使用安全防火牆和Microsoft Entra ID配置SAML的組策略分配

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[設定](#)

- [FMC SAML配置](#)
- [FMC RAVPN隧道組配置](#)
- [FMC RAVPN組策略配置](#)
- [FTD後設資料](#)
- [Microsoft Entra ID](#)

[驗證](#)

- [FTD](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何使用Microsoft Entra ID為Cisco Secure Firewall上的Cisco Secure Client進行SAML身份驗證分配組策略。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco安全使用者端AnyConnect VPN
- Cisco Firepower威脅防禦(FTD)或Cisco安全防火牆ASA遠端訪問VPN和單一登入(SSO)伺服器對象配置
- Microsoft Entra ID身份提供程式(IdP)配置

採用元件

本指南中的資訊基於以下硬體和軟體版本：

- FTD版本7.6

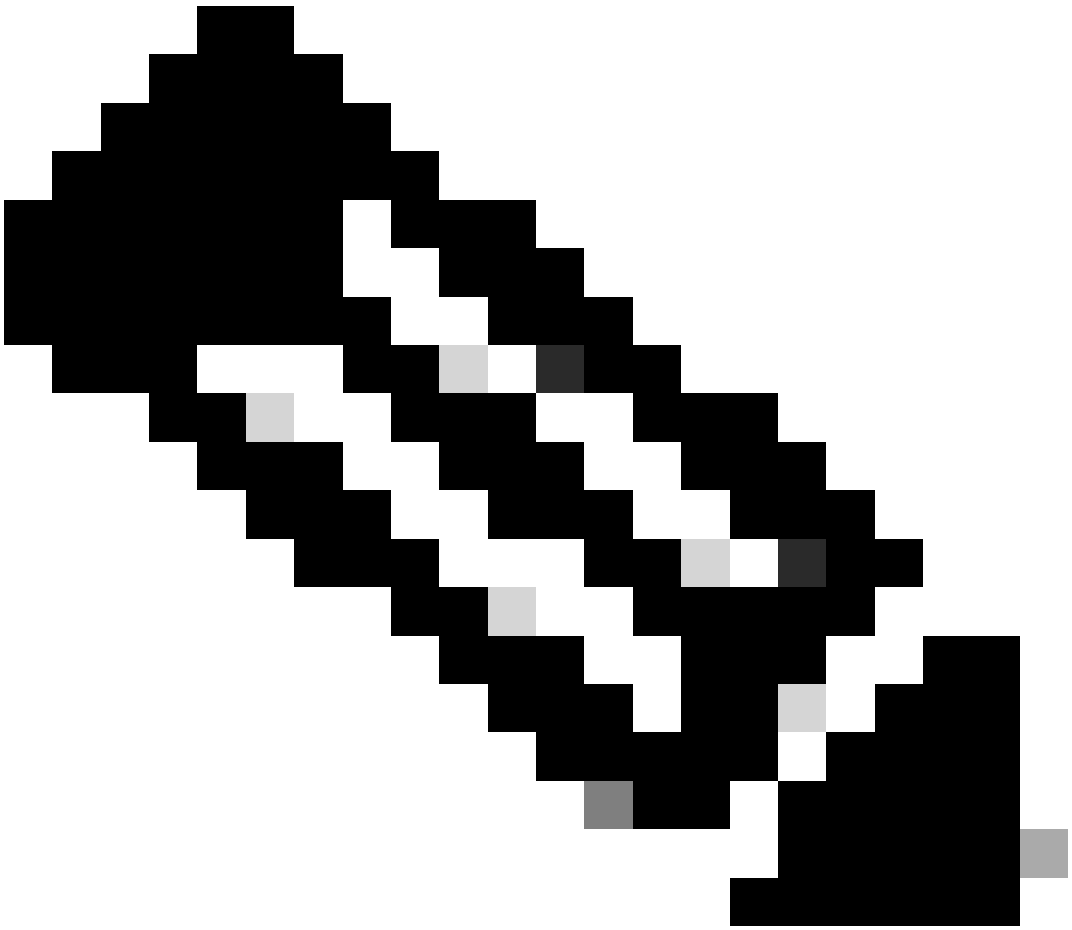
- FMC版本7.6
- MS Entra ID SAML IdP

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

SAML（Security Assertion Markup Language，安全宣告標籤語言）是一個基於XML的框架，用於在安全域之間交換驗證和授權資料。它在使用者、服務提供商(SP)和身份提供者(IdP)之間建立一個信任圈，允許使用者一次性登入多個服務。SAML可用於遠端訪問VPN身份驗證，用於思科安全客戶端連線到ASA和FTD VPN前端，其中ASA或FTD是信任圈中的SP部分。

