

在ASA上使用SAML配置多個隧道組

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[SAML SP啟動的SSO](#)

[組態](#)

[從庫中新增Cisco安全防火牆 — 安全客戶端](#)

[將Azure AD使用者分配給應用](#)

[通過CLI配置ASA](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹使用Azure身份提供程式對思科ASA上的多個隧道組進行SAML身份驗證。

必要條件

需求

思科建議瞭解以下主題：

- Adaptive Security Appliance (ASA)
- 安全斷言標籤語言(SAML)
- 安全通訊端層(SSL)憑證
- Microsoft Azure

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 9.2(1)1
- 使用SAML 2.0的Microsoft Azure Entra ID
- 思科安全使用者端5.1.7.80

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

Microsoft Azure可以支援同一實體ID的多個應用程式。每個應用程式（對映到不同的隧道組）都需要唯一的證書。在ASA上，由於IdP證書功能，可以將多個隧道組配置為使用不同的覆蓋身份提供程式(IdP)保護的應用程式。此功能允許管理員使用每個隧道組的特定IdP證書覆蓋單點登入(SSO)伺服器對象中的主IdP證書。此功能自9.17.1版本開始在ASA上引入。

SAML SP啟動的SSO

當終端使用者通過訪問ASA啟動登入時，登入行為按以下方式進行：

1. 當VPN使用者訪問或選擇啟用SAML的隧道組時，終端使用者將被重定向到SAML IdP進行身份驗證。系統會提示使用者，除非使用者直接訪問group-url，在這種情況下，重定向是靜默的。
2. ASA生成SAML身份驗證請求，瀏覽器將其重定向到SAML IdP。
3. IdP向終端使用者詢問憑據並請求終端使用者登入。輸入的憑據必須滿足IdP身份驗證配置。
4. IdP響應被傳送回瀏覽器並發佈到ASA登入URL。ASA驗證響應以完成登入。

