在ASA上使用SAML配置多个隧道组

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

SAML SP启动的SSO

配置

- 从图库添加Cisco Secure Firewall - Secure Client
- 将Azure AD用户分配给应用
- 通过CLI配置ASA

验证

故障排除

相关信息

简介

本文档介绍使用Azure身份提供程序对思科ASA上的多个隧道组进行SAML身份验证。

先决条件

要求

建议掌握下列主题的相关知识：

- Microsoft Azure

- 自适应安全设备 (ASA)
- 安全套接字层(SSL)证书
- 安全断言标记语言(SAML)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 9.2(1)1
- 思科安全客户端5.1.7.80
- 使用SAML 2.0的Microsoft Azure 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。

背景信息

Microsoft Azure可以支持同一实体ID的多个应用程序。每个应用（映射到不同的隧道组）都需要一个唯一的证书。在ASA上，由于IdP证书功能，可将多个隧道组配置为使用不同的覆盖身份提供程序(IdP)保护应用。此功能允许管理员使用每个隧道组的特定IdP证书覆盖单点登录(SSO)服务器对象中的主IdP证书。此功能从9.17.1版本开始在ASA上引入。

SAML SP启动的SSO

当最终用户通过访问ASA启动登录时，登录行为按以下方式进行：

1.当VPN用户访问或选择启用SAML的隧道组时，最终用户将被重定向到SAML IdP进行身份验证。系统将提示用户，除非用户直接访问group-url，在这种情况下，重定向是静默的。

2. ASA生成SAML身份验证请求，浏览器将其重定向至SAML IdP。

3. IdP向最终用户询问凭证和最终用户登录。输入的凭证必须满足IdP身份验证配置。

4. IdP响应将发送回浏览器并发布到ASA登录URL。ASA验证响应以完成登录。

配置

从图库添加Cisco Secure Firewall - Secure Client

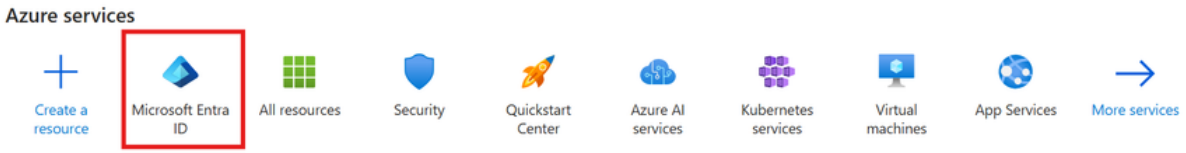
在本示例中，为ASA上配置的两个隧道组添加了Microsoft Entra SSO与Cisco Secure Firewall - Secure Client on Azure:

- SAML1
- SAML2

要配置思科安全防火墙 — 安全客户端到Microsoft Entra ID的集成，您必须从库向托管SaaS应用列表中添加Cisco安全防火墙 — 安全客户端。

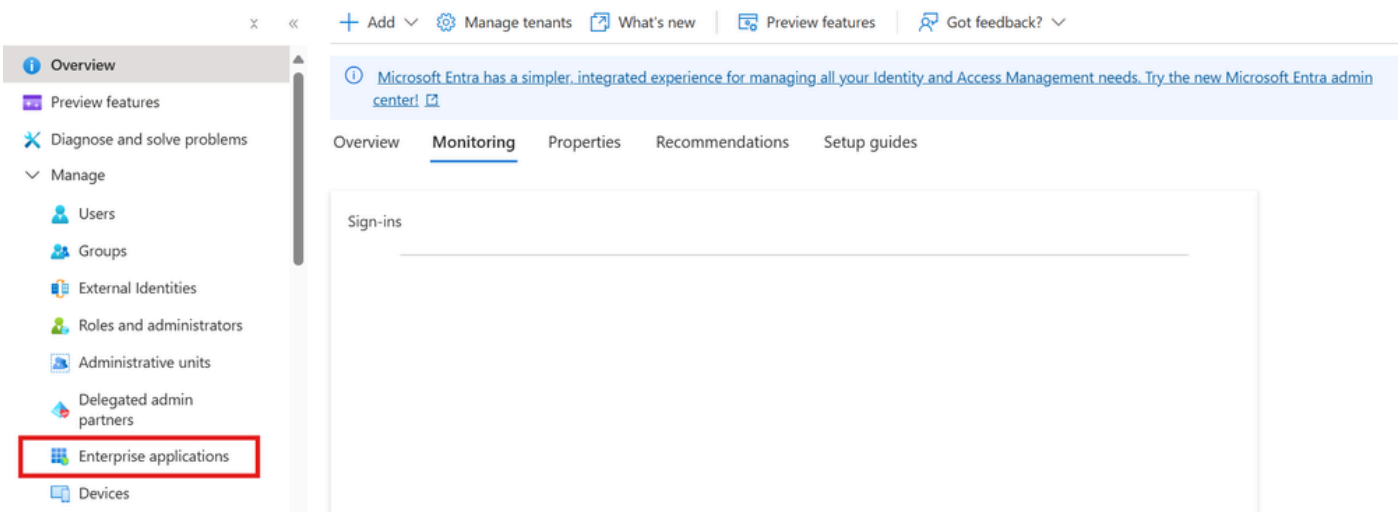
注意：这些步骤用于将思科安全防火墙 — 安全客户端添加到第一个隧道组SAML1的库中。