在本文檔中，Microsoft Entra ID/Azure用作IdP。但是，也可以使用其他IdP分配組策略，因為它基於可以在SAML斷言中傳送的標準屬性。



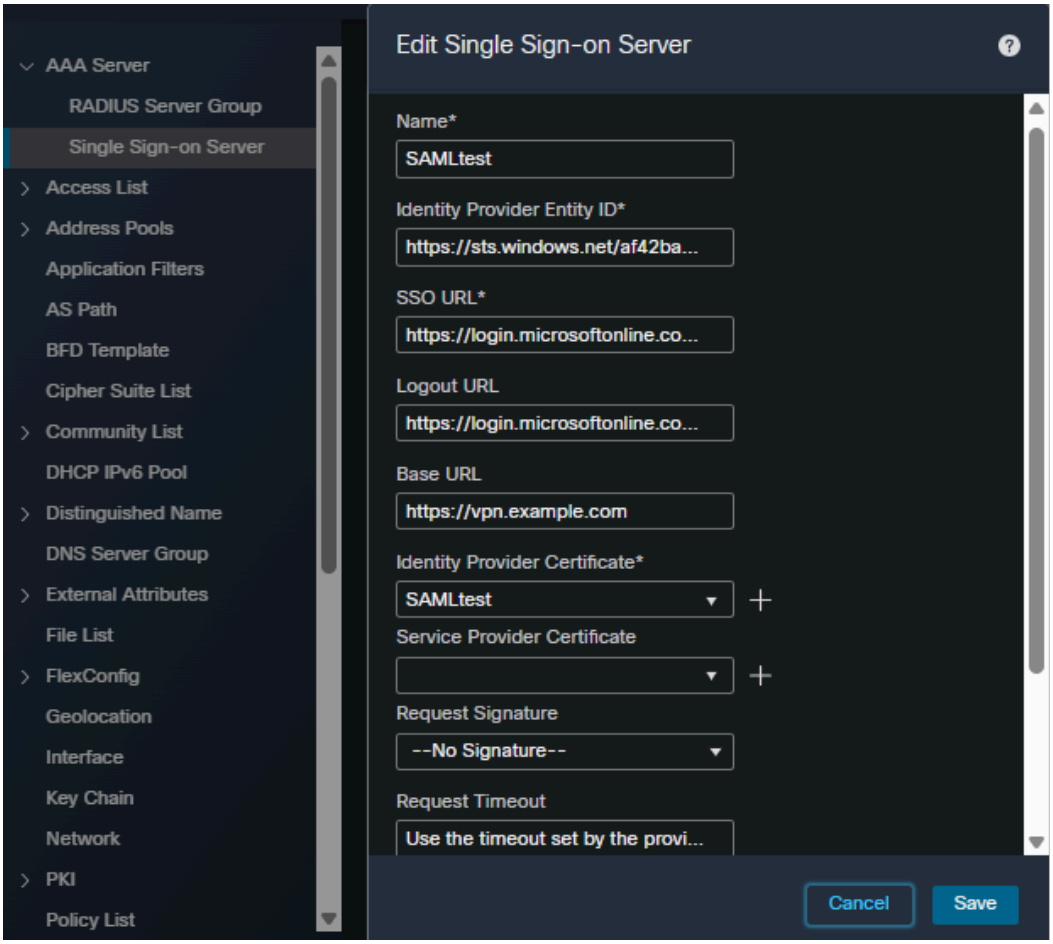
附註：請注意，每個使用者必須僅屬於一個MS Entra ID上的使用者組，因為傳送到ASA或

