配置安全防火墙和内部ID的SAML组策略

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- FMC SAML配置
- FMC RAVPN隧道组配置
- FMC RAVPN组策略配置
- FTD元数据
- Microsoft Entra ID

验证

- FTD

故障排除

相关信息

简介

本文档介绍如何使用MS Entra ID为Cisco安全防火墙上的Cisco安全客户端分配SAML身份验证组策略。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全客户端AnyConnect VPN
- Microsoft Entra ID身份提供程序(IdP)配置
- Cisco Firepower威胁防御(FTD)或思科安全防火墙ASA远程访问VPN和单点登录(SSO)服务器对象配置

使用的组件

本指南中的信息基于以下硬件和软件版本：

- FTD版本7.6
- FMC版本7.6
- MS Entra ID SAML IdP

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（Security Assertion Markup Language，安全声明标记语言）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，允许用户一次登录(SSO)多个服务。SAML可用于思科安全客户端连接到ASA和FTD VPN头端的远程访问VPN身份验证，其中ASA或FTD是信任圈的SP。

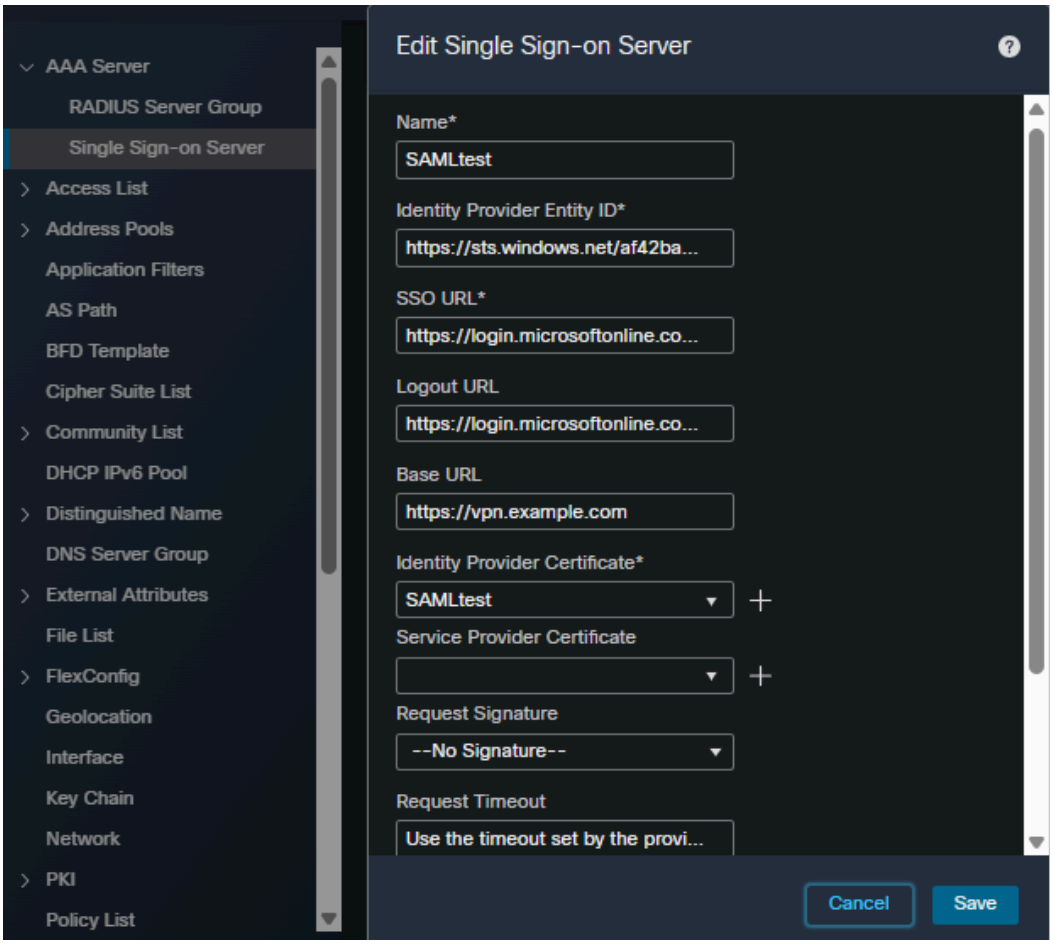
在本文档中，Microsoft Entra ID/Azure用作IdP。但是，您可以使用其他IdP分配组策略，因为它基于SAML断言中可发送的标准属性。

注意：请注意，每个用户必须仅属于MS Entra ID上的一个用户组，因为发送到ASA或FTD的多个SAML属性可能会导致组策略分配问题，详见Cisco bug ID CSCwm3613。

