整合客服中心企業版(UCCE)單一登入(SSO)憑證和設定

目錄

簡介

本文檔介紹UCCE SSO所需的證書配置。此功能的設定包括多個HTTPS、數位簽章和加密憑證。

需求

思科建議您瞭解以下主題：

- UCCE版本11.5
- Microsoft Active Directory(AD)- Windows Server上安裝的AD
- Active Directory聯合身份驗證服務(ADFS)版本2.0/3.0

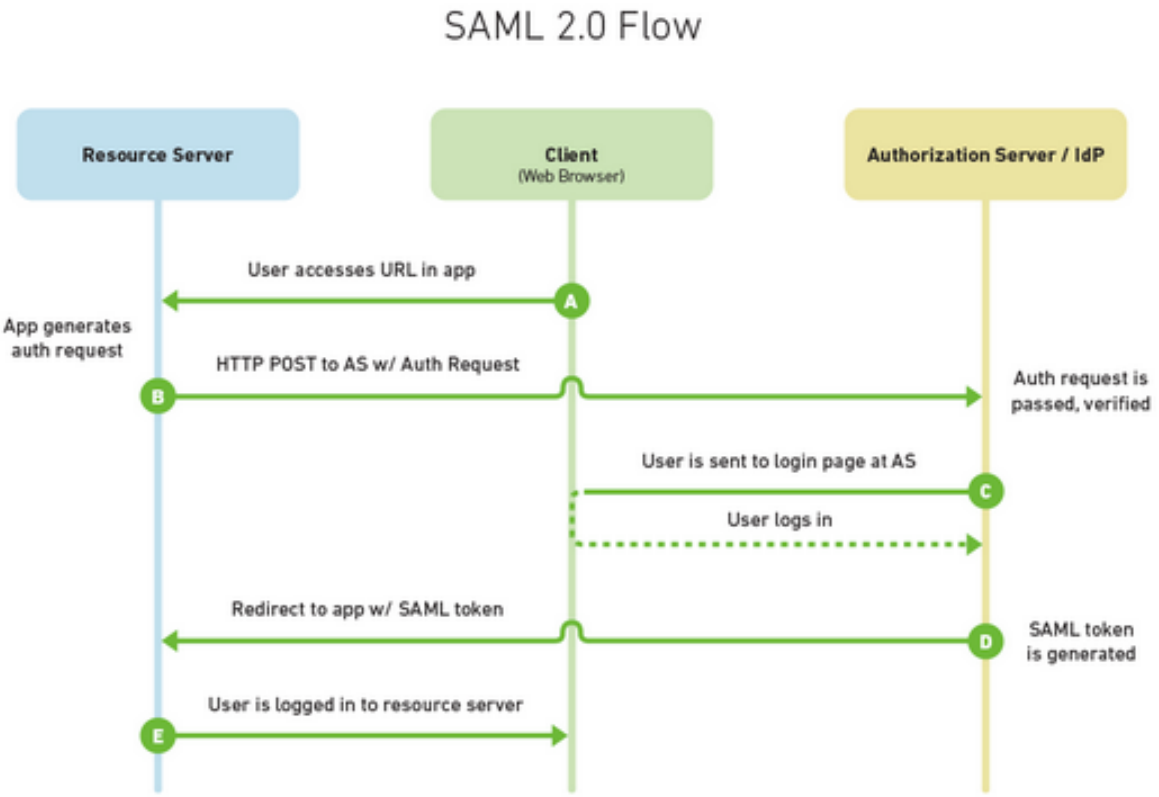
採用元件

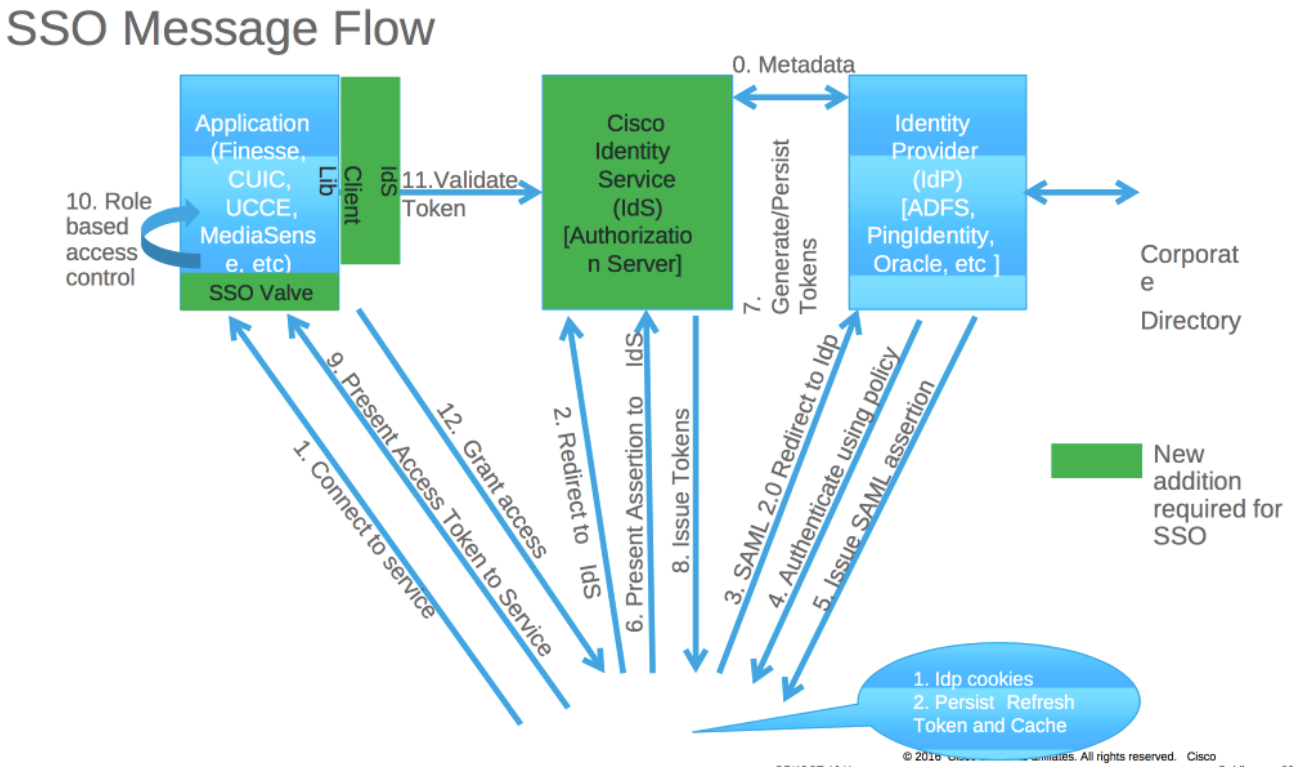
UCCE 11.5

Windows 2012 R2

A部分。SSO消息流

The most common SAML flow is shown below:

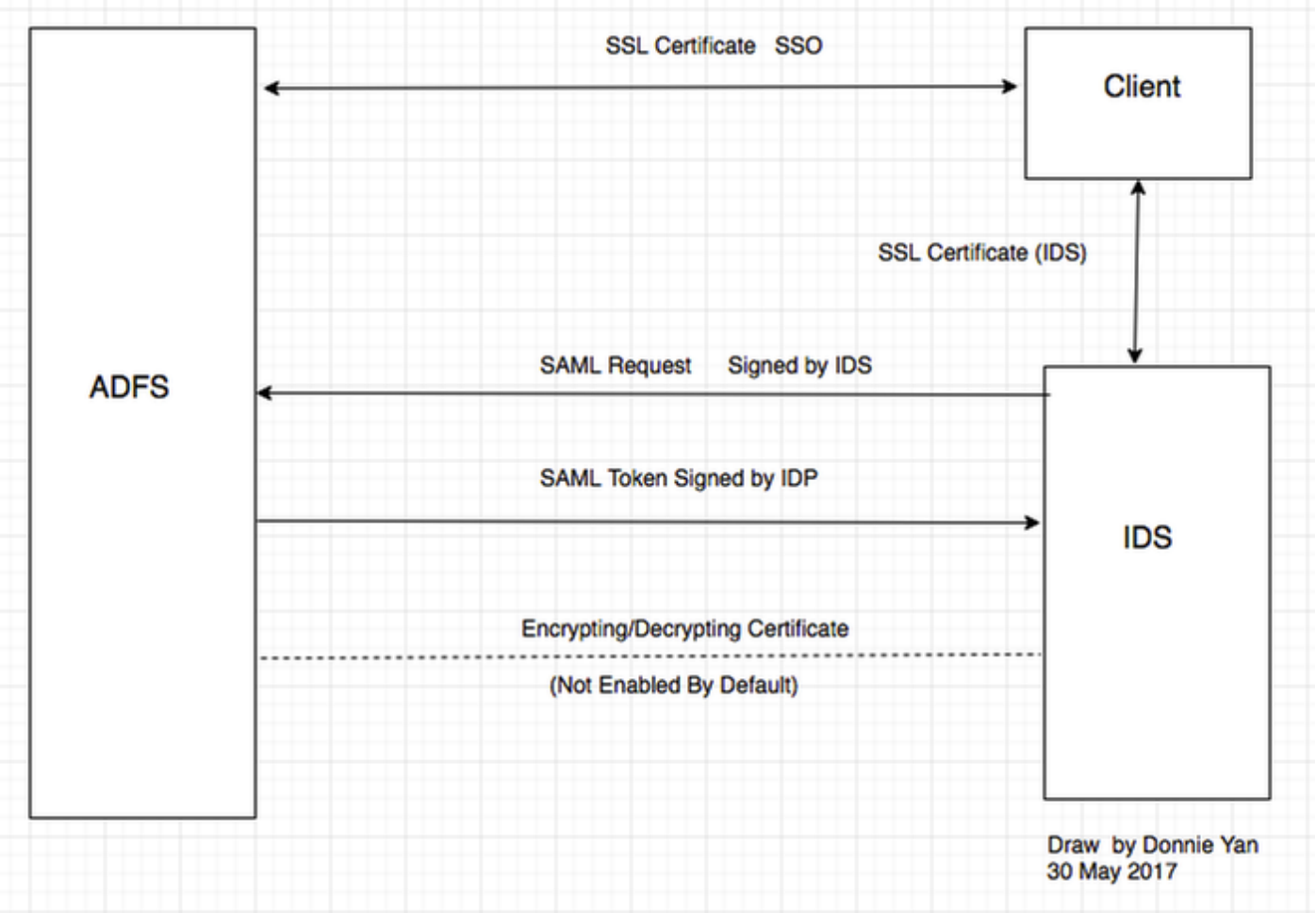




啟用SSO後，當代理登入到Finesse案頭時：

- Finesse伺服器重定向代理瀏覽器以與身份服務(IDS)通訊
- IDS使用SAML請求將代理瀏覽器重定向到身份提供程式(IDP)
- IDP生成SAML令牌並傳遞到IDS伺服器
- 生成令牌後，每次代理瀏覽到應用程式時，都會使用此有效令牌進行登入

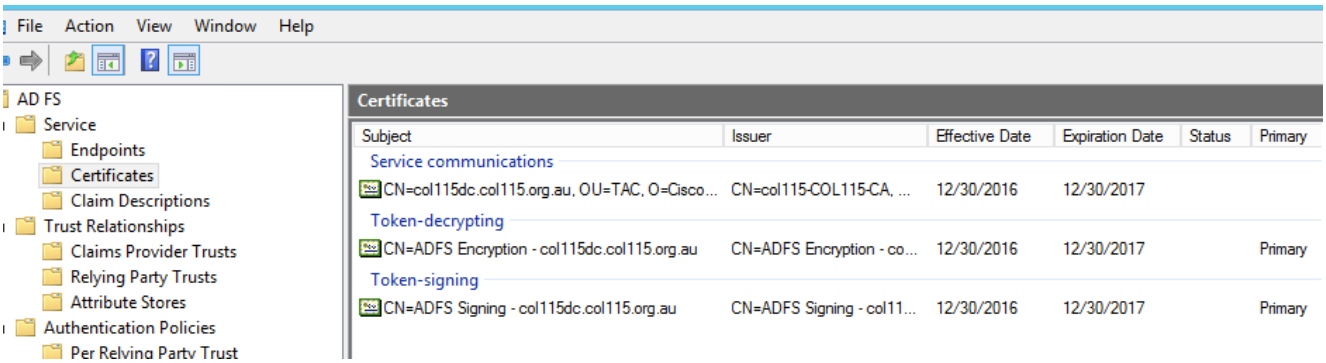
B部分.IDP和IDS中使用的證書



IDP證書

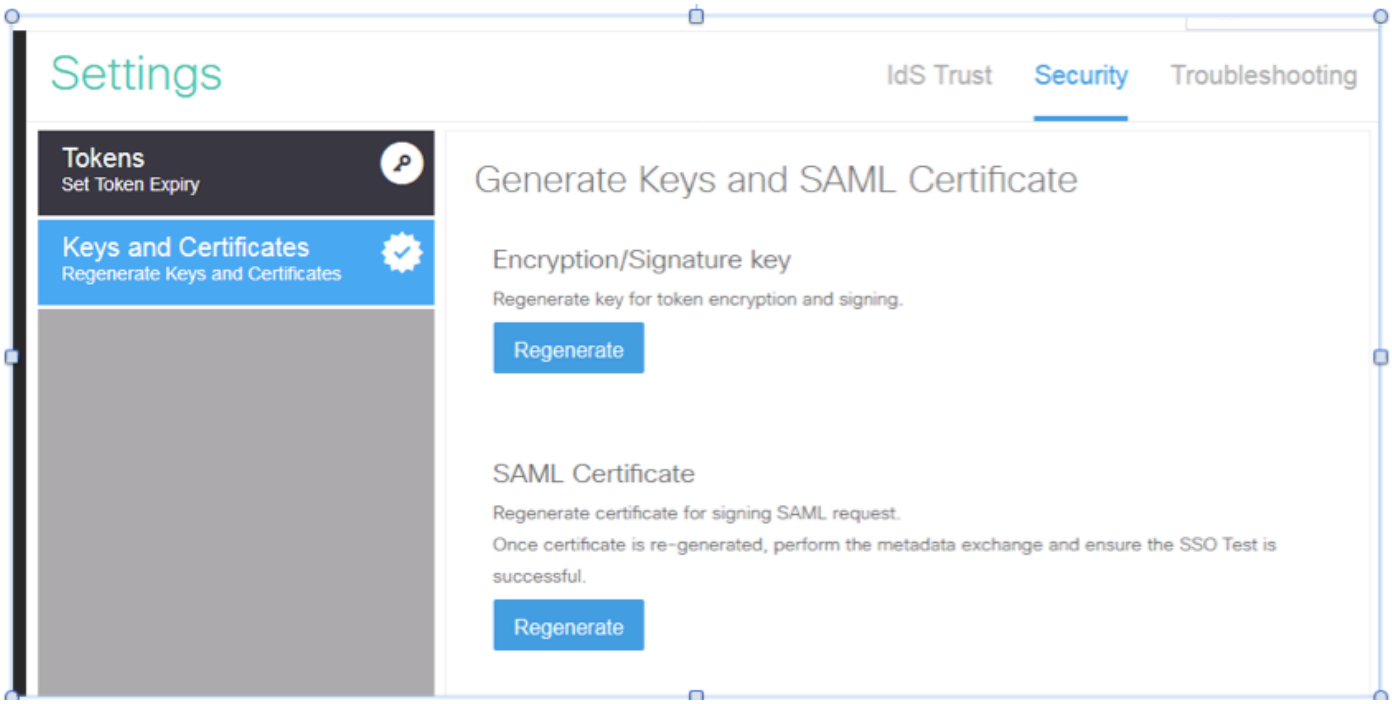
- SSL憑證(SSO)
- 令牌簽名證書
- 令牌 — 解密

1.



