

使用身份服務(IdS)證書管理排除CCE單點登入故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[SAML證書已過期](#)

[解決方案](#)

[辨識提供者\(IdP\)中的安全雜湊演算法變更](#)

[解決方案](#)

[Cisco IdS伺服器IP地址或主機名更改-已重建共存的CUIC/LiveData/IdS發佈伺服器或獨立Id發佈伺服器-已重建共存的CUIC/LiveData/IdS訂閱伺服器或獨立Id訂閱伺服器](#)

[解決方案](#)

[參考](#)

[如何在ADFS或](#)

[如何啟用已簽名的SAML斷言](#)

[如何將AD FS SSL證書上傳到Cisco IdS tomcat信任](#)

[如何刪除AD FS中的信賴方](#)

[如何檢查或變更在辨識提供者\(IdP\)中設定的安全雜湊演算法](#)

[如何檢查Cisco IdS伺服器SAML證書到期日期](#)

[如何下載Cisco IdS伺服器的後設資料](#)

[如何從sp.xml檔案中檢索SAML證書](#)

[如何替換AD FS中的SAML證書](#)

[如何在Cisco IdS伺服器中重新生成SAML證書](#)

[測試SSO](#)

簡介

本文檔介紹在UCCE/PCCE中重新生成和交換SAML證書的詳細步驟，以確保安全、清晰的流程。

作者：Nagarajan Paramasivam，思科TAC工程師。

必要條件

需求

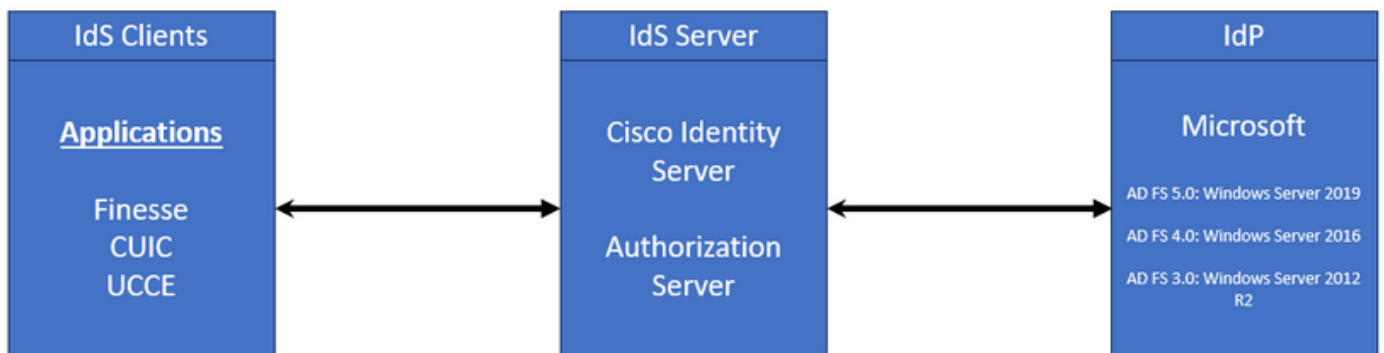
思科建議您瞭解以下主題：

- 套裝/整合客服中心企業版(PCCE/UCCE)
- 語音作業系統(VOS)平台
- 憑證管理
- 安全宣告標籤語言(SAML)
- 安全通訊端層 (SSL)
- Active Directory聯合身份驗證服務(AD FS)
- 單一登入(SSO)

採用元件

本檔案中的資訊以下列元件為基礎：

- 思科身分辨識服務(Cisco IdS)
- 辨識提供者(IdP) - Microsoft Windows ADFS



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

在UCCE/PCCE中，思科身份服務(Cisco IdS)提供身份提供者(IdP)和應用之間的授權。

在配置思科Id時，您可以在思科Id和IdP之間設定後設資料交換。此交換建立了信任關係，然後允許應用程式使用思科Id進行SSO。您可以透過從思科IdS下載後設資料檔案並將其上傳到IdP來建立信任關係。

SAML證書與SSL證書類似，在某些情況下需要更新或更改。在思科身份服務(IdS)伺服器上重新生成或交換SAML證書時，可能導致與身份提供程式(IdP)的受信任連線中斷。此中斷可能導致依賴單一登入的使用者端或使用無法取得存取系統所需的授權的問題。

本文檔旨在介紹在Cisco IdS伺服器上必須建立新SAML證書的各種常見情況。還說明如何將此新證書提供給身份提供程式(IdP)，以便重建信任。藉由執行此動作，使用者端和使用可以繼續使用單

