

透過 SAML 藉由 Microsoft Azure MFA 設定 ASA AnyConnect VPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[SAML元件](#)

[用於簽名和加密操作的證書](#)

[網路圖表](#)

[設定](#)

[從Microsoft應用庫新增Cisco AnyConnect](#)

[將Azure AD使用者分配給應用](#)

[通過CLI為SAML配置ASA](#)

[驗證](#)

[使用SAML Auth測試AnyConnect](#)

[常見問題](#)

[實體ID不匹配](#)

[時間不匹配](#)

[使用了錯誤的IdP簽名證書](#)

[斷言受眾無效](#)

[Assertion Consumer Service的URL錯誤](#)

[未生效的SAML配置更改](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何配置安全斷言標籤語言(SAML)，重點介紹通過Microsoft Azure MFA實現的自適應安全裝置(ASA)AnyConnect。

必要條件

需求

思科建議您瞭解以下主題：

- 有關ASA上RA VPN配置的基本知識。

- SAML和Microsoft Azure的基本知識。
- 已啟用AnyConnect許可證 (APEX或僅限VPN) 。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Azure AD訂閱。
- Cisco ASA 9.7+和Anyconnect 4.6+
- 使用AnyConnect VPN配置檔案

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是一個基於XML的框架，用於在安全域之間交換身份驗證和授權資料。它在使用者、服務提供者(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。Microsoft Azure MFA與Cisco ASA VPN裝置無縫整合，為Cisco AnyConnect VPN登入提供額外的安全性。

SAML元件

後設資料：它是基於XML的文檔，用於確保IdP和SP之間的安全事務。它允許IdP和SP協商協定。

裝置支援的角色(IdP、SP)

一個裝置可以支援多個角色，並且可以包含SP和IdP的值。如果包含的資訊用於單點登入IdP，則在EntityDescriptor欄位下為IDPSSODescriptor；如果包含的資訊用於單點登入SP，則為SPSSODescriptor。這很重要，因為為了成功設定SAML，必須從相應部分提取正確的值。

實體ID：此欄位是SP或IdP的唯一識別符號。單個裝置可以有多個服務，並且可以使用不同的實體ID來區分這些服務。例如，ASA對於需要驗證的不同隧道組具有不同的實體ID。對每個隧道組進行身份驗證的IdP對每個隧道組都有一個單獨的實體ID條目，以便準確地識別這些服務。

ASA可以支援多個IdP，並為每個IdP提供單獨的實體ID以區分它們。如果任一端收到來自不包含以前配置的實體ID的裝置的消息，則裝置可能會丟棄此消息，並且SAML身份驗證失敗。實體ID可在entityID旁邊的EntityDescriptor欄位中找到。

服務URL：這些定義由SP或IdP提供的SAML服務的URL。對於IdP，這通常為單一註銷服務和單一登入服務。對於SP，這通常是Assertion Consumer Service和Single Logout Service。

SP使用IdP後設資料中找到的單點登入服務URL將使用者重定向到IdP進行身份驗證。如果此值配置不正確，則IdP不會收到或無法成功處理SP傳送的身份驗證請求。

IdP使用在SP後設資料中找到的斷言使用者服務URL將使用者重定向回SP並提供有關使用者身份驗證嘗試的資訊。如果配置不正確，SP不會收到斷言 (響應) 或無法成功處理該斷言。