IDS憑證

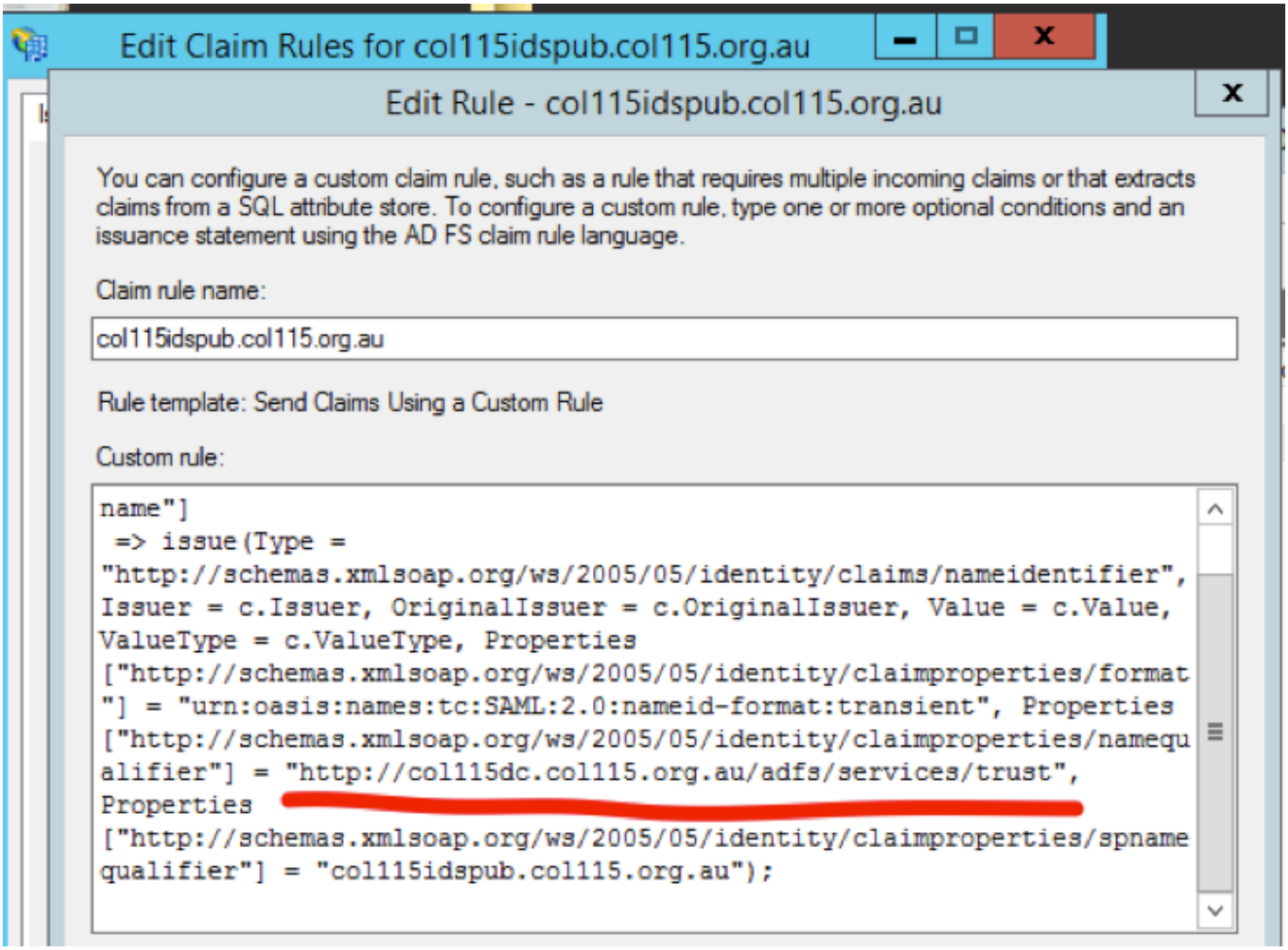
- SAML證書
- 簽名金鑰
- 加密金鑰



C部分：詳細的IDP認證和配置

SSL憑證(SSO)

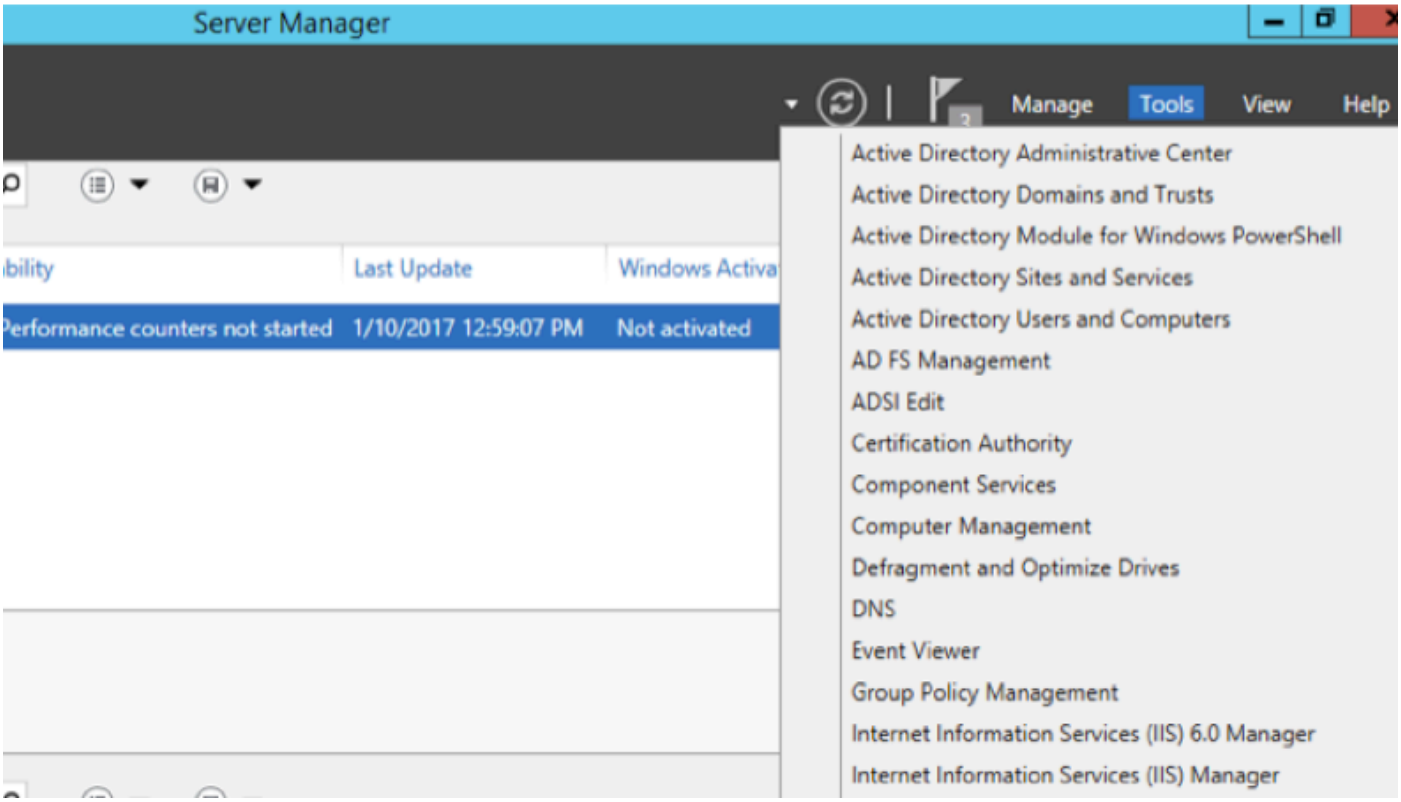
- 此證書在IDP和客戶端之間使用。客戶端必須信任SSO證書
- SSL證書用於加密客戶端和IDP伺服器之間的會話。此證書不是特定於ADFS，而是特定於IIS
- SSL證書的主題必須與ADFS配置中使用的名稱匹配

