

5.将用户组添加到身份验证结果中，以便门户使用该用户组并传递SAML身份验证：

```
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
```

数据包捕获分析

成功发起人登录期间在ISE接口（操作>故障排除>诊断工具> TCP转储）上捕获的流量仅显示两种类型的流量。门户FQDN的客户端DNS解析，以及端口8445上从客户端到门户的TLS会话，其中门户FQDN显示为TLS服务器名称指示(SNI)。

对话	方向	它是什么
客户端<-> ISE:8445（TLS、SNI =门户FQDN）	浏览器 — > PSN	门户页面+ SAML POST(ACS)
client -> DNS:门户FQDN	浏览器 — >解析程序	门户名称解析
没有通往login.microsoftonline.com的流量	—	IdP支路不会触及ISE

TLS客户端Hello — 其中门户名称可见

尽管所有内容都经过加密，但TLS客户端Hello仍以明文传输，并且它携带门户FQDN作为服务器名称指示(SNI)。 这是捕获中您可以将TCP数据流与发起人门户进行正匹配的位置。

```
Frame 96: 1981 bytes on wire
Internet Protocol Version 4, Src: 192.168.1.162 (client), Dst: 192.168.1.204 (ISE PSN)
Transmission Control Protocol, Src Port: 43395, Dst Port: 8445
Transport Layer Security
    TLSv1 Record Layer: Handshake Protocol: Client Hello
        Handshake Protocol: Client Hello
            Extension: server_name (len=24)
                Server Name Indication extension
                    Server Name: sponsor.n3tgeek.com
            Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
```

客户端上捕获的相同登录

```
  8445  sponsor.n3tgeek.com         (x12 -- the portal leg, to ISE)
  443  login.microsoftonline.com   (the IdP leg -- never seen on ISE)
  443  aadcdn.msauth.net           (Microsoft sign-in page assets)
  443  login.live.com / login.microsoft.com
(unrelated background traffic omitted for clarity)
```



注意：ISE在保证人身份验证期间从不与Entra ID通信。SAML请求和响应通过用户浏览器传输（重定向和POST绑定）。 这意味着ISE节点不需要与Microsoft的出站连接才能使门户SSO正常工作，并且在进行故障排除时，必须在客户端而不是ISE上捕获IdP分支。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。