FTD的多個SAML屬性可能會導致組策略分配問題，如Cisco錯誤ID CSCwm33613中所述

設定

FMC SAML配置

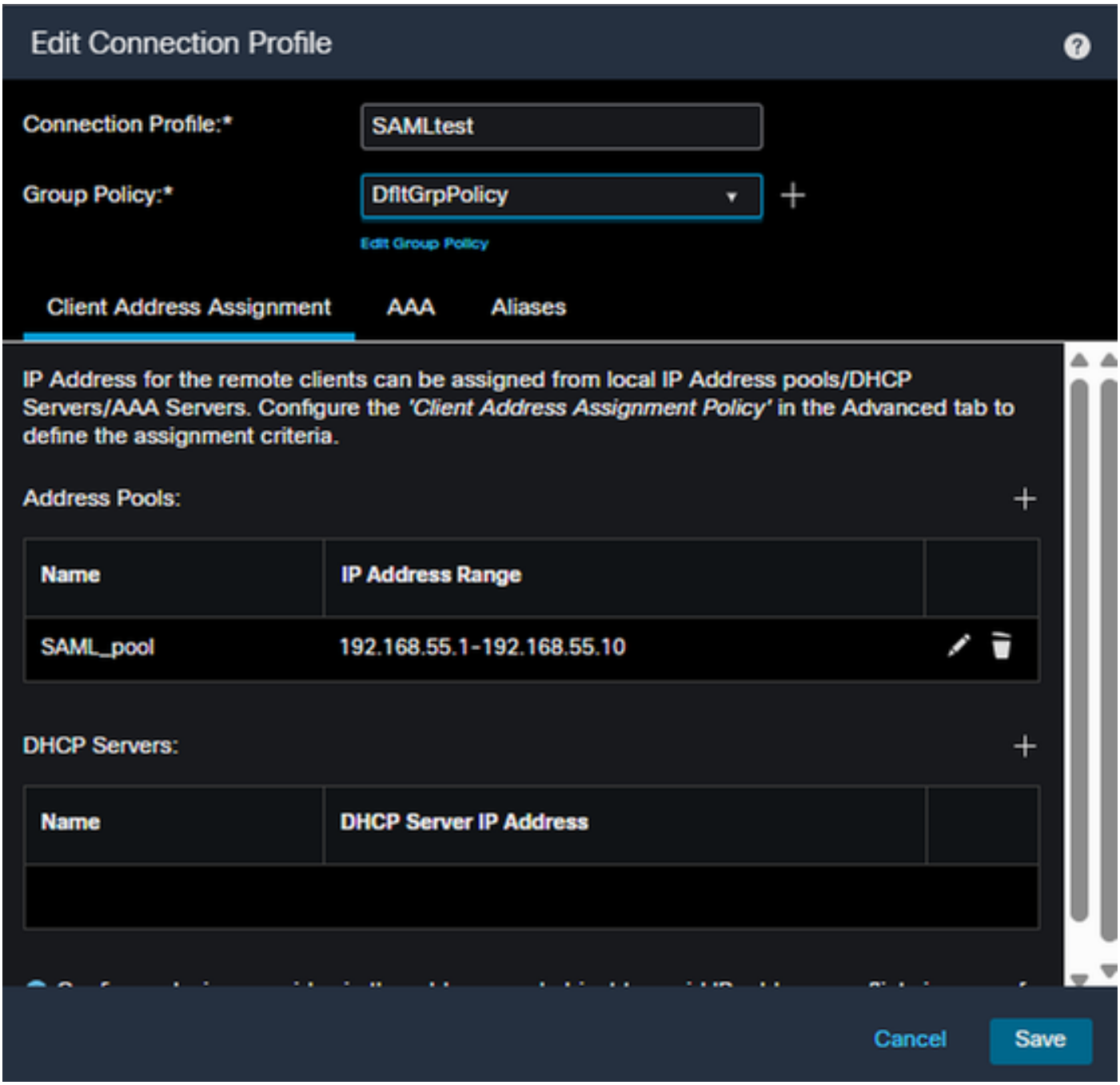
在FMC上，導航到對象>對象管理> AAA伺服器>單點登入服務器。從IdP獲取實體ID、SSO URL、註銷URL和身份提供程式證書，請參閱Microsoft Entra ID部分中的步驟6。基本URL和服務提供者憑證是待新增組態的FTD所特定的。