可在SP和IdP上找到單一註銷服務URL。它用於幫助從SP註銷所有SSO服務，並且在ASA上是可選

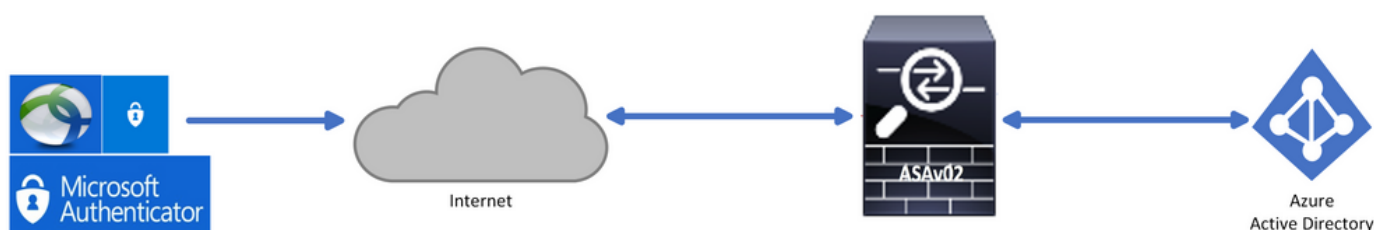
的。在SP上配置來自IdP後設資料的SLO服務URL時，當使用者從SP上的服務註銷時，SP會將請求傳送到IdP。IdP成功從服務中註銷使用者後，會將使用者重定向回到SP，並使用SP後設資料中的SLO服務URL。

服務URL的SAML繫結：繫結是SP用來將資訊傳輸到IdP的方法，反之亦然。其中包括HTTP重新導向、HTTP POST和Artifact。每種方法都有不同的資料傳輸方式。服務支援的繫結方法包含在服務的定義中。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不支援專案繫結。ASA始終對SAML身份驗證請求使用HTTP重定向方法，因此選擇使用HTTP重定向繫結的SSO服務URL以使IdP預期這一點，這一點非常重要。

用於簽名和加密操作的證書

為了為SP和IdP之間傳送的消息提供機密性和完整性，SAML提供了對資料進行加密和簽名的能力。用於對資料進行加密和/或簽名的證書可以包含在後設資料中，以便接收方可以驗證SAML消息並確保它來自預期的源。用於簽名和加密的證書可在KeyDescriptor use="signing"和KeyDescriptor use="encryption"下的後設資料中找到，依次是X509Certificate。ASA不支援加密SAML消息。