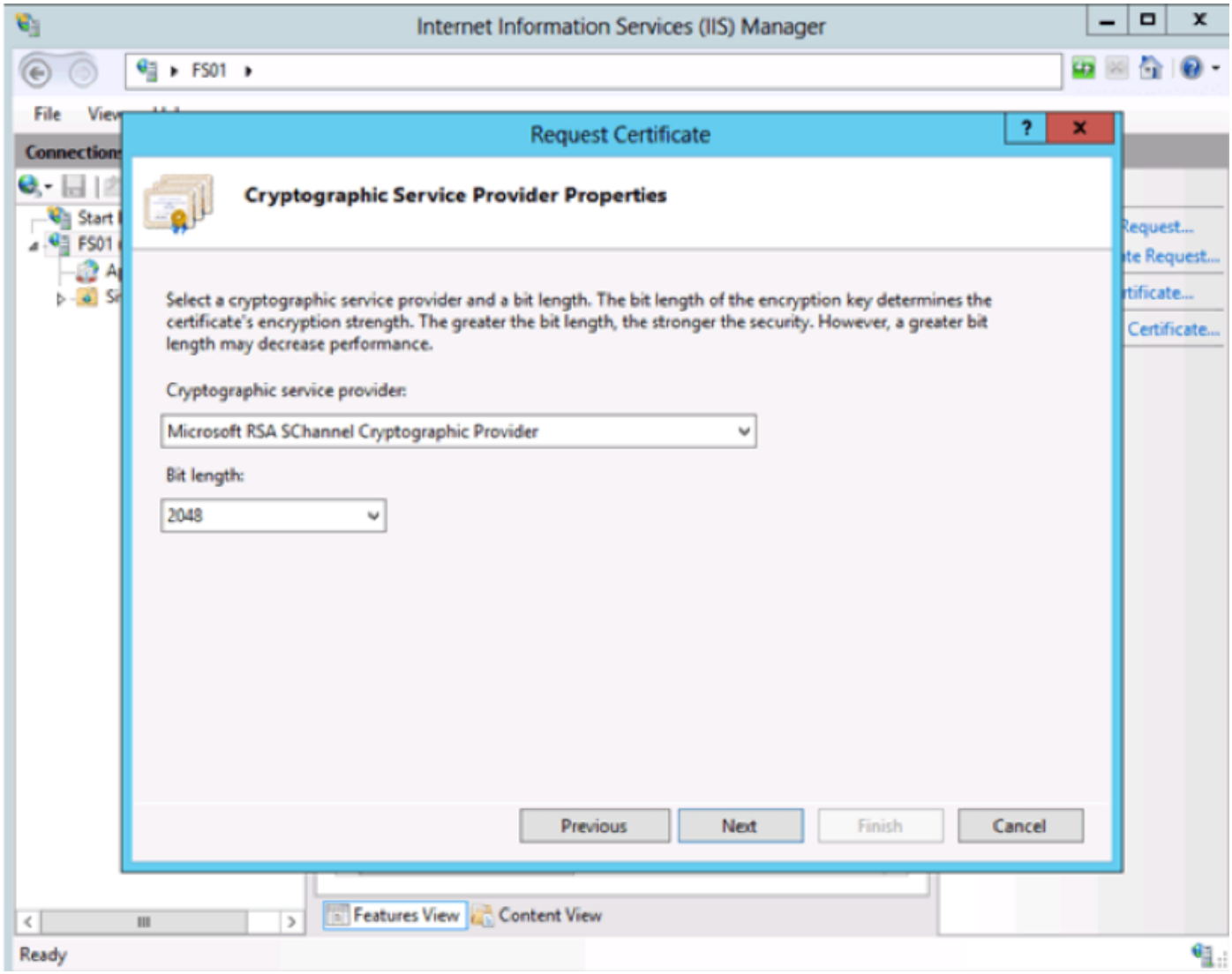


為SSO配置SSL證書的步驟（本地實驗室已簽署內部CA）

步驟1. 使用憑證簽署請求(CSR)建立SSL憑證，並由ADFS的內部CA簽署。

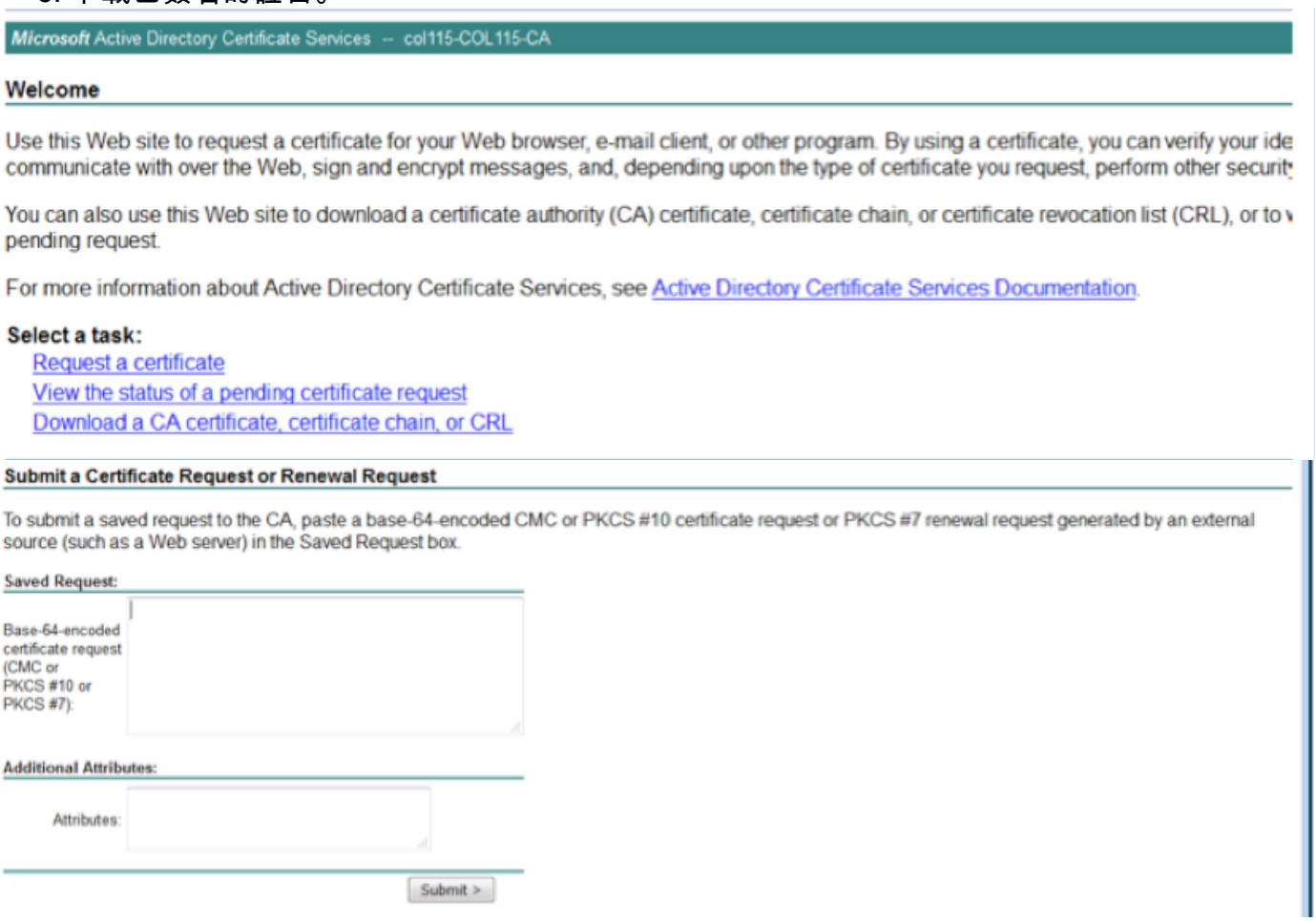
1. 開啟伺服器管理器。
2. 按一下「工具」。
3. 按一下「Internet資訊服務(IIS)管理器」。
4. 選擇本地伺服器。
5. 選擇伺服器證書。
6. 按一下「開啟特徵」（操作面板）。
7. 按一下「create certificate request」。
8. 將加密服務提供程式保留為預設值。
9. 將Bit Length更改為2048。
10. 按「Next」（下一步）。
11. 選擇儲存請求檔案的位置。
12. 按一下「Finish」（結束）。





步驟2. CA對步驟1產生的CSR進行簽名。

1. **開啟**CA伺服器以使**用此CSR http:<CA Server ip address>/certsrv/**。
2. 按一下「Request a certificate」。
3. 按一下「advanced certificate request」。
4. **將**CSR複製到Based-64編碼憑證要求。
5. **提交**。
6. 下載已簽名的證書。



步驟3.將簽名證書安裝回ADFS伺服器並分配給ADFS功能。

1.將簽名證書安裝回ADFS伺服器。為此，請開啟**Server manager>**Tools>按一下Internet Information Services(IIS)Manager**>**。