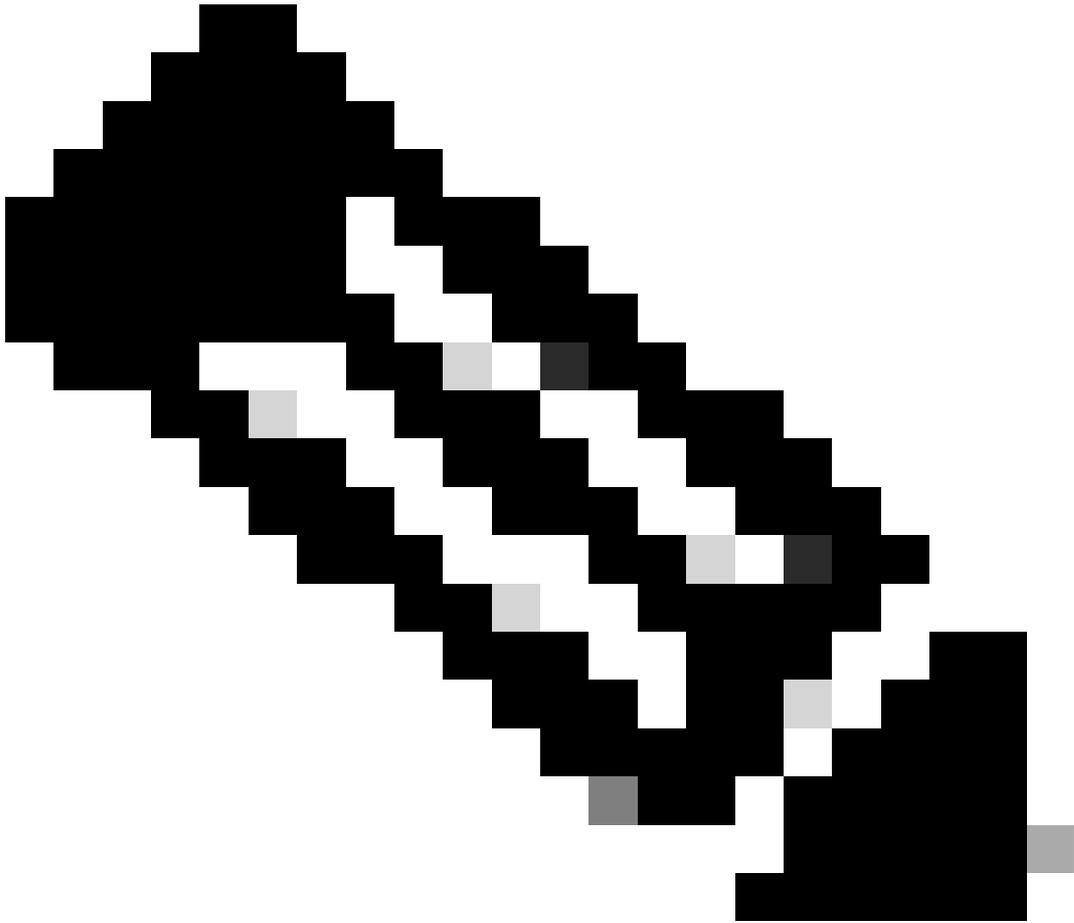
組態

從庫中新增Cisco安全防火牆 — 安全客戶端

在此示例中，為在ASA上配置的兩個隧道組新增了Microsoft Entra SSO與Cisco安全防火牆 — Azure上的安全客戶端的整合：

- SAML1
- SAML2

要配置思科安全防火牆 — 安全客戶端與Microsoft Entra ID的整合，您需要將庫中的思科安全防火牆 — 安全客戶端新增到託管SaaS應用清單中。



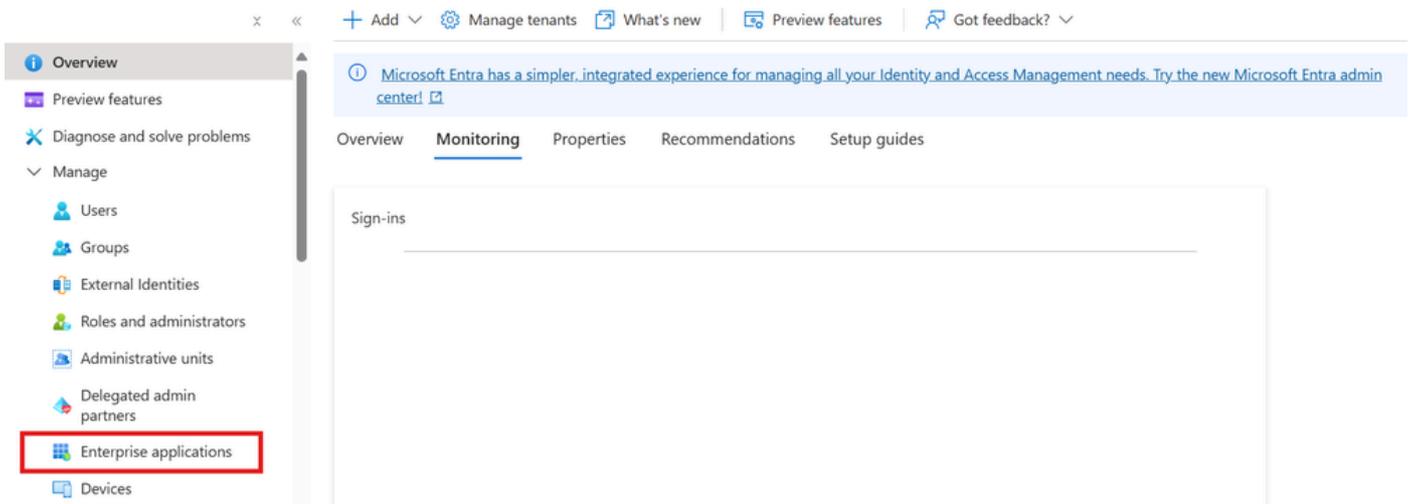
附註：以下步驟用於將思科安全防火牆 — 安全客戶端新增到第一個隧道組SAML1的庫中。

