使用 Microsoft Azure MFA 通过 SAML 配置 ASA AnyConnect VPN

目录

简介

本文档介绍如何配置安全断言标记语言(SAML)，重点介绍通过Microsoft Azure MFA的自适应安全设备(ASA)AnyConnect。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解ASA上的RA VPN配置。

- SAML和Microsoft Azure的基本知识。
- AnyConnect许可证已启用（APEX或仅VPN）。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Azure AD订阅。
- Cisco ASA 9.7+和Anyconnect 4.6+
- 使用AnyConnect VPN配置文件

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

SAML是一个基于XML的框架，用于在安全域之间交换身份验证和授权数据。它在用户、服务提供商(SP)和身份提供者(IdP)之间创建信任圈，允许用户一次性登录多个服务。Microsoft Azure MFA与Cisco ASA VPN设备无缝集成，为Cisco AnyConnect VPN登录提供额外的安全性。

SAML组件

元数据：它是基于XML的文档，用于确保IdP和SP之间的安全事务。它允许IdP和SP协商协议。

设备(IdP、SP)支持的角色

设备可以支持多个角色，并且可以同时包含SP和IdP的值。如果包含的信息用于单点登录IdP，则在EntityDescriptor字段下为IDPSSODescriptor；如果包含的信息用于单点登录SP，则此字段下为SPSSODescriptor。这很重要，因为为了成功设置SAML，必须从相应的部分获取正确的值。

实体ID：此字段是SP或IdP的唯一标识符。单个设备可以有多个服务，并且可以使用不同的实体ID来区分这些服务。例如，ASA对于需要身份验证的不同隧道组具有不同的实体ID。对每个隧道组进行身份验证的IdP对每个隧道组都有单独的实体ID条目，以便准确识别这些服务。

ASA可以支持多个IdP，并为每个IdP提供单独的实体ID以区分它们。如果任一端收到来自不包含以前配置的实体ID的设备的消息，则设备可能会丢弃此消息，并且SAML身份验证失败。实体ID位于entityID旁边的EntityDescriptor字段中。

服务URL：这些字段定义由SP或IdP提供的SAML服务的URL。对于IdP，这通常为单一注销服务和单一登录服务。对于SP，这通常是断言消费者服务和单一注销服务。

SP使用IdP元数据中找到的单点登录服务URL将用户重定向到IdP进行身份验证。如果此值配置不正确，则IdP不会接收或无法成功处理由SP发送的身份验证请求。

IdP使用在SP元数据中找到的Assertion Consumer Service URL将用户重定向回SP并提供有关用户身份验证尝试的信息。如果配置不正确，SP不会收到断言（响应）或无法成功处理该断言。

在SP和IdP上都可以找到单一注销服务URL。它用于简化从SP注销所有SSO服务的过程，并且在

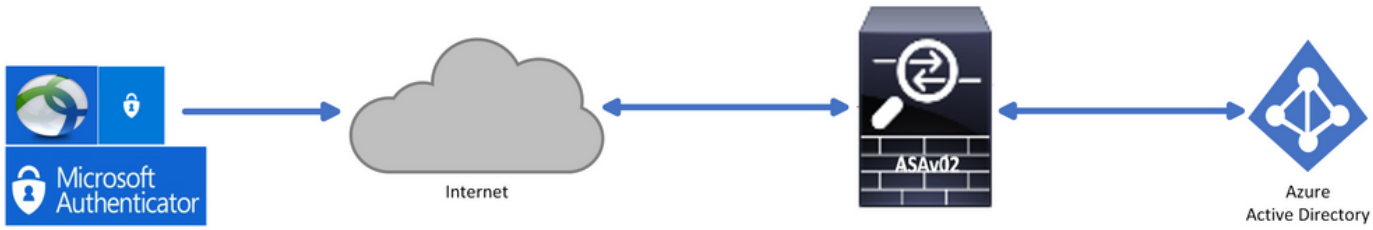
ASA上是可选的。在SP上配置来自IdP元数据的SLO服务URL时，当用户从SP上的服务注销时，SP会将请求发送到IdP。IdP成功从服务中注销用户后，会将用户重定向回SP并使用在SP的元数据中找到的SLO服务URL。

服务URL的SAML绑定：绑定是SP用来将信息传输到IdP的方法，反之亦然。这包括HTTP重定向、HTTP POST和项目。每种方法传输数据的方式各不相同。服务支持的绑定方法包含在该服务的定义中。例如：SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location=https://saml.example.com/simplesaml/saml2/idp/SSOService.php/ >。ASA不支持项目绑定。ASA始终对SAML身份验证请求使用HTTP重定向方法，因此，选择使用HTTP重定向绑定的SSO服务URL以使IdP预期这一点，这一点非常重要。

用于签名和加密操作的证书

为了为SP和IdP之间发送的消息提供机密性和完整性，SAML具有对数据进行加密和签名的功能。用于对数据进行加密和/或签名的证书可以包含在元数据中，以便接收方可以验证SAML消息并确保其来自预期源。用于签名和加密的证书可在KeyDescriptor use="signing"和KeyDescriptor use="encryption"下的元数据中找到，依次是X509Certificate。ASA不支持加密SAML消息。