配置

FMC SAML配置

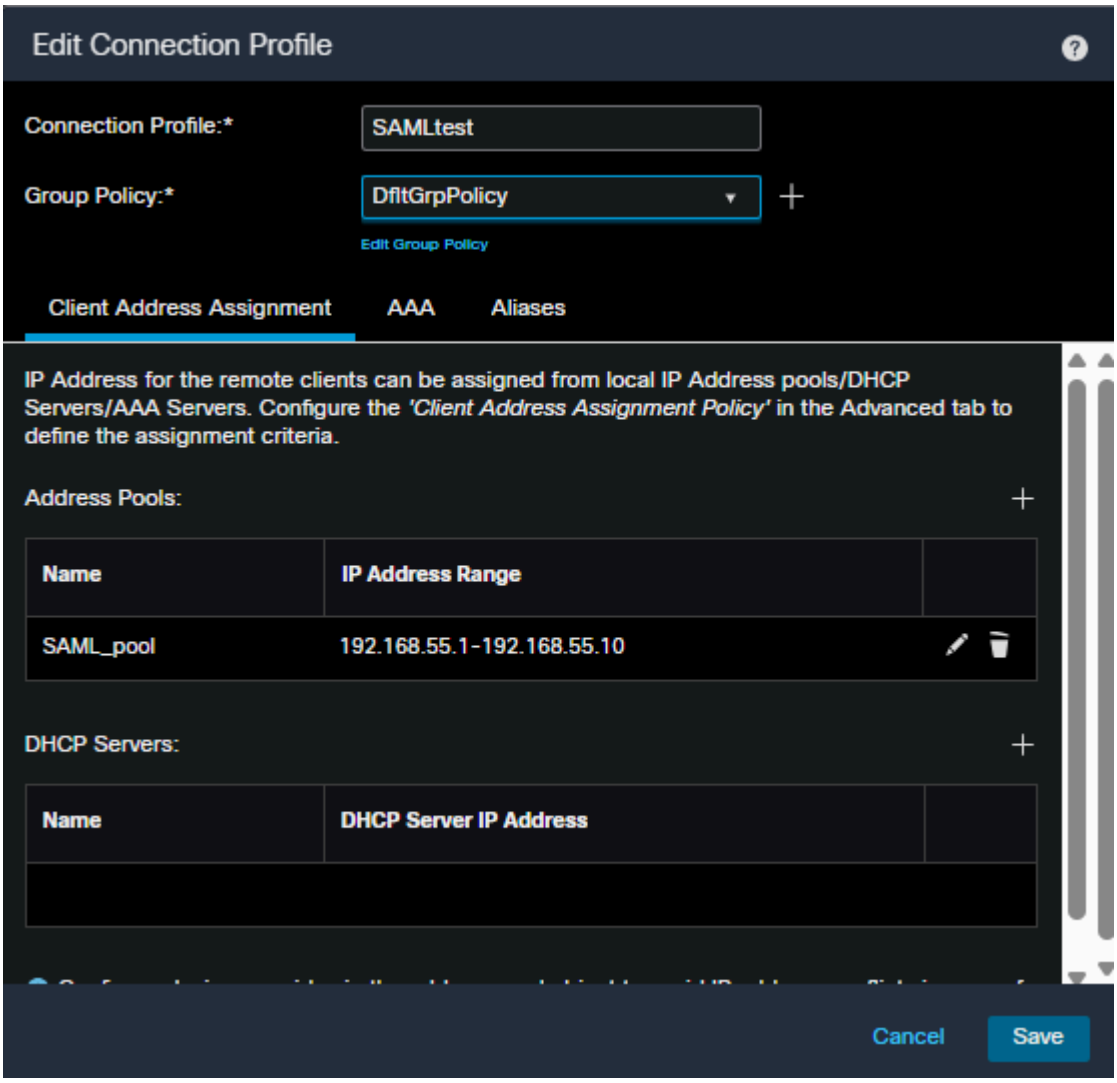
1.在FMC上，导航到对象>对象管理> AAA服务器>单点登录服务器。从IdP获取实体ID、SSO URL、注销URL和身份提供程序证书，请参阅Microsoft Entra ID部分中的步骤6。基本URL和服务提供商证书特定于添加配置的FTD。