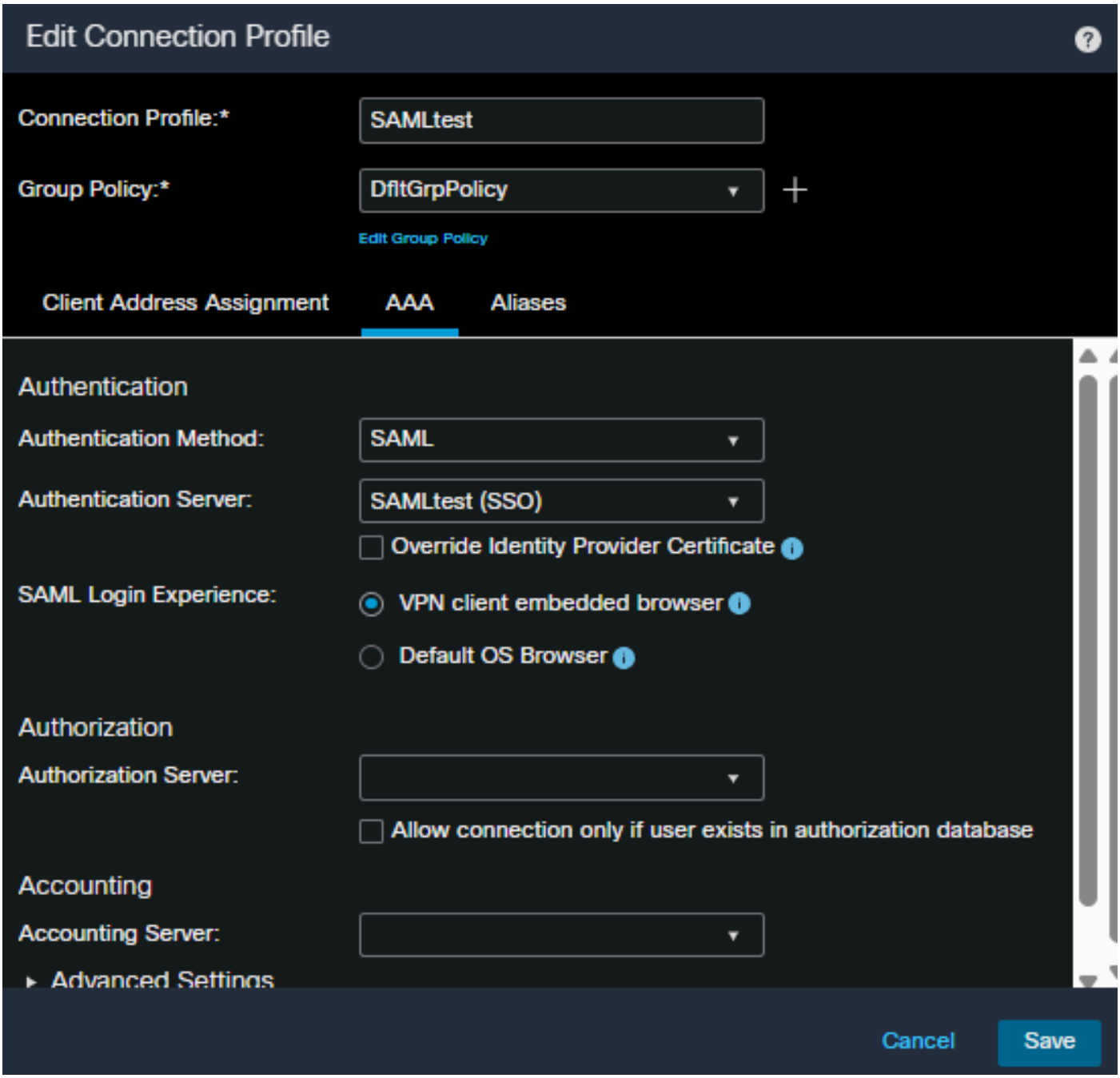
FMC SSO對象配置

FMC RAVPN隧道組配置

在FMC上，導覽至Devices > VPN > Remote Access > Connection Profile，然後選擇或建立您要配置的FTD的VPN策略。選擇後，建立與以下內容類似的連線配置檔案：