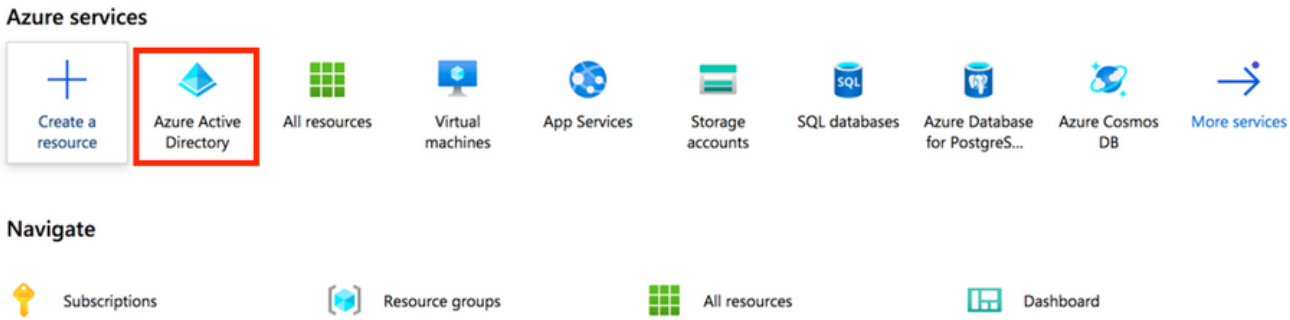
网络图



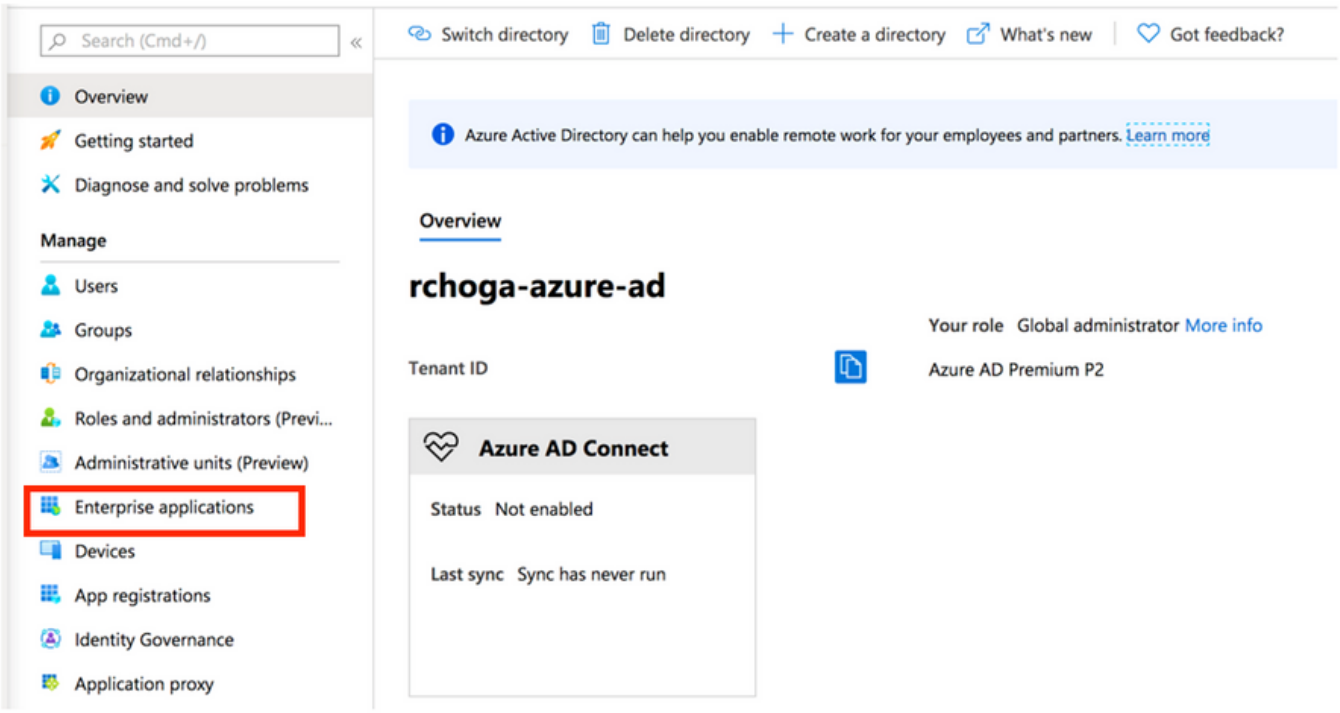
配置

从Microsoft应用库添加Cisco AnyConnect

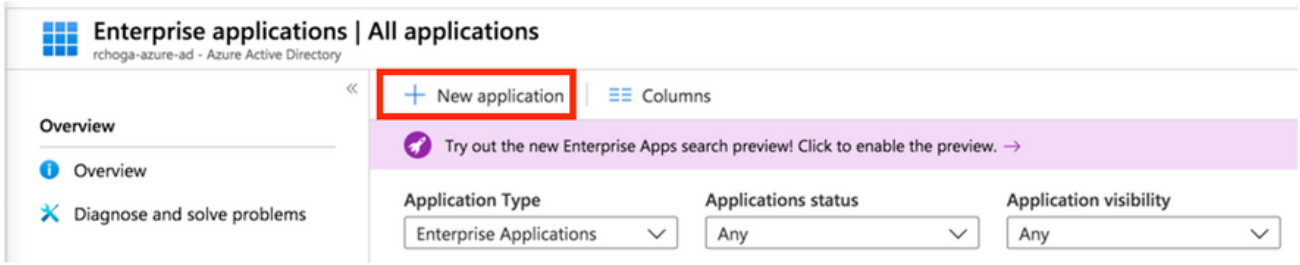
步骤1.登录到Azure门户并选择Azure Active Directory。