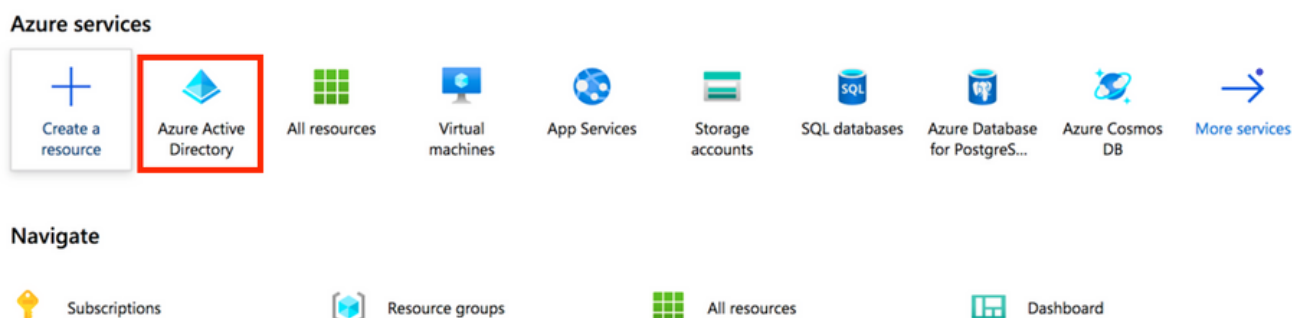
網路圖表



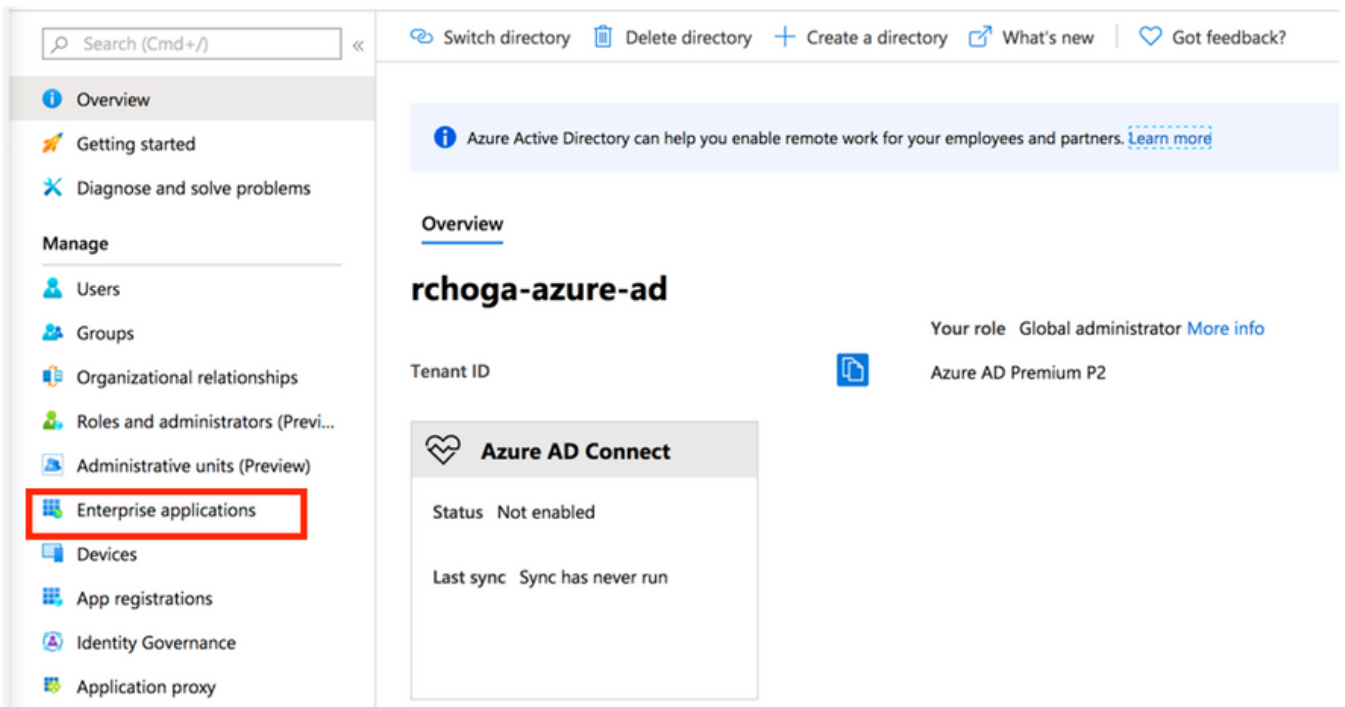
設定

從Microsoft應用庫新增Cisco AnyConnect

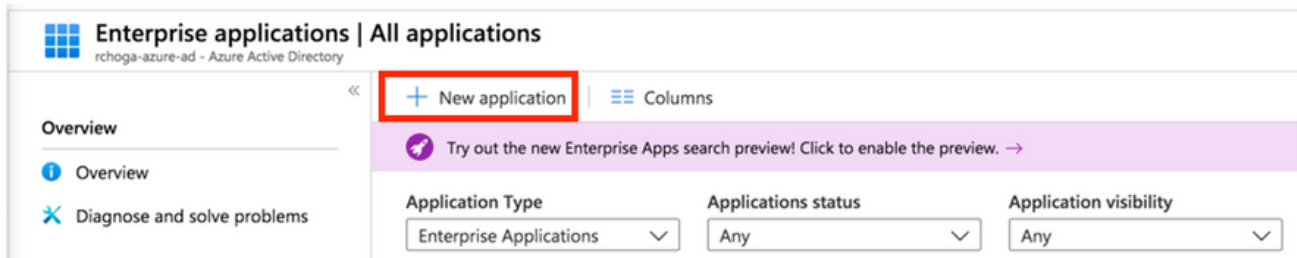
步驟1.登入到Azure門戶並選擇Azure Active Directory。