Local Server>Server Certificate>Open Feature（操作面板）。

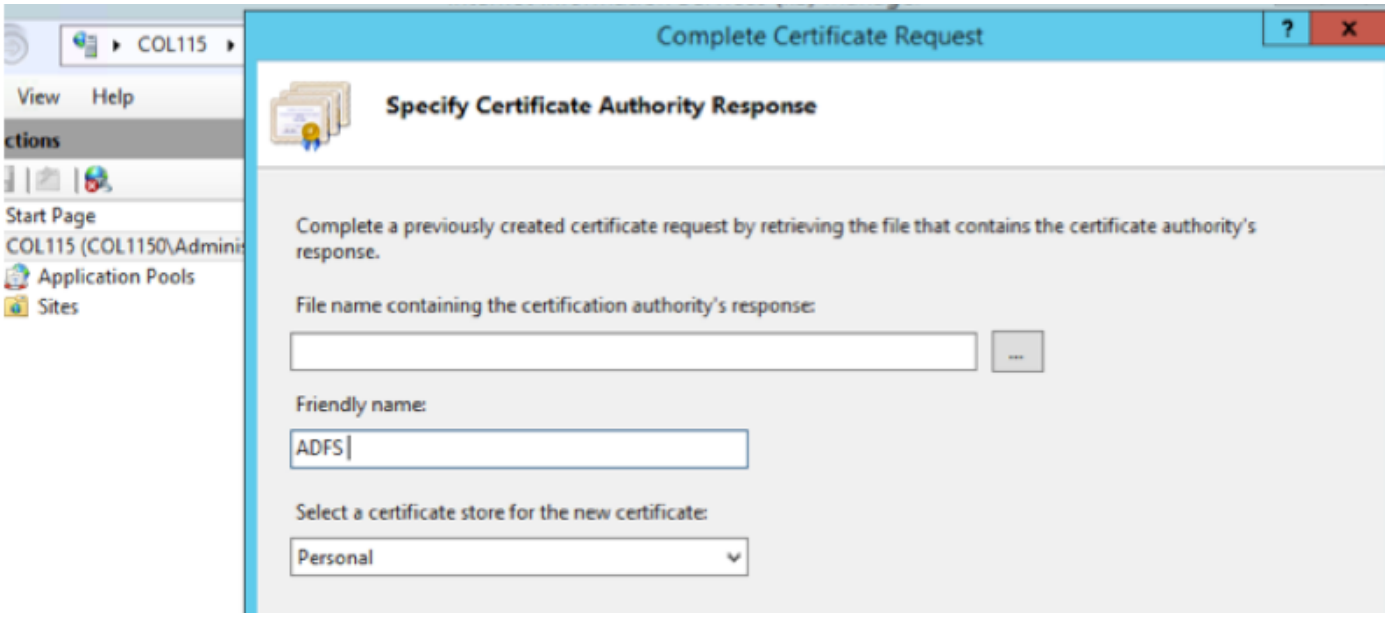
2.按一下「完成證書申請」。

3.選擇您完成並從第三方證書提供商下載的完整CSR檔案的路徑。

4. **輸入**憑證的友好名稱。

5.選擇「個人」作為證書儲存。

6.按一下**確定**。



7.在此階段，新增了所有證書。現在，必須分配SSL證書。

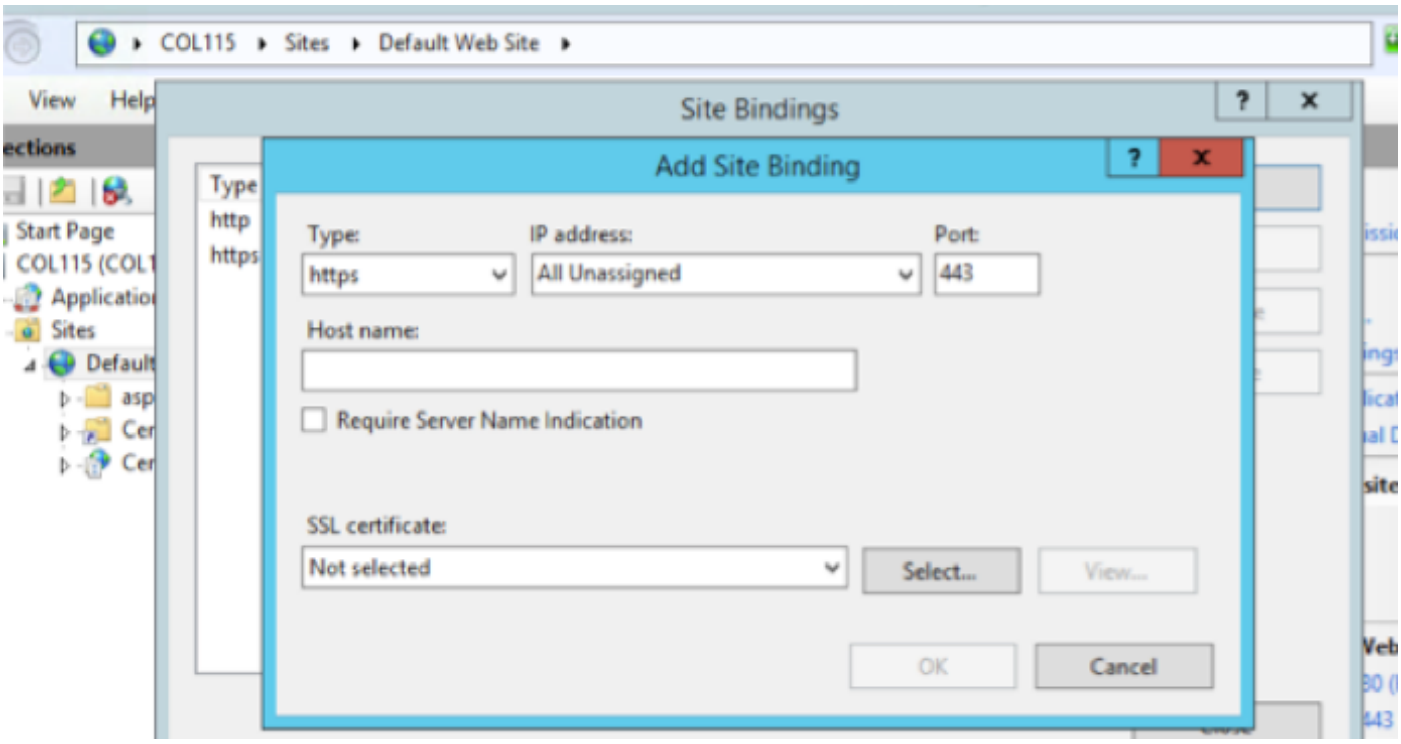
8.展開**本地**服務**器>展開站點>選擇預設網站>按一下繫結**（操作窗格）。