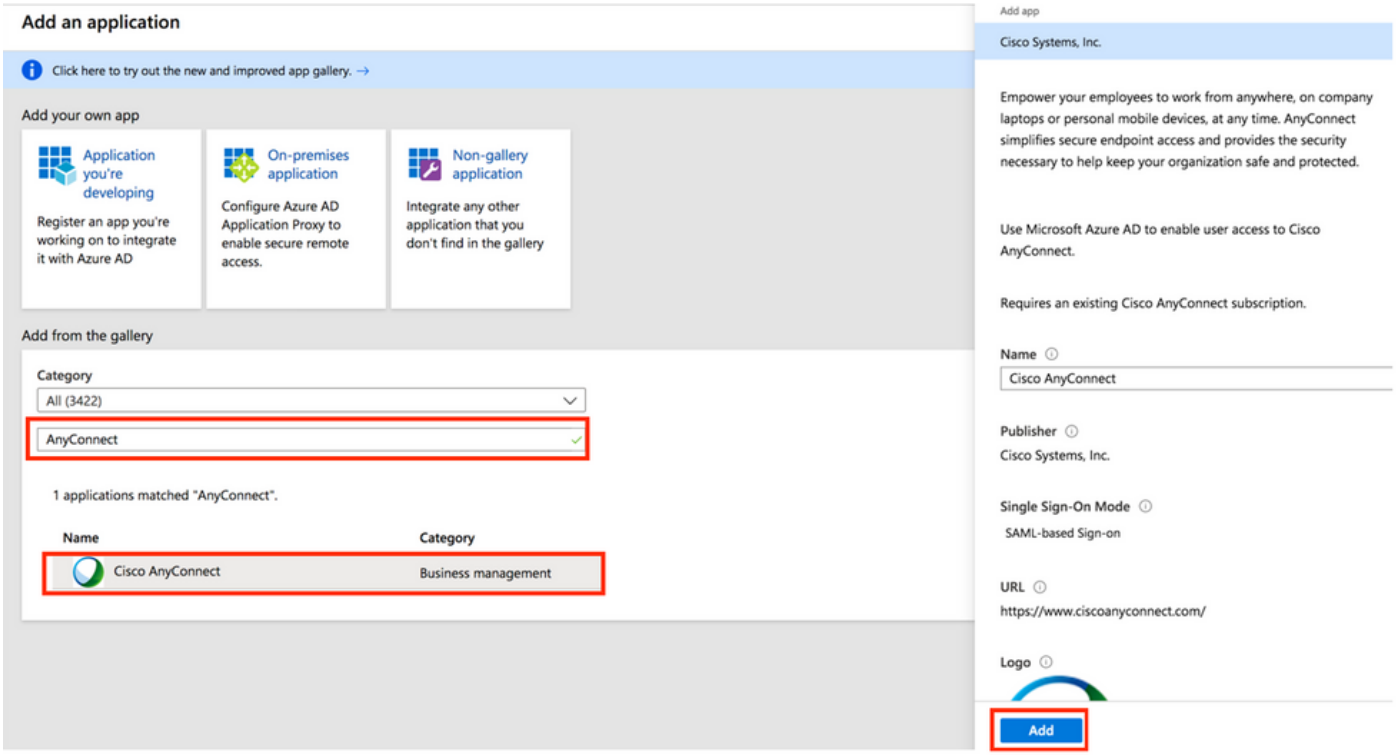
第二步：如图所示，选择Enterprise Applications。



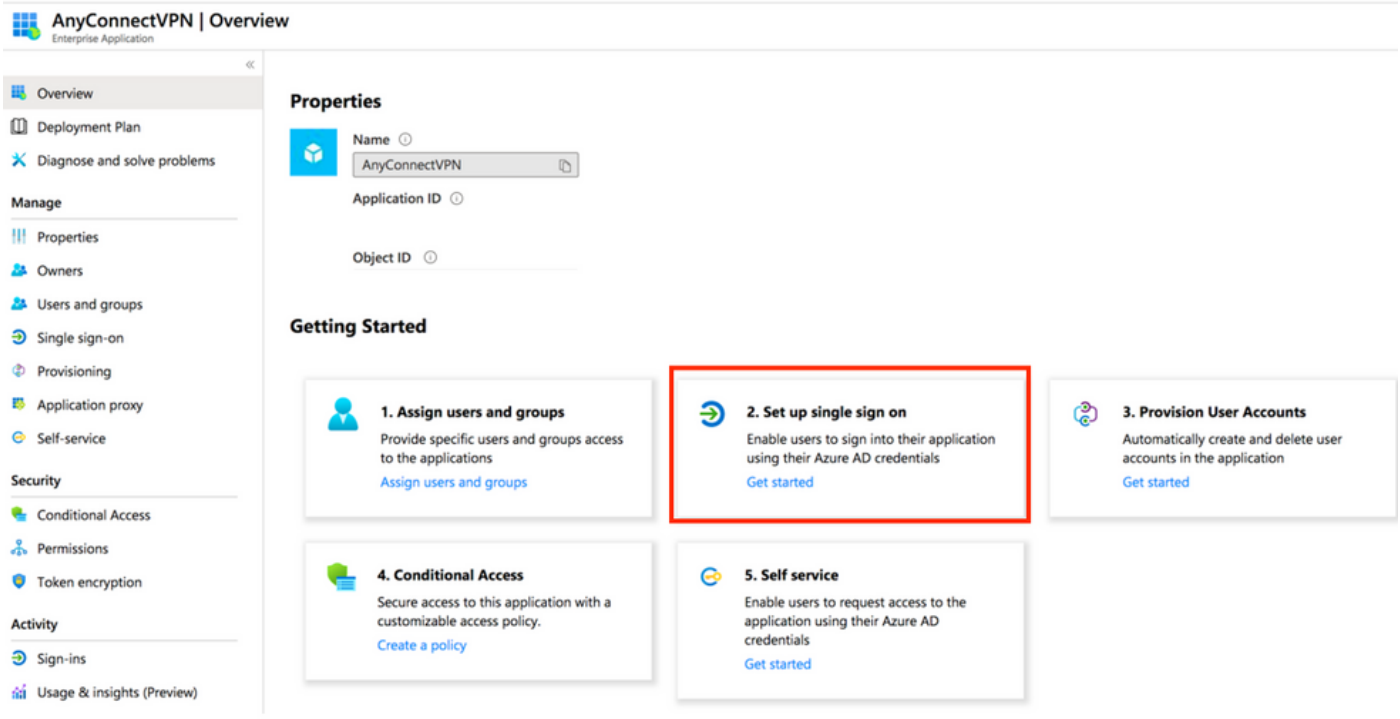
第三步： 现在，选择New Application，如下图所示。



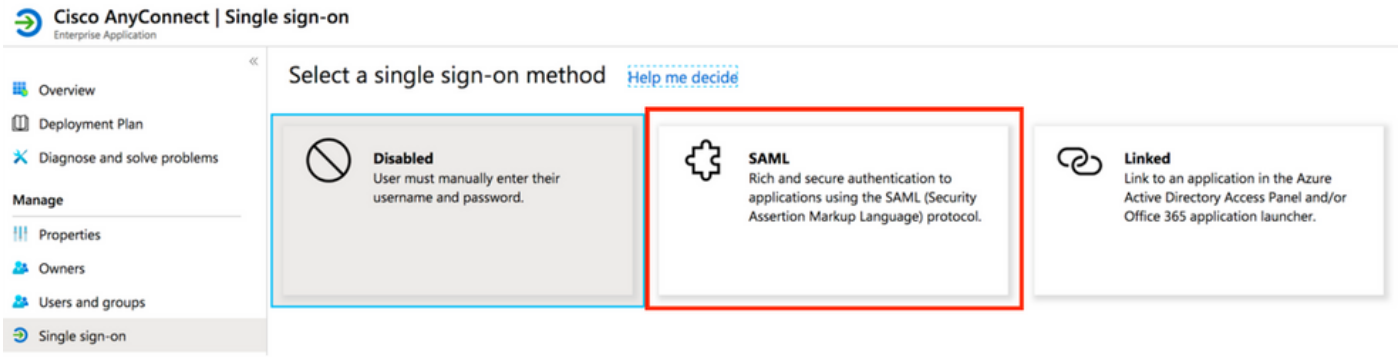
第四步：在Add from the gallery部分中，在搜索框中键入AnyConnect，从结果面板中选择Cisco AnyConnect，然后添加应用。



第五步：选择Single Sign-on菜单项，如下图所示。