步骤1.登录到Azure门户并选择Microsoft Entra ID。



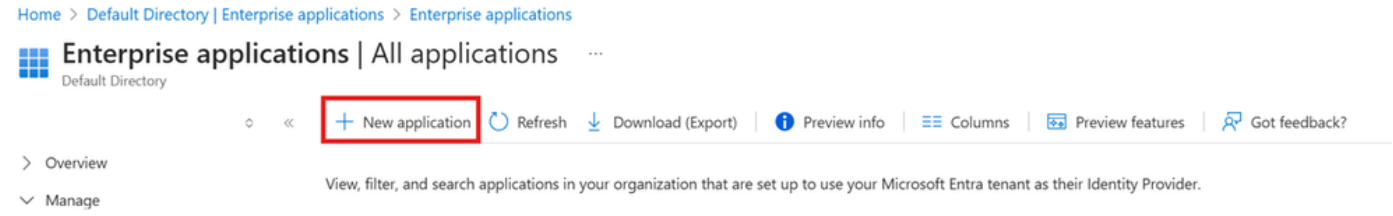
Microsoft Entra ID

步骤2.如图所示，选择Enterprise Applications。



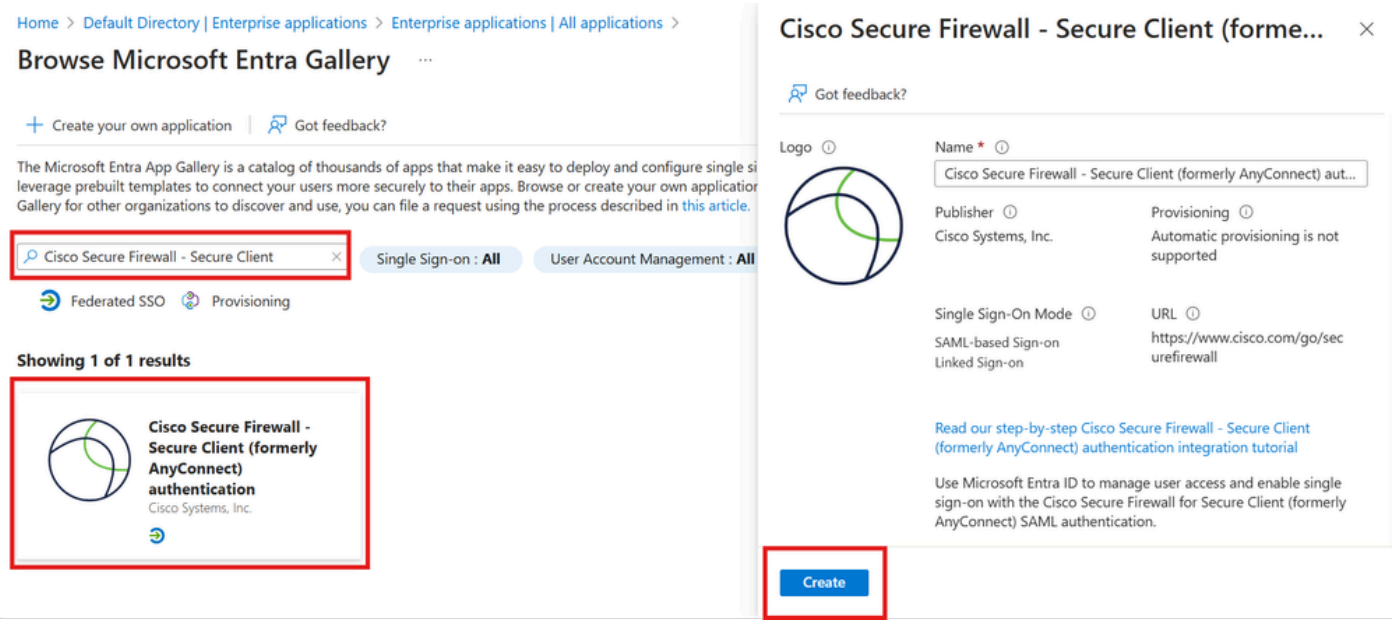
企业应用

步骤3.选择New Application。



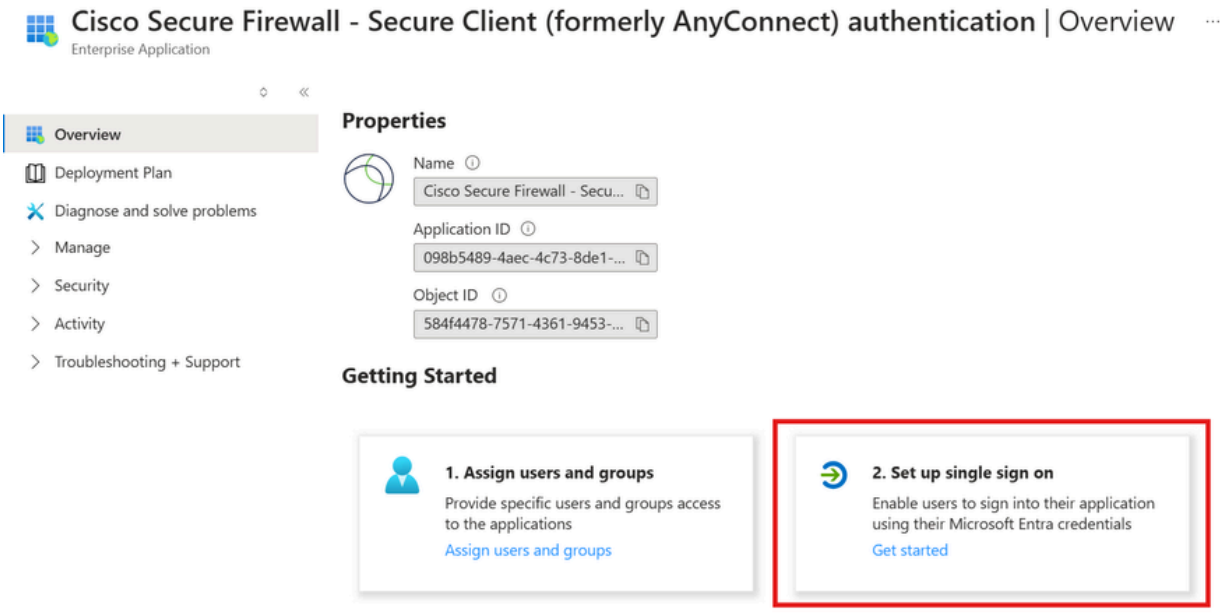
新应用程序

第4步：在Add from the gallery部分中，在搜索框中键入Cisco Secure Firewall - Secure Client，从结果面板中选择Cisco Secure Firewall - Secure Client，然后选择Add应用。