步驟 2. 如下圖所示，選擇Enterprise Applications。



步驟 3. 現在，選擇New Application，如下圖所示。



步驟 4. 在Add from the gallery部分的「搜尋」框中鍵入AnyConnect，從結果面板中選擇Cisco AnyConnect，然後add應用。

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access.
- Non-gallery application**
Integrate any other application that you don't find in the gallery

Add from the gallery

Category: All (3422) [v]
AnyConnect [v]

1 applications matched "AnyConnect".

| Name | Category |
|------------------|---------------------|
| Cisco AnyConnect | Business management |

Add app

Cisco Systems, Inc.

Empower your employees to work from anywhere, on company laptops or personal mobile devices, at any time. AnyConnect simplifies secure endpoint access and provides the security necessary to help keep your organization safe and protected.

Use Microsoft Azure AD to enable user access to Cisco AnyConnect.

Requires an existing Cisco AnyConnect subscription.

Name: Cisco AnyConnect

Publisher: Cisco Systems, Inc.

Single Sign-On Mode: SAML-based Sign-on

URL: https://www.ciscoanyconnect.com/

Logo:

Add

步驟 5.選擇Single Sign-on選單項，如下圖所示。

AnyConnectVPN | Overview
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins
- Usage & insights (Preview)

Properties

Name: AnyConnectVPN

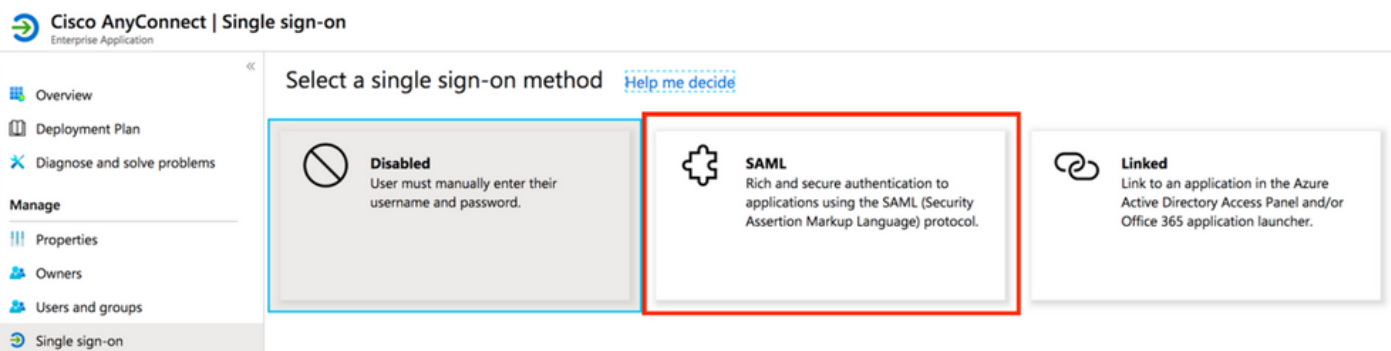
Application ID

Object ID

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 Azure AD credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)
- 4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)
- 5. Self service**
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