第六步：选择SAML，如图所示。



步骤 7.使用以下详细信息编辑第1部分。

<#root>

a. Identifier (Entity ID) - https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>

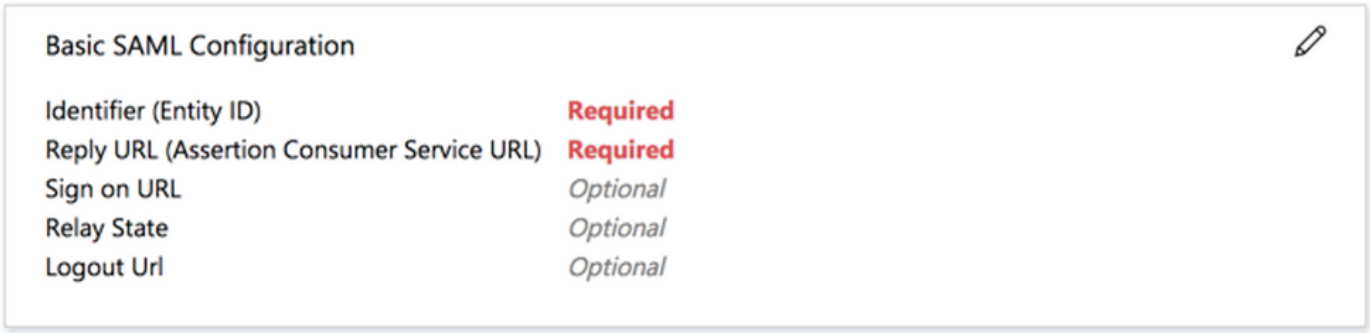
b. Reply URL (Assertion Consumer Service URL) - https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-G