步驟1. 登入到Azure門戶並選擇Microsoft Entra ID。



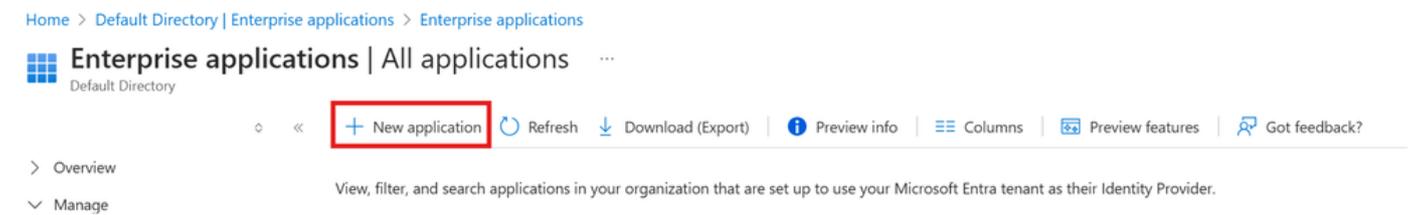
Microsoft Entra ID

步驟2. 如下圖所示，選擇Enterprise Applications。



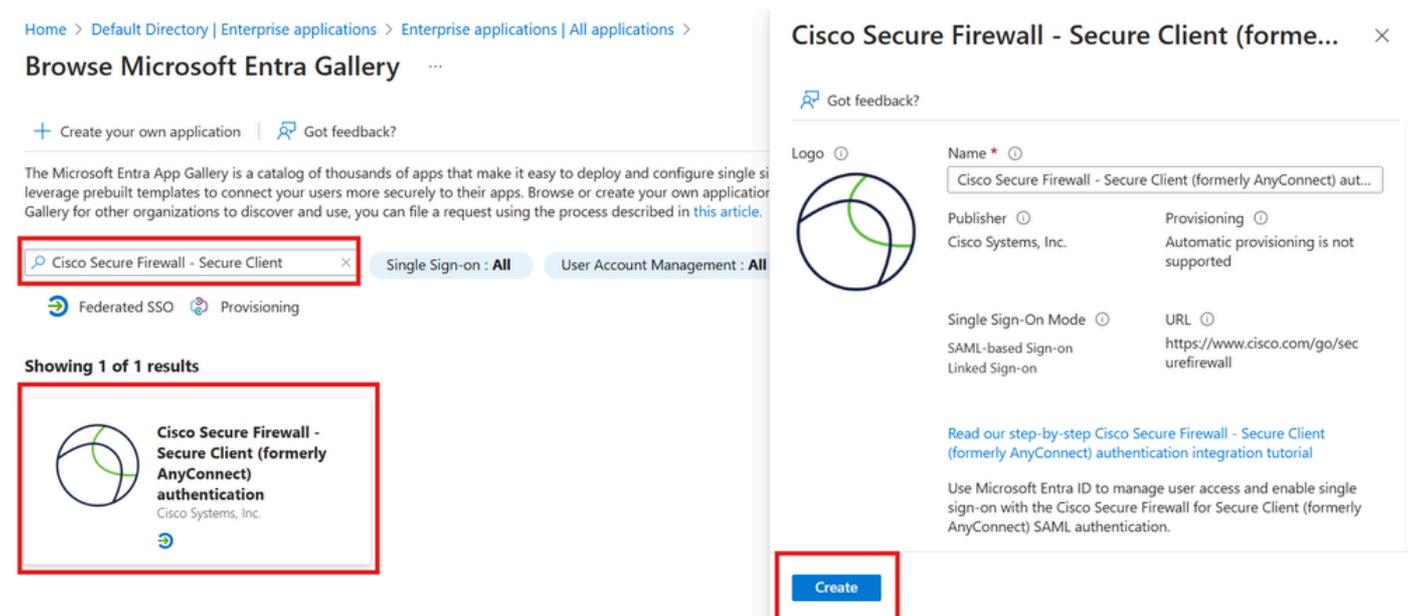
企業應用程式

步驟3.現在選擇New Application，如下圖所示。



新應用程式

步驟4.在Add from the gallery部分中，在搜尋框中鍵入Cisco Secure Firewall - Secure Client，從結果面板中選擇Cisco Secure Firewall - Secure Client，然後新增應用。



思科安全防火牆 — 安全使用者端

步驟5.選擇Single Sign-on功能表專案，如下圖所示。

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
- Security
- Activity
- Troubleshooting + Support

Properties

Name
Cisco Secure Firewall - Secu...

