在SWA中配置Kerberos單一登入身份驗證

目錄

簡介

本文描述在安全網路裝置(SWA)中通過Kerberos將代理使用者配置為具有單一登入(SSO)身份驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。
- 基本Active Directory管理。

思科建議您安裝以下工具：

- 物理或虛擬SWA。

- 對SWA圖形使用者介面(GUI)的管理訪問。
- 對Active Directory的管理訪問許可權。

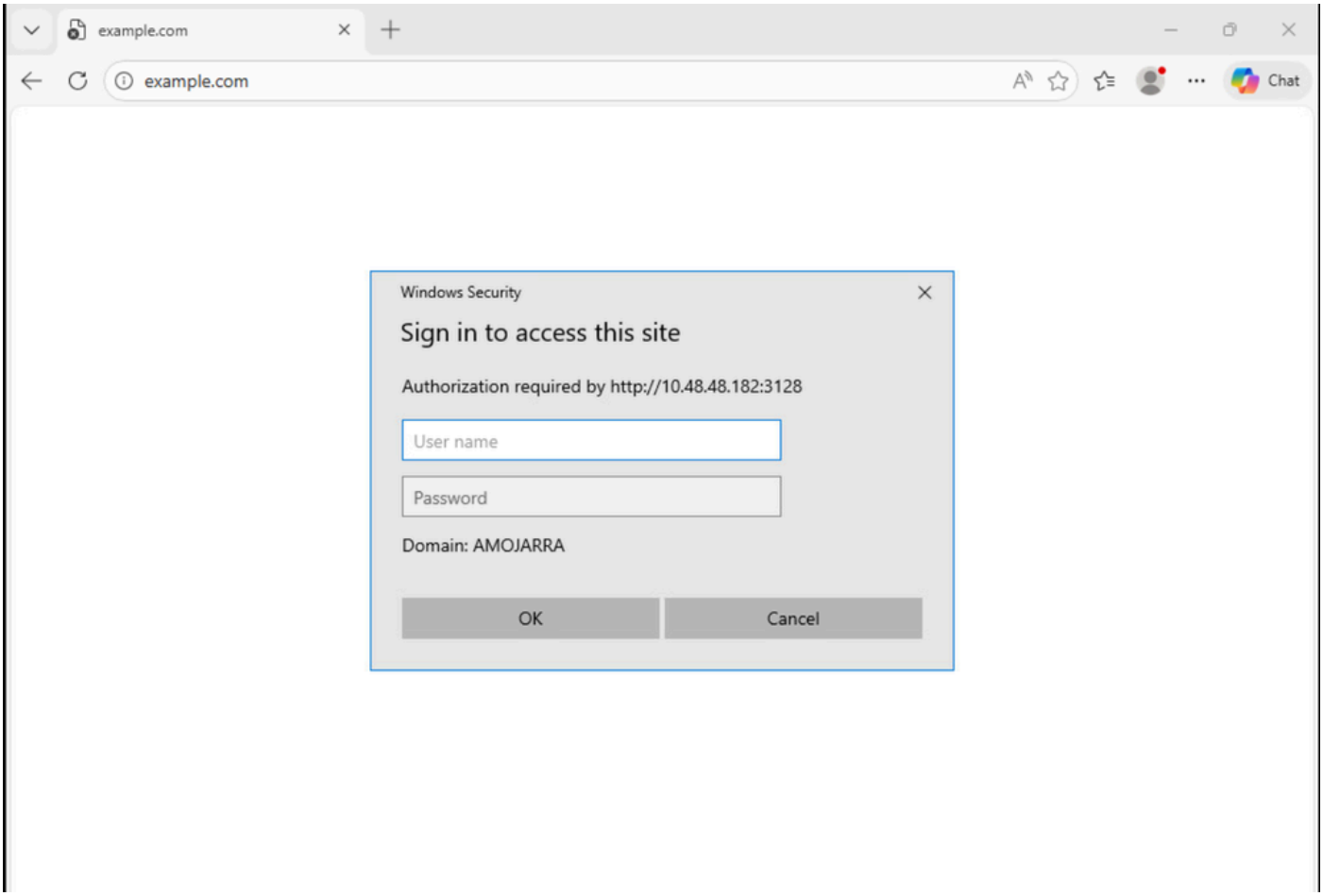
採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

開始之前

如果代理客戶端嘗試訪問網站並提示手動輸入憑證，請使用以下步驟進行故障排除。



影象 — 使用者身份驗證提示

步驟1.檢查與客戶端相關的Acesslog。

步驟1.1.登入到CLI。

步驟1.2.運行grep。

步驟1.3.選擇與相關聯的號碼。訪問日誌。

步驟1.4.在Enter the regular expression to grep中鍵入客戶端IP地址。

步驟1.5.按Enter鍵，直到顯示Do you want to tail the logs，鍵入「Y」並按Enter鍵，直到顯示Accesslogs。

步驟1.6.嘗試從客戶端PC訪問任何網站來重現問題。

步驟1.7.確認標識配置檔案流量正在命中。

在本範例中，識別設定檔是Auth_ID:

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

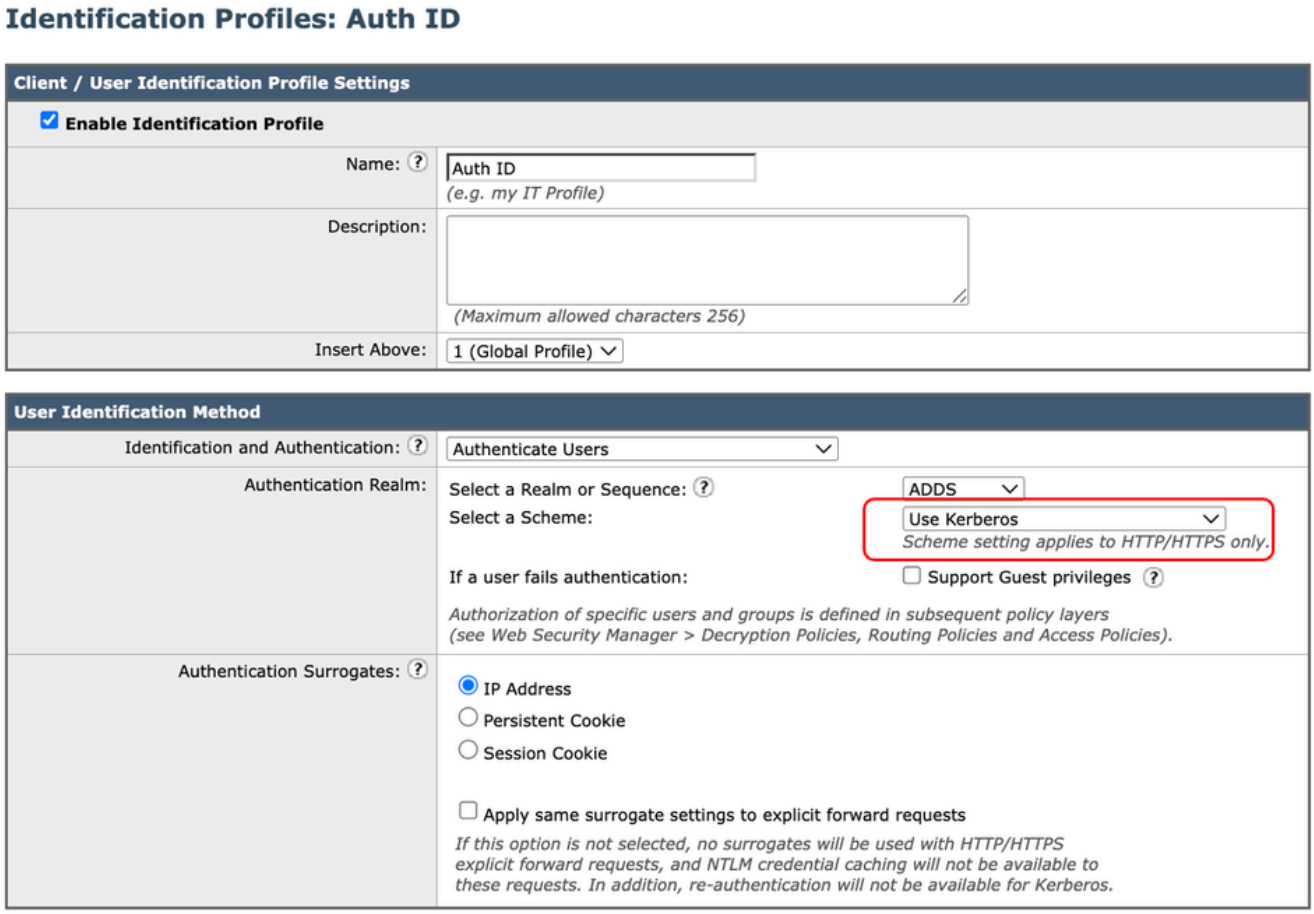
步驟2.檢查標識配置檔案。

步驟2.1.登入到SWA的GUI。

步驟2.2.從Web安全管理器選擇Identification Profiles。

步驟2.3.按一下流量所點選的標識配置檔案的名稱。

步驟2.4.確認身份驗證方案未設定為基本。



影象 — 身份驗證方案

步驟3.測試SWA和Active Directory連線。

步驟3.1.從SWA GUI導航到Network並選擇Authentication。

步驟3.2.單擊Authentication Realm Name。

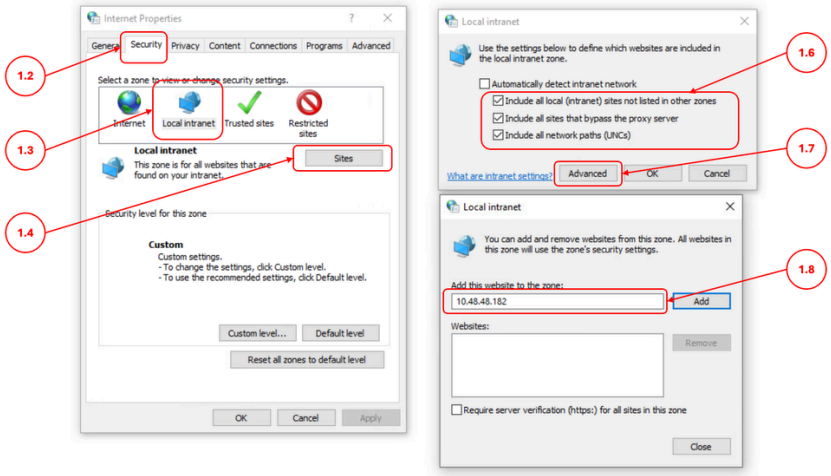
步驟3.3.單擊Start Test以檢視SWA和Active Directory連線狀態。

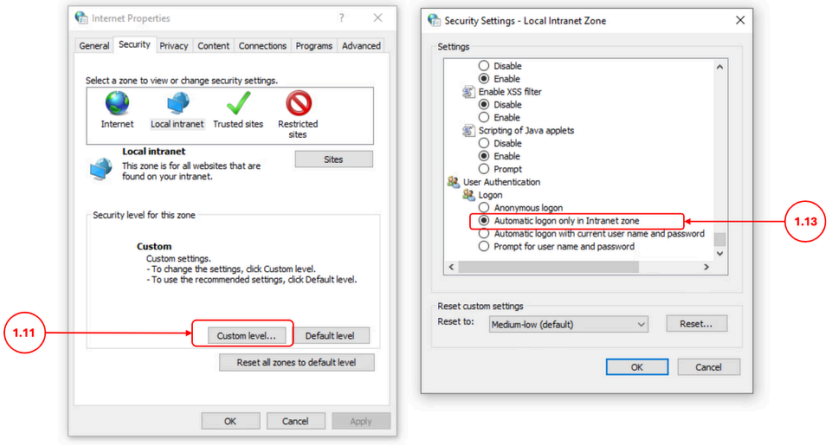
如果未發現錯誤，請按照本文所述驗證客戶端PC配置。

配置客戶端PC

使用以下步驟驗證客戶端PC配置：

步驟	詳細資料

步驟1.本地內部網站點	步驟1.1.在「開始」選單中，鍵入Internet Option，然後按Enter鍵。 步驟1.2.在「Internet屬性」視窗中，按一下Security頁籤。 步驟1.3.選擇本地Intranet。 步驟1.4.按一下Sites。 步驟1.5.確保未選中Automatically detect intranet network覈取方塊。 步驟1.6.