Example: vpn url called

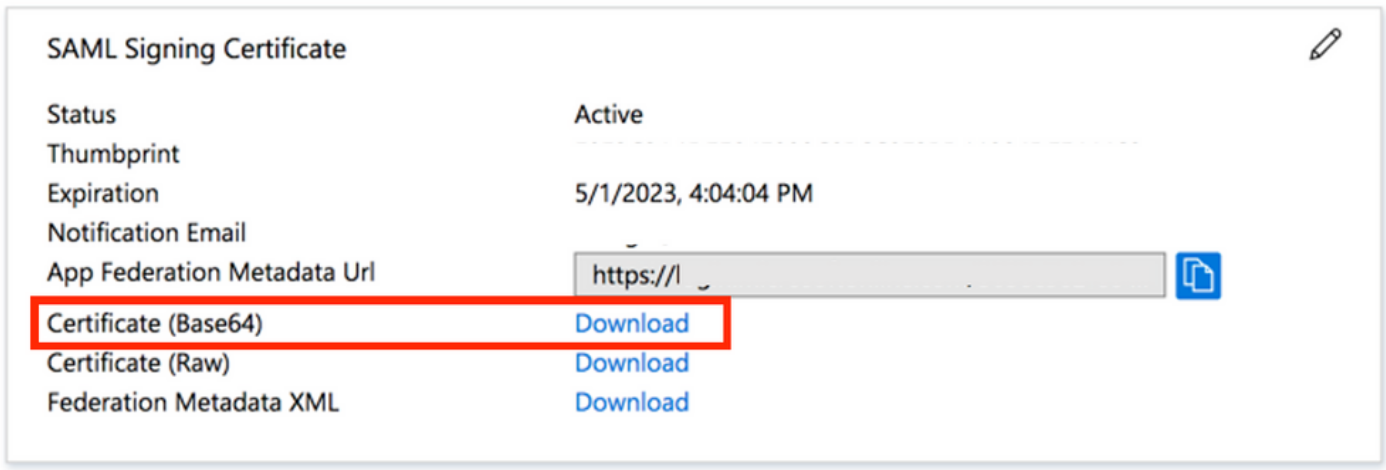
asa.example.com

and tunnel-group called

AnyConnectVPN-1

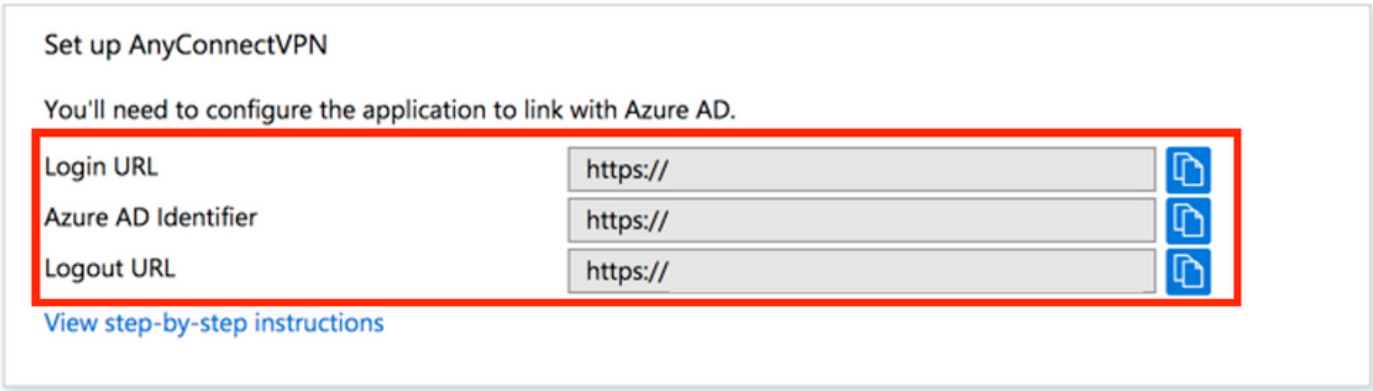


步骤 8在SAML Signing Certificate部分中，选择Download以下载证书文件，然后将其保存到您的计算机上。



步骤 9对于ASA配置，这是必需的。

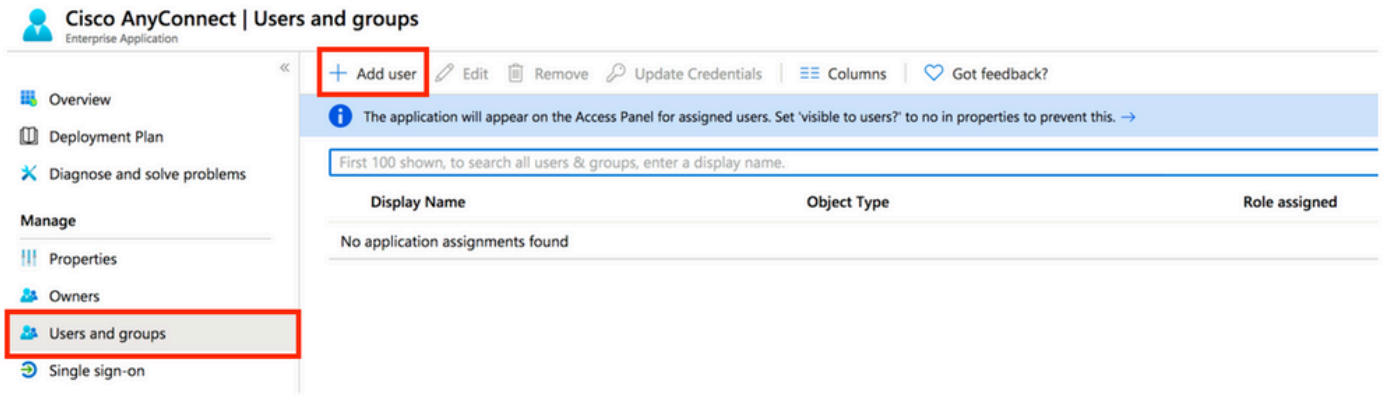
- Azure AD Identifier — 这是我们的VPN配置中的saml idp。
- 登录URL — 这是URL登录。
- 注销URL — 这是URL注销。