Application ID
098b5489-4aec-4c73-8de1-...

Object ID
584f4478-7571-4361-9453-...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
[Get started](#)

設定單一登入

步驟6. 在選擇單點登入方法頁上，選擇SAML。

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Self-service

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

SAML

步驟7. 在使用SAML設定單一登入頁面上，按一下Basic SAML Configuration的編輯/筆圖示以編輯設定。

Basic SAML Configuration



Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

基本Saml配置

步驟8. 在「使用SAML設定單一登入」頁上，輸入以下欄位的值：

a. 在Identifiertext框中，使用以下模式鍵入URL：

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

b. 在回覆URL文本框中，鍵入使用以下模式的URL：

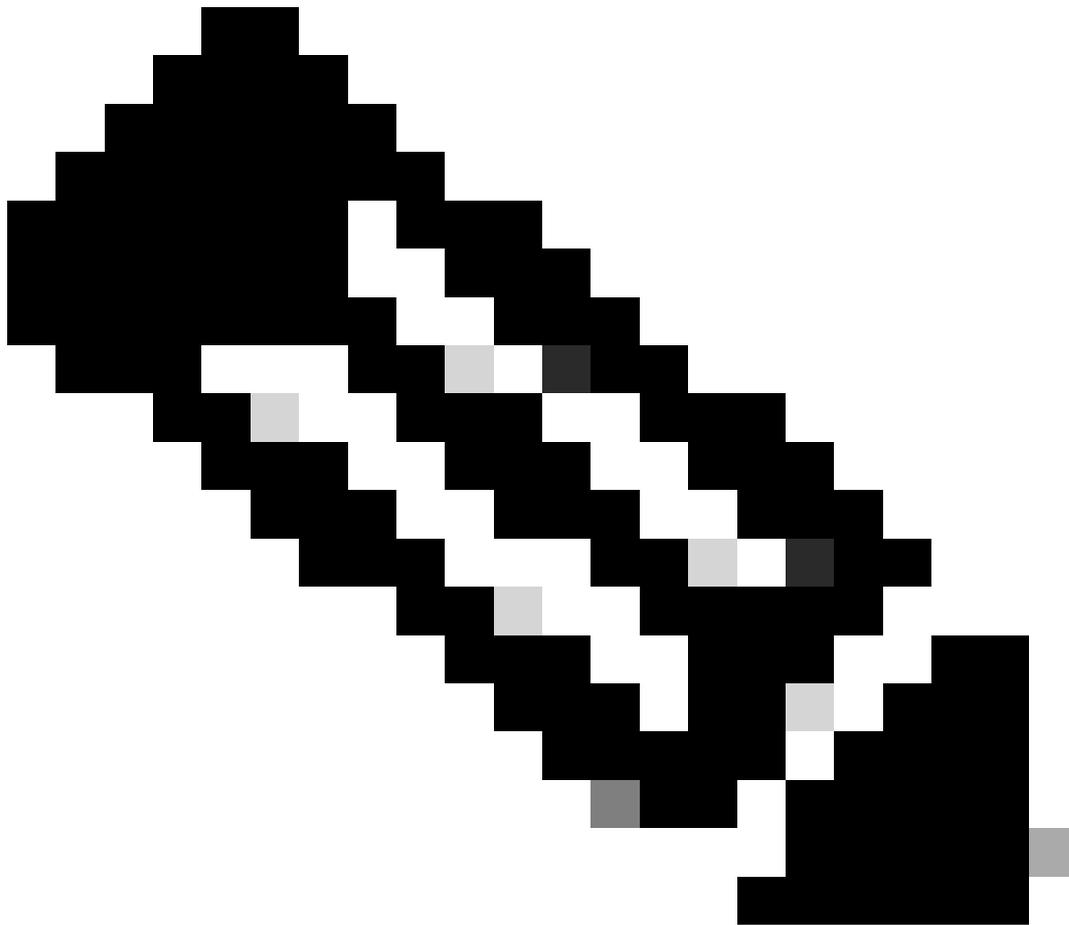
`https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<Tunnel_Group_Name>
[Tunnel_Group_Name = SAML1]`

