利用Umbrella的固定後設資料URL進行SWG SAML身份驗證

目錄

簡介

本文說明如何使用Umbrella的固定後設資料URL進行安全Web網關(SWG)SAML身份驗證。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Umbrella SWG。

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。

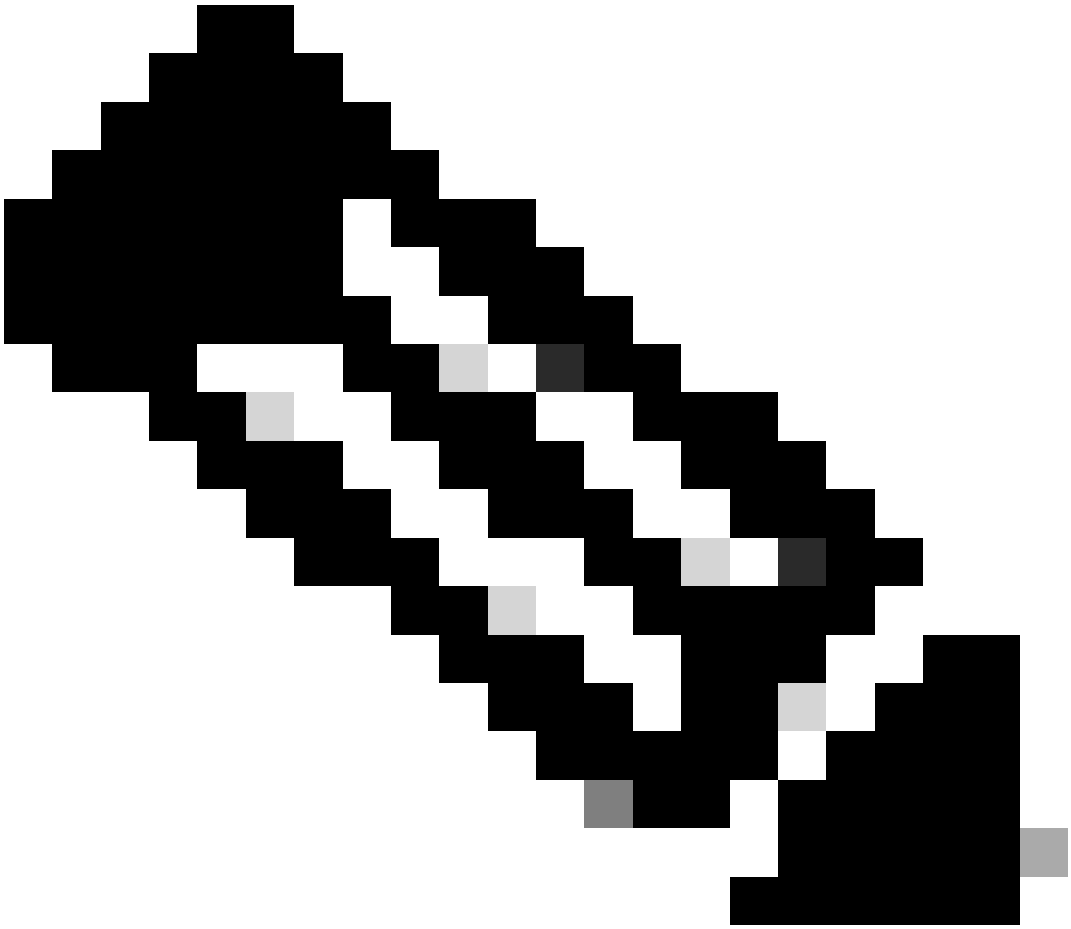
固定後設資料URL

針對Umbrella SWG使用SAML驗證時，我們提供兩個選項，用於將我們的憑證資訊匯入到您的身分識別提供者(IdP)中。 驗證請求簽名證書的IdP必須執行此操作。

1. 通過固定元資料URL自動配置：https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml
2. 手動導入我們的新簽名證書。更換證書時，需要每年執行一次。

第一個選項現在是支援基於URL的後設資料自動更新的身份提供程式(IdP)的首選配置方法。這包括常用的IdP，例如Microsoft ADFS和Ping身份。 好處在於，IdP每年自動匯入我們的新證書，無需手