選擇以下三個選項： • 包括所有未在其他區域中列出的本地(Intranet)站點 • 包括繞過代理伺服器的所有站點 • 包含所有網路路徑(UNC) 步驟1.7.單擊Advanced。 步驟1.8.輸入SWA的FQDN或IP地址並添加到清單。 第1.9步(可選)根據您的內部安全策略，您可以禁用Require Server Verification。  影象 — 配置本地Internet站點 步驟1.10。按一下Close，然後按一下OK。 步驟1.11.在「安全」頁籤中，按一下「自定義級別」。 步驟1.12.滾動到User Authentication。 步驟1.13.確保選中僅在Intranet區域中自動登入。

	 影象 — Intranet使用者的自動登入
步驟2.收集日誌	如果步驟1，則沒有通過Kerberos修復SSO身份驗證： 步驟2.1. 將SWA身份驗證日誌更改為跟蹤並檢查日誌。 步驟2.2.將[Auth-Method = %m]作為自定義欄位新增到訪問日誌。欲知更多資訊，請訪問：在訪問日誌中配置效能引數。 步驟2.3.對客戶端IP和Active Directory IP地址運行資料包捕獲過濾器，並確認客戶端PC正在將Kerberos服務票證傳送到SWA。

附註：確保在瀏覽器代理設定中配置了SWA的FQDN。

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.0使用手冊
- 為安全Web裝置配置防火牆
- 在內容安全裝置上配置資料包捕獲
- 配置訪問日誌中的效能引數
- 訪問安全Web裝置日誌
- 使用安全Web裝置最佳實踐 — 思科
- 繞過安全Web裝置中的身份驗證 — Cisco

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）。