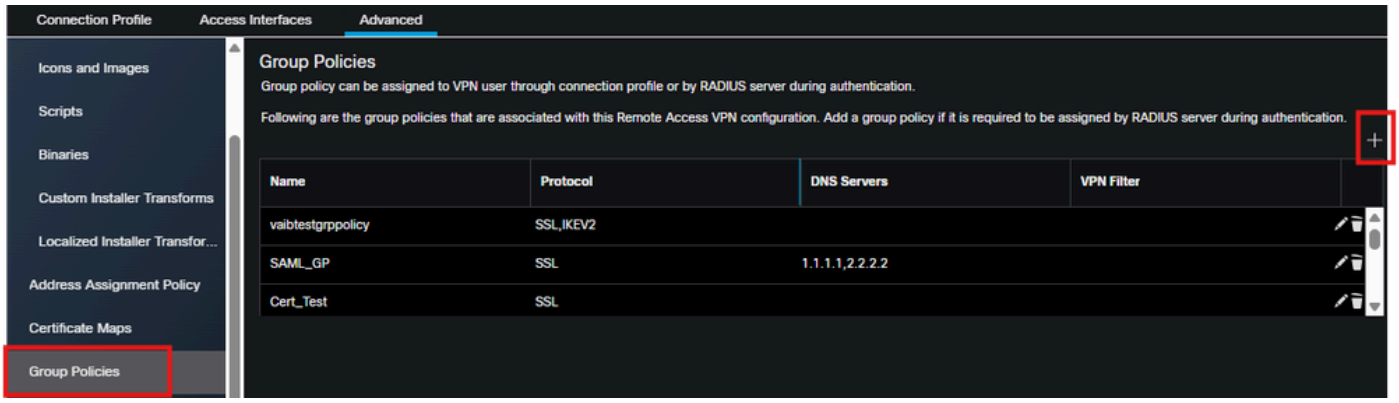
FMC連線配置檔案地址分配



FMC連線配置檔案AAA配置

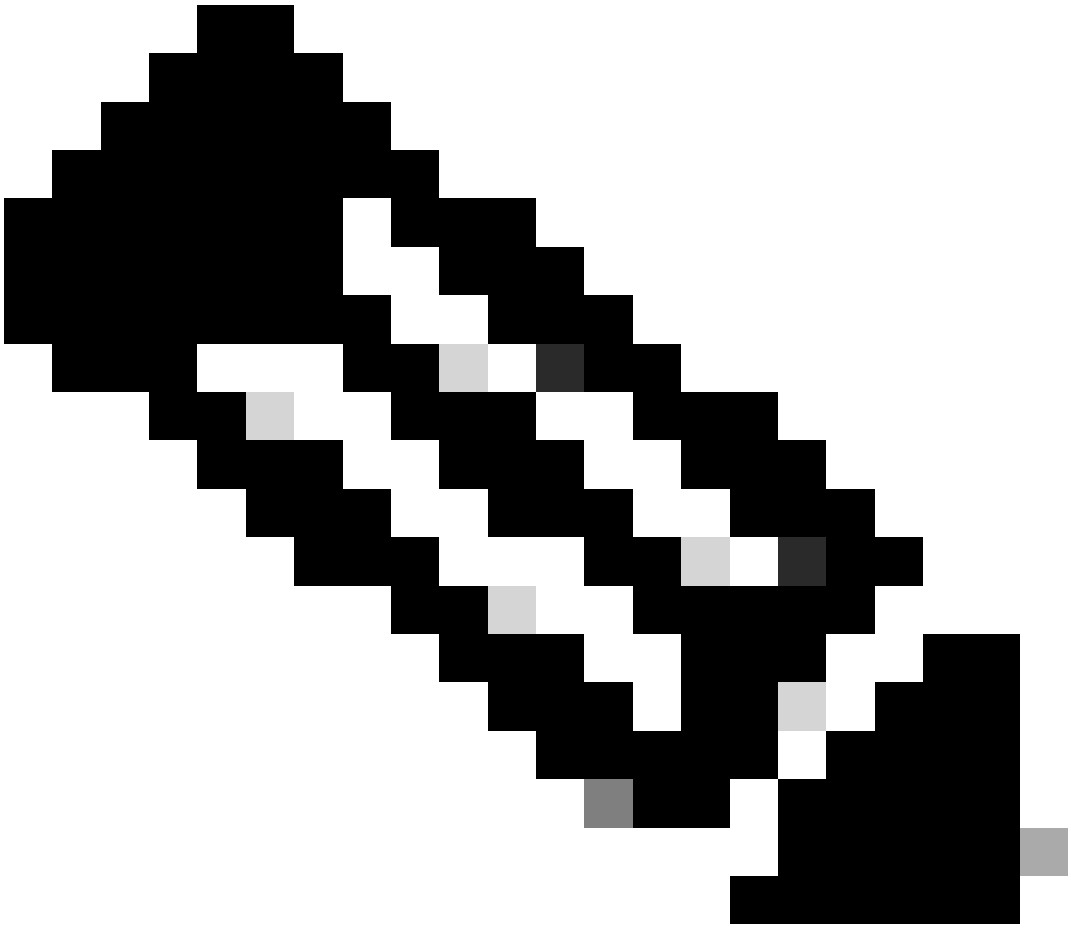
FMC RAVPN組策略配置

1.您必須為Entra ID上的每個使用者組建立一個包含所需選項的組策略，並將其新增到要配置的FTD的RAVPN策略中。這可以通過導航到Devices > VPN > Remote Access > Advanced並從左側選擇Group Policies，然後按一下右上方的+ 以新增組策略來實現。