附註：Tunnel_Group_Name區分大小寫，並且值不得包含點「。」並斜槓「/」。

步驟9. 在使用SAML設定單一登入頁面上，在SAML簽名證書部分中查詢證書(Base64)並選擇Download，下載證書檔案並將其儲存在您的電腦上。

SAML Certificates

Token signing certificate	<input type="text"/>	 Edit
Status	Active	
Thumbprint	52FE6AF989F5092280ED84C121C0A230969E - 12E	
Expiration	2/4/2028, 4:33:14 PM	
Notification Email	mihikarashmisingh2607@gmail.com	
App Federation Metadata Url	<input type="text" value="https://"/>	.. 
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	



注意：此下載的證書已匯入到ASA信任點AzureAD-AC-SAML1。有關詳細資訊，請參閱「ASA配置」部分。

步驟10.在設定Cisco安全防火牆 — 安全客戶端部分，根據您的要求複製適當的URL。這些URL用於在ASA上配置SSO伺服器對象。

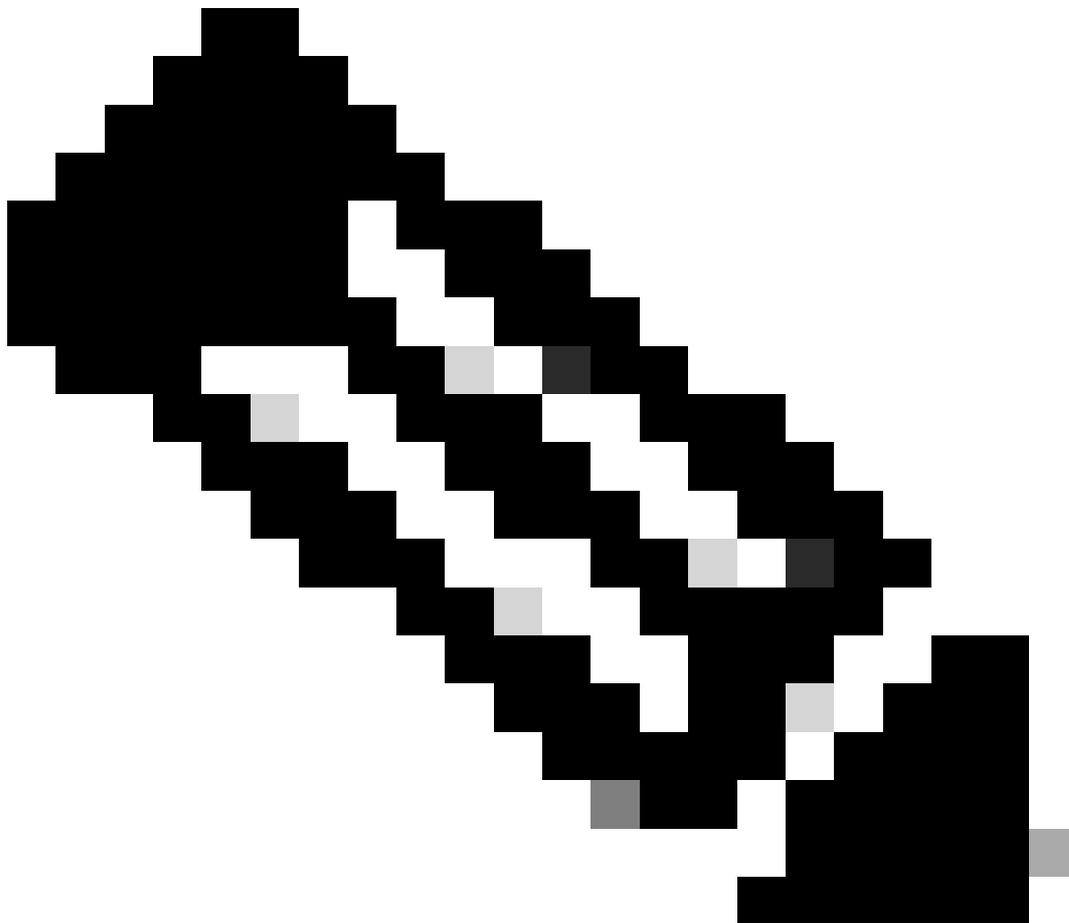
- Microsoft Entra Identifier — 這是VPN配置中的SAML idp。
- 登入URL — 這是URL登入。
- 註銷URL — 這是URL註銷。

Set up Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com/65d917a5-74a4...
Microsoft Entra Identifier	https://sts.windows.net/65d917a5-74a4-42aa-8e3...
Logout URL	https://login.microsoftonline.com/65d917a5-74a4...