一登入，而不會有任何問題。目標是確保您擁有順利地處理證書更新過程所需的所有資訊，而不會出現混淆。

需牢記的要點：

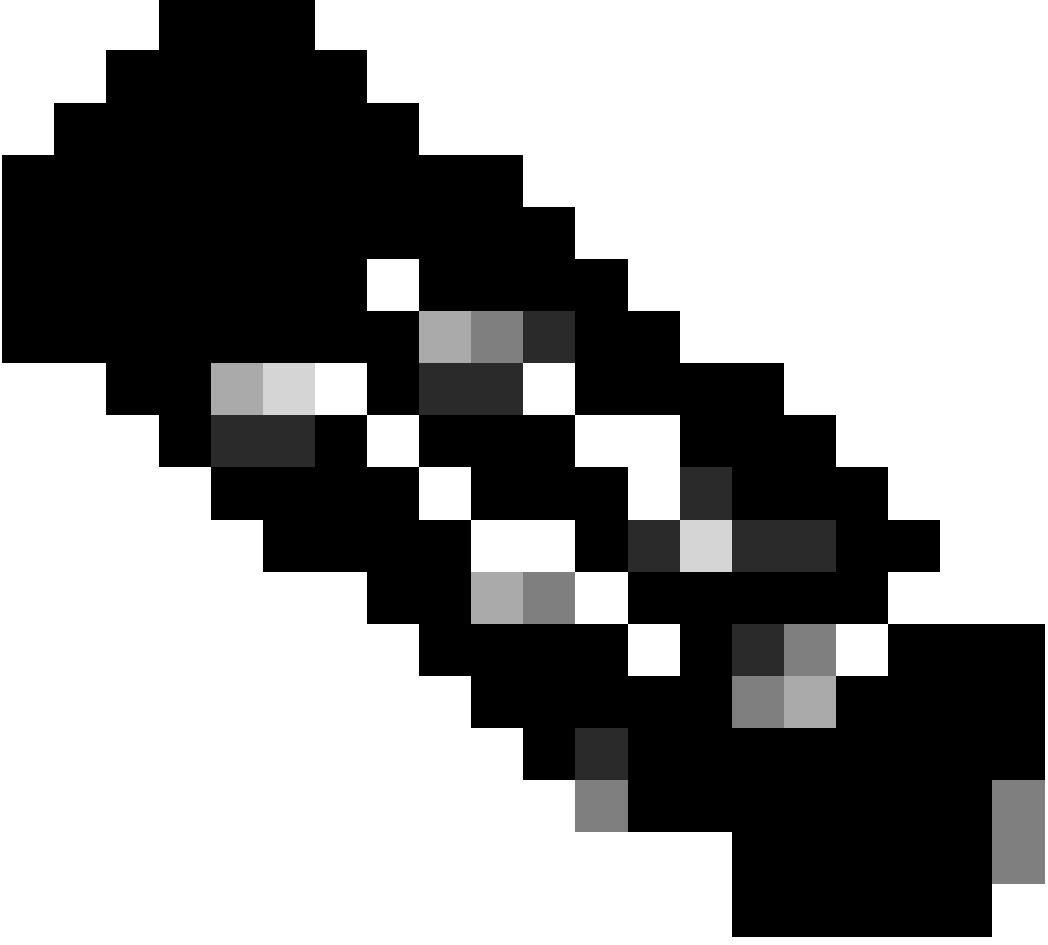
1. 預設情況下，SAML證書在安裝Cisco IdS伺服器期間生成，有效期為3年
2. SAML證書是自簽名證書
3. SAML證書是駐留在Cisco IDS發佈伺服器和訂閱伺服器上的SSL證書
4. 只能在Cisco IDS Publisher節點中執行SAML證書重新生成
5. SAML證書的安全雜湊演算法的可用型別為SHA-1和SHA-256
6. SHA-1演算法用於IdS 11.6，在以前的版本中，SHA-256演算法用於IdS 12.0和更高版本
7. 「辨識提供者」(IdP)與「辨識服務」(IdS)必須使用相同的演演算法型別。
8. 只能從Cisco IdS Publisher節點(sp-<Cisco IdS_FQDN>.xml)下載Cisco IdS SAML證書
9. 請參閱此連結瞭解UCCE/PCCE單點登入配置。 [UCCE 12.6.1功能指南](#)

SAML證書已過期

SAML證書有3年（1095天）的有效期，需要在到期之前更新SAML證書。過期的SSL證書被視為無效證書，它會中斷思科身份服務(IdS)和身份提供程式(IdP)之間的證書鏈。

解決方案

1. 檢查SAML證書到期日期
2. 重新生成SAML證書
3. 下載sp.xml檔案
4. 從sp.xml檔案中檢索SAML證書
5. 將舊的SAML證書替換為IdP中的新SAML證書
6. 詳細步驟請參見「參考」部分



(注意：{由於僅更改了SAML證書，因此不需要將IdS後設資料交換為IdP})

辨識提供者(IdP)中的安全雜湊演算法變更

假設在現有PCCE/UCCE環境中使用單點登入。IdP和Cisco IdS伺服器都配置了SHA-1安全雜湊演算法。考慮到SHA-1的弱點需要將安全雜湊演算法更改為SHA-256。

解決方案

1. 在AD FS信賴方中更改安全雜湊演算法 (SHA-1更改為SHA-256)
2. 將IdS發佈伺服器中的安全雜湊演算法在「金鑰和證書」 (SHA-1更改為SHA-256) 下更改
3. 在IdS發佈伺服器中重新生成SAML證書

4. 下載sp.xml檔案
5. 從sp.xml檔案中檢索SAML證書
6. 將舊的SAML證書替換為IdP中的新SAML證書
7. 詳細步驟請參見「參考」部分

Cisco IdS伺服器IP地址或主機名更改-已重建共存的 CUIC/LiveData/IdS發佈伺服器或獨立Id發佈伺服器-已重建共存的 CUIC/LiveData/IdS訂閱伺服器或獨立Id訂閱伺服器