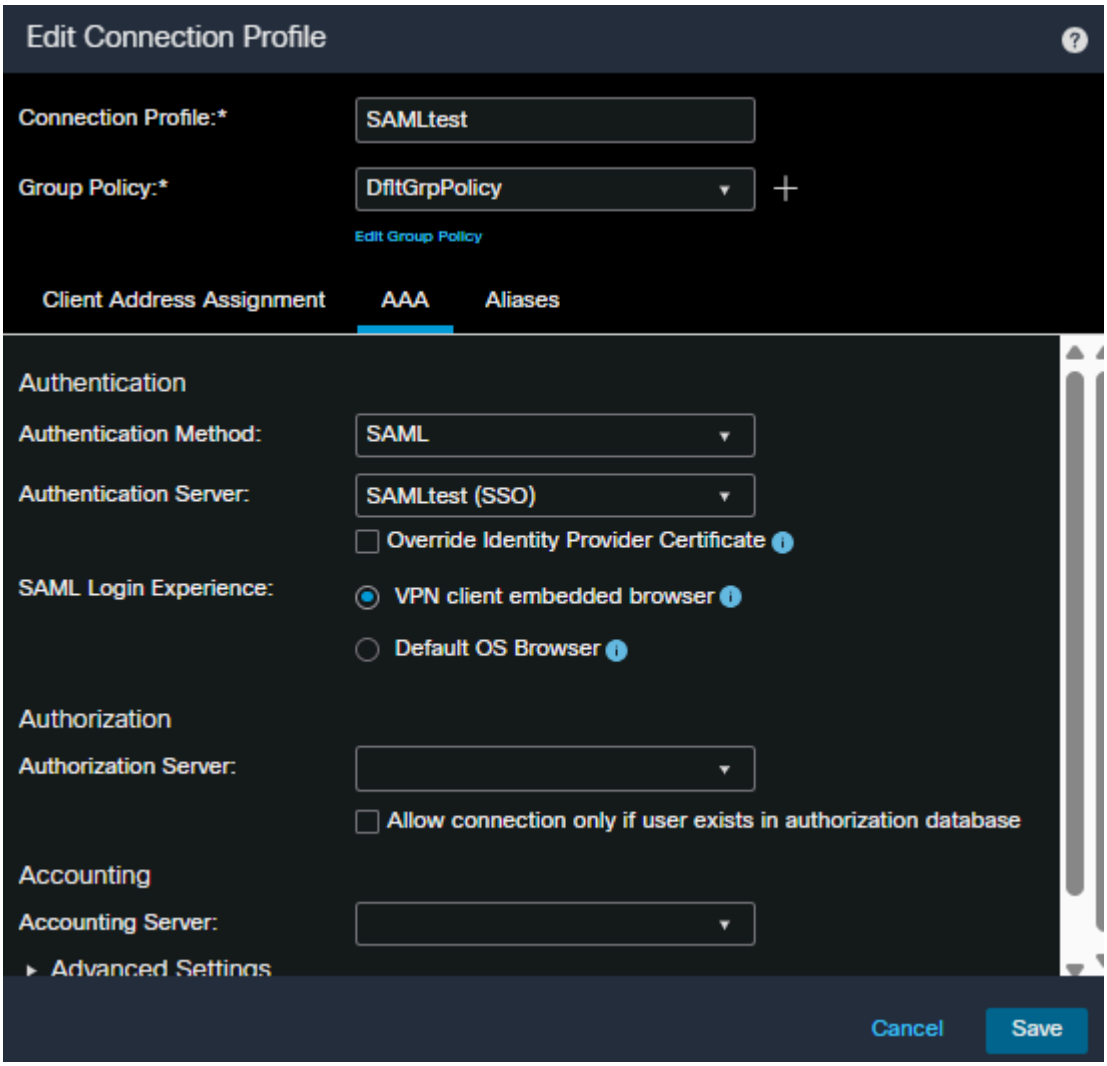
FMC SSO对象配置

FMC RAVPN隧道组配置

1.在FMC上，导航到设备> VPN >远程访问>连接配置文件，然后为正在配置的FTD选择或创建VPN策略。选择后，创建与以下内容类似的连接配置文件：



FMC连接配置文件地址分配

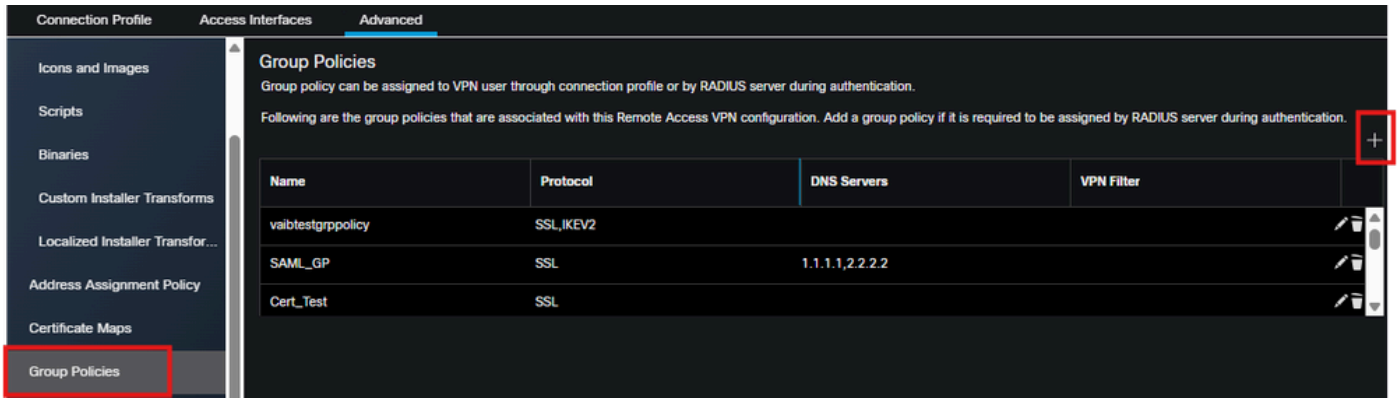


FMC连接配置文件AAA配置

FMC RAVPN组策略配置

1.您必须为Microsoft Entra ID上的每个用户组创建具有所需选项的组策略，并将其添加到正在配置的FTD的RAVPN策略中。

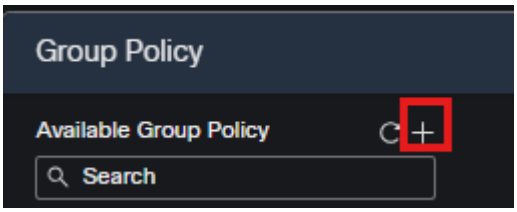
2.定位至设备> VPN >远程访问>高级，然后从左侧选择组策略。然后点击右上方的+以添加组策略。