SSO URL



附註：重複前面的配置步驟，以便為第二個隧道組從庫中新增Cisco Secure Firewall - Secure Client應用。此案例中的第二個隧道組名為SAML2。



注意：為第二個隧道組(SAML 2)新增Cisco安全防火牆 — 安全客戶端應用時，將在步驟8中下載的azure證書匯入到ASA信任點AzureAD-AC-SAML2。

將Azure AD使用者分配給應用

在本節中，Test1和Test2被啟用以使用Azure SSO，因為您授予了對思科安全客戶端應用的訪問許可權。

對於第一個IdP應用程式：

步驟1.在第一個IdP應用程式概述頁中，依次選擇Users and groups和Add user。

Cisco SAML 1 | Users and groups ...
Enterprise Application

+ Add user/group Edit assignment Remove assignment Update credential Refresh Manage view Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#)

First 200 shown, search all users & groups

Display name	Object type
No application assignments found	

Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on

使用者和組

步驟2. 在「新增分配」對話框中選擇「使用者」或「組」。

Add Assignments

Default Directory

Try changing or adding filters if you don't see what you're looking for.

Search

4 results found

All Users

Select a role
Default Access

 Test1	User
---	------

新增作業1

步驟3. 在Add Assignment對話框中，按一下Assign按鈕。

Add Assignment ...

Default Directory

Users

1 user selected.

Select a role

Default Access

Assign

測試1使用者分配

對於第二個IdP應用程式：

如這些影象所示，對第二個Idp應用程式重複上述步驟。

Add Assignment

Default Directory

Users

1 user selected.

Select a role

Default Access

Assign

新增作業2

Home > Default Dir

Add Assignm

Default Directory

Users

Try changing or adding filters if you don't see what you're looking for.

Search

4 results found

All Users

Users

None Selected

Select a role

Default Access

Selected (0)

Reset

No items selected

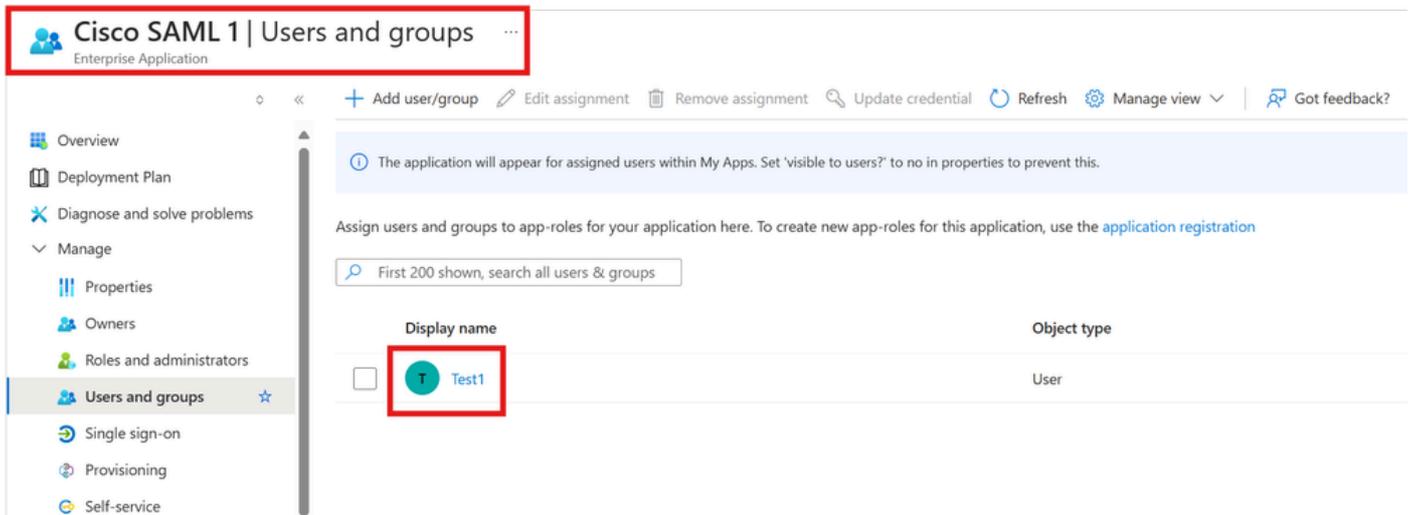
	Name	Type	Details
<input type="checkbox"/>	 Test2	User	