這些情況很少發生，強烈建議您重新開始「單一登入」(SSO)設定，以確保生產環境中的SSO功能能夠迅速而有效地還原。必須將重新配置排定優先順序，以最大限度地減少使用者所依賴的SSO服務中斷。

解決方案

1. 從AD FS中刪除現有信賴方
2. 上傳Cisco IdS伺服器tomcat信任中的AD FS SSL證書
3. 下載sp.xml檔案
4. 如需詳細步驟，請參閱「參考章節與功能指南」
5. 在AD FS中配置信賴方
6. 增加索賠規則
7. 啟用已簽名的SAML斷言
8. 下載AD FS聯合後設資料
9. 將聯合後設資料上傳到Cisco IdS伺服器
10. 執行測試SSO

參考

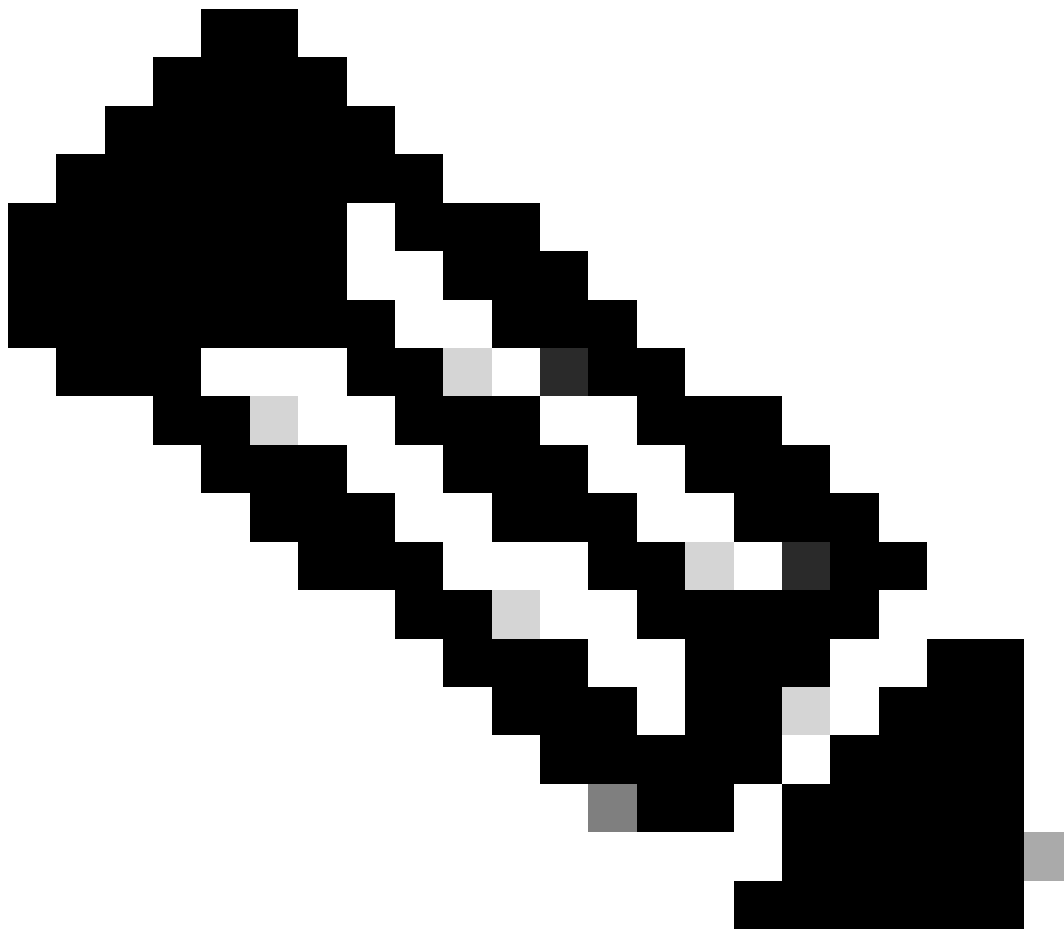
如何在ADFS或

如何啟用已簽名的SAML斷言

有關詳細步驟，請參閱本文檔：[UCCE 12.6.1功能指南](#)