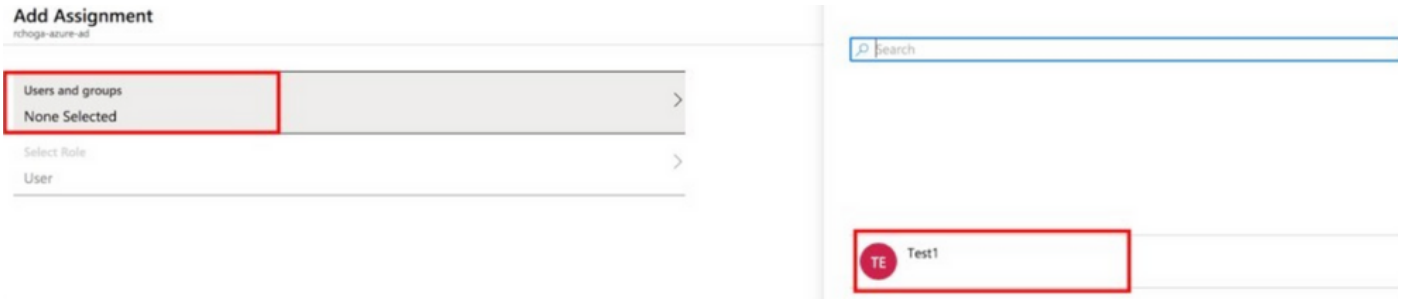
将Azure AD用户分配给应用

在本节中，当您授予Cisco AnyConnect应用的访问权限时，Test1将启用为使用Azure单点登录。

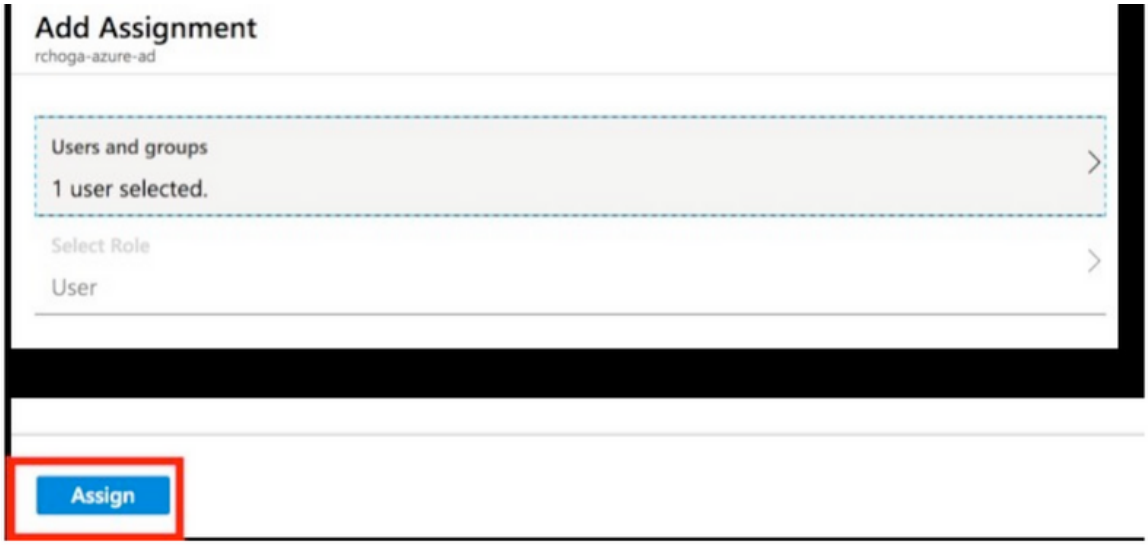
步骤1:在应用的概述页面中，选择Users and groups，然后选择Add user。



第二步：在Add Assignment对话框中选择Users and groups。



第三步： 在Add Assignment对话框中，单击Assign按钮。



通过CLI为SAML配置ASA

步骤1: 创建信任点并导入我们的SAML证书。

```
config t

 crypto ca trustpoint AzureAD-AC-SAML
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate AzureAD-AC-SAML
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded goes here
 …
 -----END CERTIFICATE-----
 quit
```

第二步： 这些命令会调配您的SAML IdP。

```
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/common/wsfederation?wa=wsignout1.0 - Logout URL
 trustpoint idp AzureAD-AC-SAML - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

第三步： 将SAML身份验证应用于VPN隧道配置。

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
  authentication saml
end

write memory
```