步驟 6.選擇SAML，如下圖所示。



步驟 7. 使用這些詳細資訊編輯第 1 部分。

<#root>

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

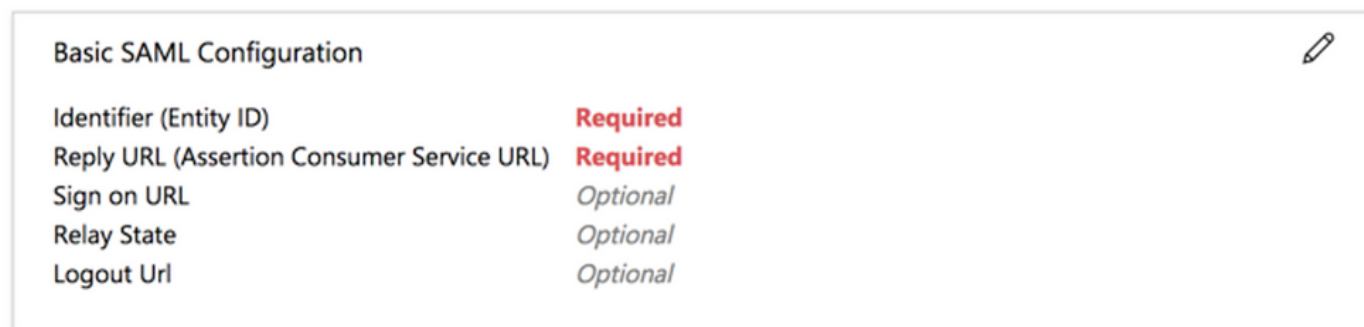
b. Reply URL (Assertion Consumer Service URL) - `https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-G`

Example: vpn url called


`asa.example.com`

and tunnel-group called

`AnyConnectVPN-1`



步驟 8. 在「SAML Signing Certificate」部分，選擇「Download」下載憑證檔案，然後將其儲存到您的電腦上。


SAML Signing Certificate 

Status: Active

Thumbprint: _____

Expiration: 5/1/2023, 4:04:04 PM

Notification Email: _____

App Federation Metadata Url: 

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)


Federation Metadata XML [Download](#)


步驟 9.對於ASA配置，這是必需的。


- Azure AD識別符號 — 這是我們的VPN配置中的同一IDP。
- 登入URL — 這是URL登入。
- 註銷URL — 這是URL註銷。

Set up AnyConnectVPN

You'll need to configure the application to link with Azure AD.

Login URL 

Azure AD Identifier 

Logout URL 

[View step-by-step instructions](#)

將Azure AD使用者分配給應用

在本節中，由於您授予了Cisco AnyConnect應用的訪問許可權，因此啟用了Test1以使用Azure單一登入。

步驟 1.在應用的概述頁面中，依次選擇使用者和組和新增使用者。

Cisco AnyConnect | Users and groups
Enterprise Application

[+ Add user](#) [Edit](#) [Remove](#) [Update Credentials](#) [Columns](#) [Got feedback?](#)

Overview

- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups**
- Single sign-on

Users and groups

Display Name **Object Type** **Role assigned**

No application assignments found

步驟 2. 在Add Assignment對話方塊中選擇Users and groups。



步驟 3. 在Add Assignment對話方塊中，按一下Assign按鈕。



通過CLI為SAML配置ASA

步驟 1. 建立信任點並匯入我們的SAML證書。

```
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
```

步驟 2. 這些命令可預配SAML IdP。


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/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
```

步驟 3. 將SAML身份驗證應用於VPN隧道配置。

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

write memory
```