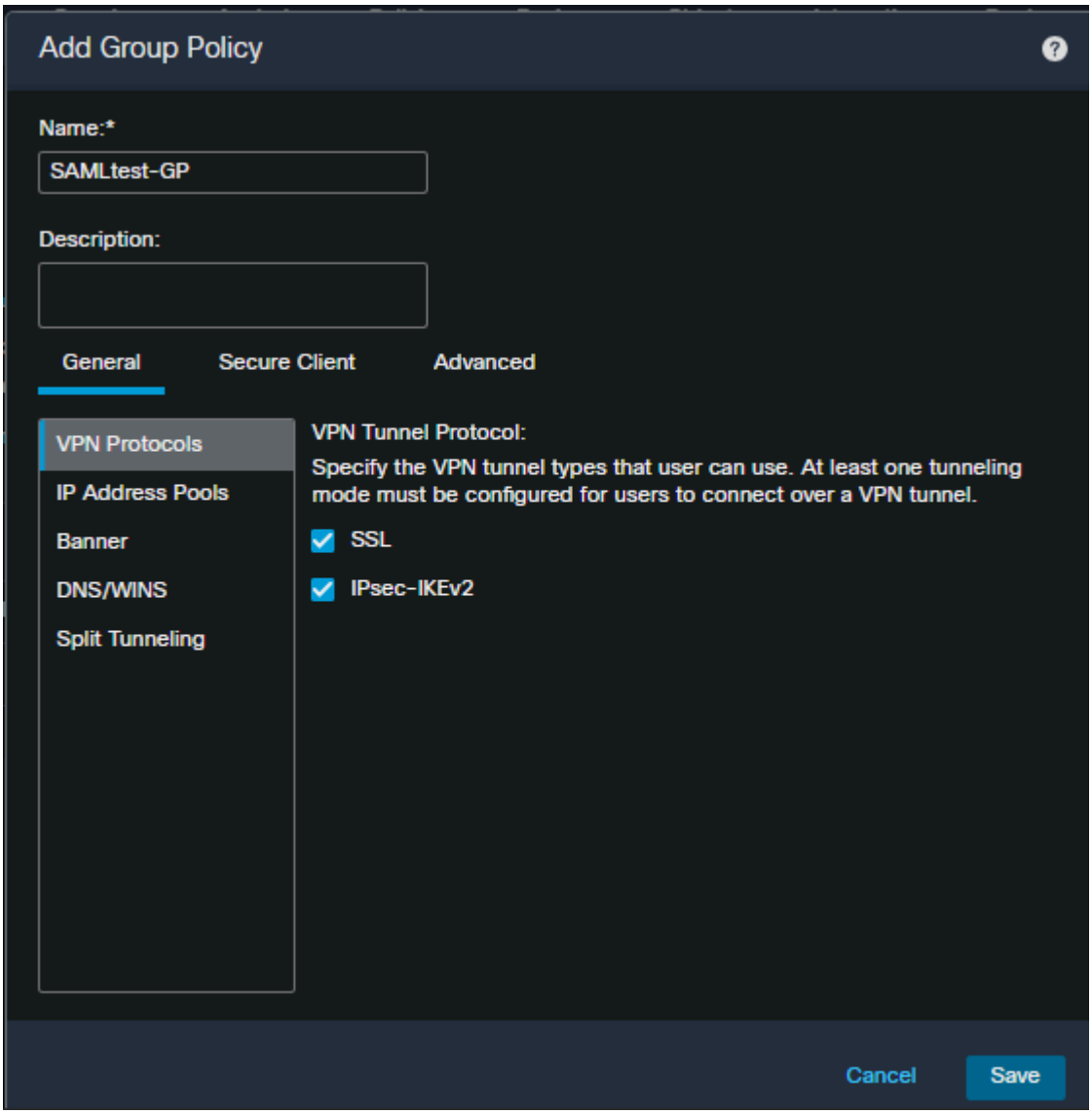
FMC添加组策略

3.单击弹出窗口中的+以查看对话框并创建新的组策略。填写所需选项并保存。

注意：如果已经创建了所需的组策略，则可以跳过此步骤并继续步骤4。

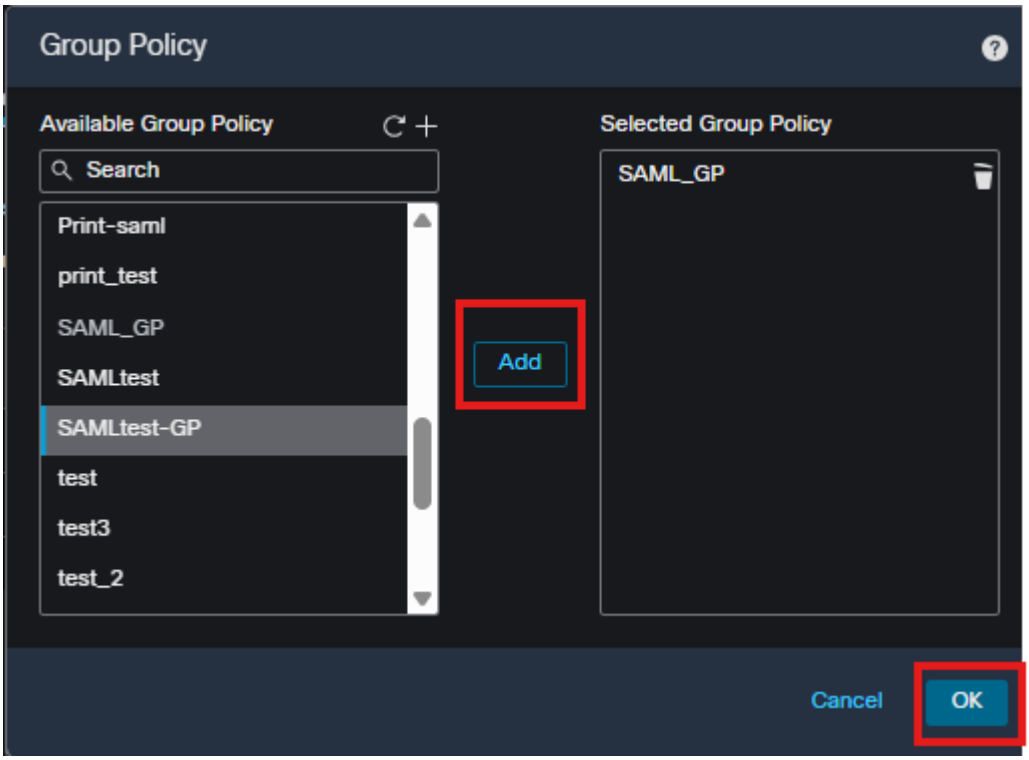


创建新组策略



组策略选项

4.在左侧列表中选择新创建的组策略，单击Add按钮，然后单击OK保存列表。



添加组策略

FTD元数据

1.将配置部署到FTD后，导航到FTD CLI并运行show saml metadata <tunnel group name> 命令，然后收集FTD Entity ID和ACS URL。

注意：为了简洁，元数据中的证书被截断。

<#root>

```
FTD# show saml metadata SAMLtest
SP Metadata
-----------
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="

https://vpn.example.net/saml/sp/metadata/SAMLtest

" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="ur
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