9.按一下**Add**。

10.**將**型別更改為HTTPS。

11.從下拉選單中選擇您的證書。

12.按一下**OK**。



現在，已分配ADFS伺服器的SSL證書。

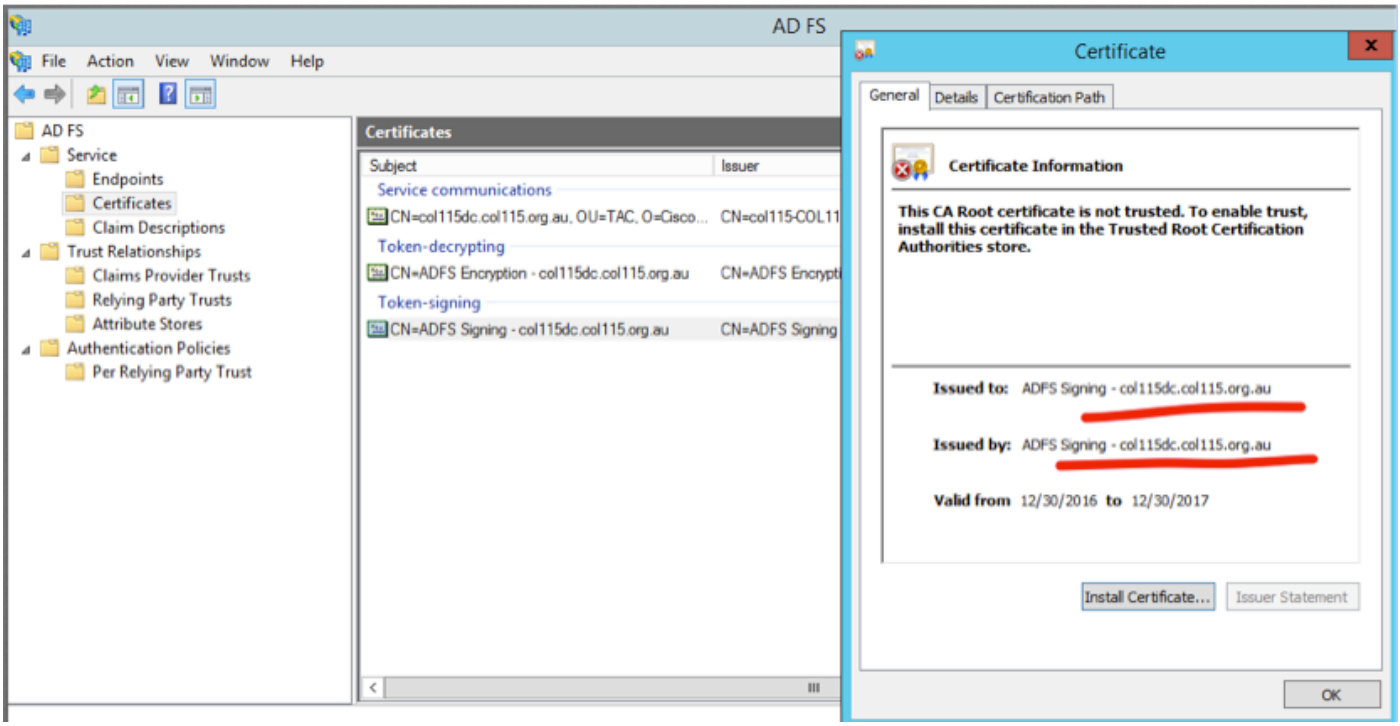
附註：在安裝ADFS功能期間，必須使用以前的SSL證書。

令牌簽名證書

ADFS為令牌簽名證書生成自簽名證書。預設情況下，它在一年內有效。

IDP生成的SAML令牌由ADFS私鑰（令牌簽名證書私密部分）簽名。 然後，IDS使用ADFS公鑰進行驗證。此保證簽名令牌不會被修改。

每當使用者需要獲取對信賴方應用程式(Cisco IDS)的訪問許可權時，都會使用令牌簽名證書。

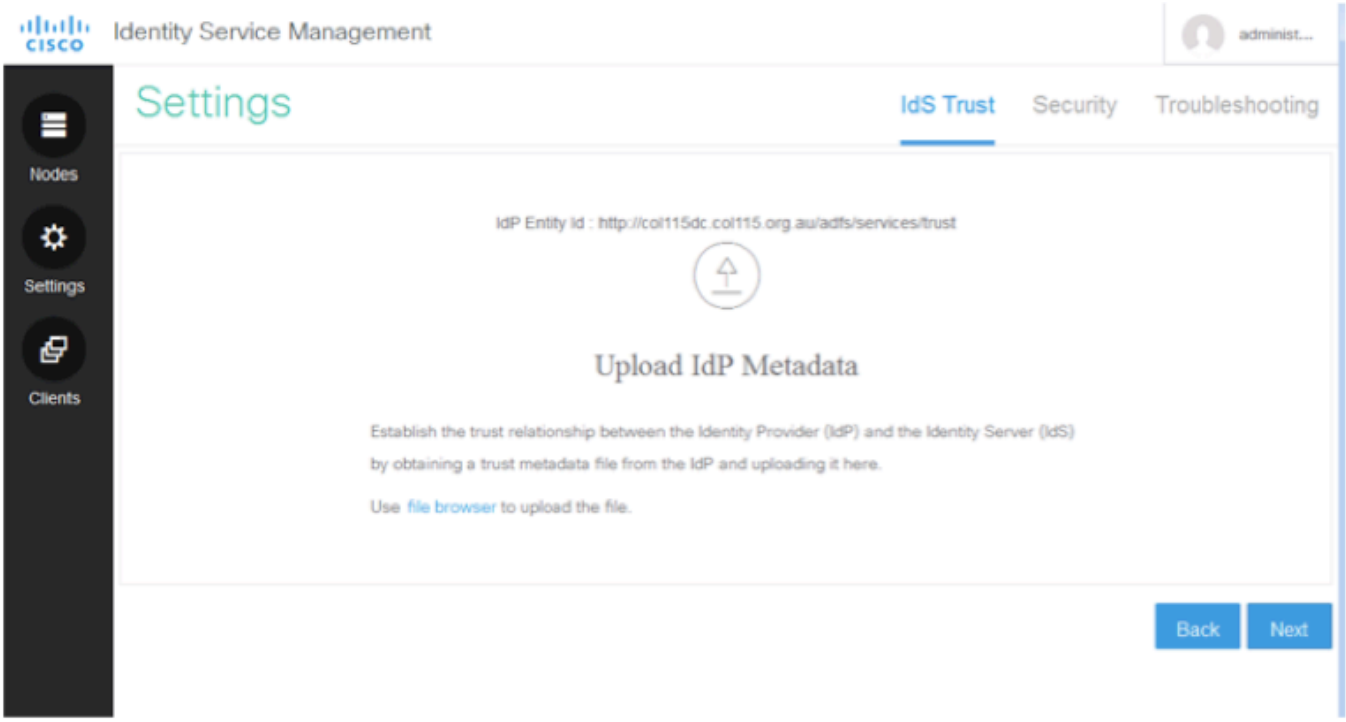


Cisco IDS伺服器如何取得權杖演唱憑證的公鑰？

這是通過將ADFS後設資料上載到IDS伺服器，然後將ADFS的公鑰傳遞到IDS伺服器來實現的。這樣，IDS就可以獲得ADFS伺服器的公鑰。

您需要從**ADFS**下載IDP後設資料。要下載IDP後設資料，請參閱連結**https:// <ADFS的FQDN>/federationmetadata/2007-06/federationmetadata.xml**。