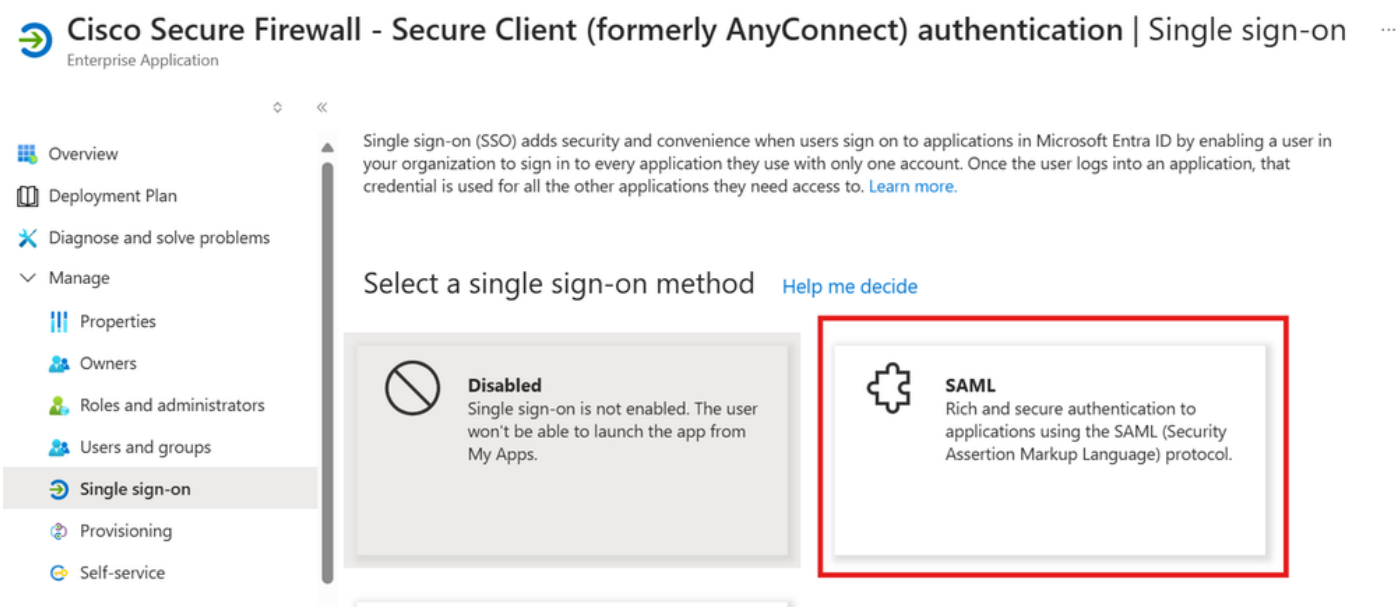
思科安全防火墙 — 安全客户端

步骤5.选择Single Sign-On菜单项。



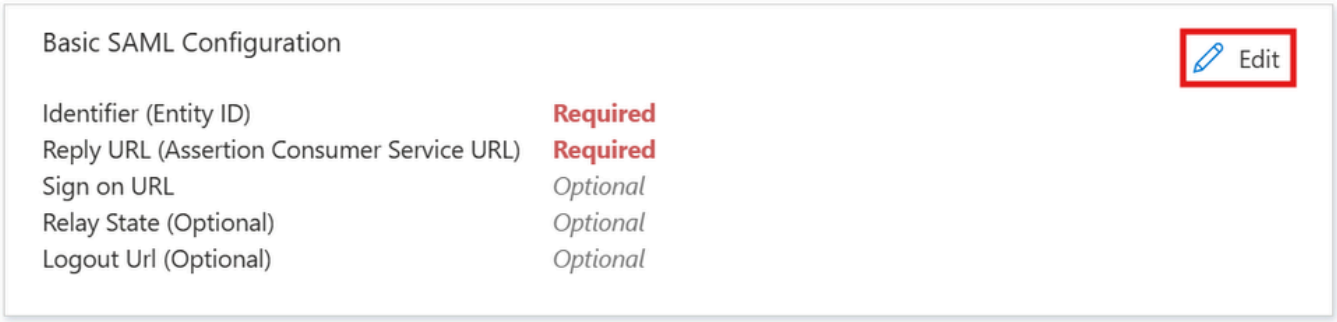
设置单一登录

第6步：在“选择单点登录方法”页上，选择SAML。



SAML

第7步：在“使用SAML设置单点登录”页面，单击“基本SAML配置”的编辑/笔图标以编辑设置。



基本Saml配置

第8步：在“使用SAML设置单点登录”页面上，输入以下字段的值：

- 在“标识符”(Identifiertext)文本框中，使用以下模式键入URL:

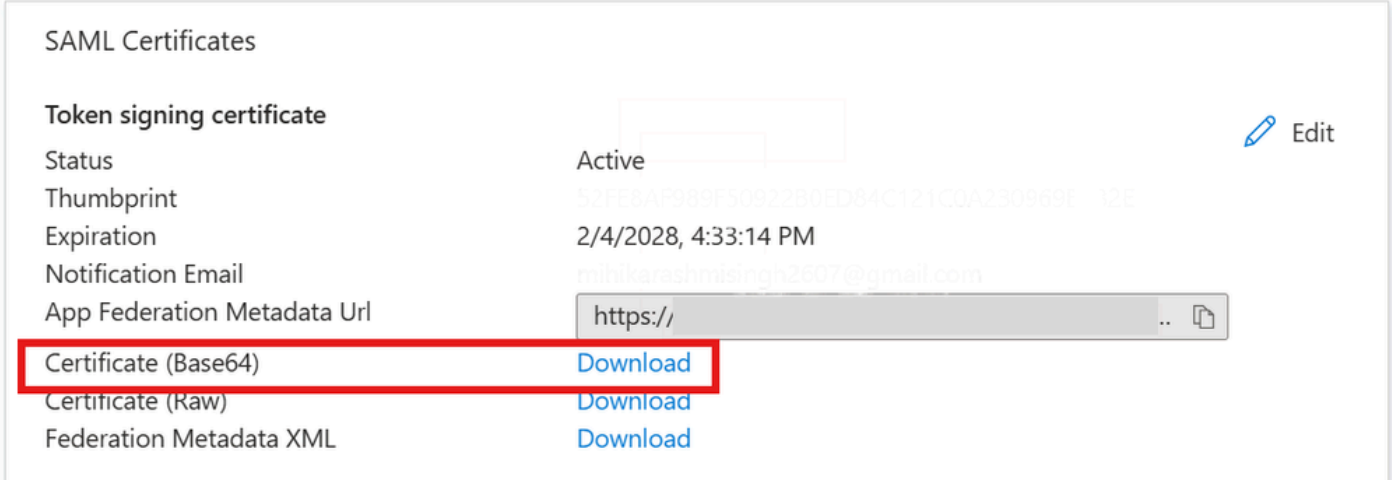
https://<VPN URL>/saml/sp/metadata/<Tunnel_Group_Name>

- 在“回复URL”(Reply URL)文本框中，使用此模式键入URL:

https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<Tunnel_Group_Name>
[Tunnel_Group_Name = SAML1]

注意：Tunnel_Group_Name区分大小写，并且值不能包含点“。” 和斜杠“/”。

步骤9.在使用SAML设置单点登录页上，在SAML签名证书部分中，查找证书(Base64)，然后选择下载以下载证书文件并将其保存在计算机上。

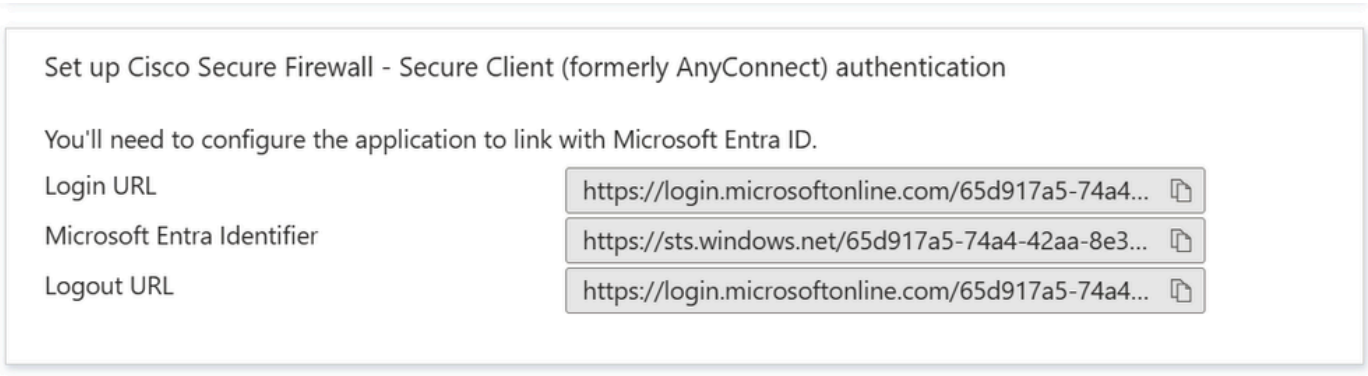


证书(Base64)下载

注意：此下载的证书已导入到ASA信任点AzureAD-AC-SAML1。有关详细信息，请参阅“ASA配置”部分。

步骤10.在设置Cisco安全防火墙 — 安全客户端部分上，根据您的要求复制适当的URL。这些URL用于在ASA上配置SSO服务器对象。

- Microsoft Entra标识符:这是VPN配置中的SAML IdP。
- 登录URL:这是URL登录。
- 注销URL:这是URL注销。



SSO URL

注意：重复上述配置步骤，从库中为第二个隧道组添加Cisco Secure Firewall - Secure Client应用。本例中的第二个隧道组名称为SAML2。

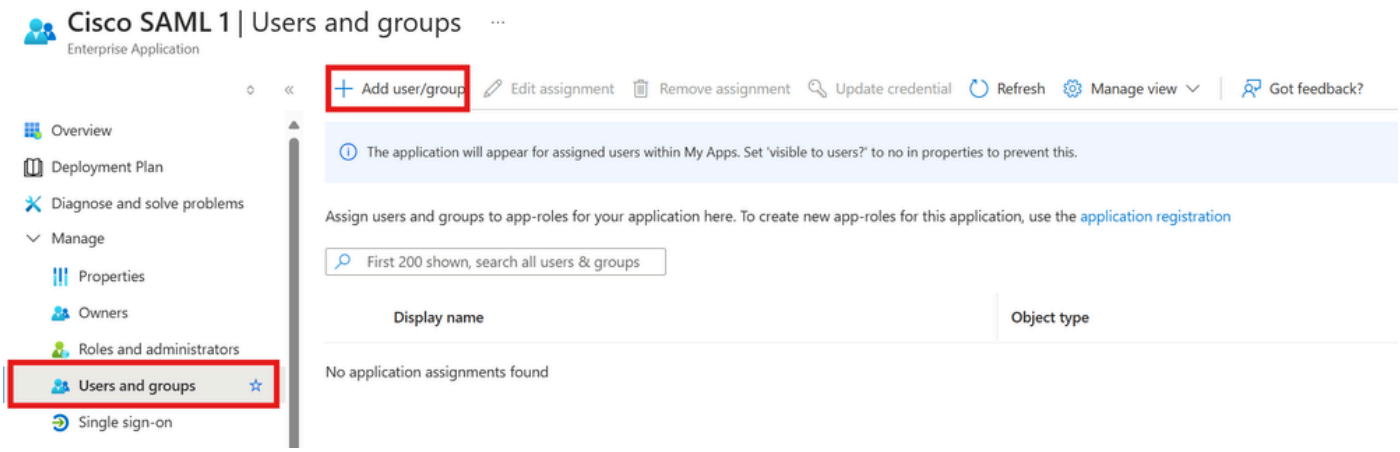
为第二个隧道组(SAML 2)添加Cisco Secure Firewall - Secure Client应用时，第8步中下载的Azure证书将导入到ASA信任点AzureAD-AC-SAML2。