如何將AD FS SSL證書上傳到Cisco IdS tomcat信任

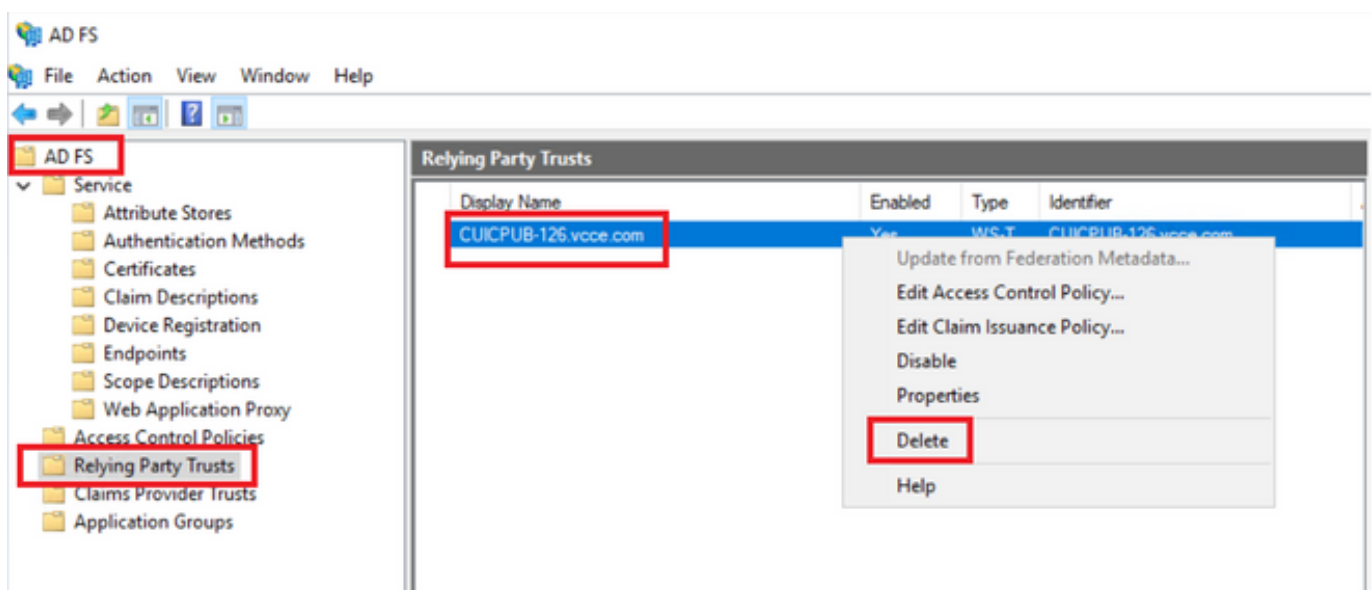
1. 下載或檢索AD FS SSL證書
 2. 訪問Cisco IdS Publisher OS Administration頁面
 3. 使用作業系統管理員憑證登入
 4. 切換作業選項至安全性>憑證管理
 5. 按一下「上傳憑證/憑證鏈結」，即會開啟蹦現視窗
 6. 按一下「下拉式功能表」，然後在「憑證用途」上選取tomcat-trust
 7. 按一下「瀏覽」並選取AD FS SSL憑證
 8. 按一下「上傳」
-



(注意：{信任證書已複製到訂閱伺服器節點。您不需要上傳至訂閱者節點。})