動干預。



附註：許多IDP不執行SAML請求簽名驗證，因此不需要這些步驟。 如有疑問，請聯絡您的身份提供商供應商進行確認。

需求

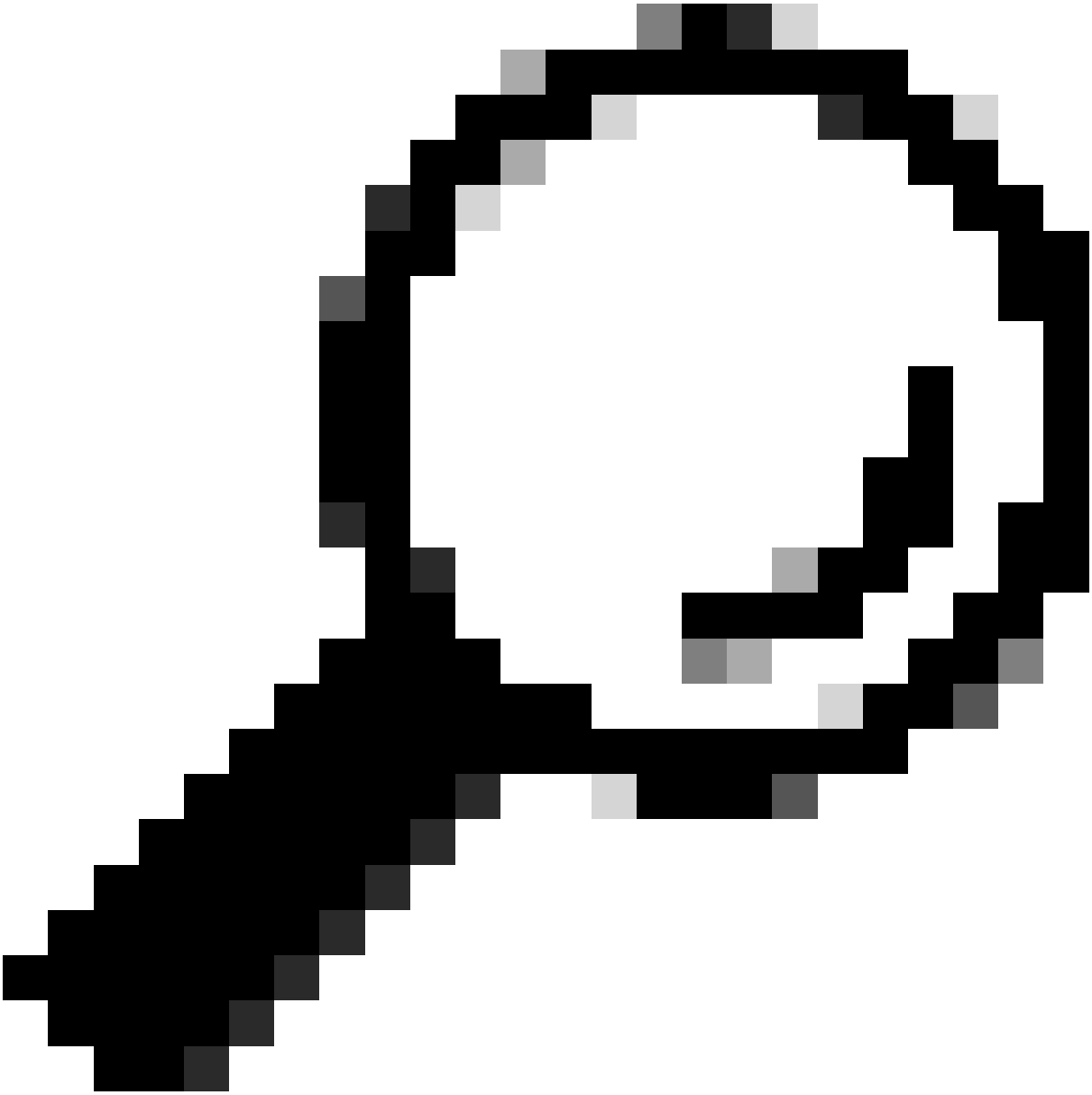
訪問後設資料URL的要求

- 支援從URL自動更新服務提供程式後設資料的IdP（例如ADFS、Ping）
- 您的IdP平台必須能夠訪問我們的元資料URL以及關聯的證書頒發機構URL
- 您的IdP平台還必須能夠訪問證書本身的證書頒發機構URL
- 您的IdP平台必須支援TLS 1.2，才能安全地連線到後設資料URL。如果IDP應用程式使用.NET framework 4.6.1或更低版本，可能需要按照Microsoft文檔進行一些進一步配置。