Assign

Select

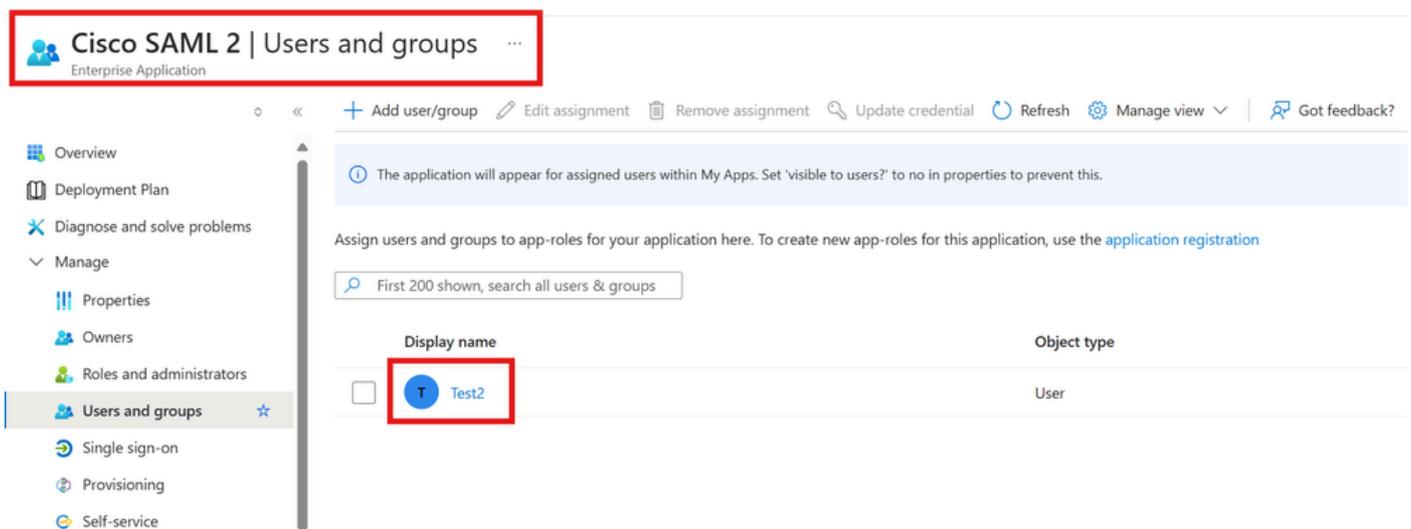
測試2使用者分配

Test1使用者分配：



測試1使用者分配

Test2使用者分配：



測試2使用者分配

通過CLI配置ASA

步驟1.建立信任點並匯入SAML證書。

配置兩個信任點，並為每個隧道組匯入各自的SAML證書。

```
<#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
```

步驟2. 配置SAML IdP。

使用這些命令設定SAML IdP設定。

webvpn

```
saml idp https://xxx.windows.net/xxxxxxxxxxxxx/ - [Azure AD Identifier]
url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxxxxx/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
```