 注意：如果更改IdP配置，則需要從隧道組中刪除同一身份提供程式配置，然後重新應用該配置以使更改生效。

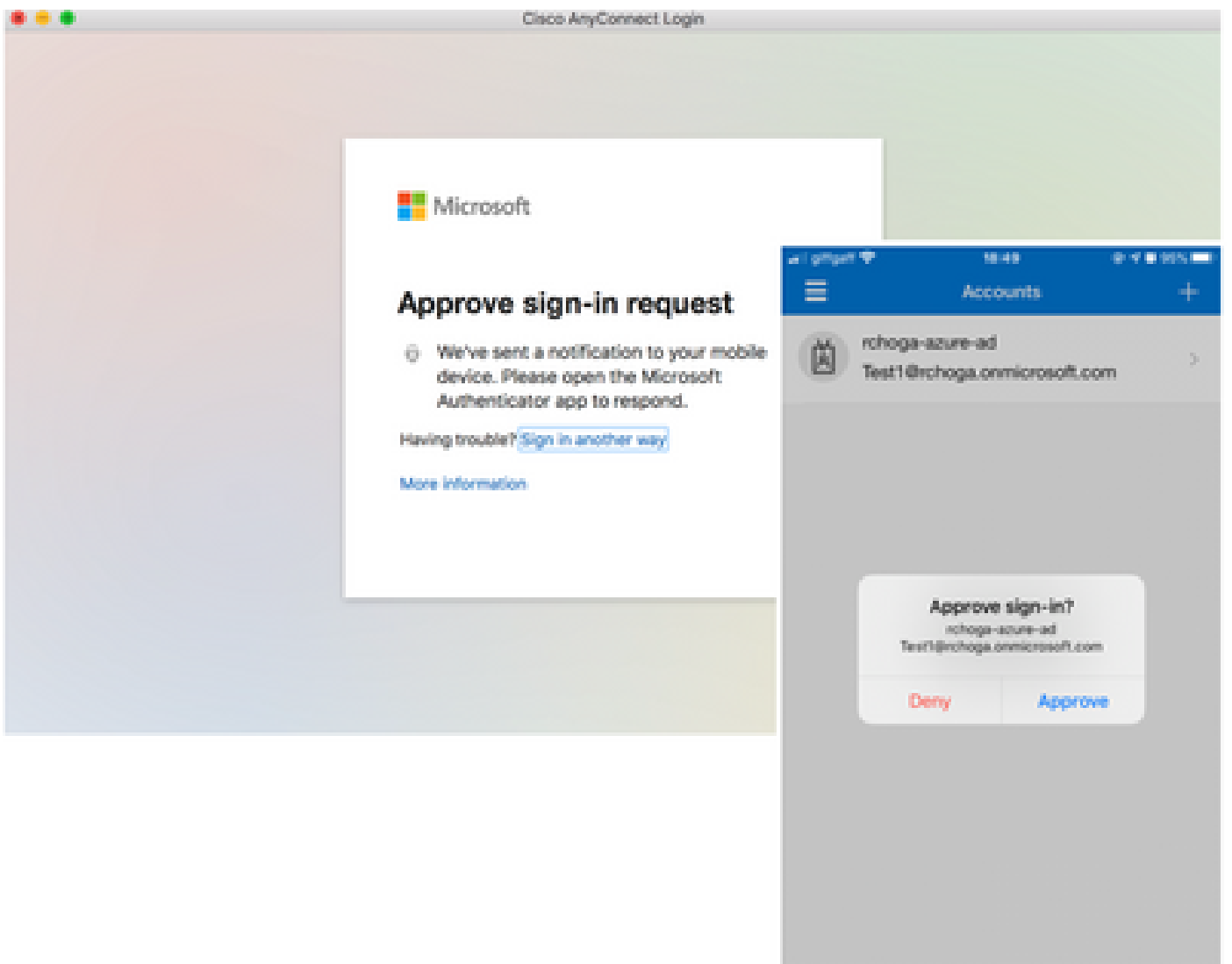
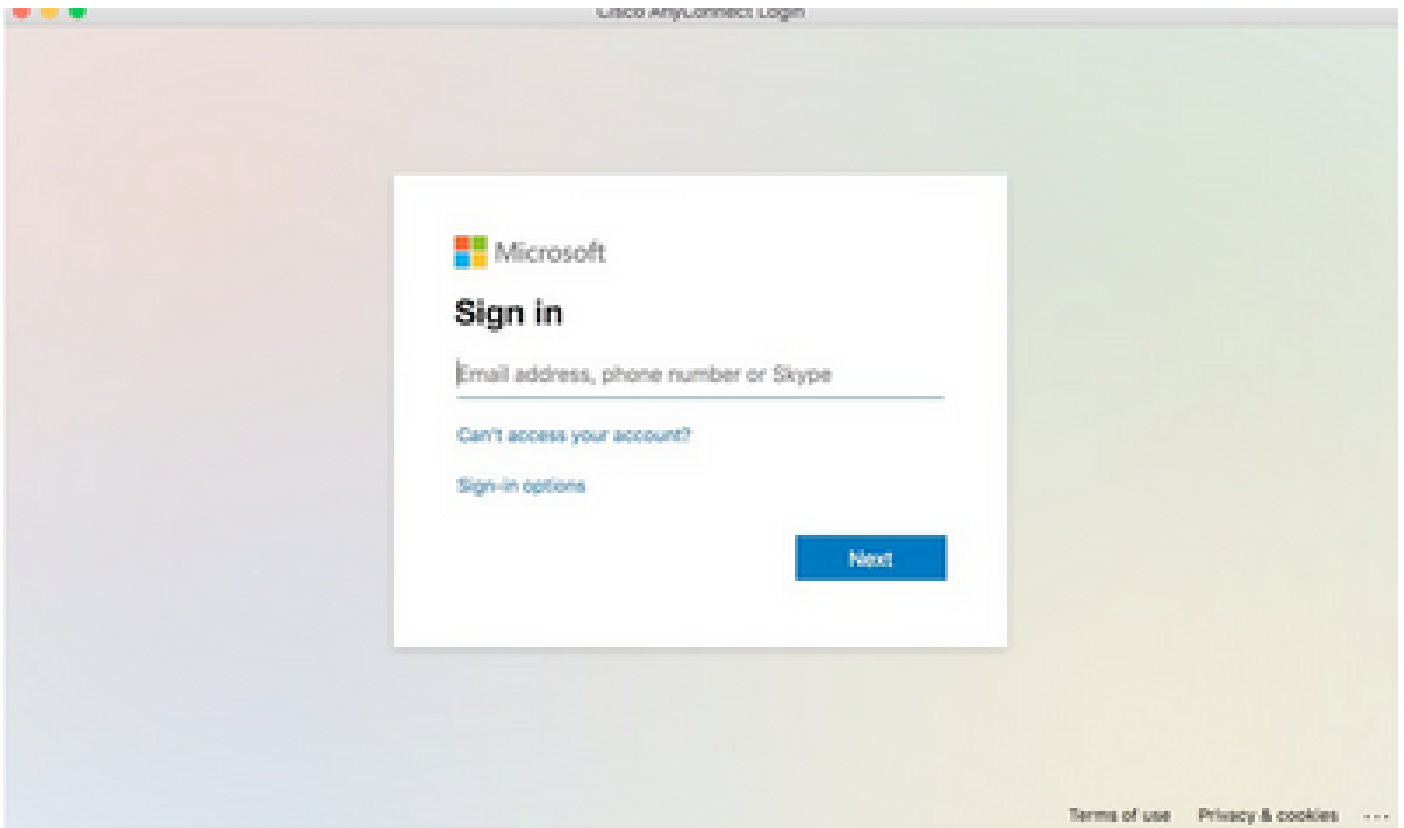
驗證