将Azure AD用户分配给应用

在本节中，Test1和Test2被启用以使用Azure SSO，因为您授予了对Cisco安全客户端应用的访问权限。

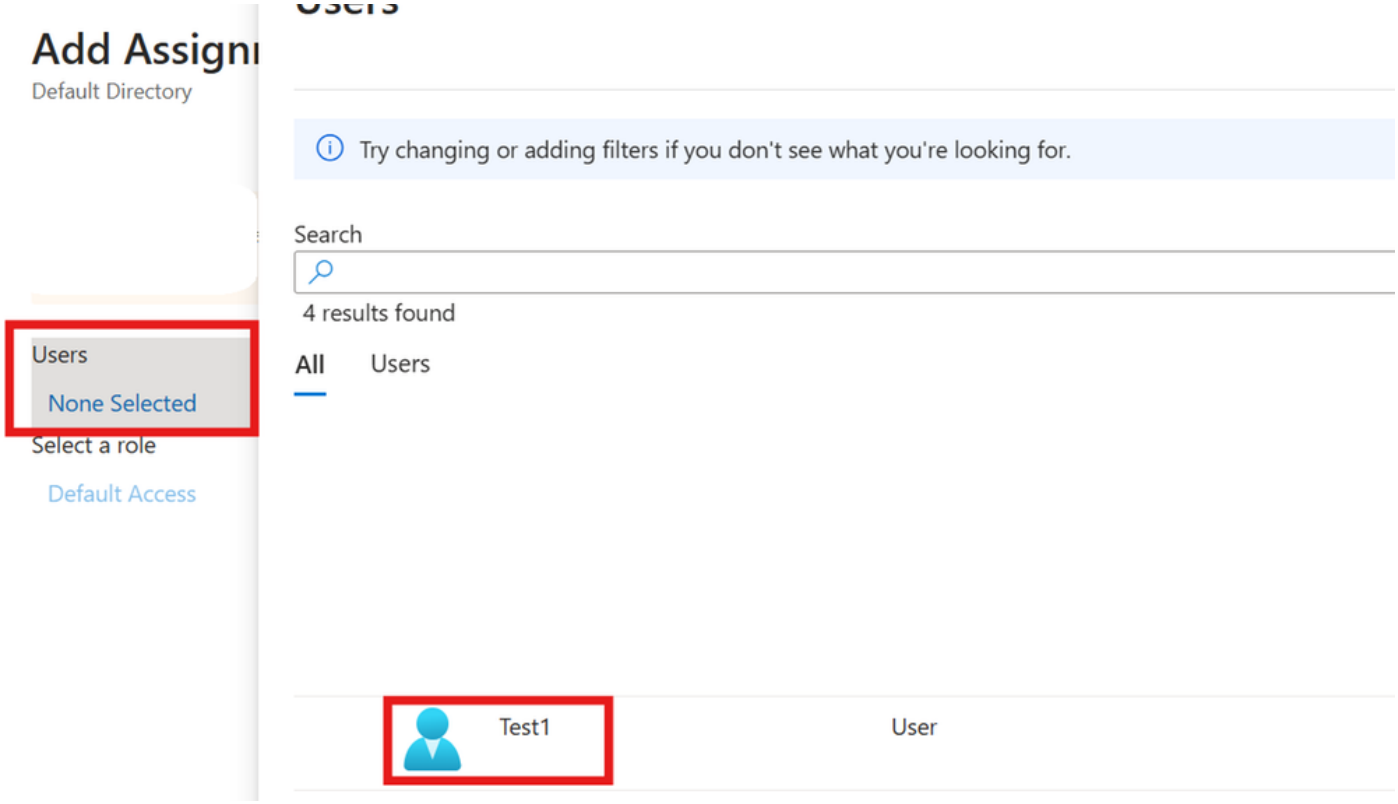
对于第一个IdP应用程序：

步骤1.在第一个IdP应用程序概述页中，依次选择Users and groups(用户和组)，然后选择Add user(添加用户)。



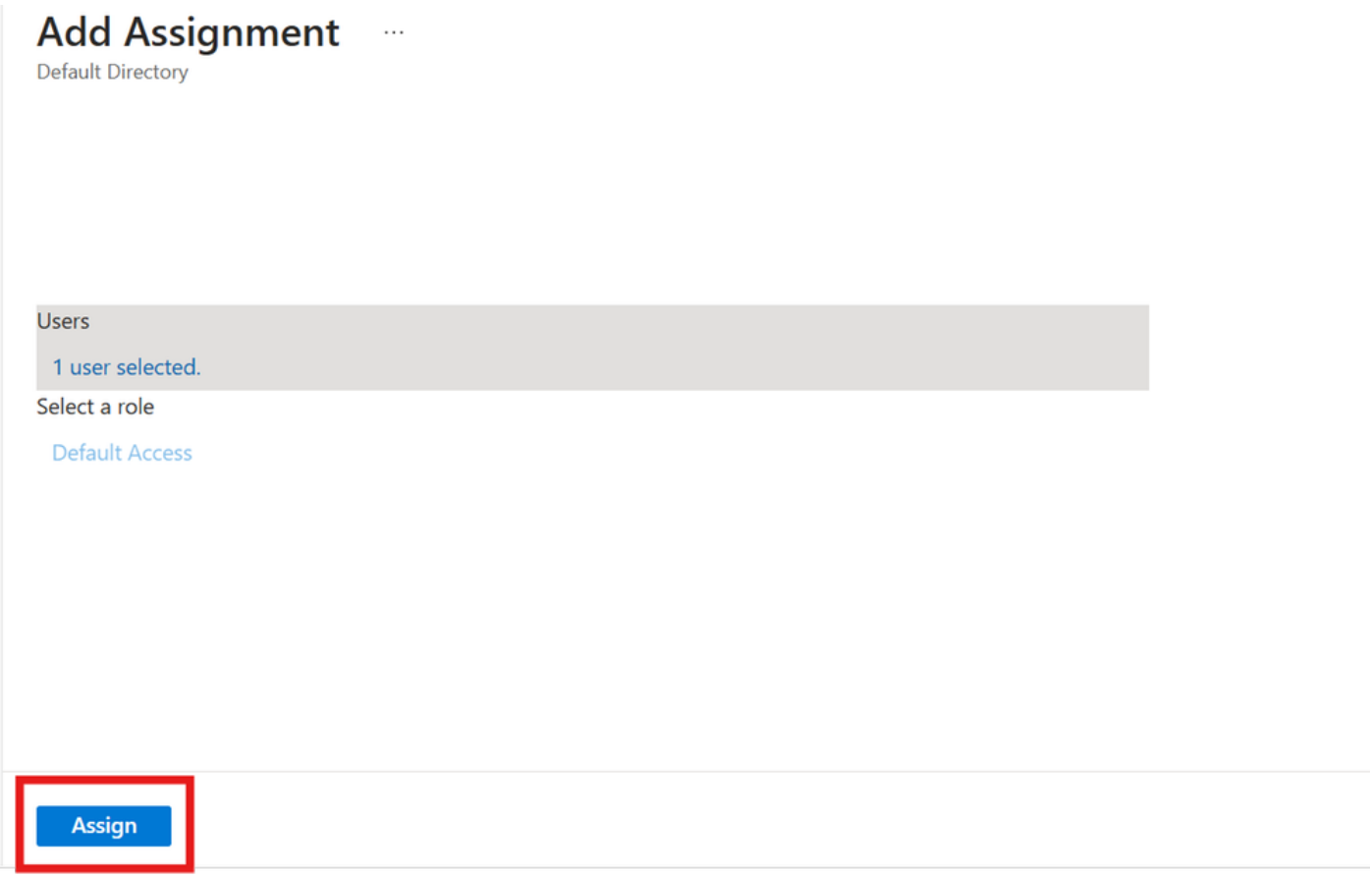
用户和组

第2步：在“添加分配”对话框中选择“用户”或“组”。



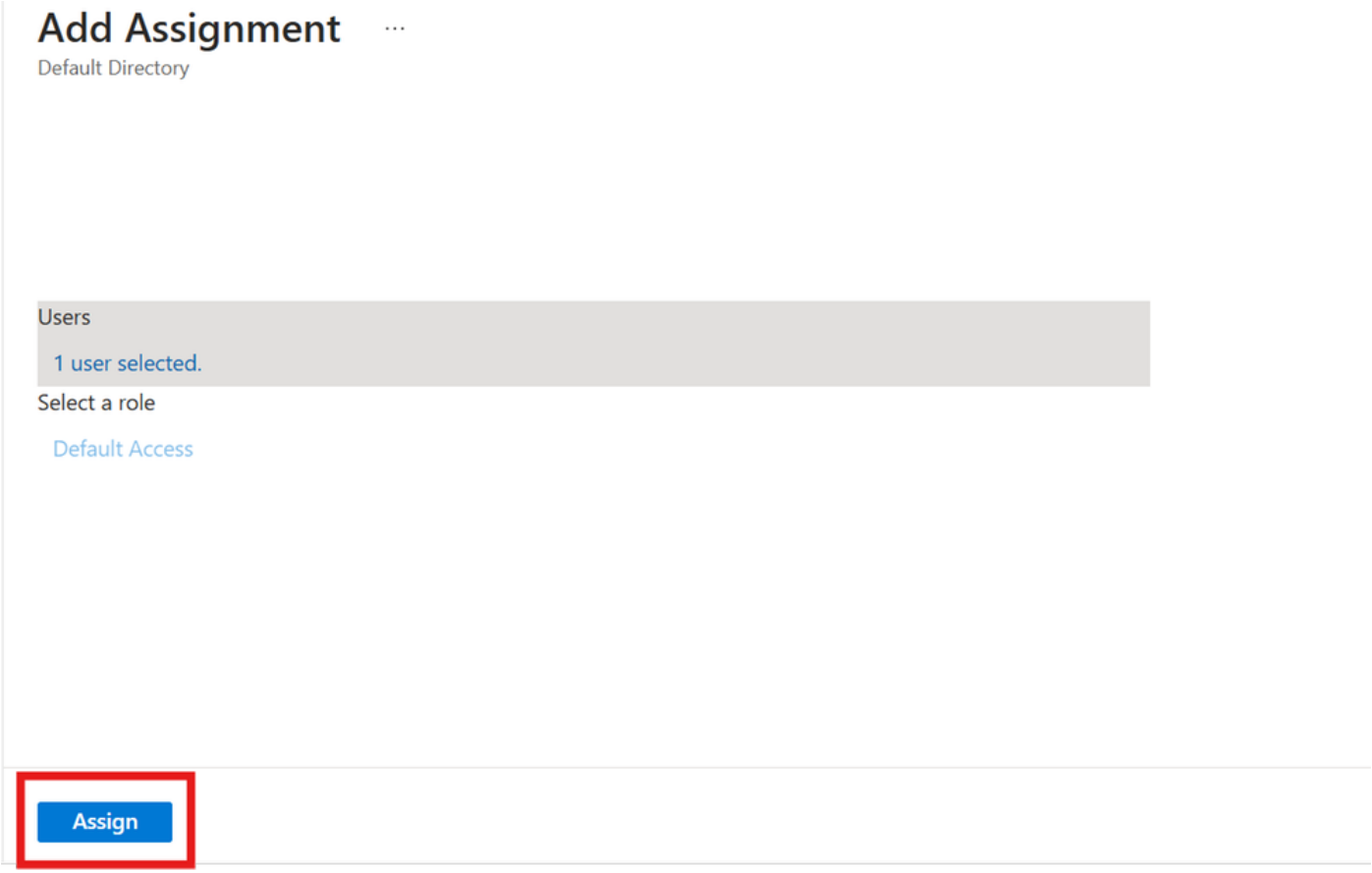
添加作业1

步骤3.在Add Assignment对话框中，点击Assign按钮。

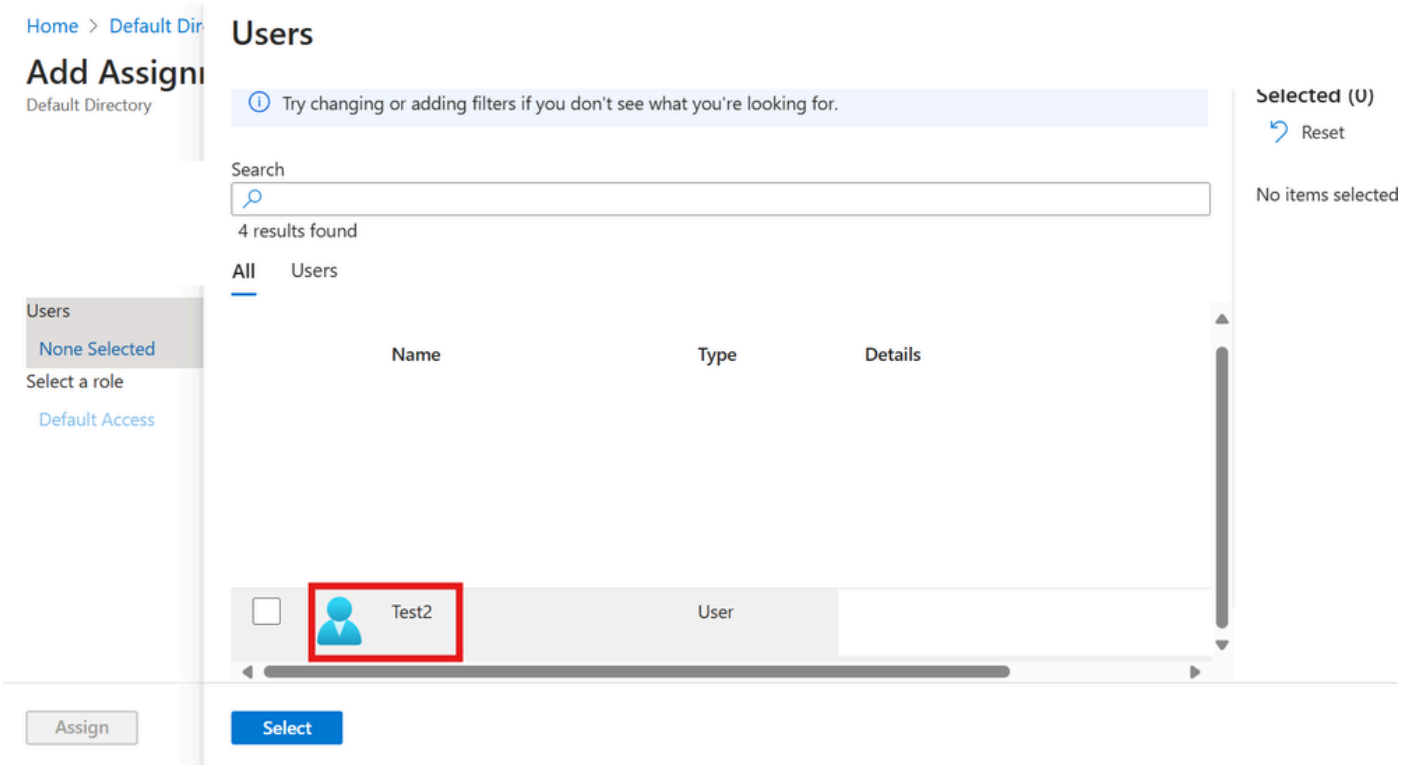


对于第二个IdP应用程序：

对第二个Idp应用程序重复上述步骤，如下图所示：

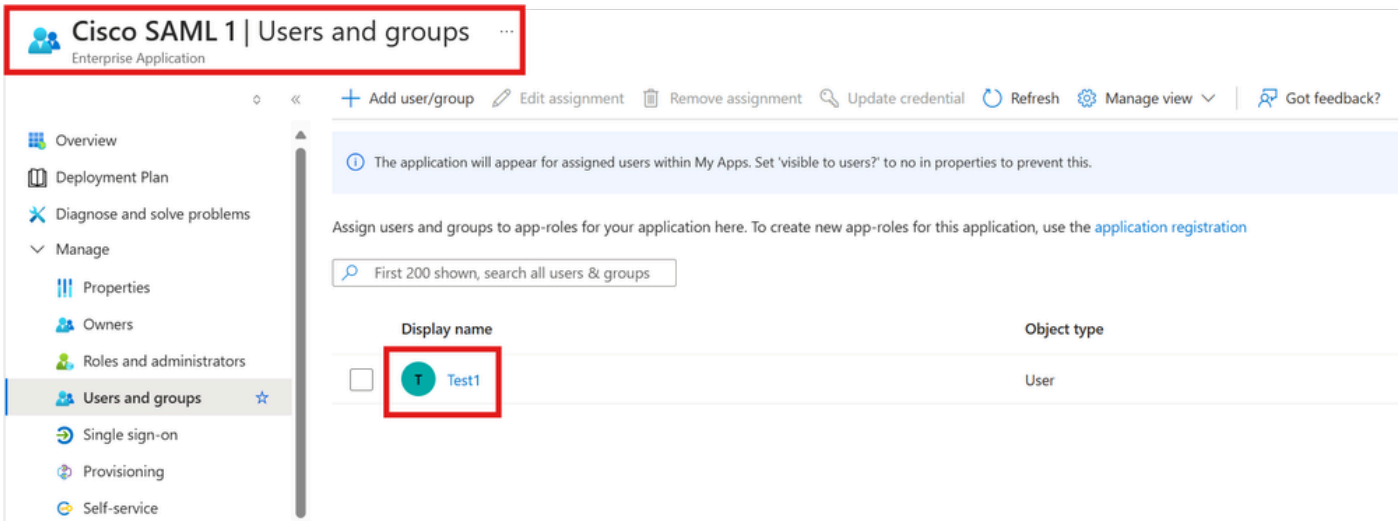


添加作业2