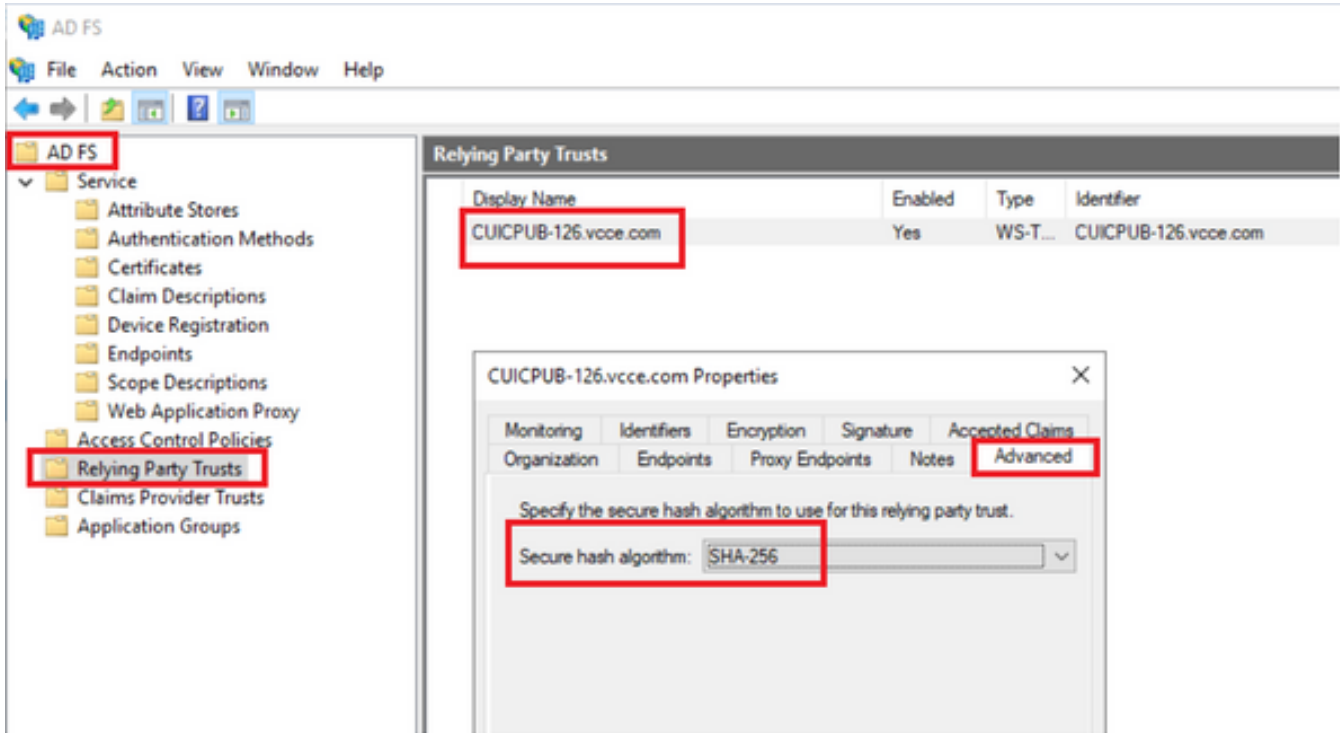
如何刪除AD FS中的信賴方

1. 使用管理員授權的憑證登入辨識提供者(IdP)伺服器
2. 開啟伺服器管理員，然後選擇「AD FS」>「工具」>「AD FS管理」
3. 在左側樹狀結構中，選取AD FS下的「信賴方信任」
4. 按一下右鍵Cisco IdS伺服器並選擇「刪除」



如何檢查或變更在辨識提供者(IdP)中設定的安全雜湊演演算法

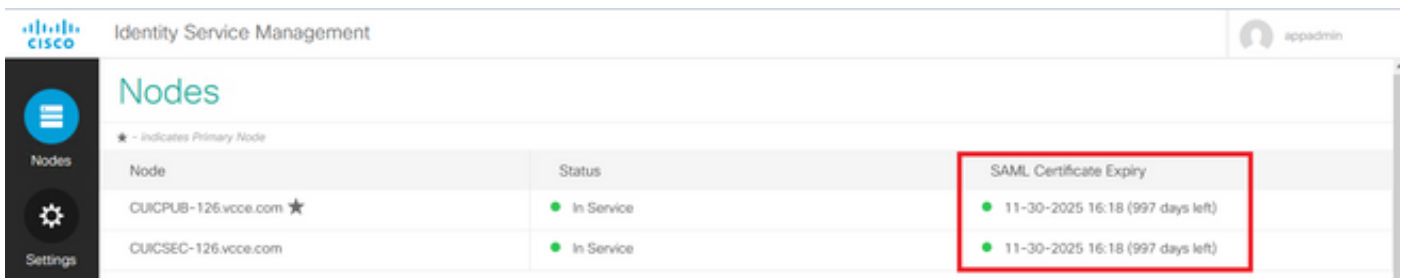
1. 使用管理員授權的憑證登入辨識提供者(IdP)伺服器
2. 開啟伺服器管理員，然後選擇「AD FS」>「工具」>「AD FS管理」
3. 在左側樹狀結構中，選取AD FS下的「信賴方信任」
4. 按一下右鍵Cisco IdS伺服器並選擇「屬性」
5. 瀏覽「進階」頁標
6. 安全雜湊演演算法選項顯示AD FS伺服器中配置的安全雜湊演演算法。



7. 按一下「下拉式」功能表，然後選取想要的安全雜湊演演算法。

如何檢查Cisco IdS伺服器SAML證書到期日期

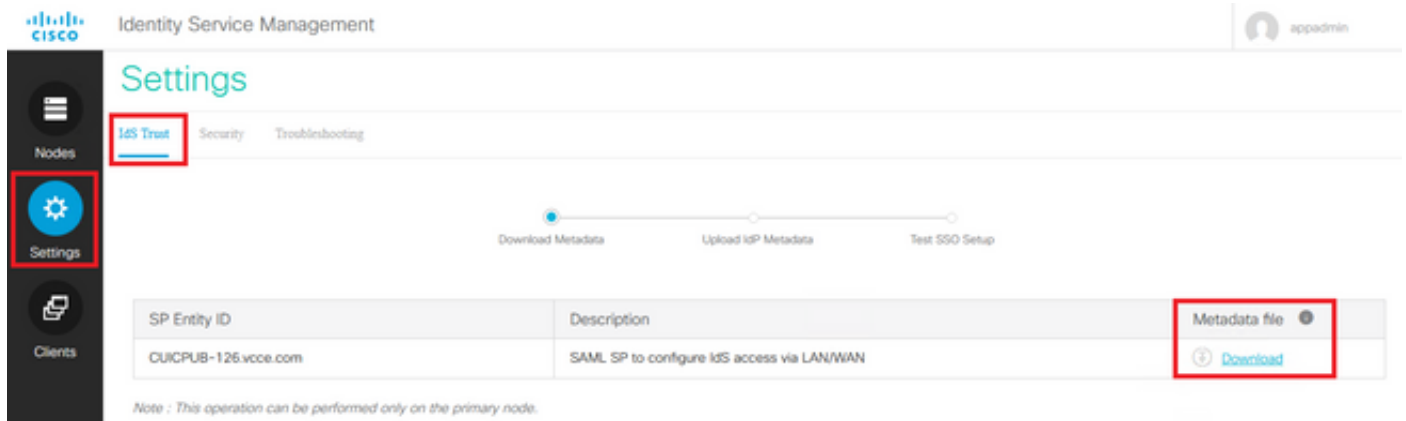
1. 使用應用程式使用者憑證登入到Cisco IdS伺服器發佈伺服器或訂閱伺服器節點
2. 成功登入頁面後，登入至「辨識服務管理」>「節點」
3. 顯示Cisco IdS發佈伺服器和訂閱伺服器節點、狀態和SAML證書到期