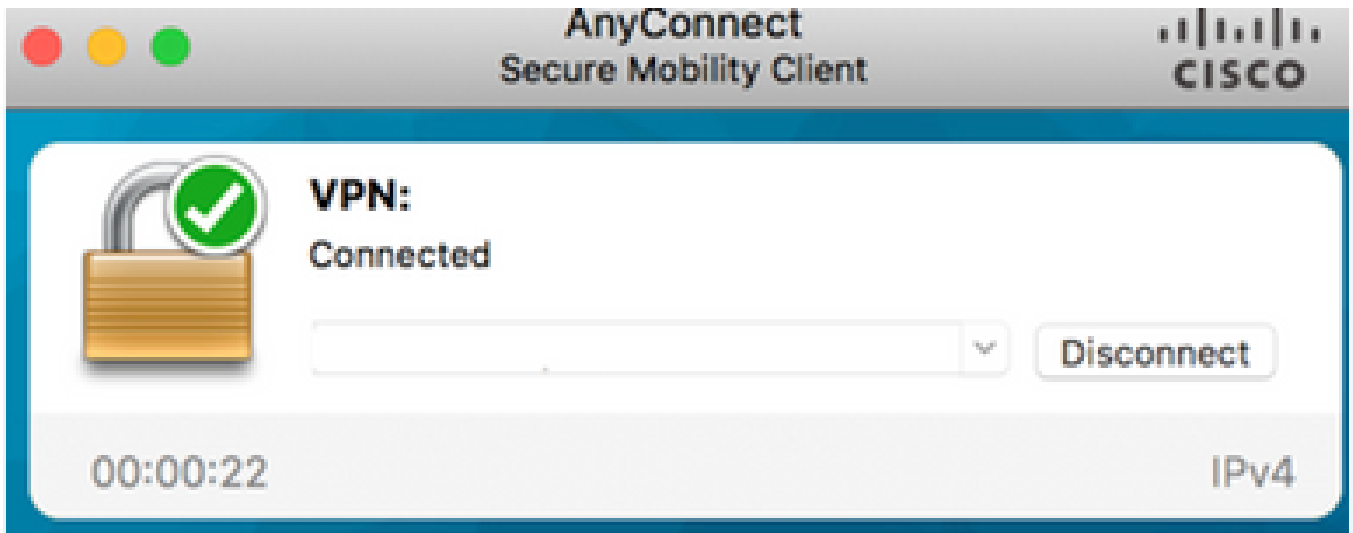
使用SAML Auth測試AnyConnect

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. 批准登入請求。

步驟3. AnyConnect已連線。





常見問題

實體ID不匹配

調試示例：

[SAML] consume_assertion : 提供程式的識別符號未知#LassoServer。若要在#LassoServer對象中註冊提供程式，必須使用方法lasso_server_add_provider()或lasso_server_add_provider_from_buffer()。

問題：通常，表示ASA WebVPN配置下的saml idp [entityID]命令與IdP後設資料中的IdP實體ID不匹配。

解決方案：檢查IdP的後設資料檔案的實體ID，並更改saml idp [entity id]命令以與此匹配。

時間不匹配

調試示例：

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

[SAML] consume_assertion : 斷言已過期或無效

問題1. ASA時間未與IdP的時間同步。

解決方案1. 使用IdP使用的同一NTP伺服器配置ASA。

問題2. 斷言在指定時間之間無效。

解決方案2. 修改ASA上配置的超時值。

使用了錯誤的IdP簽名證書

調試示例：

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

[SAML] consume_assertion：配置檔案無法驗證消息上的簽名

問題：ASA無法驗證由IdP簽名的消息，或者沒有要驗證的ASA簽名。

解決方案：檢查ASA上安裝的IdP簽名證書，以確保它與IdP傳送的內容匹配。如果這一點得到確認，請確保簽名包含在SAML響應中。

斷言受眾無效

調試示例：

[SAML] consume_assertion：斷言受眾無效

問題：IdP定義不正確的訪問群體。

解決方案：更正IdP上的受眾配置。它必須與ASA的實體ID匹配。

Assertion Consumer Service的URL錯誤

調試示例：在傳送初始身份驗證請求後，無法接收任何調試。使用者能夠在IdP中輸入憑證，但IdP不會重定向到ASA。

問題：為錯誤的斷言使用者服務URL配置了IdP。

解決方案：檢查配置中的基本URL並確保其正確。使用show檢查ASA後設資料，確保Assertion Consumer Service URL正確。要測試它，請瀏覽它。如果兩者在ASA上都正確，請檢查IdP以確保URL正確。

未生效的SAML配置更改

示例：在修改或更改一次登入URL後，SP證書SAML仍無法正常運行並傳送以前的配置。

問題：當存在影響它的配置更改時，ASA需要重新生成其後設資料。它不會自動執行此操作。

解決方案：進行更改後，在受影響的隧道組下刪除並重新應用saml idp [entity-id]命令。

疑難排解

大多數SAML故障排除都涉及配置錯誤，在選中SAML配置或運行調試時可以發現該錯誤。debug webvpn saml 255可用於排除大多數問題，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

- [使用應用代理實現本地應用的SAML單點登入](#)

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）。