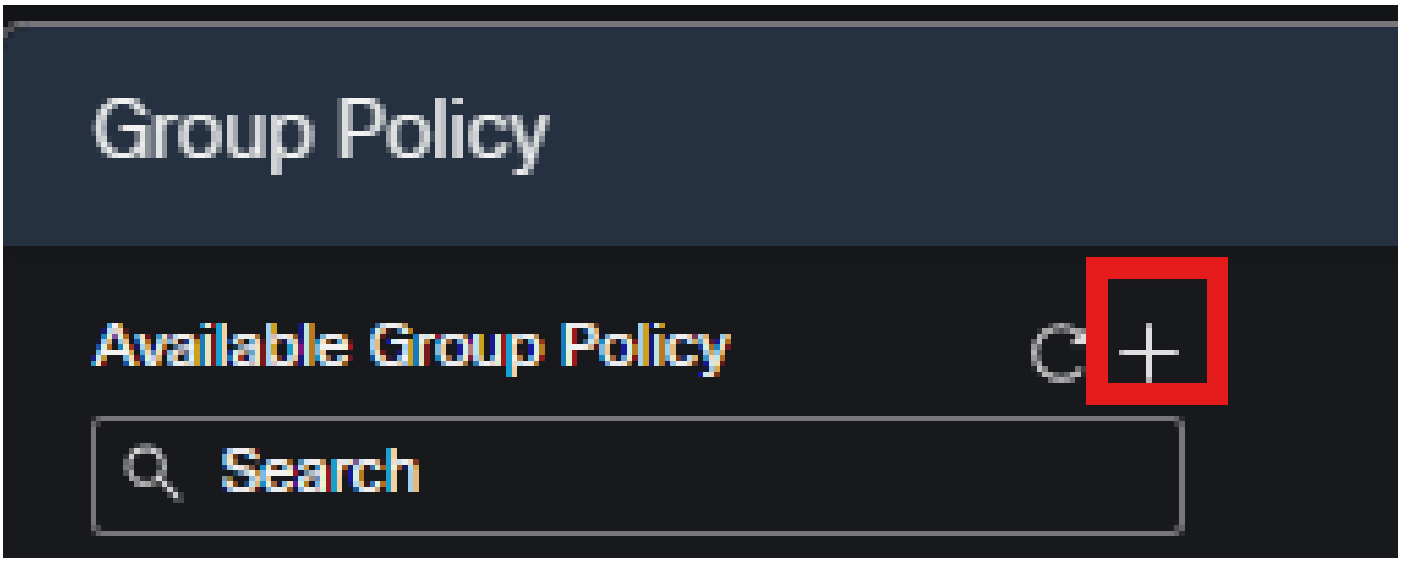


FMC新增組策略

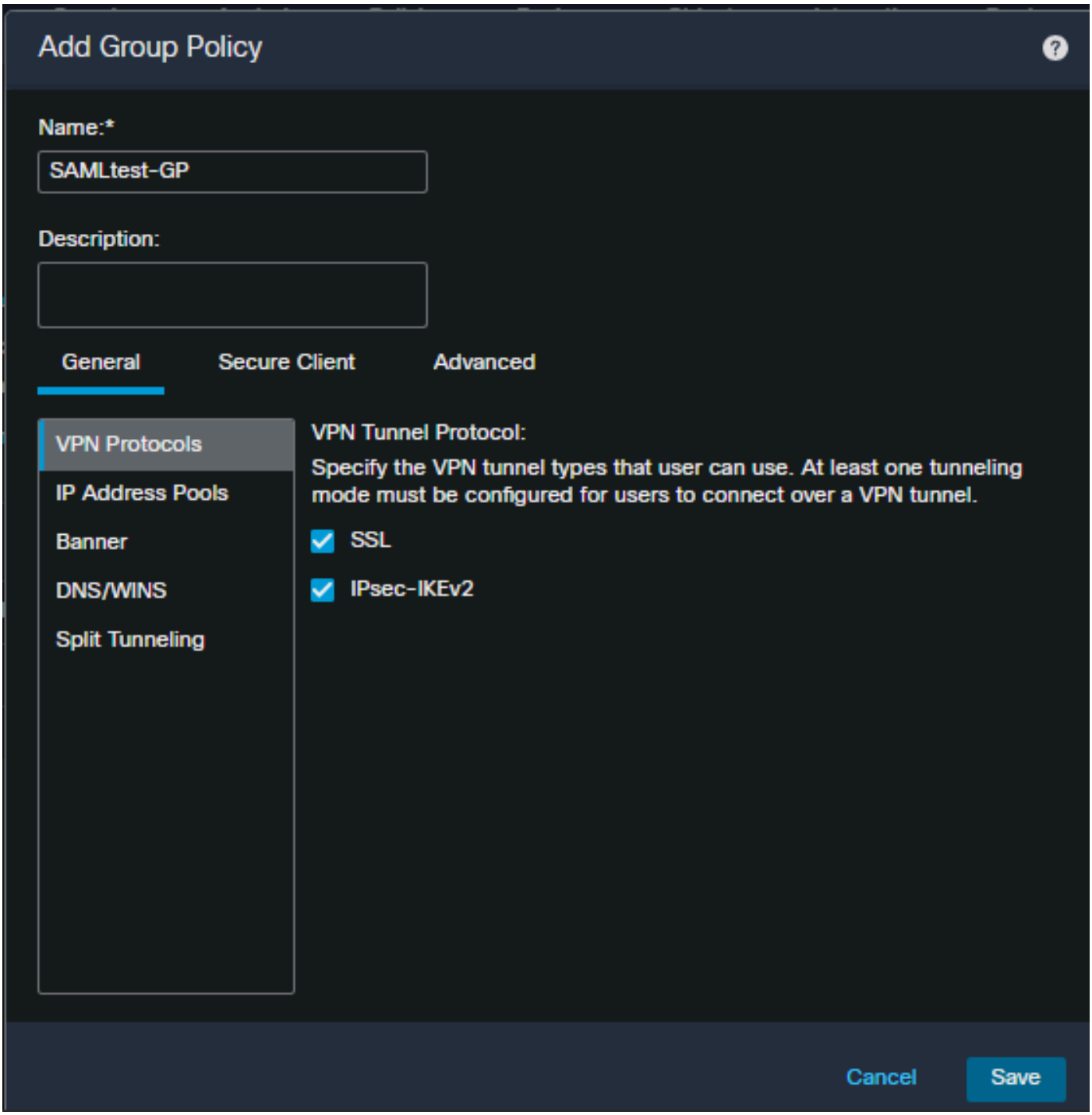
2.按一下彈出視窗中的+，開啟對話方塊以建立新的組策略。填寫所需選項並儲存。



附註：如果已經建立了所需的組策略，則可以跳過此步驟並繼續步驟3