如何下載Cisco IdS伺服器的後設資料

1. 使用應用程式使用者憑證登入到Cisco IdS發佈伺服器節點
2. 按一下「設定」圖示
3. 切換作業選項至「IDS信任」頁標

4. 按一下「下載」連結下載Cisco IdS集群的後設資料

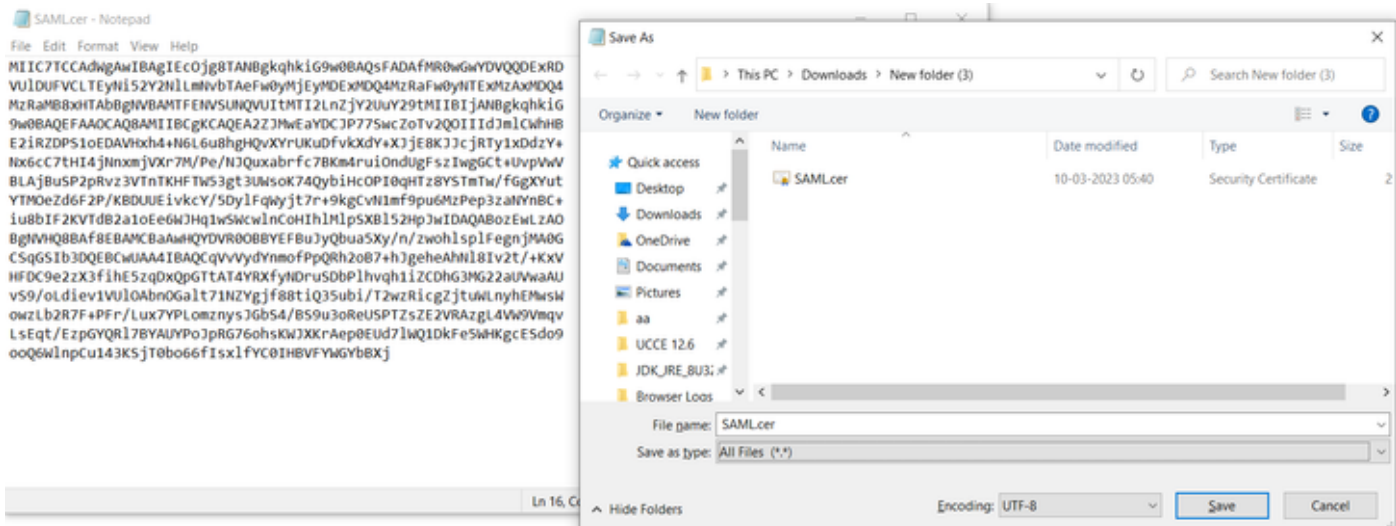


如何從sp.xml檔案中檢索SAML證書

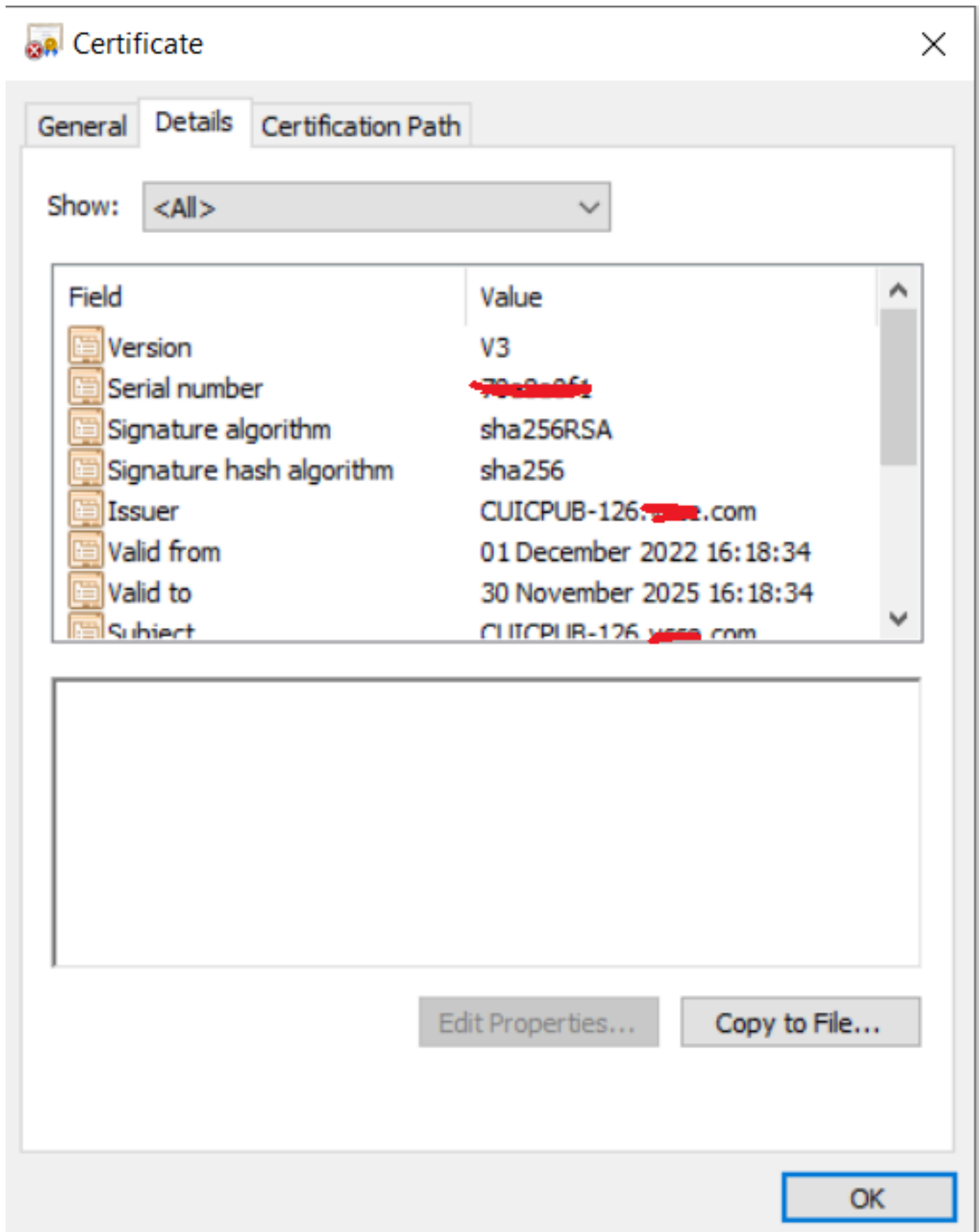
1. 使用文本編輯器打開sp.xml檔案
2. 在標頭<ds : X509Certificate></ds : X509Certificate>之間複製原始資料

```
<ds:X509Certificate>MIIC7TCCAdWgAwIBAgIEcOjg8TANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDExRD
VU1DUFVCLTEyNi52Y2N1LmNvbTAeFw0yMjE5MDExMDQ4MzRaFw0yNTE5MDQ4
MzRaMB8xHTAbBgNVBAMTFENVSUNQVUI tMTI2LnZjY2UuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA2ZJmWwEaYDCJP77SwcZoTv2QOIIdJmLCWhHB
E2iRZDPS1oEDAVHxh4+N6L6u8hgHQvXYrUKuDfvkXdY+XJjE8KJjCjRTy1xDdzY+