注：如果更改IdP配置，您需要从隧道组删除saml identity-provider配置，然后重新应用该配置，以使更改生效。

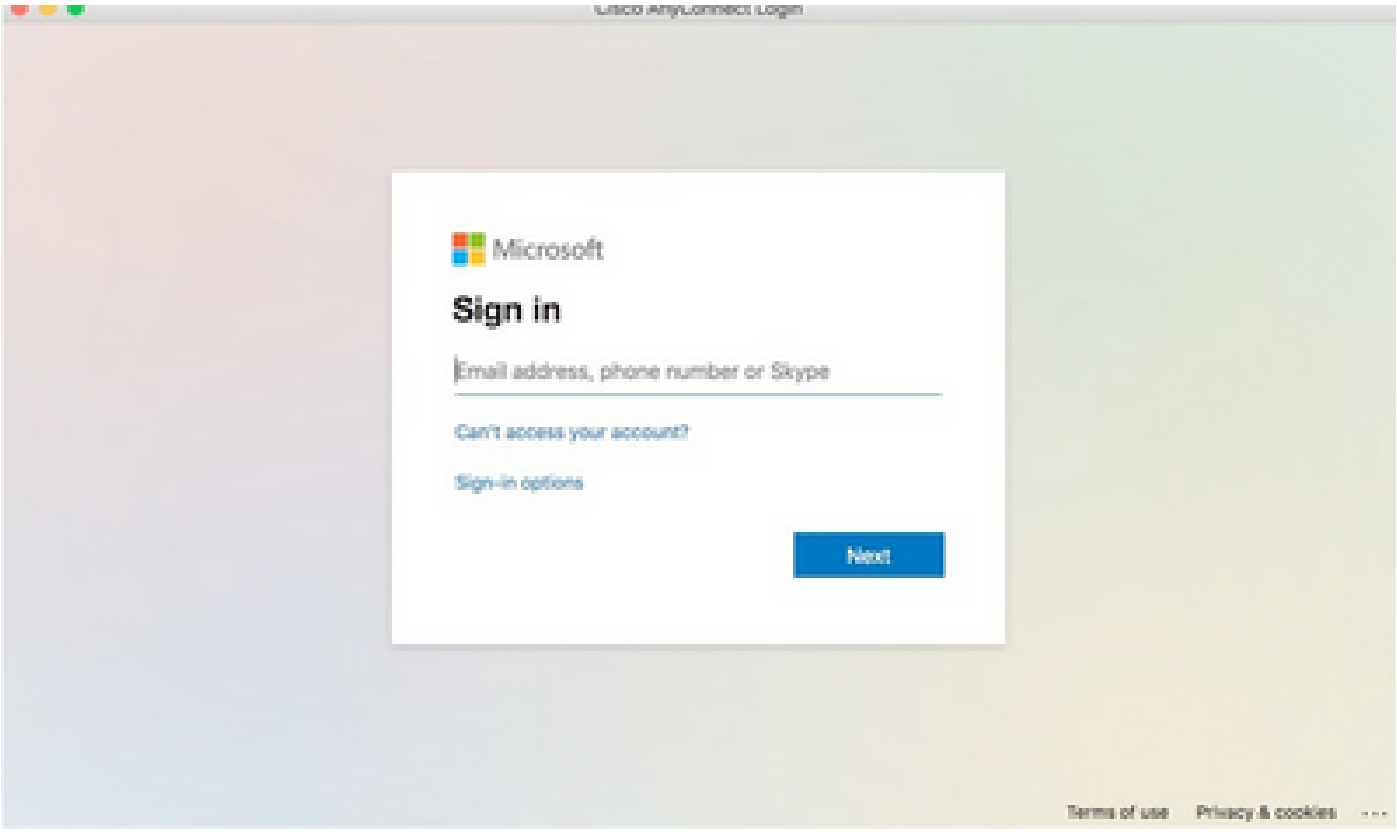
验证

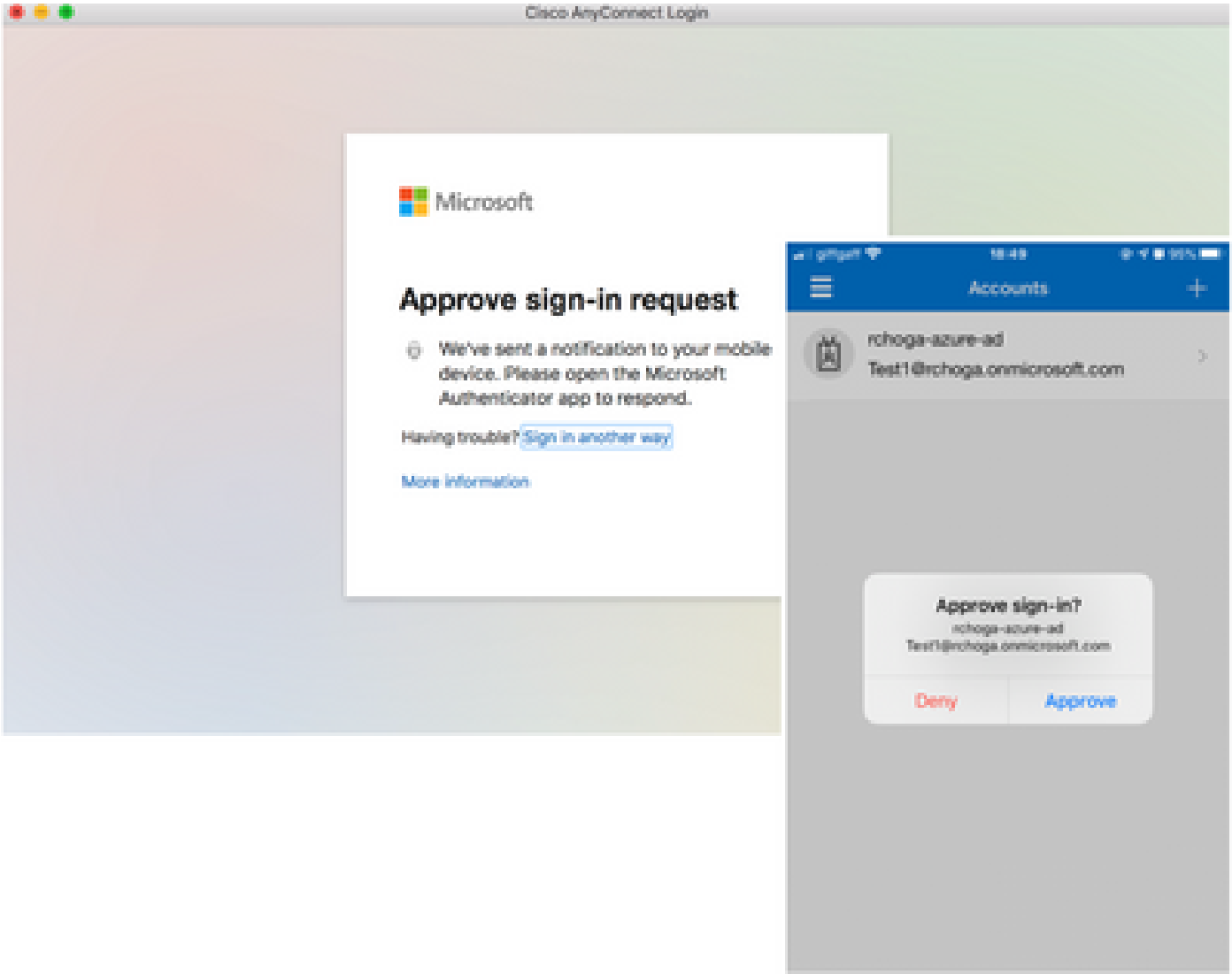
使用SAML身份验证测试AnyConnect

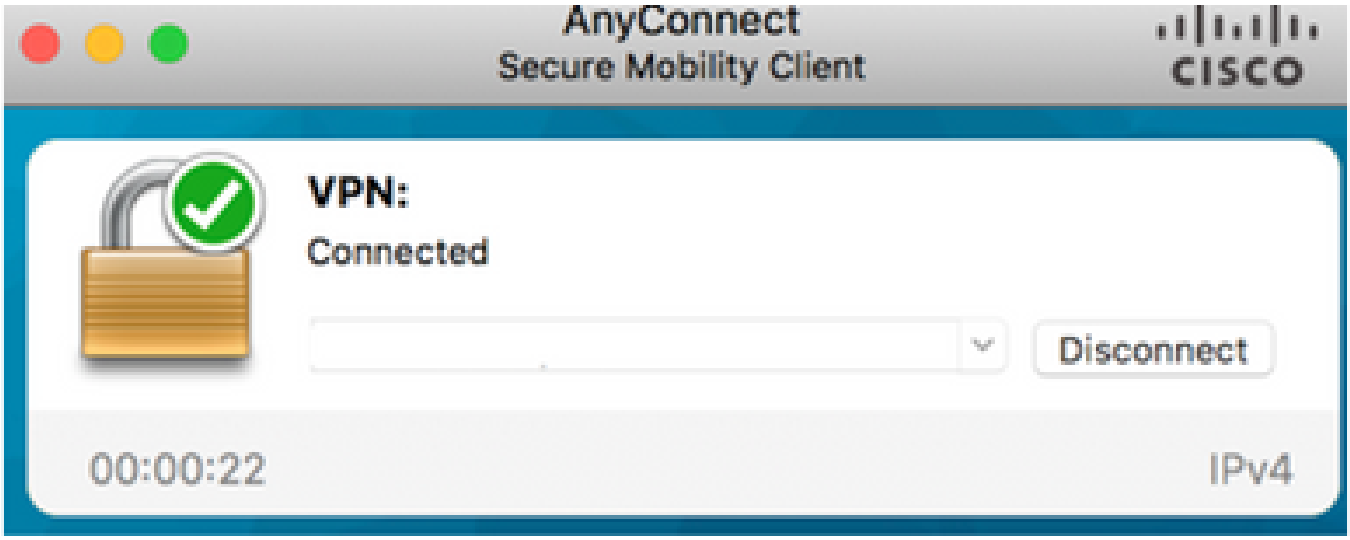
步骤1: 连接到您的VPN URL并在Azure AD详细信息中输入您的日志。

步骤2.批准登录请求。

步骤3. AnyConnect已连接。


Cisco AnyConnect Login
Microsoft
Sign in
Email address, phone number or Skype
Can't access your account?
Sign-in options
Next
Terms of use
Privacy & cookies


Cisco AnyConnect Login
Microsoft
Approve sign-in request
We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.
Having trouble? Sign in another way
More information
Accounts
rchoga-azure-ad
Test1@rchoga.onmicrosoft.com
Approve sign-in?
rchoga-azure-ad
Deny
Approve



常见问题

实体ID不匹配

调试示例：

[SAML] consume_assertion：提供商的标识符是未知的#LassoServer。要在#LassoServer对象中注册提供程序，必须使用方法lasso_server_add_provider()或lasso_server_add_provider_from_buffer()。

问题：通常，表示ASA的webvpn配置下的saml idp [entityID]命令与IdP元数据中的IdP实体ID不匹配。

解决方案：检查IdP的元数据文件的实体ID，并更改saml idp [entity id]命令以匹配此项。

时间不匹配

调试示例：

[SAML] NotBefore:2017-09-05T23:59:01.896Z NotOnOrAfter:2017-09-06T00:59:01.896Z超时：0

[SAML] consume_assertion：断言已过期或无效