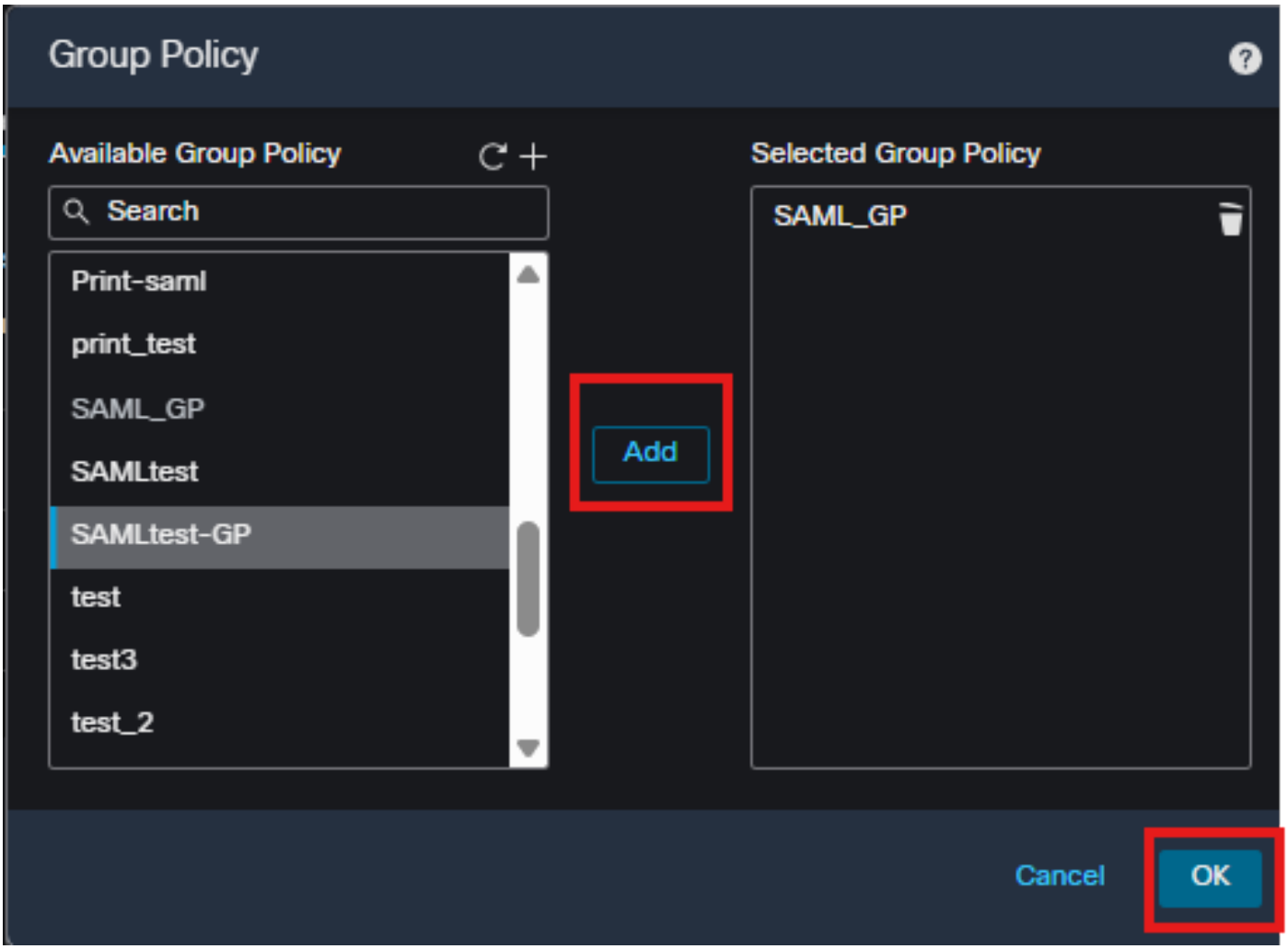


建立新的組策略



組策略選項

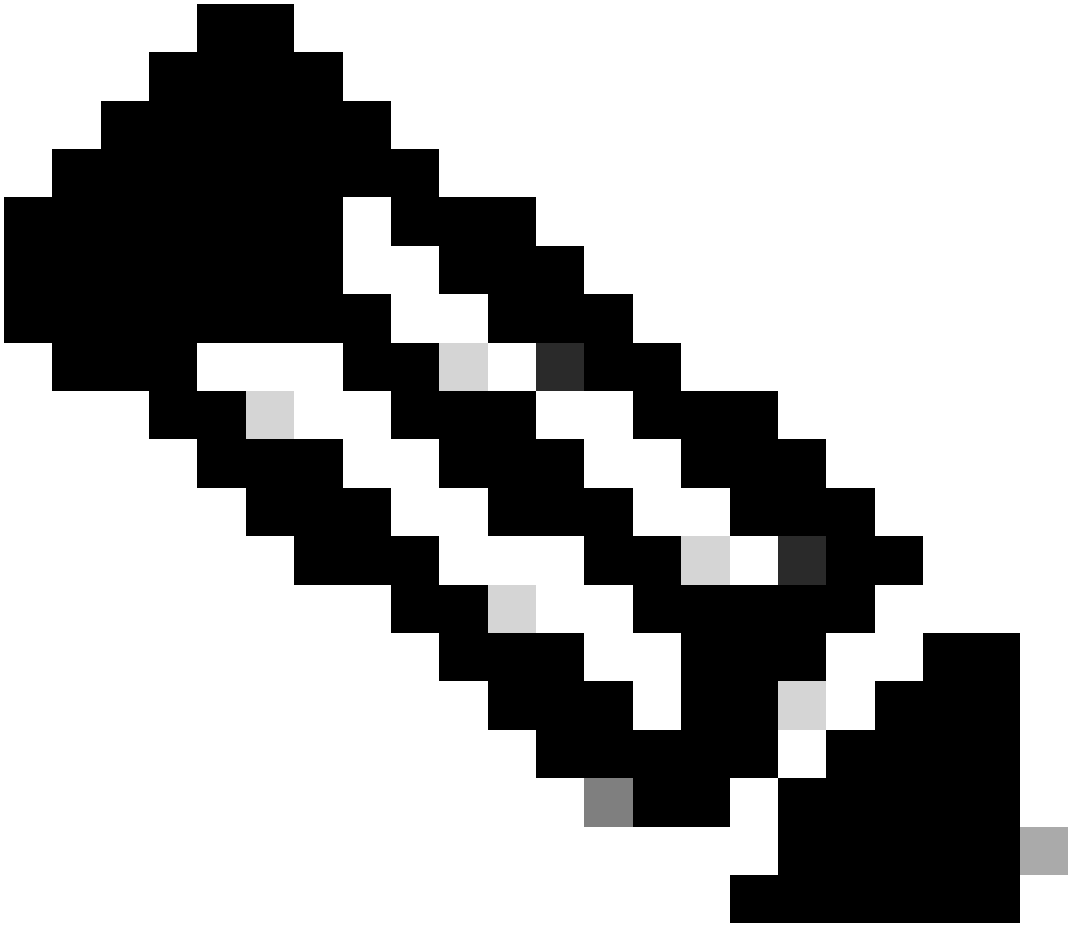
3.在左側清單中選擇新建立的組策略，然後按一下Add按鈕，然後按一下Ok以儲存清單。