Nx6cC7tHI4jNnxmjVXr7M/Pe/NJQuxabr7c7BKm4ruiOndUgFsziwgGct+UvpVwV
BLAjBuSP2pRvz3VTnTKHFTW53gt3UWsoK74QybiHcOPI0qHTz8YSTmTw/fGgXYut
YTMOeZd6F2P/KBDUUEivkcY/5DylFqWyt7r+9kgCvNlmf9pu6MzPep3zaYnBC+
iu8bIF2KVTdB2aloEe6WJHq1wSwcWlnCoHIh1MlpSXB152HpJwIDAQABozEwLzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0OBBYEFBUjYQbua5Xy/n/zwohlSplFegnJMA0G
CSqGSIb3DQEBCwUAA4IBAQCqVvVydYnmofPpQRh2oB7+hJgeheAhN18Iv2t/+KxV
HFDC9e2zX3fihE5zqDxQpGtAT4YRXfyNDruSDbPlhvqh1iZCDhG3MG22aUVwaAU
vS9/oLdievlVULOAbnOGalt71NZYgjf88tiQ35ubi/T2wzRicgZjtuWLnYhEMwsW
owzLb2R7F+PFR/Lux7YPLomznysJGbs4/BS9u3oReUSPTZsZE2VRAZg4VW9Vmqv
LsEqT/EzpgYQR17BYAUYPoJpRG76ohsKWJXKrAep0EUd71WQ1DkFe5WHKgcESdo9
ooQ6WlnpCul43KSjt0bo66fIsx1fYC0IHBVfYWGyBxj</ds:X509Certificate>
```