```

```
<ds:X509Certificate>
MIIFWzCCBEOgAwIBAgITRwAAAAgZ9Nmfv5mpJQAAAAAACDANBgkqhkiG9w0BAQsF
ADBJMRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGcnRwdnBu
MRowGAYDVQQDExFydHB2cG4tV0lOQVVUSC1DQTAeFw0yNTAzMjUxNzU5NDZaFw0y
NzAzMjUxNzU5NDZaMDAxDzANBgNVBAoTBlJUUFZQTjEdMBsGA1UEAxMUcnRwdnBu
LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9FO4LE88attuGuVMquV+1ODRPAO6a6QNwkehBOUn7XzTNepJO2JQtxdNR2t

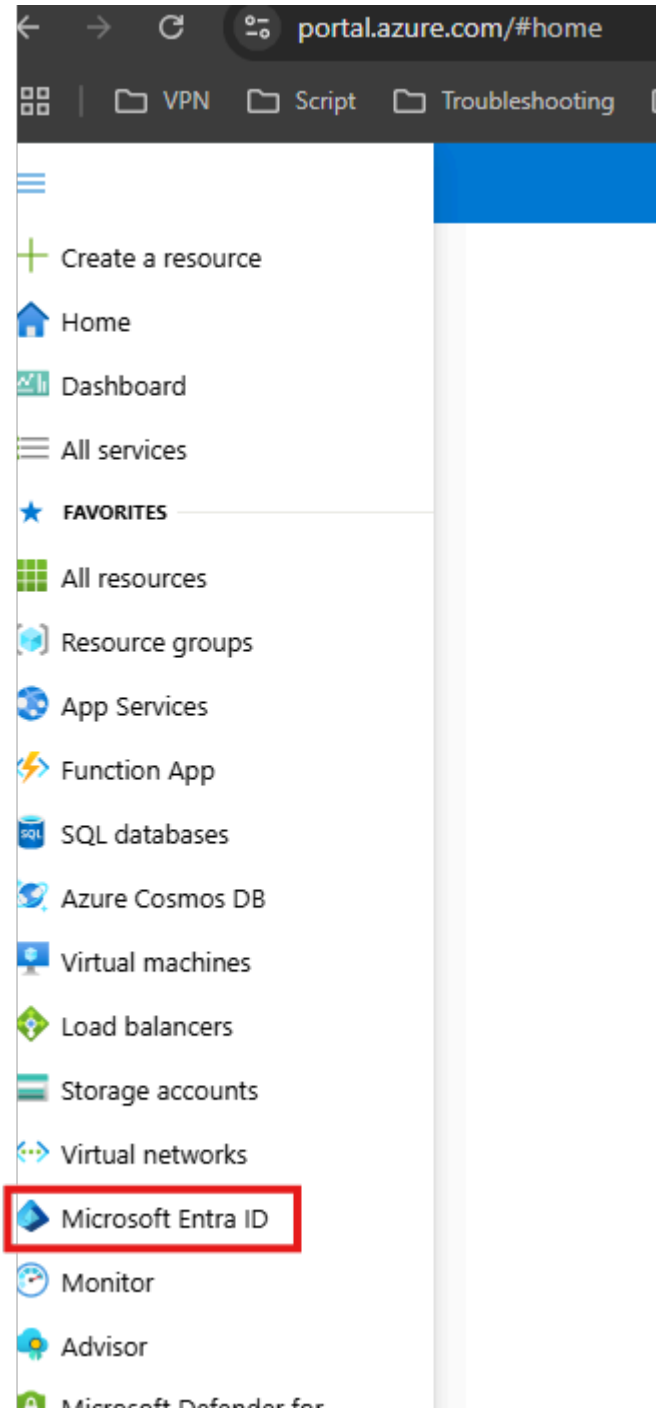
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP

https://vpn.example.net/+CSCOE+/saml/sp/acs?tgname=SAMLtest

" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn
</EntityDescriptor>
```