问题 1. ASA时间未与IdP的时间同步。

解决方案 1.为ASA配置IdP使用的同一NTP服务器。

问题 2. 断言在指定时间之间无效。

解决方案 2. 修改ASA上配置的超时值。

使用了错误的IdP签名证书

调试示例：

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsa-sha1:subj=EVP_VerifyFinal:error=18:data do not match:signature do not match

[SAML] consume_assertion：配置文件无法验证消息上的签名

问题：ASA无法验证由IdP签名的消息，或者没有供ASA验证的签名。

解决方案：检查ASA上安装的IdP签名证书，以确保其与IdP发送的内容匹配。如果确认这一点，请确保签名包含在SAML响应中。

断言受众无效

调试示例：

[SAML] consume_assertion：断言受众无效

问题：IdP定义不正确的受众。

解决方案：更正IdP上的受众配置。它必须与ASA的实体ID匹配。

Assertion Consumer Service的URL错误

调试示例：发送初始身份验证请求后，无法接收任何调试。用户能够在IdP输入凭证，但IdP不会重定向到ASA。

问题：为错误的断言消费者服务URL配置了IdP。

解决方案：检查配置中的基本URL并确保其正确。使用show检查ASA元数据，确保Assertion Consumer Service URL正确。要测试它，请浏览它。如果两者在ASA上都正确，请检查IdP以确保URL正确。

未生效的SAML配置更改

示例：在修改或更改单点登录URL后，SP证书SAML仍然无法正常运行并发送之前的配置。

问题：当存在影响它的配置更改时，ASA需要重新生成其元数据。它不会自动执行此操作。

解决方案：进行更改后，在受影响的隧道组下删除并重新应用saml idp [entity-id]命令。

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可用于排除大多数问题，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：

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

相关信息

- 使用应用代理实现本地应用的SAML单点登录

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）。