範例：Microsoft ADFS

通過編輯Umbrella的信賴方信任設定，可以配置固定後設資料URL:

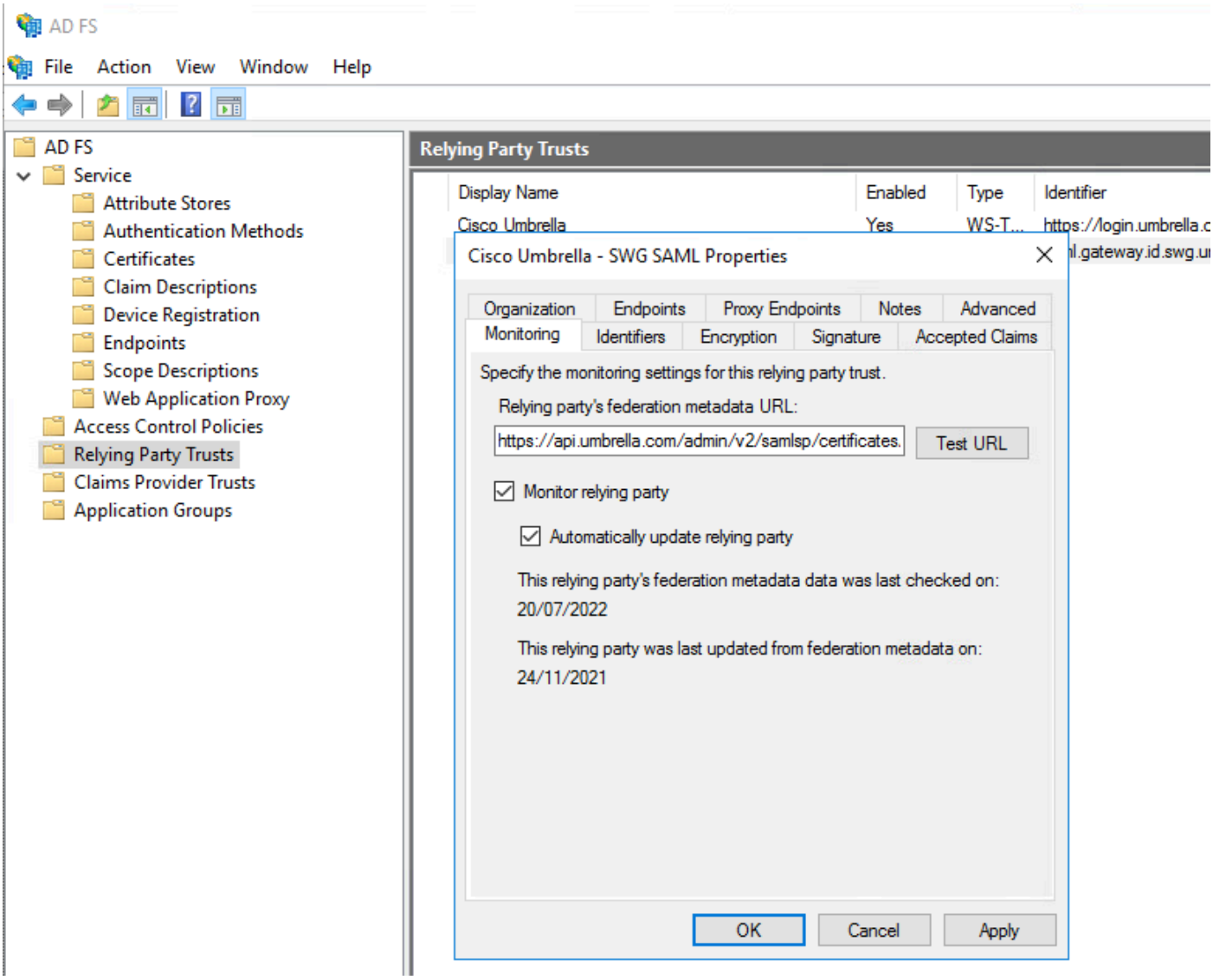
1. 導航到Monitoring頁籤並輸入後設資料URL。
2. 選擇監視信賴方並自動更新信賴方。