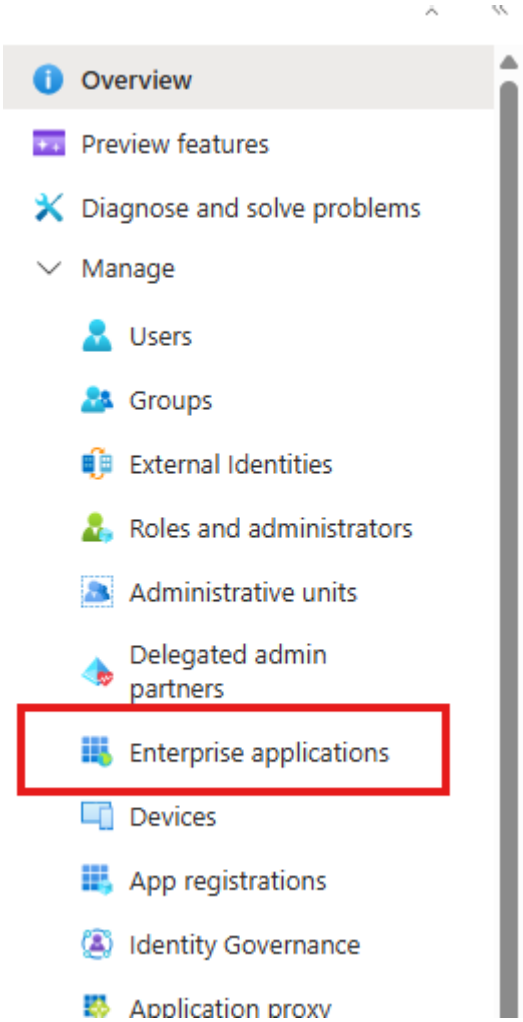
Microsoft Entra ID

1.在Microsoft Azure门户上，从左侧的菜单中选择Microsoft Entra ID。



Microsoft Entra ID

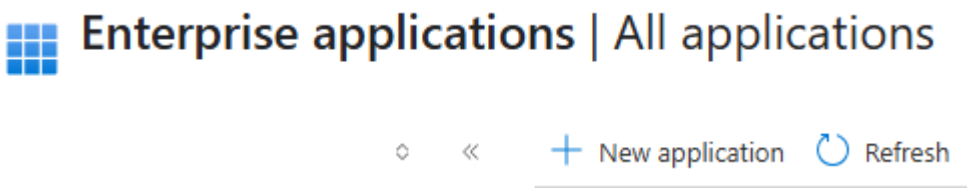
2.选择企业应用。



企业应用

3.选择New Application。

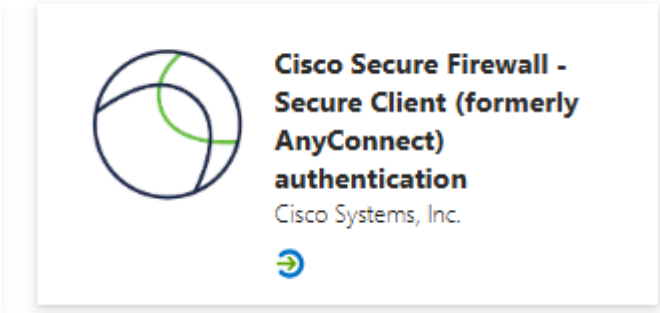
注意：如果已经为FTD RAVPN配置了企业应用，请跳过后续步骤，继续执行步骤7。



MS Entra ID企业应用程序

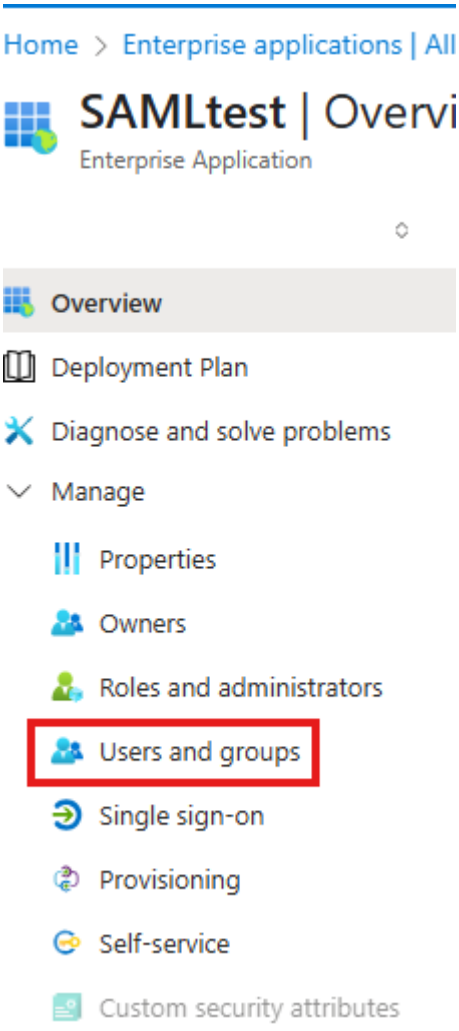
4.选择Featured Applications下的Cisco Secure Firewall - Secure Client（以前称为