新增組策略

FTD後設資料

將組態部署到FTD後，導覽至FTD CLI並執行命令「show saml metadata <tunnel group name>」，蒐集FTD Entity ID和ACS URL。



附註：為了簡潔，後設資料中的證書被截斷。

<#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
```

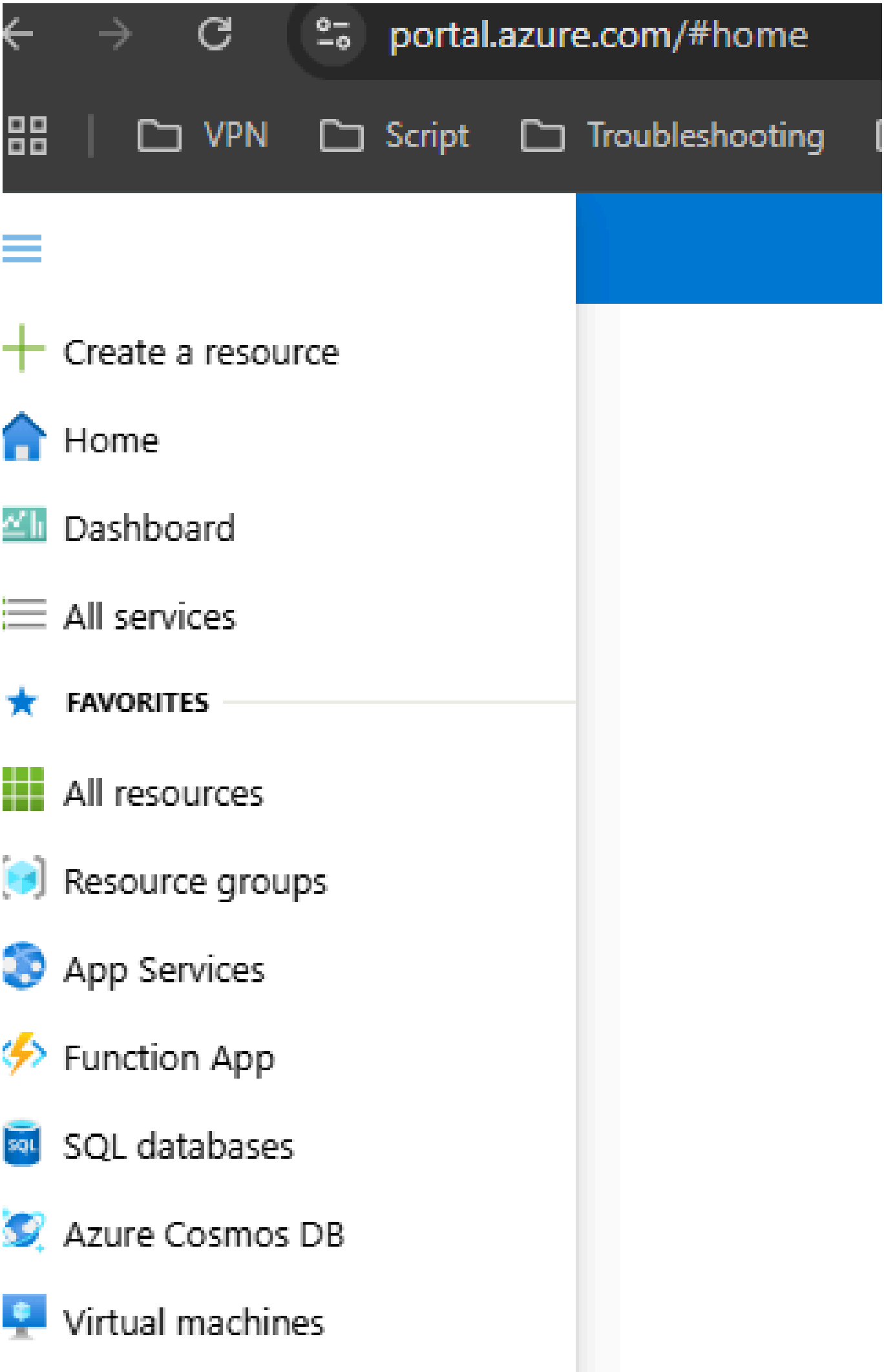
```
LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9FO4LE88attuGuVMquV+1ODRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

</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門戶上，從左側的選單中選擇Microsoft Entra ID。


portal.azure.com/#home
VPN
Script
Troubleshooting
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines

```
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
```

要驗證IdP是否正在傳送所需的宣告，請在連線到VPN時收集「debug webvpn saml 255」的輸出。分析debugs中的斷言輸出，並將屬性部分與IdP上的配置進行比較。

<#root>

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

SAMLtest-GP

```
</AttributeValue>
</Attribute>
```

疑難排解

<#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
```

相關資訊

[思科技術支援和下載]

[ASA配置指南]

[FMC/FDM配置指南]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。