步驟3. 將SAML身份驗證應用到第一個VPN隧道組。

使用AzureAD-AC-SAML1 IdP信任點配置SAML1隧道組。

```
<#root>
```

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

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

步驟4.將SAML身份驗證應用到第二個VPN隧道組。

使用AzureAD-AC-SAML2 IdP信任點配置SAML2隧道組。

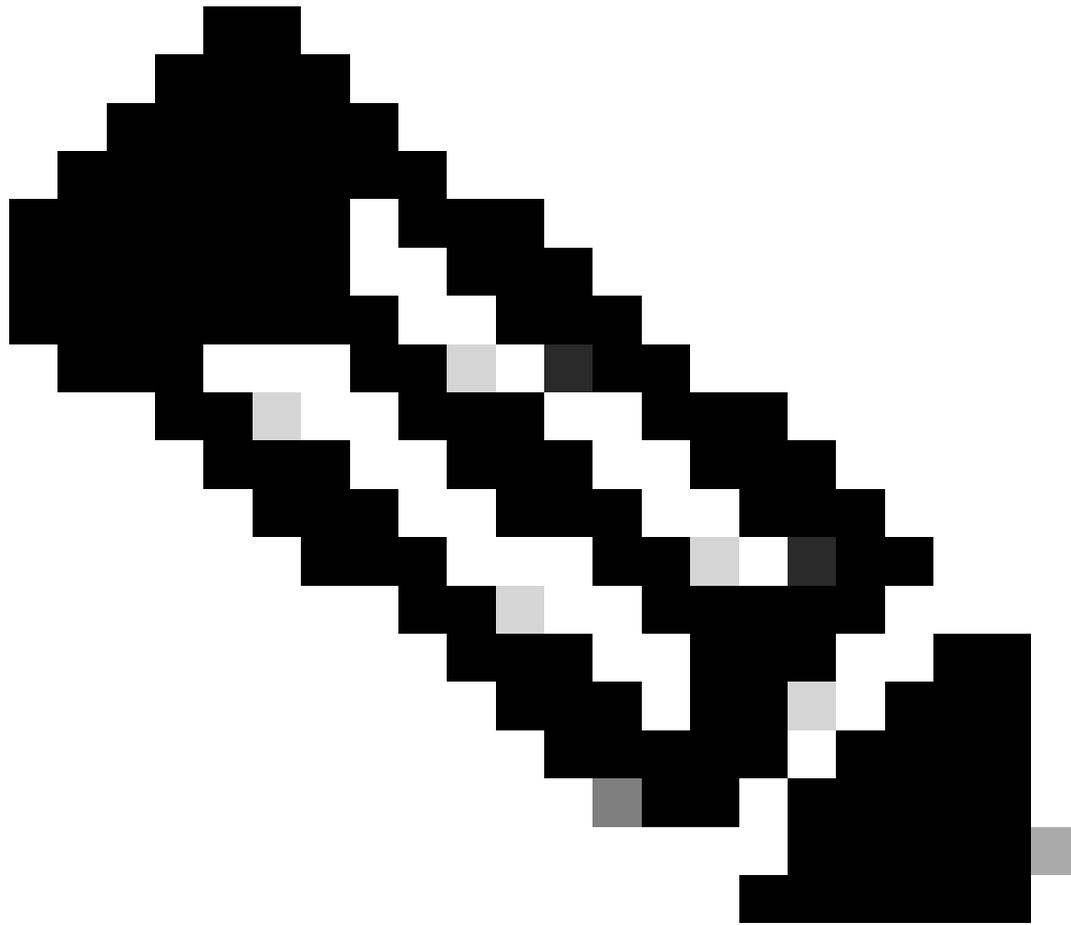
```
<#root>
```

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

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

步驟 5:儲存組態。

```
write memory
```



附註：如果更改IdP配置，則需要從隧道組刪除SAML身份提供程式配置，然後重新應用該配置以使更改生效。

驗證

使用SAML身份驗證測試AnyConnect。

步驟1。連線到您的VPN URL並在Azure AD詳細資訊中輸入您的日誌。

步驟2. (可選) 批准登入請求。

步驟3. AnyConnect已連線。

疑難排解

大多數SAML故障排除都涉及配置錯誤，在檢查SAML配置或運行調試時可以發現該錯誤。debug webvpn saml 255可用於解決大多數問題，但是，在此調試不提供有用資訊的情況下，可以運行其他調試：

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

相關資訊

- [透過 SAML 藉由 Microsoft Azure MFA 設定 ASA AnyConnect VPN](#)
- [技術支援與文件 - Cisco Systems](#)

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）。