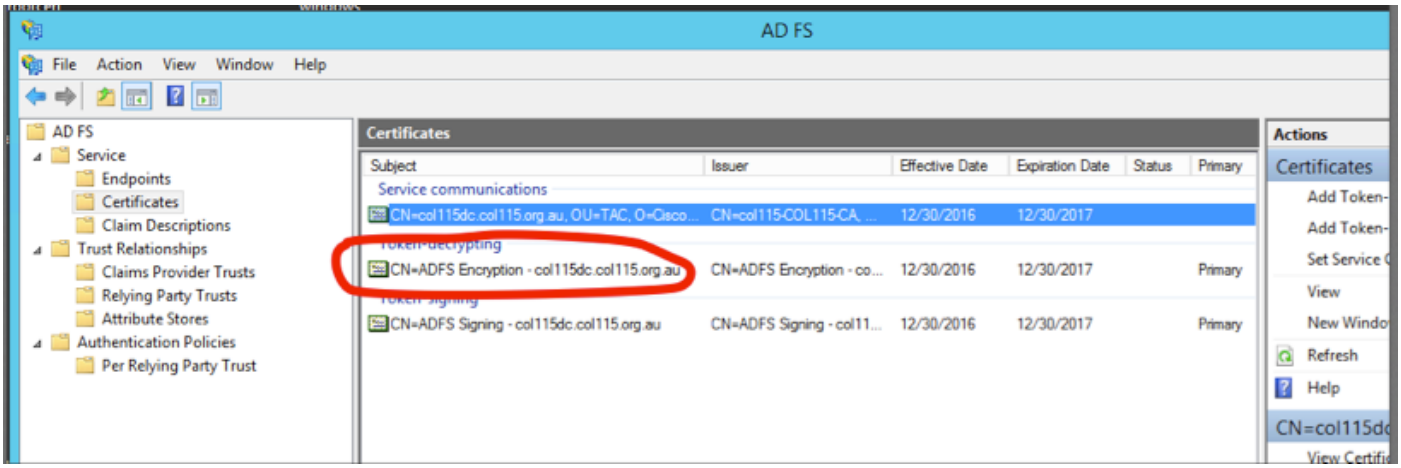
從ADFS後設資料



將ADFS後設資料上載到IDS

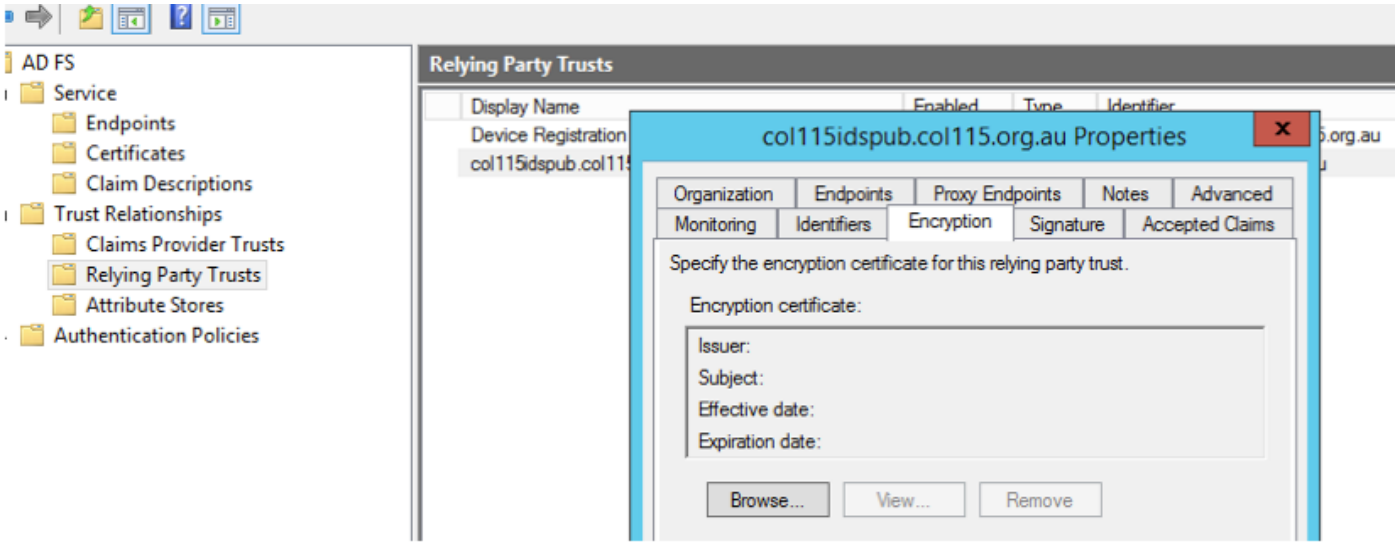
權杖解密

此證書由ADFS伺服器（自簽名）自動生成。 如果令牌需要加密，ADFS使用IDS公鑰對其進行解密。但是，當您看到ADFS令牌加密時，並不意味著令牌已加密。



如果要檢視是否對特定信賴方應用程式啟用了令牌加密，則需要檢查特定信賴方應用程式上的「加密」頁籤。

下圖顯示，未啟用令牌加密。



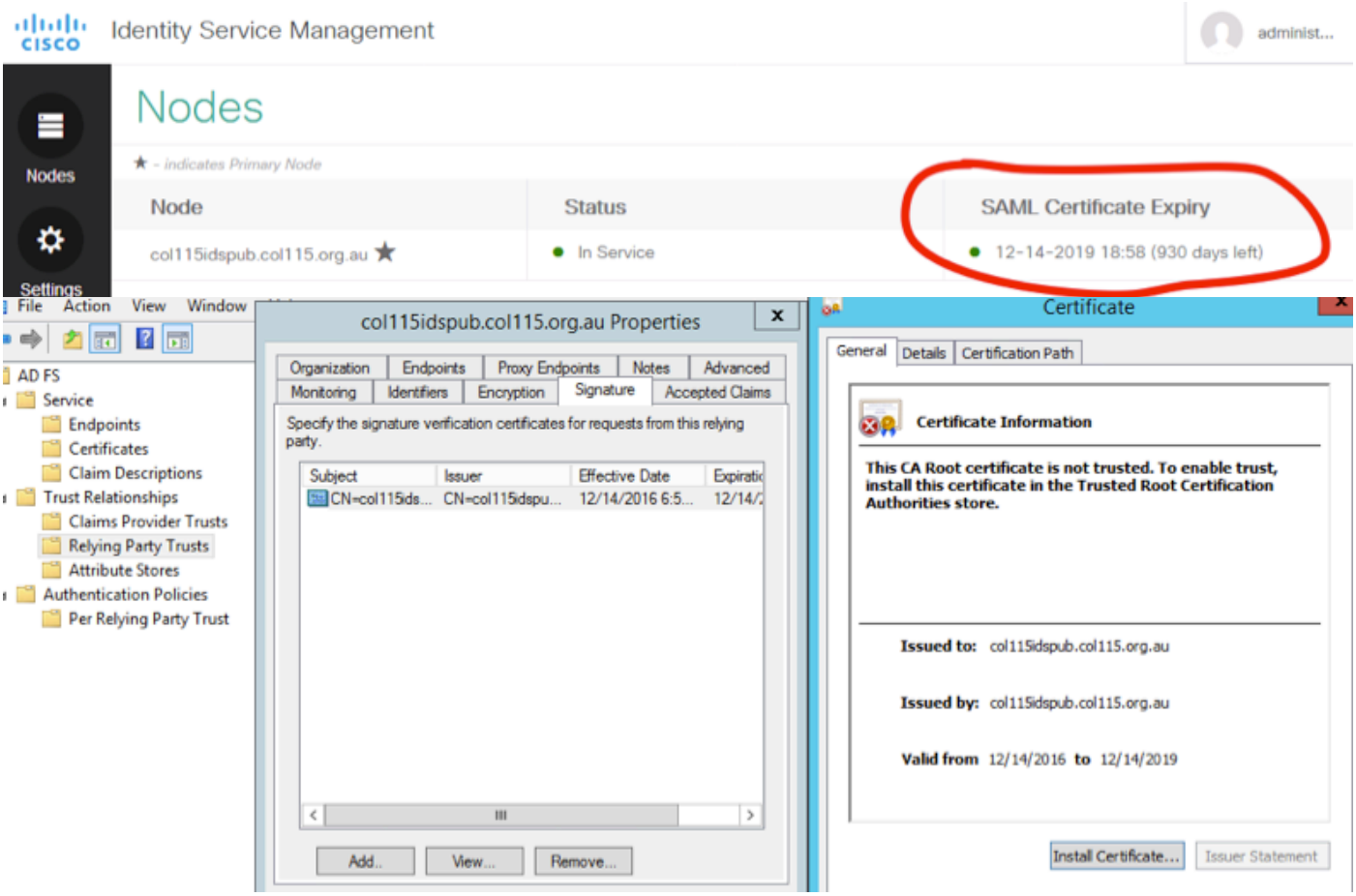
未啟用加密

D部分。Cisco IDS端證書

- SAML證書
- 加密金鑰
- 簽名金鑰

SAML證書

此證書由IDS伺服器（自簽名）生成。 預設情況下，有效期為3年。

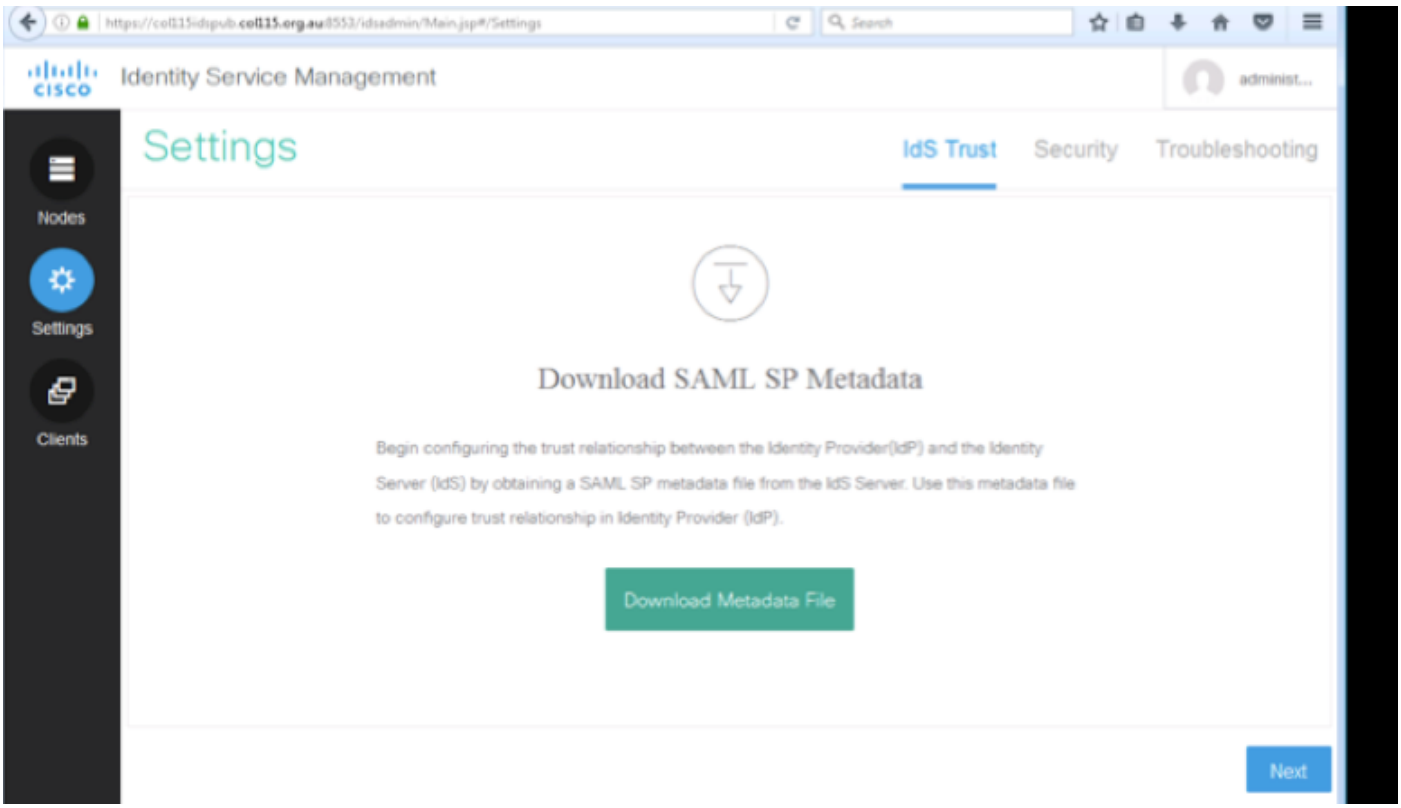


此證書用於簽署SAML請求並傳送到IDP(ADFS)。 此公鑰在IDS後設資料中，必須匯入到ADFS伺服器。

1.從**IDS**伺服器下載SAML SP後設資料。

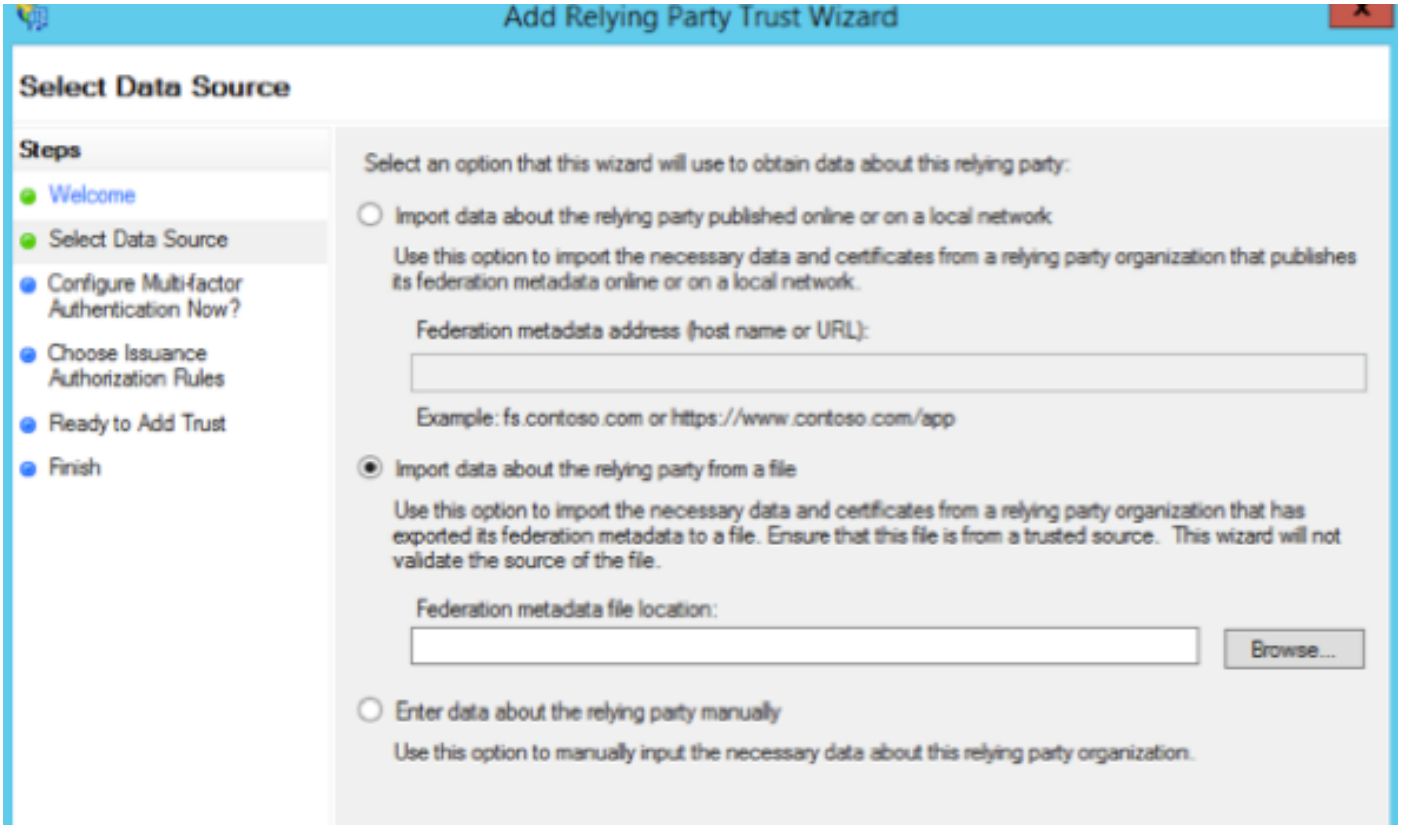
2.瀏覽到**https://<ids server FQDN>:8553/idsadmin/**。