3. 開啟另一個文字編輯器，並貼上複製的資料
4. 儲存檔案.CER格式

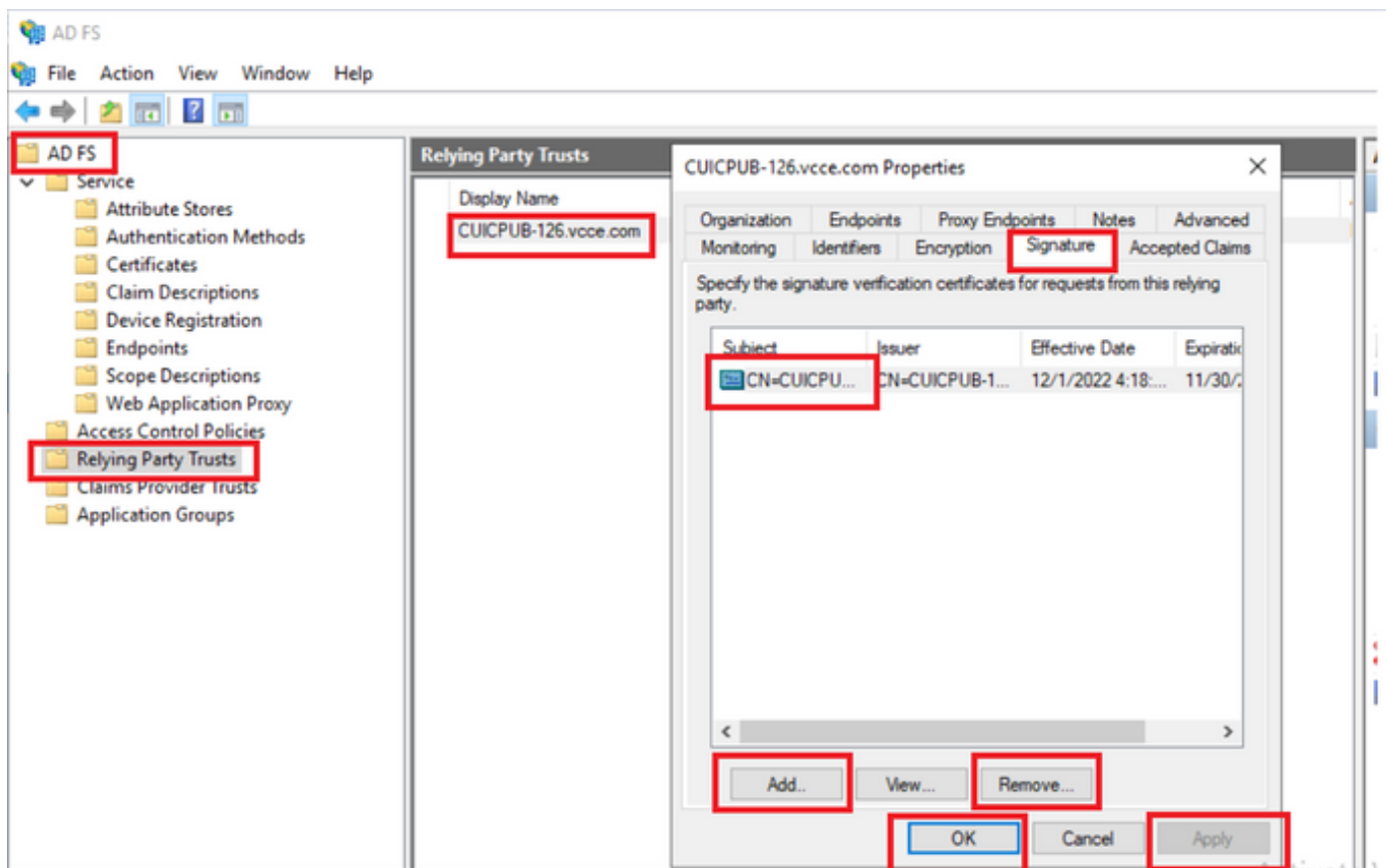


5. 開啟憑證以複查憑證資訊



如何替換AD FS中的SAML證書

1. 將SAML證書檔案複製到從sp.xml檢索的AD FS伺服器
2. 開啟伺服器管理員，然後選擇「AD FS」>「工具」>「AD FS管理」
3. 在左側樹狀結構中，選取AD FS下的「信賴方信任」
4. 按一下右鍵Cisco IdS伺服器並選擇「屬性」
5. 切換作業選項至「簽名」頁標
6. 按一下「新增」，然後選擇新產生的SAML憑證
7. 選取舊的SAML憑證，然後按一下移除
8. 套用並儲存



如何在Cisco IdS伺服器中重新生成SAML證書

1. 使用應用程式使用者憑證登入到Cisco IdS發佈伺服器節點
2. 按一下「設定」圖示
3. 切換作業選項至「安全性」頁標
4. 選擇「金鑰和證書」選項

5. 按一下SAML certificate部分下的Regenerate按鈕 (突出顯示)

The screenshot shows the Cisco Identity Service Management interface. The left sidebar contains navigation options: Nodes, Settings (highlighted with a red box), and Clients. The main content area is titled 'Settings' and has three tabs: 'IdS Trust', 'Security' (highlighted with a red box), and 'Troubleshooting'. Under the 'Security' tab, there are two sub-sections: 'Tokens' (Set Token Expiry) and 'Keys and Certificates' (Regenerate Keys and Certificates, highlighted with a red box). The 'Keys and Certificates' section contains two main areas: 'Generate Keys and SAML Certificate' and 'SAML Certificate'. The 'Generate Keys and SAML Certificate' section has a 'Regenerate' button. The 'SAML Certificate' section has a dropdown menu set to 'SHA-256' and a 'Regenerate' button. The 'SAML Certificate' section is also highlighted with a red box.

測試SSO

每當SAML證書發生更改時，請確保TEST SSO在Cisco IdS伺服器中成功，並從CCEAdmin頁面重新註冊所有應用。

1. 從「主參與者AW」伺服器存取「CCEAdmin」頁面
2. 以管理員級別許可權登入到CCEAdmin門戶
3. 切換作業選項至概要>功能>單一登入
4. 點選Register with Cisco Identity Service下的Register按鈕
5. 執行測試SSO

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）。