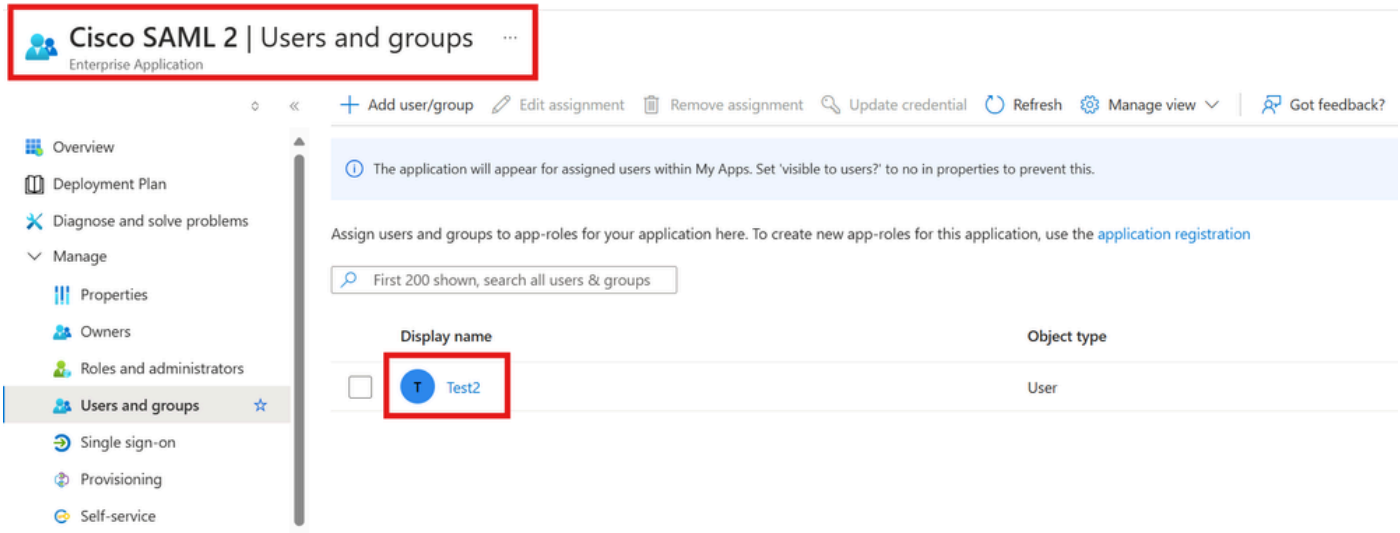
Test2用户分配

Test1用户分配：



测试1用户分配

Test2用户分配：



测试2用户分配

通过CLI配置ASA

步骤1.创建信任点并导入SAML证书。

配置两个信任点并为每个隧道组导入各自的SAML证书:

<#root>

```
config t

 crypto ca trustpoint
```

AzureAD-AC-SAML1

```
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML1

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit

!
!
```

```
crypto ca trustpoint
```

AzureAD-AC-SAML2

```
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML2

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit
```

步骤2.配置SAML IdP。

运行这些命令以调配SAML IdP设置。

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2  - [Logout URL]
 trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

步骤3.将SAML身份验证应用于第一个VPN隧道组。

使用AzureAD-AC-SAML1 IdP信任点配置SAML1隧道组。

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

```
saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (
```

步骤4.将SAML身份验证应用到第二个VPN隧道组。

使用AzureAD-AC-SAML2 IdP信任点配置SAML2隧道组。

<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (
```

步骤 5：保存配置。

```
write memory
```



注意：如果更改IdP配置，则必须从隧道组删除SAML身份提供程序配置，然后重新应用该配置以使更改生效。

验证

使用SAML身份验证测试AnyConnect。

步骤1.连接到您的VPN URL并在Azure AD详细信息中输入您的日志。

步骤2.(可选)批准登录请求。

步骤3. AnyConnect已连接。

故障排除

大多数SAML故障排除都涉及配置错误，在选中SAML配置或运行调试时可以找到该错误配置。debug webvpn saml 255可用于解决大多数问题，但是，在此调试不提供有用信息的情况下，可以运行其他调试，例如：

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

相关信息

- 技术支持和文档 - Cisco Systems
- 使用 Microsoft Azure MFA 通过 SAML 配置 ASA AnyConnect VPN

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）。