AnyConnect）Authentication。为应用程序指定一个名称，然后选择创建。



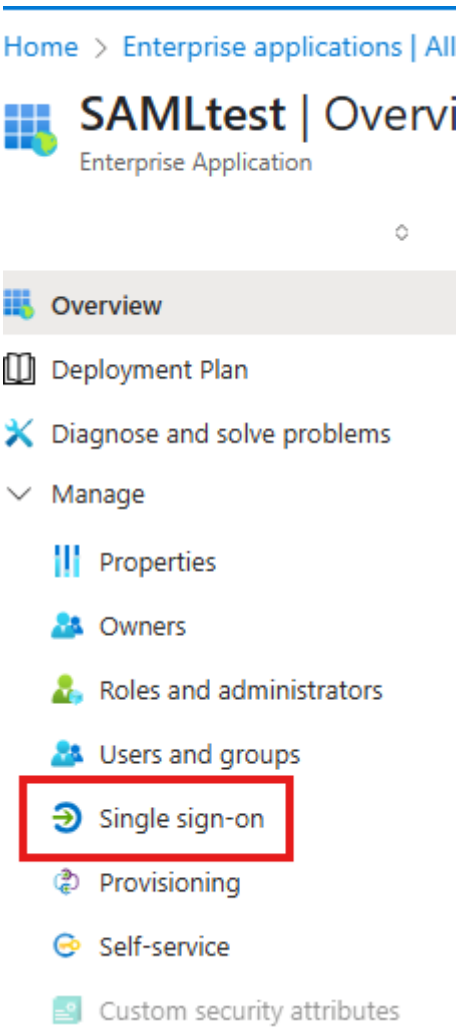
MS Entra ID思科安全防火墙安全客户端（以前称为AnyConnect）身份验证应用