3.選擇設定並下載SAML SP後設資料並**儲存**。

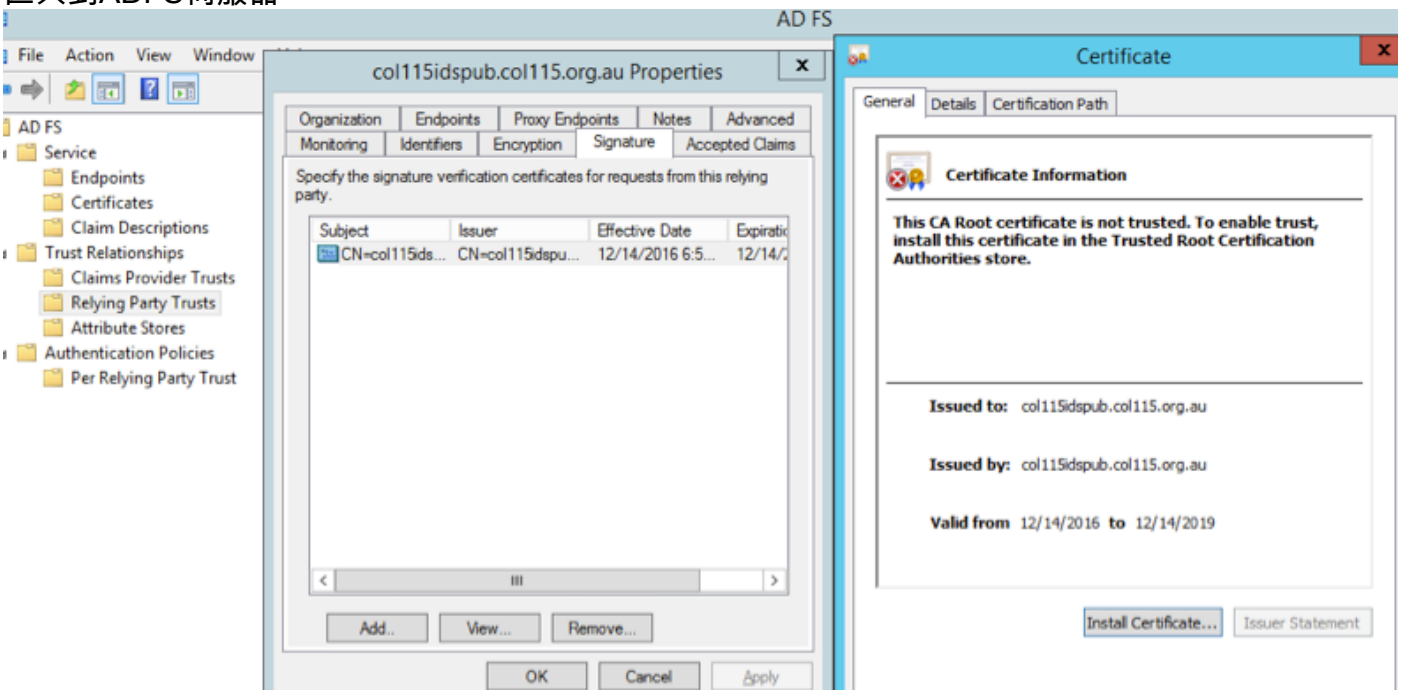


來自IDS伺服器的後設資料

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor entityID="col115idspub.col115.org.au" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  - <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
      - <KeyDescriptor use="signing">
          - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              - <ds:X509Data>
                  <ds:X509Certificate>MIIC+TCCAeGgAwIBAgIEWD4KtDANBgkqhkiG9w0BAQUFADAlMSMwIQYDVQQDExpjb2wxMTVpZHNw
                  dWIuY29sMTE1Lm9yZy5hdTAeFw0xNjEyMTQwNzU4MjVaFw0xOTEyMTQwNzU4MjVaMCUxIzAhBgNV
                  BAMTGmNvbDExNWlkc3B1Yi5jb2wxMTUub3JnLmF1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```



匯入到ADFS伺服器

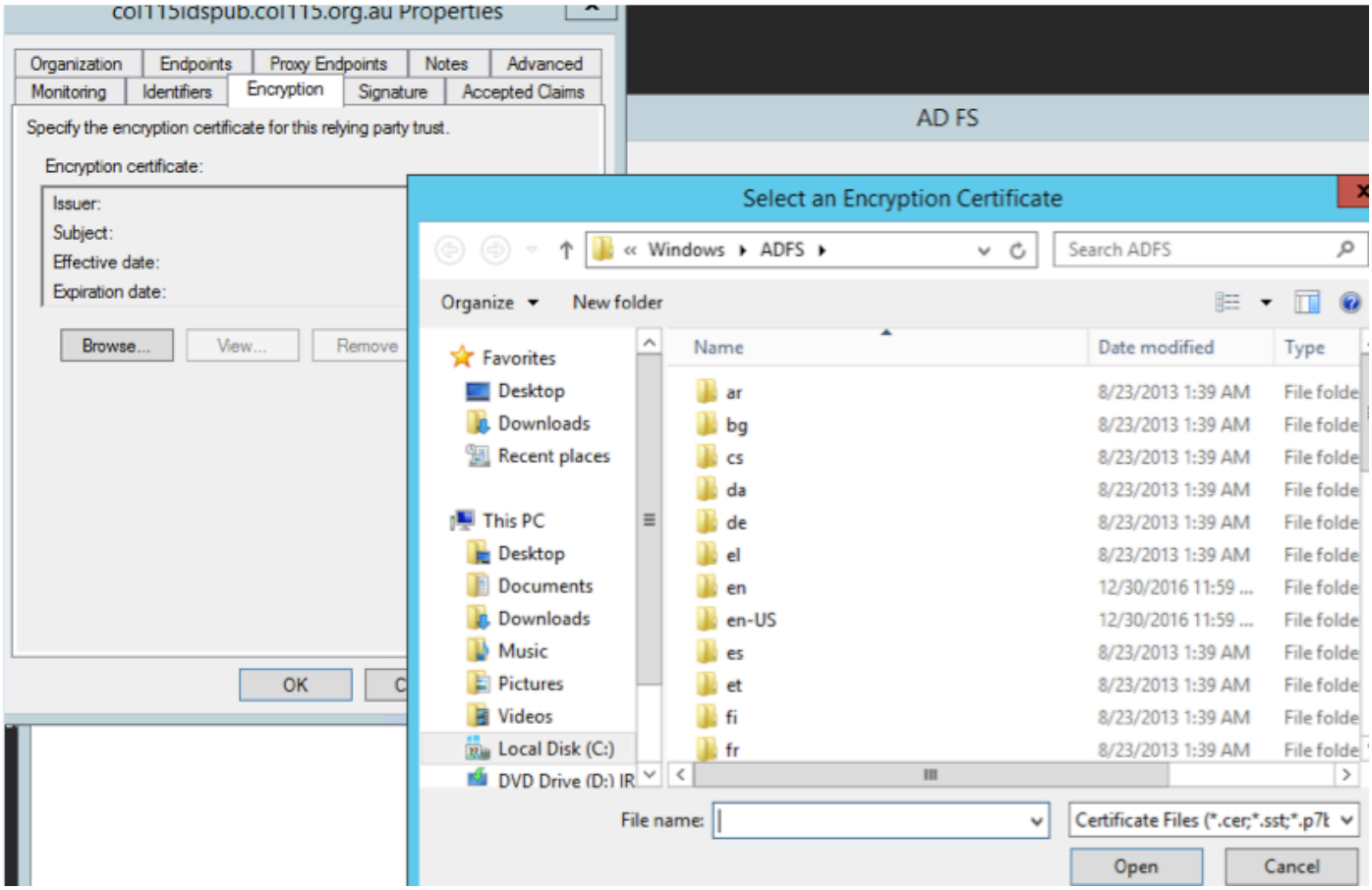


從ADFS端驗證

當IDS重新生成SAML證書時（該證書用於對SAML請求進行簽名），它將執行後設資料交換。

加密/簽名金鑰

預設情況下未啟用加密。如果啟用加密，則需要將其上載到ADFS。



參考：

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-features-guide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf