# Cisco安全存取 — 使用IDP的SAML憑證續訂(Microsoft Entra ID)

## 目錄

## 問題

將SSO身份驗證與Microsoft Entra ID SAML一起用作思科安全訪問的身份提供程式(IdP)時，SAML驗證證書即將過期。

組織需要瞭解正確的證書續訂流程，以避免身份驗證中斷，並確定續訂Entra ID SAML證書時，是否必須在Secure Access中建立新的單一登入配置。

## 環境

- 配置了SSO身份驗證的Cisco安全訪問
- 作為身份提供程式的Microsoft Entra ID SAML
- 具有即將到期日期的SAML驗證證書
- SWG（安全Web網關）和ZTNA（零信任網路訪問）的現有SSO配置

## 解析

### 第1步 — 檢測證書續訂

- 身份提供程式(IdP)更新或輪換其SAML簽名證書。
- 這通常發生在憑證快要到期時。

### 第2步 — 獲取更新的IdP後設資料

- 從IdP匯出新的IdP元資料XML或新簽名證書。

### 步驟3 — 驗證憑證變更

確認證書已實際更改。

檢查：

- 指紋
- 到期日期
- 發行商

這可確保使用正確的證書更新SP

### 更新服務提供商配置

登入到Cisco Secure Access Dashboard並更新配置。

導航至Connect - User and Groups。

點選配置管理(Configuration Management)

在SSO Authentication - Edit the SSO Authentication Profile（編輯SSO身份驗證配置檔案）下 — 使用新證書上傳後設資料檔案，或上傳證書（如果手動配置）。

### 步驟5 — 儲存並應用組態

- 儲存更新的配置

### 第6步 — 驗證SSO身份驗證

執行SSO登入測試。

## 原因

身份提供程式(IdP)簽名證書用於驗證SAML斷言簽名，當IdP更新證書時，SP必須更新其受信任的證書以繼續驗證身份驗證請求

## 相關內容

- 思科安全訪問 — SAML單點登入概述和配置
- 為Cisco安全訪問配置SAML SSO（Microsoft Entra ID示例）
- 思科技術支援與下載

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）。