5.在应用程序中，选择用户和组，然后将所需的用户名或组名分配给应用程序。

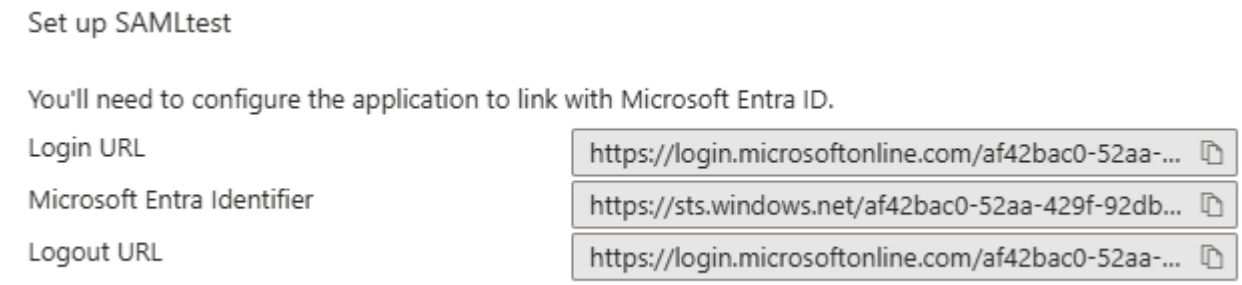


用户和组

6.选择Single Sign-On > SAML，并检索本指南的FMC SAML配置部分的登录URL、Microsoft Entra标识符和注销URL。

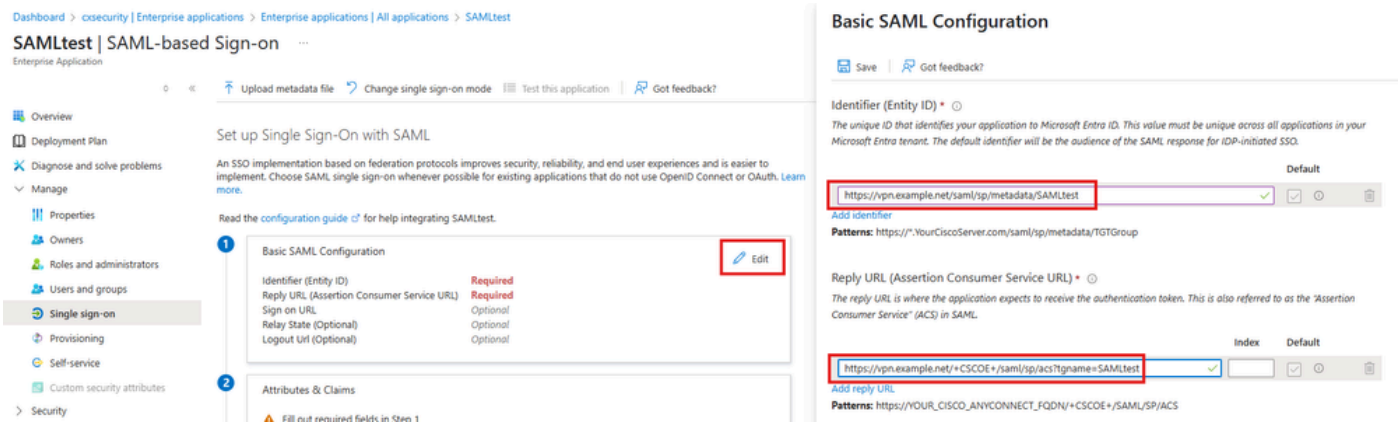


单一登录



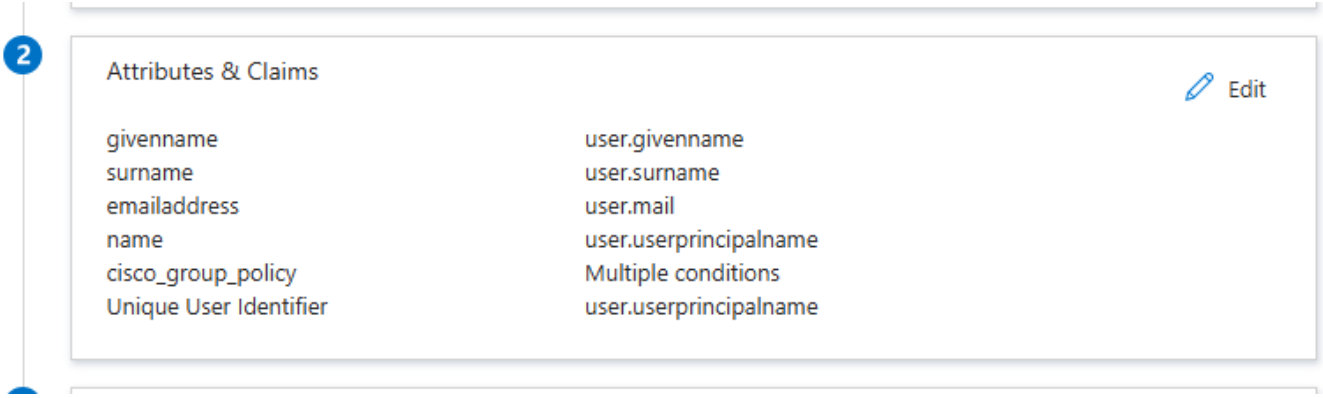
IdP URL

7.使用从FTD元数据中检索到的标识符（实体ID）和应答(ACS)URL配置基本SAML配置并保存(Save)。



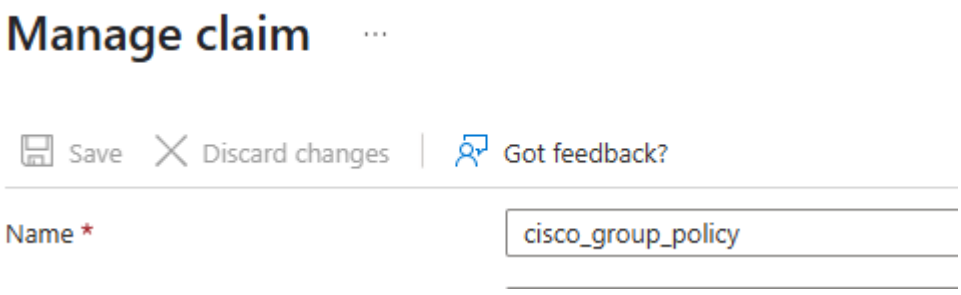
基本SAML配置

8.选择Attribute & Claims的Edit，然后单击Add New Claim。



属性和索赔

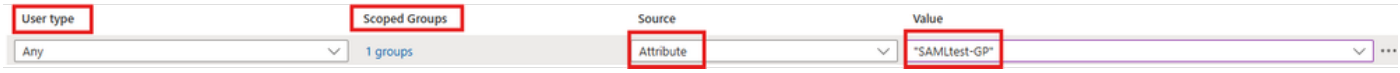
9.新领款申请名称必须是cisco_group_policy。



管理领款

10.展开索赔条件一节。选择User type and Scoped Groups，然后在Source下，选择Attribute，然后在Value下拉菜单中的FTD配置中添加正确的组策略名称，然后单击Save。

注意：此示例中使用的FTD中的自定义组策略名称为SAMLtest-GP，它是在本指南的FMC RAVPN组策略配置部分中创建的。此值必须替换为与IdP上的每个用户组对应的FTD中的组策略名称。



MS Entra ID声明条件

验证

FTD

要验证所需的组策略，请通过运行show vpn-sessiondb anyconnect命令验证输出：

<#root>

```
FTD# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : RTPVPNtest
Index : 7110
Assigned IP : 192.168.55.3 Public IP : 10.26.162.189
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA256
Bytes Tx : 105817 Bytes Rx : 63694
Group Policy :
```

SAMLtest-GP

```
 Tunnel Group : SAMLtest
Login Time : 16:54:17 UTC Fri May 9 2025
Duration : 0h:11m:19s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : ac127ca101bc6000681e3339
Security Grp : none Tunnel Zone : 0
```

要验证IdP是否发送正确的声明，请在连接到VPN时运行debug webvpn saml 255命令以检索输出。分析调试中的断言输出，并将属性部分与IdP上的配置进行比较。

<#root>

```
<Attribute Name="cisco_group_policy">
<AttributeValue>

SAMLtest-GP

</AttributeValue>
</Attribute>
```

故障排除

<#root>

```
firepower#

show run webvpn


firepower#

show run tunnel-group


firepower#

show crypto ca certificate

firepower#

 debug webvpn saml 255

firepower#

debug webvpn 255

firepower#

debug aaa authorization
```

相关信息

- 思科技术支持和下载
- ASA配置指南
- FMC/FDM配置指南

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）。