將Umbrella與NetIQ整合，以便使用SAML進行SSO

目錄

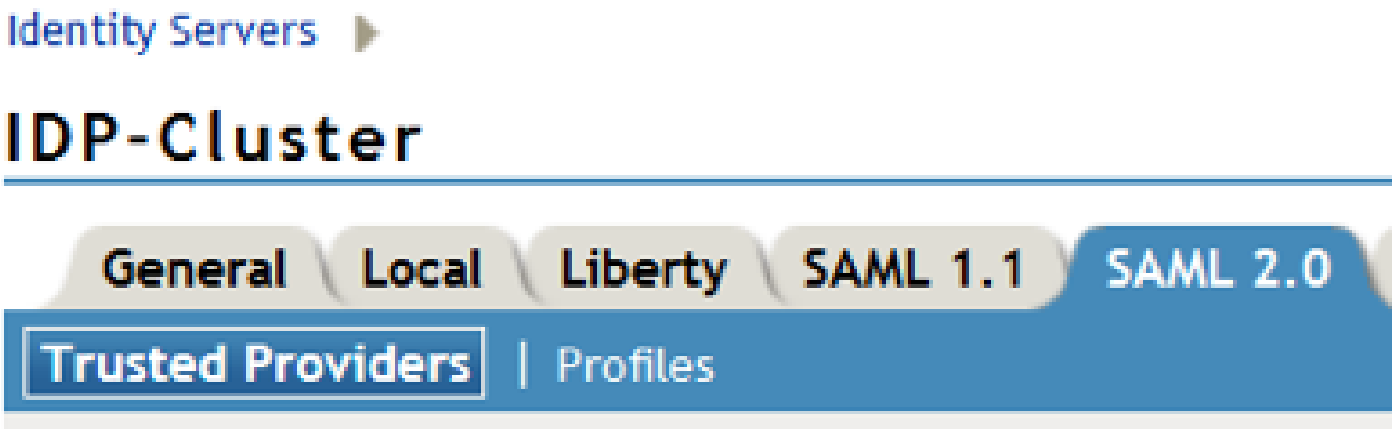
簡介

本文檔介紹如何將Cisco Umbrella與NetIQ整合，以實現單點登入(SSO)和SAML。

適用於NetIQ的Umbrella SAML整合概述

使用NetIQ配置SAML不同於其他SAML整合，因為它不是嚮導中一兩次按一下的過程，但需要對NetIQ進行更改才能正常工作。本文檔介紹了為使SAML和NetIQ協同工作而需要進行的詳細修改。因此，此資訊按「原樣」提供，並與現有客戶一起開發。對此解決方案的可用支援有限，思科Umbrella支援無法提供此處提供的總大綱之外的幫助。

有關SAML整合如何與Umbrella配合使用的詳細資訊，請在此處閱讀我們的評論：開始單一登入。

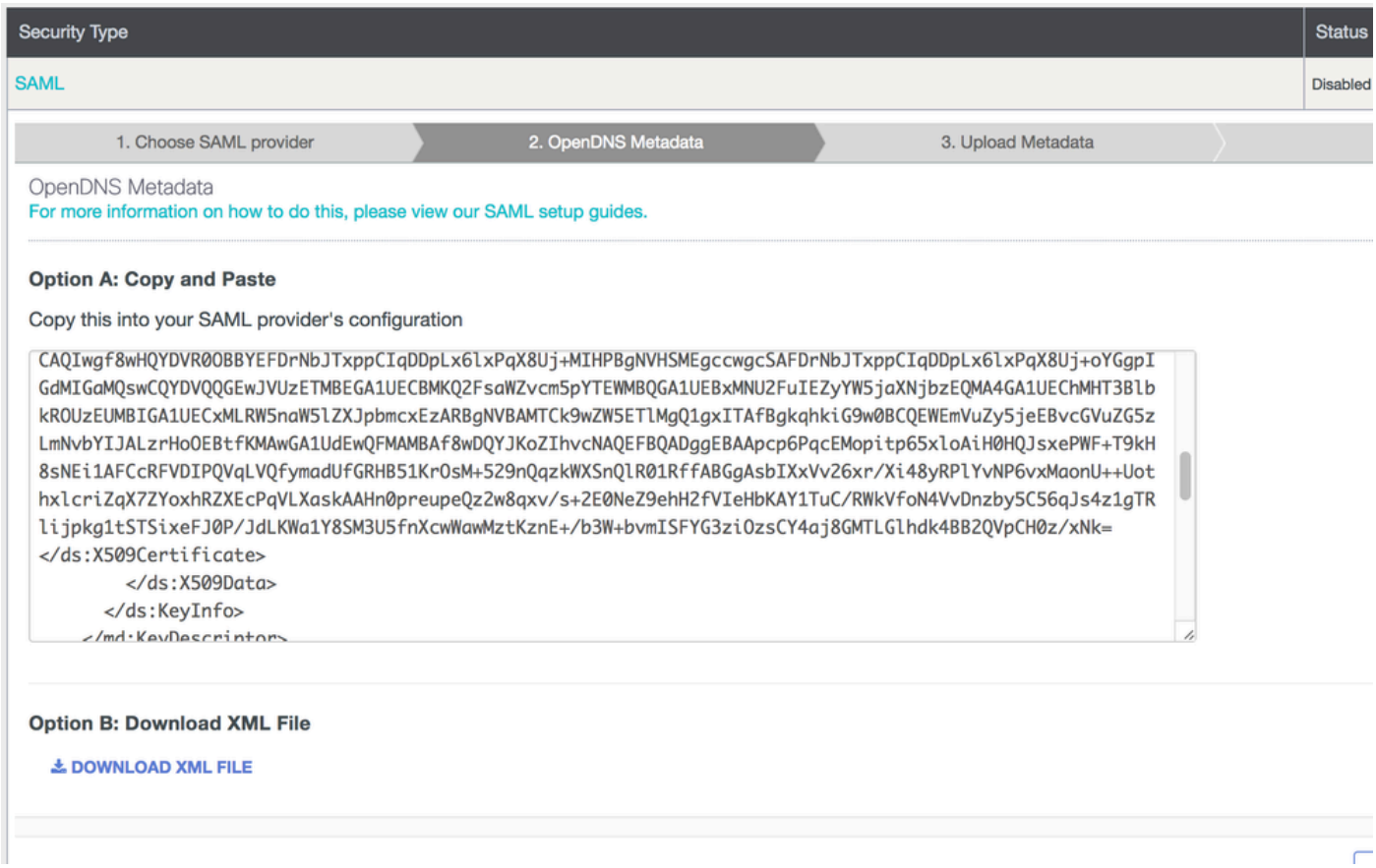


115000348788

必要條件

您可以在以下找到完成初始SAML設定的步驟：身份整合：必要條件.完成包括下載Cisco Umbrella後設資料的這些步驟後，您可以繼續使用這些NetIQ特定說明完成配置。

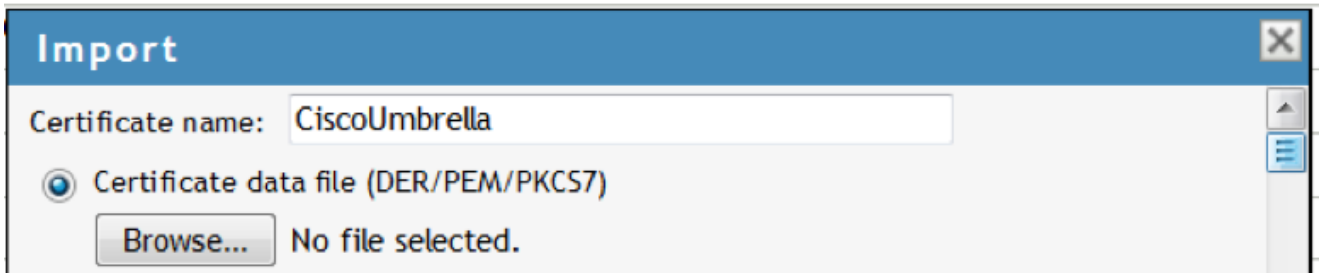
可在Cisco Umbrella SAML安裝嚮導(「設定」>「身份驗證」>「SAML」)中找到後設資料。



115001332488

匯入後設資料和Cisco Umbrella證書

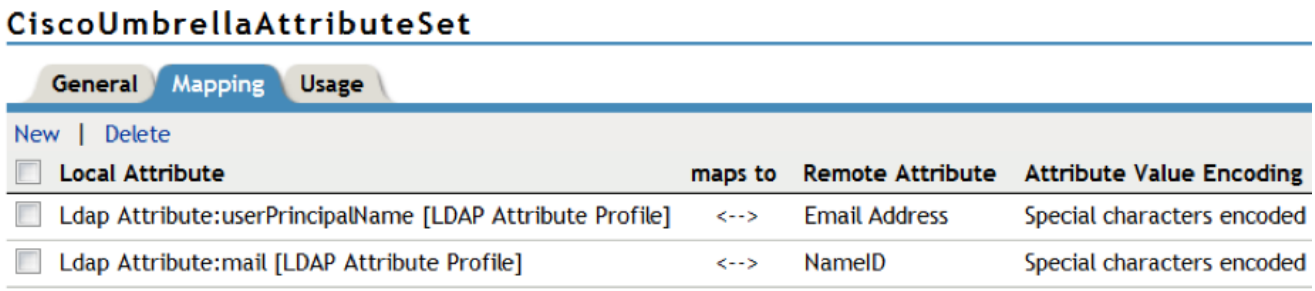
1. 在文本編輯器中開啟Cisco Umbrella後設資料（在先決條件中下載）並提取X509證書。證書以ds:X509Certificate開頭，以/ds:X509Certificate結尾 — 僅從開始到結束進行複製。
2. 將此新檔案另存為CiscoUmbrella.cer。
3. 將x509證書轉換為PKCS7 / PEM。執行此命令的方法各不相同，但此命令可以執行此操作：
   openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM
4. 在NetIQ中，在Trusted Root下啟動NAM。
5. 選擇New > Browse並匯入CiscoUmbrella.pem。



115000349367

建立屬性組

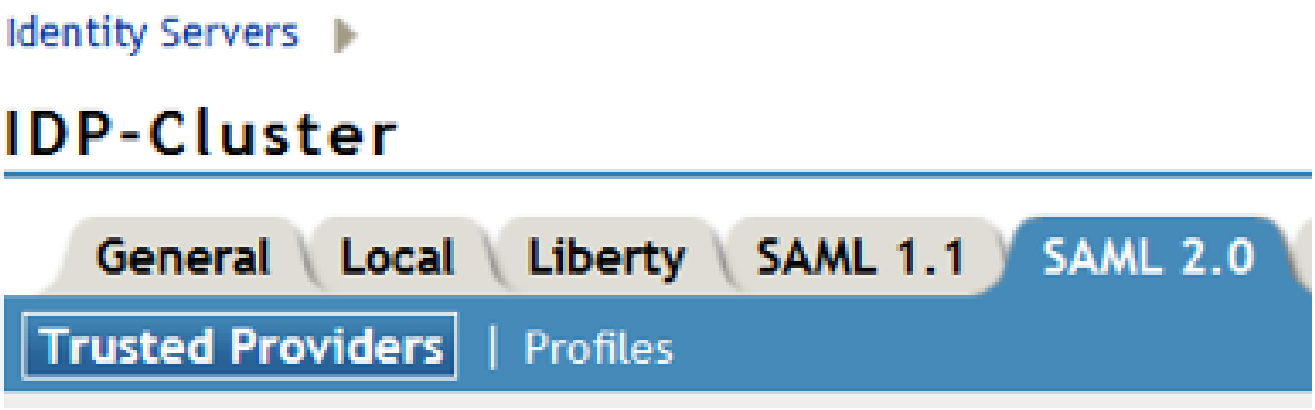
1. 轉到身份伺服器> NetIQ NAM。
2. 按一下屬性集。
3. 選擇New並對映LDAP屬性：



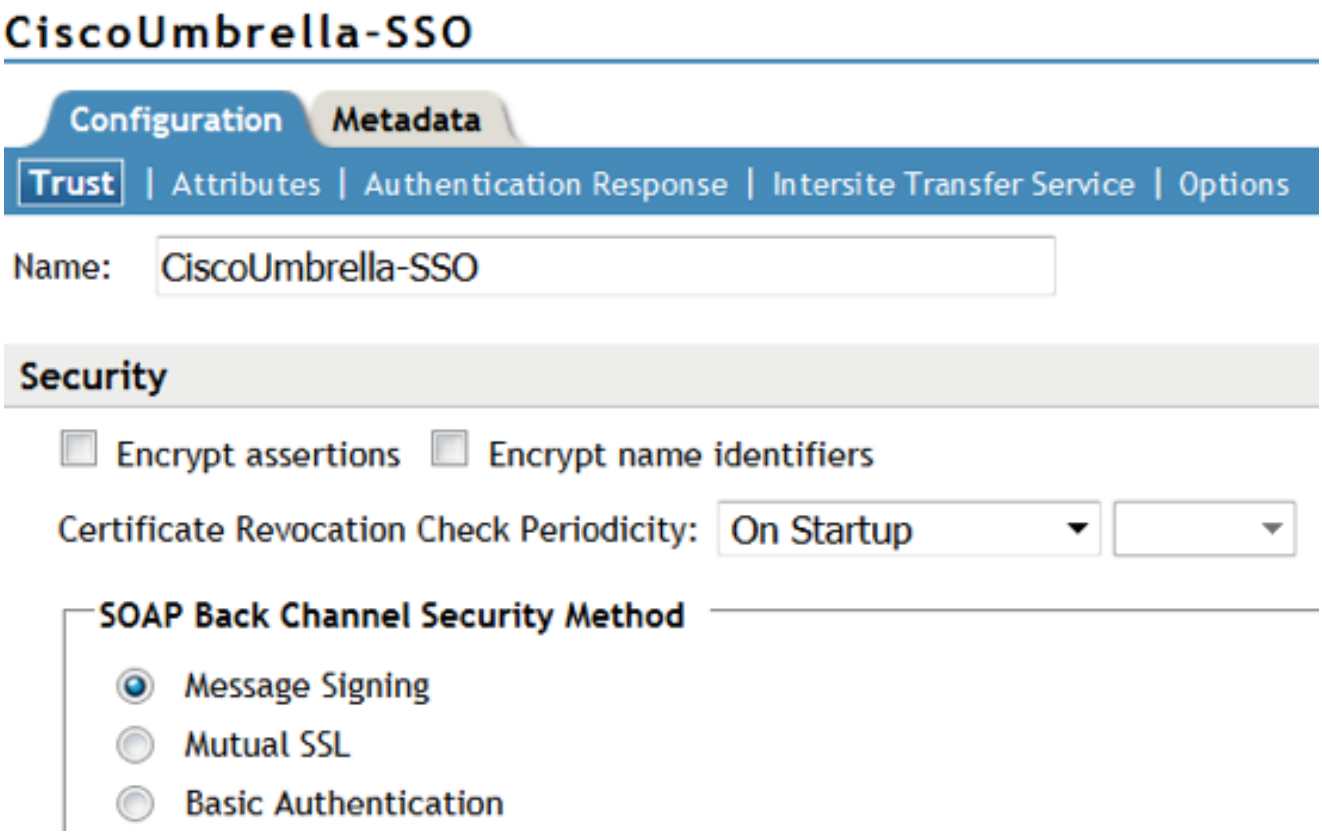
115000349567

建立新的信任提供程式

1. 轉到IDP General頁籤，然後選擇SAML 2.0。
2. 選擇Create New Trust Provider。

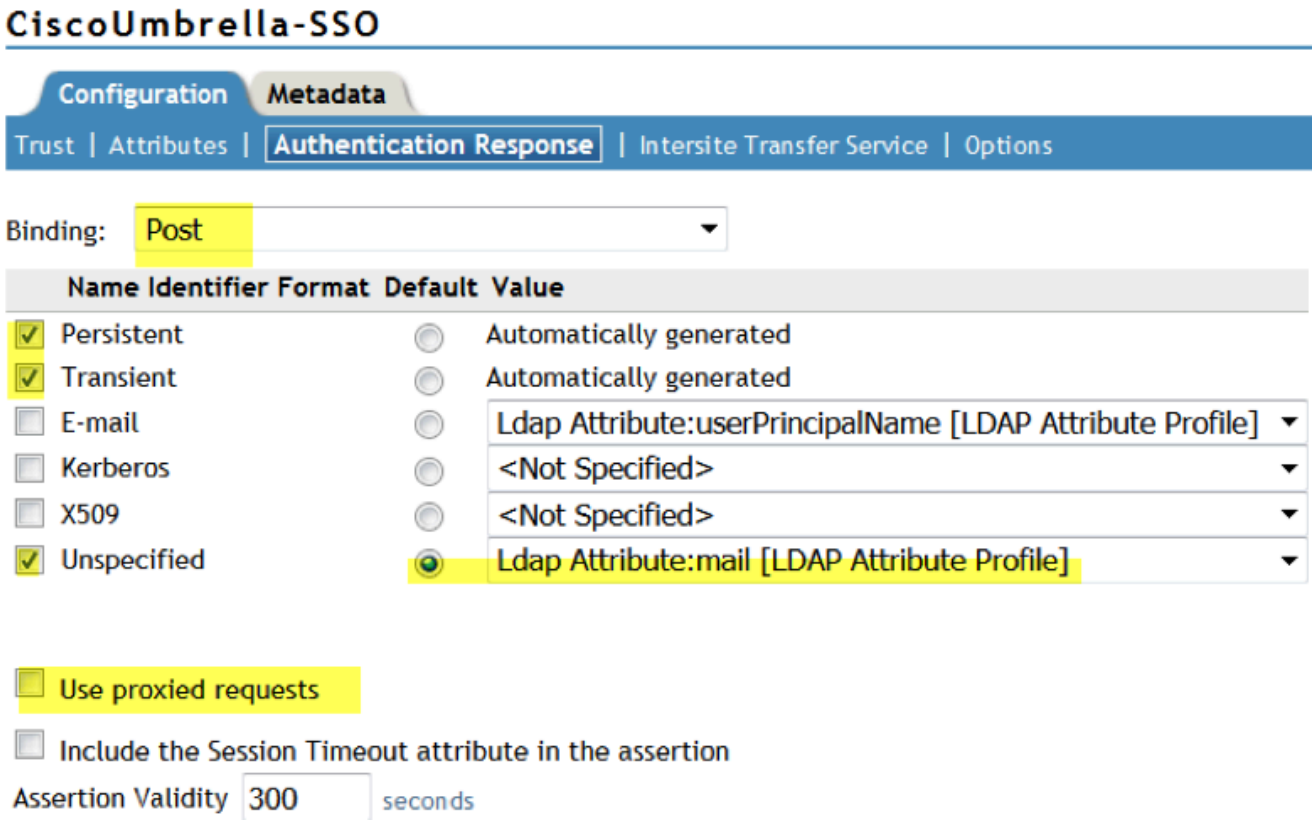


115000348788



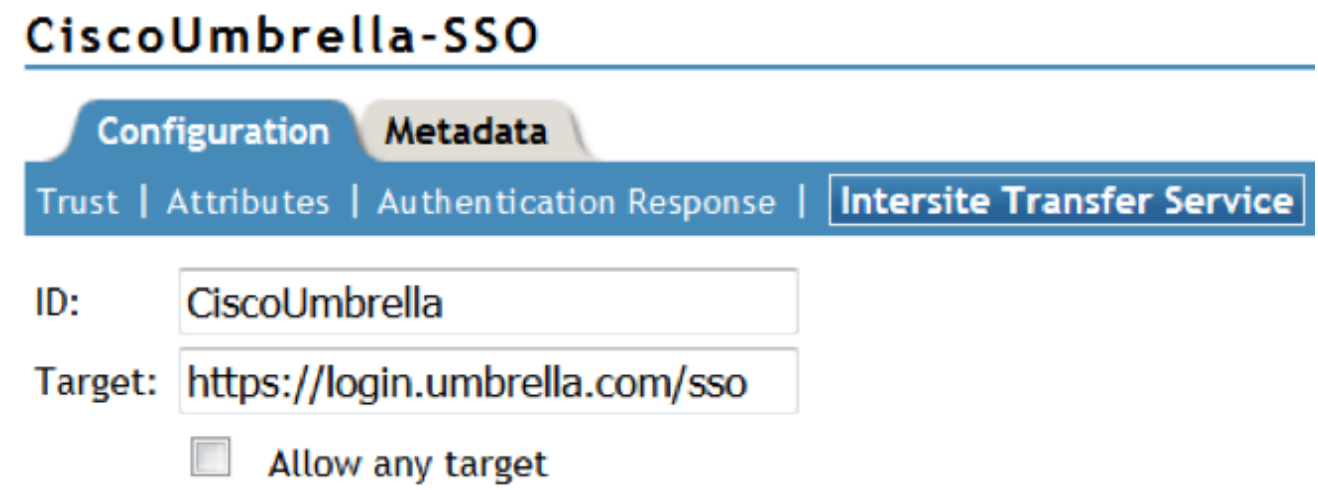
115000349827

3. 選擇您剛剛建立的屬性，然後選擇Send with Authentication。對於身份驗證響應，請選擇Post Binding、Persistent、Transient和Unspecified。
4. 選擇LDAP屬性：郵件[LDAP屬性配置檔案]並將其設為預設值。



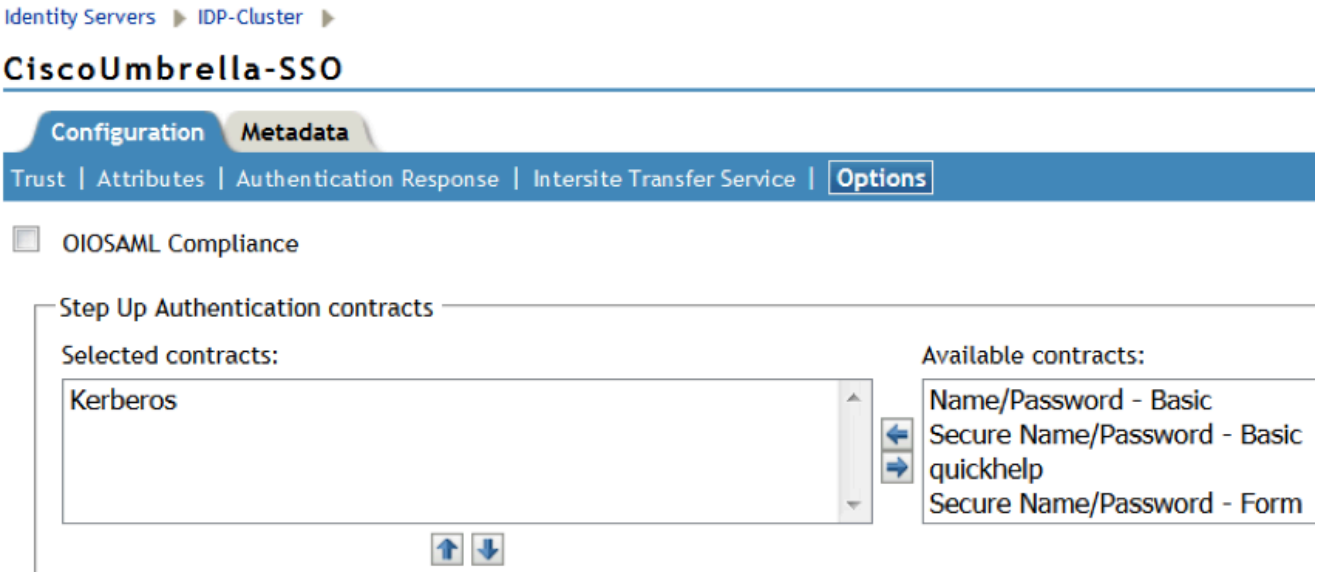
115000355688

5. 導航到Configuration > Intersite Transfer Service。為其指定類似於Cisco Umbrella SAML的名稱，並將Cisco Umbrella SSO登入URL新增為目標(https://login.umbrella.com/sso)。



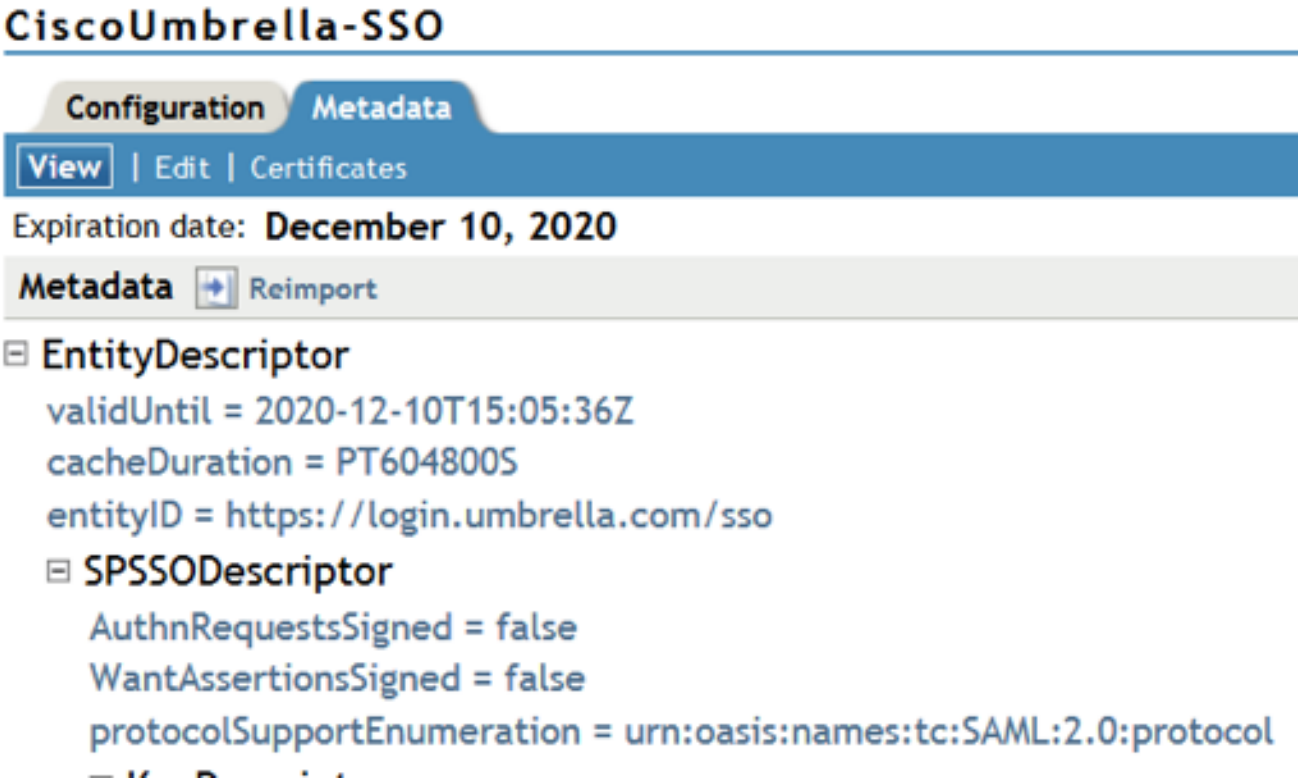
115000356827

6. 前往Configuration > Options，然後選擇Kerberos作為所選合約：



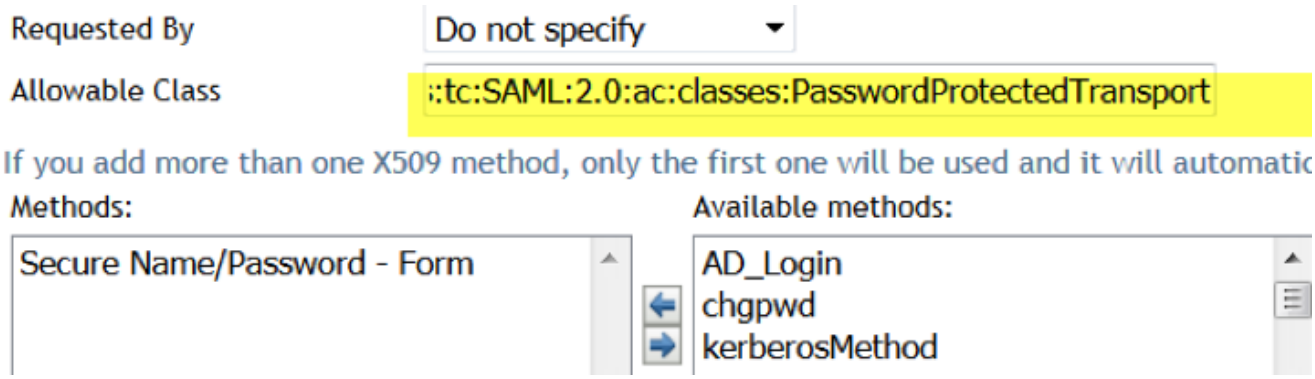
115000356068

7. 開啟Cisco Umbrella Metadata檔案。將EntityDescription欄位valdUntil日期更新為將來資料，例如2020-12-10T20:50:59Z（如螢幕截圖所示）。
8. 返回到NetIQ > Metadata並匯入更新的後設資料檔案。



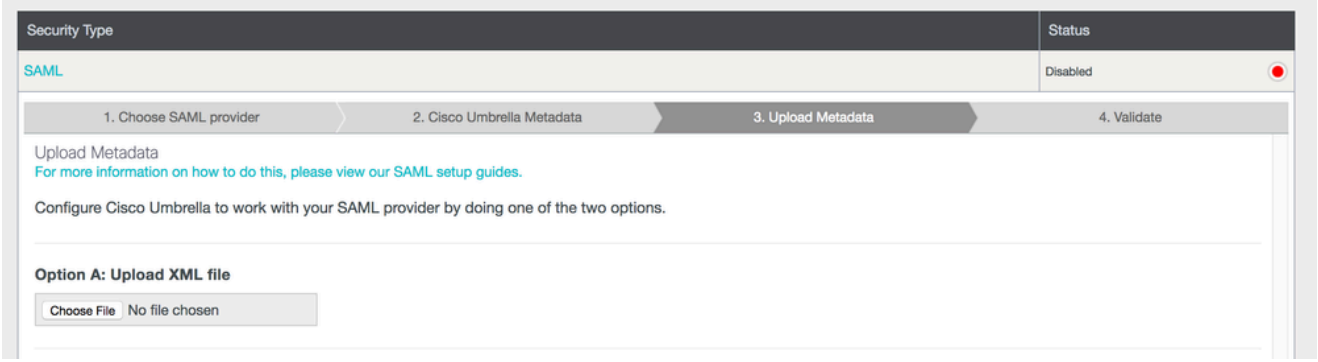
115000357147

9. 向斷言新增類。Cisco Umbrella斷言需要該類
   urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
10. 轉至Local > Contracts，選擇Secure Name/Password並新增到Allowable Class欄位，然後新增上述類：



115000357247

11. 更新身份服務和訪問網關以確保它們有效且是最新的，然後下載NetIQ後設資料。
12. 使用下載的後設資料通過Cisco Umbrella「其他」 SAML嚮導運行。第3步是要求您上傳後設資料的位置：



115001186107

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）。