提示：選擇測試URL按鈕以驗證ADFS是否已成功聯絡該URL。

---

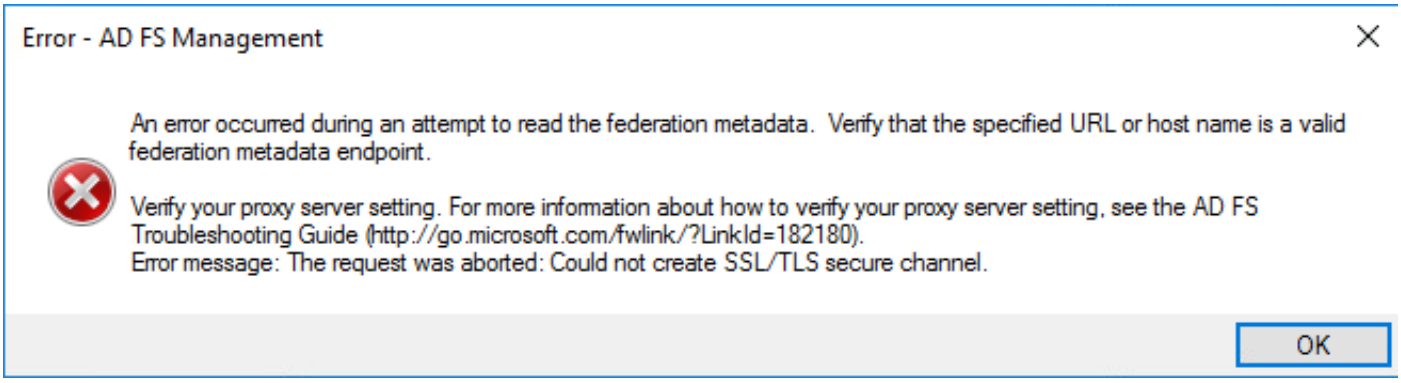
3. 選擇Apply。



ADFS_ReliingPartyTrust.png

疑難排解

如果收到該錯誤，「嘗試讀取聯合後設資料時出錯。在測試URL時，驗證指定的URL或主機名稱是否是有效的聯合後設資料終結點「，這通常表示需要更改登錄檔才能將.NET Framework版本設定為使用強加密並支援TLS 1.2。



ADFS後設資料_TLS_error.png

有關這些更改的完整詳細資訊由Microsoft發佈在Microsoft文檔的.Net Framework部分。

但是，通常這需要建立此金鑰，然後關閉並重新開啟ADFS管理控制檯：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto" = dword:00000001
```

限制：特定於組織的EntityID功能

如果使用Umbrella SAML Org-Specific EntityID功能，則不得使用基於URL的後設資料更新機制。僅當多個傘狀組織連結到同一身份提供方時，組織特定實體ID才適用。在這種情況下，您必須手動將證書新增到每個IDP配置中。

手動證書匯入（備選）

如果IdP不支援基於URL的更新，則必須每年手動將新的Umbrella請求簽名證書匯入身份提供程式。

- 每年在到期日前不久，證書都會在我們的公告入口網站中提供。訂閱門戶以獲取通知
- 將新證書新增到IdP中的服務提供商/信賴方證書清單中。
  - 請勿刪除任何當前證書。 Umbrella繼續使用舊證書進行簽名，直到到期為止。
- 如果您的IdP不包含匯入服務提供商/信賴方證書的功能，則這強烈表明它不會驗證SAML請求，無需執行進一步的操作。 請與您的IdP供應商聯絡以確認。

如果您在匯入新證書後遇到「UPN is not configured」錯誤，則表示發生了錯誤。 請參閱以下文章進行疑難排解：SWG SAML - UPN Not Configured錯誤

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）。